网络安全

全球网络安全指数和网络健康状况

报告

ABIresearch®

电信发展部门

ITU

全球网络安全指数和网络健康状况

2015 年 4 月

致谢

国际电联谨对ABI Research团队的Aaron Boyd和Michela Menting在本报告撰写过程中给予的宝贵贡献表示感谢。国家网络健康概况的汇集工作得到了Shao Tong Zhang、Qin Chuan The、Aliya Abdul Razack以及Ineze Anni的支持。如您有任何意见，请邮件联系国际电联网络安全团队：cybersecurity@itu.int

节约纸张，关爱环境，请谨慎打印本刊物。

序言

技术在不断发展，新的网络威胁亦出现。在拥抱技术进步的同时，我们有必要将网络安全以完整的不可分割部分的形式置入这一进程。不幸的是，网络安全尚未进入很多国家和业界技术策略的核心视野。各国有必要检视其在网络安全方面的现有能力储备，并找出网络安全亟待加强的部分。

全球网络安全指数（GCI）是衡量各国网络安全发展程度的一个手段。GCI 目的是要为各国提供一个正当的动机，以加强其网络安全建设。其最终目标是要帮助建设一个全球性网络安全文化，并将其以核心身份融入信息和通信技术。

经与我们的合作伙伴 ABI Research 共同努力，GCI 得以为各国提供了统计分析和业界基准方面的专业知识。2013 年，国际电联向各成员国发送了一份通知和调查问卷。根据收到的反馈情况，我们发布了各区域的大致情况报告。现在，在全体成员国的倾力支持下，国际电联荣幸发布 2014 年全球网络安全形势报告。

我要感谢所有成员国对国际电联工作的支持。GCI 正在不断完善之中，我邀请各方继续向我们提供并更新相关重要信息。通过有效分享专业知识、观点和关切，希望有助于 GCI 不断走向成熟。作为一个不断发展演进的工具，GCI 将致力于帮助各国监测网络安全的健康程度，并在提供明智决策推动建立全球网络安全文化方面做出不懈的努力。

电信发展局主任

布哈伊马•萨努

ABI Research

在历经三年艰辛但代表了国际电联领导层坚强承诺的工作后，国际电联与私营部门合作推动实现了一个重要的建立全球社区的目标，即发布了第一份年度全球网络安全指标（GCI）。ABI Research 在此方面深感荣幸。

今天 GCI 能够展现在大家眼前，这要归功于国际电联领导层的远见卓识，即致力于提高各国对网络安全就绪程度的重视程度。作为一个拥有 25 年经验的技术情报公司，ABI Research 非常自豪能够成为这一项目的核心国际合作方。

网络犯罪的成本越来越低，而拥有高超技术和能力的网络威胁机构发起的复杂网络攻击造成的破坏越来越大。在此情况下，全球 ICT 的安全发展不断受到阻碍。为了维持网络空间的经济稳定性，为了向各个组织和个人开展贸易和自由沟通提供关键可靠环境，必须要确保 ICT 的安全运行。

GCI 的目标是要建立一个衡量手段，以此确保技术和基于互联网的创新能够在安全和保密的条件下得以实现。通过技术、政策、立法、组织和学术方面的严格措施，相信能够将投机性、窃取钱财或政治性的犯罪压缩在最低限度。

我们希望继续与国际电联在网络安全指数方面开展合作。网络安全指数是我们在提高网络安全方面迈出的重要第一步。这一步找出了网络安全需要改进的领域，并必将有助于推动所有相关方在分享和相互学习方面开展开放性合作。

ABI Research 创始人兼
首席执行官
Tim Archdeacon

目录

1 介绍

全球网络安全指数（GCI）是私营部门和国际组织合作的产物，目的是为了推动各国将网络安全置于国家议程的首要位置。GCI 是 ABI Research 和国际电信联盟开展的联合项目，为主权国家参与网络安全提供资深意见。

根植于国际电联全球网络安全议程，GCI 考察各国在五个领域的参与程度：立法措施、技术措施、组织措施、能力建设和国际合作。由此得出各国的就绪程度指数以及全球各国在网络安全就绪度方面的排名。GCI 并不着眼于判定一个具体措施是否有效或是否能成功，相反，该指数只是简单地确定各国是否存在实施和促进网络安全的架构。

该项目是国际电联和 ABI Research 在开展高强度的初次和二次调研后得出的成果。我们向所有国际电联成员国都发送了国家层面的调查以及深入的定性调研。收集到的信息包括法律、监管、CERT 和 CIRT、政策、国家战略、标准、资质、职业培训、宣传活动以及合作伙伴等多个方面。

GCI 的目标是要为各国提供其在国家层面对网络安全介入程度的快照。ABI Research 和国际电联的愿望是推动各国认识到网络安全的重要性，同时推动政府发挥重要作用，采取适当措施来支持和推动这一关键领域工作。保障网络安全的完整性必然涉及到网络安全的发展问题。

2 关键结论

2.1 全球排名

很多国家的排名是并列的，这表示他们具有相同的网络安全应对能力。该指数并未细化，这是因为其目的是为了显示各国在网络安全方面的承诺/就绪程度，the same ranking which indicates that they have the same level of readiness. The index has a low level of granularity since it aims at capturing the cybersecurity commitment/preparedness of a country and not its detailed capabilities or possible vulnerabilities.而并非其详尽能力或可能的薄弱环节。

表 1: 按指数排名的国家列表

国家	指数	全球排名
美国*	0.824	1
加拿大*	0.794	2
澳大利亚*	0.765	3
马来西亚	0.765	3
阿曼	0.765	3
新西兰*	0.735	4
挪威*	0.735	4
巴西	0.706	5
爱沙尼亚*	0.706	5
德国*	0.706	5
印度*	0.706	5
日本*	0.706	5
韩国	0.706	5
英国	0.706	5
奥地利*	0.676	6
匈牙利*	0.676	6

国家	指数	全球排名
以色列*	0.676	6
荷兰*	0.676	6
新加坡	0.676	6
拉脱维亚*	0.647	7
瑞典*	0.647	7
土耳其	0.647	7
香港	0.618	8
芬兰	0.618	8
卡塔尔	0.618	8
斯洛伐克	0.618	8
乌拉圭	0.618	8
哥伦比亚	0.588	9
丹麦*	0.588	9
埃及	0.588	9
法国*	0.588	9
毛里求斯	0.588	9
西班牙*	0.588	9
意大利	0.559	10
摩洛哥	0.559	10
乌干达	0.559	10
阿塞拜疆	0.529	11
波兰*	0.529	11
卢旺达	0.529	11
突尼斯	0.529	11
捷克共和国	0.500	12
格鲁吉亚	0.500	12
俄罗斯*	0.500	12
印度尼西亚	0.471	13
卢森堡*	0.471	13
罗马尼亚	0.471	13
比利时*	0.441	14
保加利亚	0.441	14
中国*	0.441	14
立陶宛	0.441	14
尼日利亚	0.441	14
苏丹	0.441	14
阿根廷*	0.412	15
喀麦隆	0.412	15
克罗地亚	0.412	15
肯尼亚	0.412	15
蒙古	0.412	15

国家	指数	全球排名
斯里兰卡	0.412	15
泰国*	0.412	15
文莱	0.382	16
智利*	0.382	16
摩尔多瓦*	0.382	16
黑山	0.382	16
缅甸	0.382	16
南非	0.382	16
哥斯达黎加 *	0.353	17
厄瓜多尔	0.353	17
马耳他*	0.353	17
菲律宾	0.353	17
瑞士	0.353	17
乌克兰*	0.353	17
阿联酋*	0.353	17
布基纳法索	0.324	18
墨西哥*	0.324	18
秘鲁*	0.324	18
越南*	0.324	18
巴林	0.294	19
孟加拉	0.294	19
塞浦路斯*	0.294	19
加纳*	0.294	19
伊朗*	0.294	19
利比亚	0.294	19
巴拿马	0.294	19
葡萄牙*	0.294	19
沙特*	0.294	19
阿富汗	0.265	20
塞尔维亚	0.265	20
多哥	0.265	20
科特迪瓦	0.235	21
牙买加*	0.235	21
阿尔巴尼亚	0.206	22
萨尔瓦多*	0.206	22
希腊*	0.206	22
危地马拉	0.206	22
冰岛*	0.206	22
爱尔兰*	0.206	22
约旦	0.206	22
利比里亚	0.206	22

国家	指数	全球排名
巴拉圭*	0.206	22
坦桑尼亚	0.206	22
特立尼达和多巴哥	0.206	22
委内瑞拉	0.206	22
阿尔及利亚	0.176	23
亚美尼亚	0.176	23
巴巴多斯	0.176	23
白俄罗斯*	0.176	23
伯利兹*	0.176	23
贝宁*	0.176	23
波斯尼亚和黑塞哥维那	0.176	23
博茨瓦纳	0.176	23
哈萨克斯坦*	0.176	23
马拉维	0.176	23
巴基斯坦*	0.176	23
萨摩亚	0.176	23
塞内加尔*	0.176	23
斯洛文尼亚*	0.176	23
叙利亚	0.176	23
巴哈马*	0.147	24
毛里塔尼亚*	0.147	24
尼加拉瓜*	0.147	24
圣基茨和尼维斯	0.147	24
巴勒斯坦国*	0.147	24
塔吉克斯坦*	0.147	24
马其顿*	0.147	24
乌兹别克斯坦*	0.147	24
瓦努阿图	0.147	24
赞比亚	0.147	24
安提瓜和巴布达*	0.118	25
不丹	0.118	25
玻利维亚 *	0.118	25
布隆迪	0.118	25
柬埔寨	0.118	25
多米尼亚共和国	0.118	25
格林纳达	0.118	25
圭亚那*	0.118	25
吉尔吉斯坦*	0.118	25
列支敦士登*	0.118	25
密克罗尼西亚	0.118	25
尼泊尔*	0.118	25

国家	指数	全球排名
巴布亚新几内亚	0.118	25
圣卢西亚*	0.118	25
塞舌尔*	0.118	25
苏里南*	0.118	25
圣马力诺	0.118	25
安哥拉*	0.088	26
冈比亚	0.088	26
基里巴斯	0.088	26
黎巴嫩	0.088	26
马达加斯加	0.088	26
马尔代夫	0.088	26
马里	0.088	26
摩纳哥*	0.088	26
尼日尔*	0.088	26
南苏丹*	0.088	26
汤加	0.088	26
土库曼斯坦*	0.088	26
津巴布韦	0.088	26
安道尔*	0.059	27
刚果	0.059	27
吉布提	0.059	27
多米尼加*	0.059	27
斐济	0.059	27
海地*	0.059	27
科威特*	0.059	27
老挝	0.059	27
莫桑比克*	0.059	27
圣多美和普林西比	0.059	27
塞拉利昂	0.059	27
斯威士兰	0.059	27
图瓦卢	0.059	27
也门*	0.059	27
佛得角	0.029	28
乍得*	0.029	28
科摩罗	0.029	28
古巴*	0.029	28
刚果民主共和国	0.029	28
厄立特里亚*	0.029	28
埃塞俄比亚*	0.029	28
加蓬	0.029	28
几内亚	0.029	28

国家	指数	全球排名
几内亚比绍*	0.029	28
伊拉克*	0.029	28
瑙鲁	0.029	28
帕劳*	0.029	28
所罗门群岛	0.029	28
索马里	0.029	28
中非共和国 *	0.000	29
朝鲜民主主义人民共和国*	0.000	29
赤道几内亚*	0.000	29
洪都拉斯*	0.000	29
莱索托	0.000	29
马绍尔群岛	0.000	29
纳米比亚	0.000	29
圣文森特和格林纳丁斯	0.000	29
东帝汶*	0.000	29
* 基于次级数据（资料来源：ABI Research）。		

2.2 区域排名

表 2: 非洲区域指数排名

非洲	法律	技术	组织	能力建设	合作	指数	区域排名
毛里求斯	0.7500	0.6667	0.6250	0.5000	0.5000	0.5882	1
乌干达	0.7500	0.5000	0.8750	0.2500	0.5000	0.5588	2
卢旺达	1.0000	0.5000	0.5000	0.3750	0.5000	0.5294	3
尼日利亚	0.2500	0.3333	0.5000	0.5000	0.5000	0.4412	4
喀麦隆	0.7500	0.5000	0.3750	0.5000	0.1250	0.4118	5
肯尼亚	1.0000	0.3333	0.2500	0.2500	0.5000	0.4118	5
南非	0.2500	0.5000	0.6250	0.2500	0.2500	0.3824	6
布基纳法索	0.0000	0.5000	0.7500	0.0000	0.2500	0.3235	7
加纳*	0.7500	0.3333	0.2500	0.2500	0.1250	0.2941	8
多哥	0.0000	0.3333	0.3750	0.2500	0.2500	0.2647	9
科特迪瓦	0.7500	0.3333	0.1250	0.1250	0.1250	0.2353	10
利比里亚	0.0000	0.0000	0.2500	0.3750	0.2500	0.2059	11
坦桑尼亚	0.5000	0.3333	0.0000	0.1250	0.2500	0.2059	11
贝宁*	0.5000	0.0000	0.2500	0.1250	0.1250	0.1765	12
博茨瓦纳	0.7500	0.1667	0.2500	0.0000	0.0000	0.1765	12
马拉维	0.0000	0.0000	0.1250	0.3750	0.2500	0.1765	12
塞内加尔*	1.0000	0.0000	0.1250	0.0000	0.1250	0.1765	12
赞比亚	0.2500	0.3333	0.1250	0.1250	0.0000	0.1471	13
布隆迪	0.2500	0.0000	0.1250	0.1250	0.1250	0.1176	14
塞舌尔*	0.7500	0.0000	0.0000	0.0000	0.1250	0.1176	14

非洲	法律	技术	组织	能力建设	合作	指数	区域排名
安哥拉*	0.5000	0.0000	0.0000	0.0000	0.1250	0.0882	15
冈比亚	0.5000	0.0000	0.1250	0.0000	0.0000	0.0882	15
马达加斯加	0.5000	0.0000	0.0000	0.0000	0.1250	0.0882	15
马里	0.5000	0.0000	0.0000	0.0000	0.1250	0.0882	15
尼日尔*	0.2500	0.0000	0.0000	0.1250	0.1250	0.0882	15
南苏丹*	0.5000	0.0000	0.0000	0.0000	0.1250	0.0882	15
津巴布韦	0.2500	0.0000	0.1250	0.0000	0.1250	0.0882	15
刚果	0.0000	0.0000	0.1250	0.0000	0.1250	0.0588	16
莫桑比克*	0.2500	0.0000	0.0000	0.0000	0.1250	0.0588	16
圣多美和普林西比	0.0000	0.0000	0.1250	0.0000	0.1250	0.0588	16
塞拉利昂	0.0000	0.0000	0.2500	0.0000	0.0000	0.0588	16
斯威士兰	0.2500	0.0000	0.1250	0.0000	0.0000	0.0588	16
佛得角	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	17
乍得*	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	17
刚果民主共和国	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	17
厄立特里亚*	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	17
埃塞俄比亚*	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	17
加蓬	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	17
几内亚	0.0000	0.0000	0.1250	0.0000	0.0000	0.0294	17
几内亚比绍*	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	17
中非共和国*	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	18
赤道几内亚*	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	18
莱索托	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	18
纳米比亚	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	18
* 基于次级数据。							

表 3: 美洲指数排名

美洲	法律	技术	组织架构	能力建设	合作	指数	区域排名
美国*	1.0000	0.8333	0.8750	1.0000	0.5000	0.8235	1
加拿大*	0.7500	1.0000	0.8750	0.8750	0.5000	0.7941	2
巴西	0.7500	0.6667	0.8750	0.7500	0.5000	0.7059	3
乌拉圭	1.0000	0.6667	0.6250	0.5000	0.5000	0.6176	4
哥伦比亚	0.7500	0.5000	0.7500	0.7500	0.2500	0.5882	5
阿根廷*	1.0000	0.3333	0.3750	0.5000	0.1250	0.4118	6
智利*	0.7500	0.5000	0.2500	0.3750	0.2500	0.3824	7
哥斯达黎加*	0.7500	0.3333	0.2500	0.1250	0.5000	0.3529	8
厄瓜多尔	0.2500	0.6667	0.1250	0.5000	0.2500	0.3529	8
墨西哥*	0.2500	0.5000	0.1250	0.3750	0.3750	0.3235	9
秘鲁*	0.7500	0.3333	0.2500	0.1250	0.3750	0.3235	9
巴拿马	0.2500	0.5000	0.3750	0.2500	0.1250	0.2941	10
牙买加*	0.7500	0.0000	0.1250	0.1250	0.3750	0.2353	11
萨尔瓦多*	0.0000	0.3333	0.2500	0.1250	0.2500	0.2059	12
危地马拉	0.0000	0.3333	0.1250	0.3750	0.1250	0.2059	12
巴拉圭*	0.0000	0.3333	0.1250	0.2500	0.2500	0.2059	12
特立尼达和多巴哥	0.2500	0.0000	0.5000	0.1250	0.1250	0.2059	12
委内瑞拉	0.5000	0.3333	0.0000	0.2500	0.1250	0.2059	12
巴巴多斯	0.5000	0.0000	0.1250	0.2500	0.1250	0.1765	13
伯利兹*	0.2500	0.0000	0.2500	0.1250	0.2500	0.1765	13
巴哈马*	0.7500	0.0000	0.0000	0.1250	0.1250	0.1471	14
尼加拉瓜*	0.5000	0.0000	0.2500	0.1250	0.0000	0.1471	14

美洲	法律	技术	组织架构	能力建设	合作	指数	区域排名
圣基茨和尼维斯	0.7500	0.0000	0.1250	0.0000	0.1250	0.1471	14
安提瓜和巴布达*	0.7500	0.0000	0.0000	0.1250	0.0000	0.1176	15
玻利维亚*	0.0000	0.0000	0.2500	0.1250	0.1250	0.1176	15
多米尼加共和国	0.2500	0.0000	0.1250	0.1250	0.1250	0.1176	15
格林纳达	0.7500	0.0000	0.0000	0.1250	0.0000	0.1176	15
圭亚那*	0.0000	0.3333	0.1250	0.0000	0.1250	0.1176	15
圣卢西亚*	0.7500	0.0000	0.0000	0.0000	0.1250	0.1176	15
苏里南*	0.2500	0.0000	0.1250	0.1250	0.1250	0.1176	15
海地*	0.0000	0.0000	0.0000	0.1250	0.1250	0.0588	16
多米尼加*	0.2500	0.0000	0.0000	0.0000	0.1250	0.0588	16
古巴*	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	17
洪都拉斯*	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	18
圣文森特和格林纳丁斯	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	18
* 基于次级数据。							

表 4: 阿拉伯国家地区指数排名

阿拉伯国家	法律	技术	组织	能力建设	合作	指数	区域排名
阿曼	0.7500	0.6667	1.0000	0.7500	0.6250	0.7647	1
卡塔尔	0.7500	0.8333	0.5000	0.6250	0.5000	0.6176	2
埃及	0.5000	0.5000	0.3750	1.0000	0.5000	0.5882	3
摩洛哥	0.5000	0.6667	0.7500	0.5000	0.3750	0.5588	4
突尼斯	1.0000	0.5000	0.6250	0.2500	0.5000	0.5294	5
苏丹	0.7500	0.5000	0.5000	0.2500	0.3750	0.4412	6
阿联酋*	0.7500	0.3333	0.2500	0.5000	0.1250	0.3529	7
巴林	0.7500	0.1667	0.1250	0.3750	0.2500	0.2941	8
利比亚	0.2500	0.3333	0.3750	0.1250	0.3750	0.2941	8
沙特阿拉伯*	0.7500	0.3333	0.1250	0.3750	0.1250	0.2941	8
约旦	0.5000	0.0000	0.5000	0.0000	0.1250	0.2059	9
阿尔及利亚	0.7500	0.0000	0.0000	0.1250	0.2500	0.1765	10
叙利亚	0.2500	0.3333	0.1250	0.1250	0.1250	0.1765	10
毛里塔尼亚	0.2500	0.1667	0.2500	0.0000	0.1250	0.1471	11
巴勒斯坦国*	0.2500	0.0000	0.3750	0.1250	0.0000	0.1471	11
黎巴嫩	0.0000	0.0000	0.0000	0.2500	0.1250	0.0882	12
吉布提 i	0.2500	0.0000	0.0000	0.0000	0.1250	0.0588	13
科威特*	0.0000	0.0000	0.0000	0.1250	0.1250	0.0588	13
也门*	0.2500	0.0000	0.0000	0.0000	0.1250	0.0588	13
科摩罗	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	14
伊拉克*	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	14
索马里	0.0000	0.0000	0.0000	0.1250	0.0000	0.0294	14
* 基于次级数据。							

表 5：亚太地区指数排名

亚太	法律	技术	组织	能力建设	合作	指数	区域排名
澳大利亚*	0.7500	0.6667	0.8750	0.8750	0.6250	0.7647	1
马来西亚	0.7500	0.8333	1.0000	0.6250	0.6250	0.7647	1
新西兰*	1.0000	0.8333	0.8750	0.6250	0.5000	0.7353	2
印度*	1.0000	0.6667	0.7500	0.8750	0.3750	0.7059	3
日本*	1.0000	0.6667	0.7500	0.6250	0.6250	0.7059	3
韩国	1.0000	0.6667	0.8750	0.6250	0.5000	0.7059	3
新加坡	0.7500	0.6667	0.7500	0.7500	0.5000	0.6765	4
香港	0.7500	0.6667	0.5000	0.7500	0.5000	0.6176	5
印度尼西亚	1.0000	0.3333	0.2500	0.5000	0.5000	0.4706	5
中国*	0.7500	0.5000	0.2500	0.5000	0.3750	0.4412	6
蒙古	0.5000	0.8333	0.6250	0.1250	0.1250	0.4118	7
斯里兰卡	0.5000	0.3333	0.2500	0.5000	0.5000	0.4118	7
泰国*	0.5000	0.3333	0.5000	0.2500	0.5000	0.4118	7
文莱	0.7500	0.3333	0.1250	0.3750	0.5000	0.3824	8
缅甸	0.2500	0.5000	0.2500	0.5000	0.3750	0.3824	8
菲律宾	1.0000	0.3333	0.3750	0.3750	0.0000	0.3529	9
越南*	0.5000	0.3333	0.1250	0.5000	0.2500	0.3235	10
孟加拉	0.5000	0.3333	0.1250	0.2500	0.3750	0.2941	11
伊朗*	0.5000	0.3333	0.5000	0.1250	0.1250	0.2941	11
阿富汗	0.0000	0.5000	0.3750	0.2500	0.1250	0.2647	12
巴基斯坦*	0.2500	0.1667	0.0000	0.3750	0.1250	0.1765	13
萨摩亚	0.5000	0.0000	0.1250	0.1250	0.2500	0.1765	13
瓦努阿图	0.0000	0.0000	0.2500	0.1250	0.2500	0.1471	14
不丹	0.2500	0.3333	0.1250	0.0000	0.0000	0.1176	15

亚太	法律	技术	组织	能力建设	合作	指数	区域排名
柬埔寨	0.2500	0.3333	0.1250	0.0000	0.0000	0.1176	15
密克罗尼西亚	0.0000	0.0000	0.2500	0.1250	0.1250	0.1176	15
尼泊尔*	0.5000	0.0000	0.1250	0.0000	0.1250	0.1176	15
巴布亚新几内亚	0.0000	0.0000	0.3750	0.0000	0.1250	0.1176	15
基里巴斯	0.0000	0.0000	0.1250	0.0000	0.2500	0.0882	16
马尔代夫	0.0000	0.0000	0.1250	0.0000	0.2500	0.0882	16
汤加	0.5000	0.0000	0.1250	0.0000	0.0000	0.0882	16
斐济	0.2500	0.0000	0.0000	0.0000	0.1250	0.0588	17
老挝	0.0000	0.3333	0.0000	0.0000	0.0000	0.0588	17
图瓦卢	0.0000	0.0000	0.1250	0.0000	0.1250	0.0588	17
瑙鲁	0.0000	0.1667	0.0000	0.0000	0.0000	0.0294	18
帕劳*	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	18
所罗门群岛*	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	18
朝鲜民主主义人民共和国*	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	19
马绍尔群岛	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	19
东帝汶*	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	19
* 基于次级数据。							

表 6: 独联体（CIS）指数排名

独联体	法律	技术	组织	能力建设	合作	指数	区域排名
阿塞拜疆	0.7500	0.5000	0.5000	0.5000	0.5000	0.5294	1
格鲁吉亚	0.7500	0.6667	0.7500	0.2500	0.2500	0.5000	2
俄罗斯*	1.0000	0.3333	0.5000	0.3750	0.5000	0.5000	2
摩尔多瓦*	0.7500	0.5000	0.2500	0.2500	0.3750	0.3824	3
乌克兰*	0.7500	0.3333	0.2500	0.1250	0.5000	0.3529	4

独联体	法律	技术	组织	能力建设	合作	指数	区域排名
亚美尼亚	0.5000	0.5000	0.0000	0.0000	0.1250	0.1765	5
白俄罗斯*	0.7500	0.3333	0.0000	0.0000	0.1250	0.1765	5
哈萨克斯坦*	0.7500	0.3333	0.0000	0.0000	0.1250	0.1765	5
塔吉克斯坦*	0.7500	0.0000	0.0000	0.0000	0.2500	0.1471	6
乌兹别克斯坦*	0.7500	0.1667	0.0000	0.0000	0.1250	0.1471	6
吉尔吉斯坦*	0.5000	0.0000	0.0000	0.0000	0.2500	0.1176	7
土库曼斯坦*	0.7500	0.0000	0.0000	0.0000	0.0000	0.0882	8
* 基于次级数据。							

表 7: 欧洲指数排名

欧洲	法律	技术	组织	能力建设	合作	指数	区域排名
挪威*	1.0000	0.6667	0.7500	0.8750	0.5000	0.7353	1
爱沙尼亚*	1.0000	0.6667	1.0000	0.5000	0.5000	0.7059	2
德国*	1.0000	1.0000	0.6250	0.6250	0.5000	0.7059	2
英国	1.0000	0.6667	0.7500	0.7500	0.5000	0.7059	2
奥地利*	1.0000	0.3333	0.8750	0.7500	0.5000	0.6765	3
匈牙利*	1.0000	0.6667	0.7500	0.6250	0.5000	0.6765	3
以色列*	1.0000	0.6667	0.6250	0.7500	0.5000	0.6765	3
荷兰*	0.7500	0.5000	0.8750	0.6250	0.6250	0.6765	3
拉脱维亚*	1.0000	0.6667	0.7500	0.5000	0.5000	0.6471	4
瑞典*	0.7500	0.6667	0.6250	0.6250	0.6250	0.6471	4
土耳其	0.5000	0.6667	0.7500	0.7500	0.5000	0.6471	4
芬兰	0.5000	0.6667	0.8750	0.5000	0.5000	0.6176	5
斯洛伐克	1.0000	0.6667	0.8750	0.2500	0.5000	0.6176	5
丹麦*	1.0000	0.6667	0.5000	0.5000	0.5000	0.5882	6

欧洲	法律	技术	组织	能力建设	合作	指数	区域排名
法国*	1.0000	0.1667	0.5000	0.7500	0.6250	0.5882	6
西班牙*	1.0000	0.6667	0.6250	0.6250	0.2500	0.5882	6
意大利	0.7500	0.3333	0.6250	0.6250	0.5000	0.5588	7
波兰*	1.0000	0.3333	0.6250	0.6250	0.2500	0.5294	8
捷克共和国	0.7500	0.6667	0.6250	0.3750	0.2500	0.5000	9
卢森堡*	0.7500	0.3333	0.5000	0.3750	0.5000	0.4706	10
罗马尼亚	0.7500	0.3333	0.6250	0.2500	0.5000	0.4706	10
比利时*	0.7500	0.5000	0.2500	0.3750	0.5000	0.4412	11
保加利亚	0.7500	0.6667	0.5000	0.3750	0.1250	0.4412	11
立陶宛	1.0000	0.3333	0.7500	0.1250	0.2500	0.4412	11
克罗地亚	0.7500	0.6667	0.2500	0.3750	0.2500	0.4118	12
黑山	1.0000	0.5000	0.5000	0.0000	0.2500	0.3824	13
马耳他*	0.7500	0.5000	0.2500	0.2500	0.2500	0.3529	14
瑞士	0.5000	0.3333	0.2500	0.2500	0.5000	0.3529	14
塞浦路斯	0.7500	0.1667	0.3750	0.1250	0.2500	0.2941	15
葡萄牙*	0.7500	0.5000	0.1250	0.1250	0.2500	0.2941	15
塞尔维亚	0.7500	0.0000	0.3750	0.2500	0.1250	0.2647	16
阿尔巴尼亚	0.7500	0.3333	0.1250	0.1250	0.0000	0.2059	17
希腊*	0.5000	0.3333	0.1250	0.1250	0.1250	0.2059	17
冰岛*	0.7500	0.3333	0.0000	0.0000	0.2500	0.2059	17
爱尔兰*	0.5000	0.1667	0.0000	0.3750	0.1250	0.2059	17
波斯尼亚和黑塞哥维纳	0.7500	0.0000	0.1250	0.1250	0.1250	0.1765	18
斯洛文尼亚*	0.5000	0.3333	0.0000	0.1250	0.1250	0.1765	18
马其顿*	0.7500	0.1667	0.0000	0.0000	0.1250	0.1471	19

欧洲	法律	技术	组织	能力建设	合作	指数	区域排名
列支敦士登*	0.7500	0.0000	0.0000	0.0000	0.1250	0.1176	20
圣马力诺	0.5000	0.0000	0.0000	0.0000	0.2500	0.1176	20
摩纳哥*	0.5000	0.0000	0.0000	0.0000	0.1250	0.0882	21
安道尔*	0.5000	0.0000	0.0000	0.0000	0.0000	0.0588	22
* 基于次级数据。							

2.3 其他分析

全球	非洲	美洲	阿拉伯	亚太	独联体	欧洲
0.28	0.16	0.26	0.27	0.29	0.27	0.45

指数得分最高的是欧洲，最低的是非洲。

区域	法律	技术	组织	能力建设	合作
全球	0.50	0.27	0.28	0.24	0.24

全球而言，看来在法律方面做了较多工作，而得分最低的是能力建设。

区域	法律	技术	组织	能力建设	合作
非洲	0.31	0.13	0.17	0.11	0.16
美洲	0.44	0.24	0.24	0.25	0.20
阿拉伯	0.42	0.24	0.27	0.26	0.23
亚太	0.41	0.30	0.30	0.27	0.25
独联体	0.73	0.31	0.19	0.13	0.26
欧洲	0.79	0.42	0.45	0.37	0.34

得分最高的是欧洲法律，最低的是非洲能力建设。

3 良好实践

3.1 非洲

毛里求斯

具备**四个方面的立法措施：**

1. ICT Act 2001
2. 计算机滥用和网络犯罪法案 2003
3. 电子交易法案 2000
4. 数据保护法案 2004

正在与欧洲理事会**合作**起草商业垃圾电子邮件法案。

法律

技术

为民用业务定义风险**评估方法：**

作为 2007-2011 及 2011-2014 **国家信息和通信技术战略规划**(NICTSP)的组成部分，IT 安全部门正在牵头在民用业务上实施 **ISO/IEC 27001** 信息安全标准。

卢旺达

能力建设

- 在卢旺达国家警察学院开展针对 IT 安全的项目：

BSc 信息安全项目

- 教育部在高等教育综合 IT 或计算机工程项目中引入不同的**信息安全课程模块**
- 在 ICT 技能开发规划中，设置 IT 安全培训和许可项目
- 开展**国家网络安全宣传和培训项目，**提高互联网用户对网络安全的重视程度，并促进培养更多的网络安全专家，以确保公立和私立研究所关键系统不受网络威胁的破坏

喀麦隆

能力建设

- 为公众网络安全宣传活动设立**专项预算：**
  - 每两个星期在周四举办一次小测验、论坛和无线电节目
  - 计划在 Yaoundé 和 Douala 两个大城市开展宣传活动
- **国家 ICT 机构（ANTIC）**与高等教育部合作开发工程学校和大学网络安全项目
- 2010 年和 2013 年与 **IMPACT** 合作举办两次**网络安全研讨会，**主题包括普及率测试、安全审计和法政调查

科特迪瓦

法律

2013 年设立打击网络犯罪的国家性机构--打击网络犯罪（PLCC）平台：

- 登记了 9 497 个投诉
- 处理了 552 个投诉
- 逮捕了 70 人
- 以网络欺诈罪判处 65 人入狱

自 2009 年以来：

- **收到并处理了 5 000 多个投诉**
- 250 人因网络欺诈被判处监禁（其中 62.5%来自象牙海岸）

3.2 美洲

乌拉圭

法律

- **网络安全监管框架**
- 公共部门信息安全政策
- 信息安全导则
- 国家计算机应急处理中心 CERTuy 法令
- 个人数据保护和人身数据行动法案
- 欧盟理事会有关对乌拉圭个人数据给予适当保护的决定（2012 年）
- 乌拉圭成为**首个加入欧洲委员会个人数据保护公约（2013 年）的非欧洲国家**

美国

技术

工业控制系统网络安全应急响应团队（ICS-CERT）

国家标准和技术研究所

- 提高关键基础设施网络安全度的 1.0 版本框架
- 800 系列特别出版物
- 联邦信息处理标准
- 智能制造系统网络安全

国家网络安全教育举措(NICCS)

- 专业证书
- 国家网络安全用工框架

巴西

能力建设

- ABNT 制定了**巴西版本的 ISO IEC 标准**（如 ABNT NBR ISO/IEC 27000 系列）
- CEPESC – **通信安全研究开发中心** – 开展有关通信安全的科研和技术研究，包括技术转移
- CAIS RNP – **安全应急响应小组** – 负责侦测、解决并保护巴西科研网络不受安全事件的破坏，同时创建、促进并宣传网络安全最佳实践
- CEGSIC / UnB – 信息安全和通信管理**专业课程**
- CGI.br – **巴西互联网指导委员会** – 负责提供有关互联网的技术标准建议，并推动更多采纳最佳安全实践。

3.3 阿拉伯国家

阿曼

组织

- 在以下五个领域制定高级别网络安全战略和总体规划以及全方位路线图：
  1. 组织架构
  2. 法律措施
  3. 能力建设
  4. 技术和程序措施
  5. 区域和国际合作

摩洛哥

组织

- 作为国家网络安全战略的组成部分，摩洛哥的大部分科学和技术学校及大学将网络安全课程纳入其整体课程范围，以满足国家层面对系统信息安全技能的需求。

埃及

能力建设

- 通信和信息技术部推出了若干旨在建立国家网络安全框架的举措，包括设立一个由 ITIDA 运营的国家 PKI 中心（根 CA），并发放了一个政府 CA 牌照和三个私营部门 CA 牌照

突尼斯

法律

- 采取法律措施，定期对公共管理和其他选定的组织进行强制性信息安全检查，并制定有关信息安全检查机构执照申请的条件和程序。

3.4 亚太地区

澳大利亚

法律

- 澳大利亚已加入**欧洲委员会网络犯罪公约。**该公约于 2013 年 3 月 1 日生效。
- 发布 **2012 网络犯罪立法修正案，**2012 年第 120 号。
- 建立澳大利亚**网络犯罪在线举报网络**和**网络犯罪战略框架**
- 澳大利亚通信和媒体管理局（ACMA）负责执行 2003 反垃圾邮件法案。ACMA 开发了一个**在线举报垃圾邮件工具。**
- 澳大利亚竞争和消费者委员会（ACCC）提供**有关垃圾邮件**以及如何举报它们的**建议。**
- 澳大利亚联邦警察局（AFP）高科技犯罪行动（HTCO）部门负责**调查**澳大利亚**高科技犯罪。**
- 澳大利亚证券和投资委员会 (ASIC) 对诸如网络欺诈之类的**与金融服务相关的骗局**开展调查

马来西亚

技术

- **马来西亚计算机应急小组**(MyCERT)成立于 1997 年 1 月 13 日，在马来西亚网络安全办公室内开展工作。
- 根据政府 ICT 安全政策框架(PA 3/2000)，2001 年 1 月成立了 **GCERT MAMPU，**以确保政府 ICT 工作的连续性。
- GCERT 与 **55 个其他 CERT 组织**建立联络：
  - **国家网络安全框架**
    - 国家网络安全政策(NCSP)
    - 第 24 号指令 (NSC 第 24 号指令)
    - 2010 年内阁决定
    - 政府安全总办公室(CGSO)安全指令
    - NCSP – 政策要点 3: 网络安全技术框架

印度

能力建设

- 在知名学术和科研机构支持下，开展下述重要领域**科研项目：**（a）密码学和密码分析，（b）信息伪装，（c）网络和系统安全保证体系；（d）网络监控；（e）网络取证以及（f）在网络安全领域的能力建设。该国开发了很多网络取证工具。
- **全国范围的信息安全教育和宣传计划**

  在 CII、NASSCOM 以及微软合作下，CERT-In 创建**"secureyourpc.in"**门户网站，为用户提供网络安全方面的知识。
- 建立**网络安全培训设施，**为法律实施机构提供培训，并为网络犯罪调查提供协助。
- 在中央调查局（CBI）及加济阿巴德和喀拉拉邦警察局建立**培训中心，**为网络犯罪调查提供高级培训。
- J&K 邦和东北部邦正在建立**计算机取证实验室和培训机构。**
- 在 NASSCOM 帮助下，在孟买、班加罗尔、博帕尔以及加尔各答建立**取证中心。**
- 编制基于**虚拟培训环境**的培训模块。
- CERT-In 开展了 **94 个针对网络安全的培训项目，**其中，**已培训人员达 3392 人。**

韩国

组织机构

- **制定国家网络安全措施，**系统性组织政府层面对国家安全构成威胁的网络事件做出反应，包括制定四个旨在实现强有力网络安全的战略：
  - 加强网络威胁应急系统反应能力
  - 为相关机构建立智能合作系统
  - 加强网络空间安全措施的可靠性
  - 为网络安全建立创新性基础
- 制定**个人信息保护正常化规划，**推动采取通用的做法来开展信息管理工作，并对系统、技术和权利进行保护。
- **科学、ICT 和未来规划部负责监管工作**
- **国家信息安全指数：**采取客观和定量措施评估韩国私营部门（企业和个人互联网用户）信息安全程度
- 参考各国案例以及典型案例开展**全方位政治性活动**

日本

合作

- 在亚太地区，**JPCERT/CC 帮助建立了 APCERT**（亚太计算机应急响应小组），并为 APCERT 提供秘书处职能。
- 在全球层面，日本作为计算机事件响应与安全工作组论坛（**FIRST**）的成员，与全球值得信赖的 CSIRT 保持合作。
- **国际网络安全战略 –** 网络安全日本举措
- 与美国、欧盟、以色列、南美开展**国际合作**
- **与 UNGGE、G8、OECD、APEC、NATO、ASEAN 开展合作**
- **子午线和国际监测及预警网络**
- 签署**布达佩斯公约**
- 国防部信息共享计划
- **METI 日本网络安全信息共享合作伙伴** (J-CSIP)

3.5 独联体(CIS)

阿塞拜疆

能力建设

- 阿塞拜疆通信和高技术部正式认可国家性或部门性**网络安全研发项目/计划**标准以及适用于私营和公共部门的良好实践及指导原则。
- 技术委员会将在国际（区域）和国家间标准基础上**起草国家标准。**
- 阿塞拜疆开展**短期电子政务和信息安全培训课程**
- AZ-CERT 组织**夺旗竞赛，**以增强信息安全专业竞争力
- CERT GOV AZ 获得 FIRST、Trusted Introducer 和 CERT 的认证
- 阿塞拜疆共和国国家石油公司(SOCAR)的信息技术和通信部门获得 **ISO 27001:2005 认证**
- 得到 ISO 27001:2005 认证的 SOCAR IT 和通信部

俄罗斯联邦

法律

- **个人数据保护** – 根据联邦法第 152 条，由联邦电信、信息技术和大众媒体部（Roscomnadzor）负责监管
- **黑名单和 ISP 控制**– 根据联邦法第 139 条，由 Roscomnadzor 负责监管
- **关键基础设施保护** – 由 FSTEC RF 负责监管，保密且仅分发给具有许可证的公司和产业部门
- 关键基础保护– FSB RF 已发布 CIP 保护战略
- **加密** – 由 FSB RF 负责监管
- 政府部门**信息安全**– 由 FSB RF、FSTEC RF 和 FSO RF 负责监管
- 海外政府部门信息安全– 由 SVR RF 负责监管
- MoD 信息安全 – 由 MoD 和 FSB RF 负责监管
- **机密数据保护**信息安全– 由 FSTEC RF 负责监管
- 信息安全**解决方案的兼容性**（软件，硬件）- 由 FSTEC RF 负责监管
- **网络犯罪调查** – 由内政部负责监管
- 每个机构都有其自身**网络安全解决方案**及数据保护**许可和要求**：所有这些方案和要求相互之间都很类似，但许可的程序不同，且由各个机构分别负责控制。

摩尔多瓦

合作

- 2013 年，**爱沙尼亚电子政务学院和摩尔多瓦共和国电子政务中心**实施了一个网络安全项目，包括 3 个组成部分：
  - 第一部分是为摩尔多瓦政府机构制定**网络安全路线图**
  - 第二部分是为政府机构确定**数字信息安全最低要求**，或政府在确保数字信息安全可靠方面应开展哪些工作
  - 第三部分更具一般性，即**提高**政府官员和摩尔多瓦市民对当前网络安全风险和威胁的**重视程度**

3.6 欧洲

土耳其

组织机构

- 制定 2013-2014 **国家网络安全战略和行动计划**
- 行动计划包括 **29 个主要行动和 95 个子行动，**并就立法、能力建设、技术基础设施开发等分配了职责。
- 设立**网络安全委员会，**负责确定应采取的网络安全措施，批准提交的规划、项目、报告、程序、原则和标准，并确保其得到应用及相互协调。
- 在过去三年，**在国家层面**开展了**三个网络安全演练，**参与者包括公共和私营部门。演练对于**提高网络安全重视程度**发挥了重要作用，同时也是一个很好的**测量网络安全发展程度**的工具。

英国

能力建设

- **CESG 是 GCHQ 负责信息安全的部门，**同时也是英国国家技术和信息安全保障管理局。
- CESG 是**通用标准互认协定**的授权成员
- 英国研究理事会与 CESG 一道开展了名为“**全球不确定性**”的项目，其中网络安全是其关键议题。
- 英国设立了一系列**网络安全研究学术中心**以及配套的研究机构，其中一个是牛津大学互联网研究所，其中包括了一个能力建设中心
- **政府为 IA 专家提供了**名为 CCP **IA 认证项目**
- 英国政府强烈支持 IISP 认证，并鼓励更多机构参与 IISP 和 CCP

爱沙尼亚

技术

- **ISKE** 是为爱沙尼亚公共部门制定的**信息安全标准，**并强制要求有关处理数据库/注册表的负责**国家层面和地方政府**组织必须遵循。
- 编制了**三级基线系统，**其中，三类不同安全要求对应三套不同安全措施。
- 爱沙尼亚**电子政务和 IT 基础设施**系统使用 **2048 比特的加密算法，**以增强爱沙尼亚电子身份、数字签名和 X 道路系统的安全。
- 爱沙尼亚**实施了一套国家 PKI。**与 PKI 相关的最重要领域由国家层面负责组织管理：
  - 开发**一整套** PKI（ID 卡的基本软件）必备**应用。**此项工作由信息系统管理局（RIA）负责处理。
  - 开展**立法**工作，以明确 PKI 业务的**质量和信任要求。**此项工作由经济事务和通信部国家信息系统司负责处理。
  - 发布**确保电子认证和签名**（ID 卡等）的方法。此项工作由警察和边防局负责处理。

荷兰

合作

- **机构内合作**由荷兰警务局（KLPD）高技术犯罪组织负责，并通过**国家网络安全中心**（NCSC）实施。NCSC 负责收集 ICT 安全方面的信息，并就安全问题为各组织提供咨询意见。
- NCSC 提供的服务大部分源自**公共和私营部门合作**获得的增值收益。
- NCSC 的职能主要集中于那些对社会发展起关键作用的部门，即所谓的**重要部门：**能源公司、电信和金融部门。
- **参与** NCSC PPP 的**政府部门**包括安全和司法部、经济事务部、农业和创新部、内政和王国关系部、外交和国防部、公诉机关、情报和安全总局以及国家警务局。

4 国家网络健康概况[1]

作为国际电联对其193个成员国在全球网络安全议程[2]框架内给予的整体支持的一个组成部分，我们发布了网络安全健康度概况，以介绍各国在网络安全发展上的事实情况。该报告旨在就当前网络安全状况提供一个清晰的阐述，其主要内容基于全球网络安全议程的五个支柱，即法律措施、技术措施、组织措施、能力建设和合作。儿童上网保护问题作为国际电联的一个关键举措也纳入在内。

单独一份出版物不可能深度覆盖所有问题。尽管如此，我们还是希望这份网络健康度概况能够有助于当前各方开展讨论和研究，并能够提供当前在网络安全上面临的挑战和机遇的真实情况。

附件3是本出版物发布时国际电联所有成员国在网络健康度概况方面的更新汇总。概况的最新版本可通过以下网址查阅：www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.asp

5 结论

GCI已在国际电联釜山全权代表大会上成功获得认可，并已纳入第130号决议（2014年修订，釜山）：增强国际电联在树立信息通信技术使用的信心和安全方面的作用。需要特别要指出的是，各成员国被邀请“支持国际电联在网络安全包括全球网络安全指数（GCI）方面的举措，以促进各国战略的实施，并推动各个产业和部门共享各自开展工作的信息”。

《全球网络安全指数》第一版成功实现了衡量各成员国在网络安全方面履行承诺程度的目标，并激发了各成员国对网络安全评估的兴趣。GCI已调动起各国的积极性，加强各自的网络安全工作，提高各国对开展双边合作的重视程度，并增强了各国在网络安全方面开展工作的能见度。

为使GCI在推动各方持续高度重视这一全球性崭新问题方面继续发挥作用，有必要保持GCI的连续性。我们欢迎各成员国和业界利益攸关方参与后续的研究和开发，对目前的参考模式加以提升，并引入新的做出贡献的合作伙伴。

这些合作伙伴能够提供更多的资源，从而增强GCI问卷表的颗粒度，并提供更多基于次级数据的证据，通过专家定性评估以及与其他现有指标，比如国际电联ICT发展指数和世界经济论坛网络就绪指数等，进行定量比较，从而对收集到的数据作更进一步的分析。

这一庞大的数据收集工作得以成功，在很大程度上要归功于问卷表的回复率。我们呼吁所有成员国积极参与GCI工作。GCI今后的工作将提供更多与国际电联成员国及相关利益攸关方开展开放磋商的机会。这项工作将成为年度性工作，其成果将向WSIS提交报告。这项工作的最终目的是帮助促进建立一个网络安全的全球文化，并将其作为国际电联的一项重要职责嵌入ICT的核心。

[1] 目前现有193个国家的网络安全健康度概况。详情请咨询国际电联（cybersecurity@itu.int），以便了解网络安全健康状况的最新情况，同时欢迎国际电联成员特别是那些由于缺乏可信数据而尚未纳入概况列表的国家提供最新数据。附件3是本出版物印刷时所有成员国的网络健康度概况汇总。最新概况情况可查询：www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.asp

[2] www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

附件 1: 概念性框架

信息和通信技术（ICT）已经成为现代社会发展的强劲动力，为个人、组织以及政府在社会、经济和政治方面的发展提供有力的支持。ICT 覆盖范围越来越广，同时对社会发展进步也起到了越来越关键的推动作用。包括智能设备、M2M 通信和云服务等在内的这些技术正在推动建立下一代网络（NGN）社会。由于数字技术和互联网连接在促进生产率、提高速度和节约成本方面的显著优势，它们已经与私营和公共部门各个层面系统联系在一起。新的平台如零售 RFID 系统和车辆远程信息处理系统等越来越多地用到了 ICT。但更值得注意的，ICT 正在应用于能源网、交通网和医疗系统等关键基础设施上，以实现这些基础设施的升级换代。

网络安全对于保持先进技术模式的可持续发展来说非常重要。由于 ICT 网络干扰造成的停电或金融系统受损事件屡见不鲜；这些事件对国家安全构成了威胁。网络上有数不清的有组织的恶意代理服务器，而且来源也非常广泛：政治、罪犯、恐怖组织、黑客组织等应有尽有。他们使用的工具随着时间的推进，也变得越来越高级和复杂，而且越来越有经验。日益涌现的网络连接平台，只能成为新的网络攻击的猎物。要想回到以前较单纯的时代已经不可能了。在拥抱技术进步的同时，网络安全必须成为这一进程不可分割的整体性组成部分。

但不幸的是，网络安全尚未成为各国和产业界技术战略关注的核心。各方在网络安全治理方面下了很大功夫，但这些工作五花八门、零零散散，不成系统。各国在互联网普及率、技术发展、私营部门动力、政府战略方面存在差异，这意味着网络安全正在以一种自下而上的方式出现；呈现出一种在各个国家、公共和私营部门以及不同产业之间仍存差异情况下自然发生的过程。但实际上，自上而下方式更有助于全球网络安全文化的顺利建立。信息共享和相互合作对于处理跨界威胁来说非常关键。解决上述问题需要采取一种兼有法律、技术、教育等各行各业的组织形式。很多情况下在一个国家或具体部门内部可能会发展和采纳一种高度有效的网络安全框架，但这方面的知识共享却很难迈出这一圈子之外。

这其中的主要障碍在于，不论是从政府还是从私营部门的观点来看，网络安全都是一个敏感议题。容忍漏洞可能被视为一种弱势表现。这对讨论和分享有关威胁的信息和最佳实践形成了很大障碍。在现代化网络威胁面前采取不了了之的态度，这显然不是一个可行的防范模式。要想解决问题，就必须在社会的各个层面都要部署网络安全机制。但是，采取这些措施的动力和动机还不足，这其中原因可能出于成本制约，也可能是缺乏重视程度。补救这一情况的第一步是要对各国的网络安全能力进行比较，并发布一个有关他们状况的有效排名。排名系统将披露那些做的不好的地方，并鼓励各国政府强化其在网络安全方面的努力。只有通过比较，才能真正看出各国网络安全方面具备的真实能力。

全球网络安全指数（GCI）项目旨在有效测量各国在网络安全方面的工作开展的程度。最终目标是要帮助促成一种全球网络安全文化，并将其以核心方式整合进信息和通信技术。该项目由国际电信联盟（ITU）和私营公司 ABI Research 推出。从当前国际电联的职责以及国际电联电信发展局（BDT）开展的有关项目和活动中，可以找到设立 GCI 项目的基础根据。

国际电联是 WSIS（信息社会世界峰会）第 C5 行动方面的牵头协调机构，任务是帮助各利益攸关方在国家、区域及国际层面树立使用 ICT 的信心和安全。国际电联在网络安全方面的职责进一步体现在第五届世界电信发展大会（WTDC-10）通过的第 69 号决议“关于特别为发展中国家成立国家计算机事件响应组（CIRT）并开展这些组之间的合作”以及第 130 号决议（2014 年，釜山）“关于加强国际电联在树立使用信息通信技术的信心和安全方面的作用”。在这一框架下，国际电联秘书长推出了全球网络安全议程（GCA），作为国际电联有关国际多利益攸关方合作共建更加安全可靠的信息社会的框架，并重点在以下五个领域开展工作：

- 法律措施
- 技术措施
- 组织措施
- 能力建设
- 合作

这五个指定领域将构成 GCI 指标的基础内容。对于测量各国网络安全能力来说，这五个指标非常关键，因为它们是建设国家文化的不可或缺的组成部分。网络安全能够应用在从纵向到横向贯穿于所有产业和所有部门的领域。因此，为确保国家能力的发展，有必要加大政治、经济和社会力量的投入。这可以通过法律实施和司法部门、教育机构和各部委、私营部门运营商和技术开发机构、公众-私营合作伙伴以及国内机构之间的合作来实现。

GCI 的长期目标是要推动在全球范围进一步采取网络安全措施，并将网络安全整合进入各国战略。对各国网络安全战略进行比较，将凸显那些在具体领域具有较高排名的国家，同时也将曝光那些目前为止仍未制定网络安全战略的国家。这能够有效推动这些处于不同发展阶段的国家在部署网络安全时更多地分享有关信息。通过开展对各个领域网络安全措施到位程度的衡量工作，该指数将使各国有机会评估其发展规模，了解在哪些方面尚需进一步改进，同时明晓其距离可接受的网络安全基准还有多远。当前，各国都在向更加数字化和更加互联的环境积极迈进。在此过程中，越早采取网络安全措施，就越能够确保建立长期的更为安全可靠的基础设施。

GCI 项目将是 BDT（具体而言是网络安全和信息通信技术应用处（CYB））和 ABI Research 精诚合作的成果。CYB 负责作为该项目的焦点联系及所有者，而 ABI Research 负责提供项目开展所必须的战略发展、竞争情报、商业规划、技术评估和业界基准等核心技能。ABI Research 是一家专注于全球技术市场情报研究的公司，擅长开展定量预测和对关键指标和趋势进行分析。在提供技术前瞻决策参考和可行、及时、真实数据方面，ABI Research 具有独一无二的竞争力，其专家力量将及时研究和出台可信赖的指数。根据协议，国际电联和 ABI Research 将开展以下工作：

- 确定绩效指标；
- 建立全球排名的确定机制；
- 研究并收集各国网络安全能力；
- 与各国及相关组织进行接洽和联系；
- 在指数中确定并添加相关数据；
- 发布全球网络安全指数。

分类和绩效指标

GCI 将成为衡量主权国家网络安全发展程度的基准排名措施。该指数主要是一个由多项指标叠加而成的复合指标。网络安全的发展程度可通过对五个重要而宽泛的类别进行分析而得。我们确定了以下指标和子类别，各国将按照每项指标提供的基准来进行排名。

法律措施

立法的目的是要为相关实体提供一个统一框架，以便其遵守共同的监管基准，其中既涉及禁止开展特定的犯罪行为，也包括最低监管要求。法律措施也使各国有机会制定一个基本的应对违法行为的机制：对犯罪行为进行调查和起诉，并对不遵守或违反法律的行为进行处罚。立法框架设定了对任何人都适用的、全体必须遵循的行为标准，并在此基础上开展网络安全能力建设。其最终目标是要使所有国家都具备适当的立法，以便协调开展超越国家边界的行动，提供互联的措施，并促进国际社会对网络犯罪的打击。

法律环境可以基于现有的处理网络安全和网络犯罪的法律机构和框架的数量进行测定。其分类别包括以下绩效指标：

A. 刑事立法

刑事立法指的是指定有关法律负责管辖计算机、系统和数据的非授权（无权）接入、干扰、截获等行为。这些法律的排序分为以下类别：无，部分或全面。部分立法指的是在现有刑法或法典中简单加入有关计算机的措辞，且仅限于将诸如欺诈、造假、监控或偷窃等词句扩展至网络空间范畴。全面立法指的是制定一部专门的有关计算机犯罪方面的法律或法案（如英国 1990 计算机滥用法）。对于案例法或法理学相当完善的部分立法情况，可以将之归为全面立法。请列出法律和规章的类别，并将其标注为“无”、“部分”或“全面”。

B. 监管和合规

网络安全监管指的是指定有关法律负责处理数据保护、资料外泄通知以及认证/标准化要求。这些法律可按以下进行排序：无，部分或全面。部分监管是指在现有刑法或民法中加入有关计算机的措辞，从而将那些并非专门或唯一处理网络安全的法律扩展至网络空间（如 EU 第 95/46/EC 号有关个人处理私人数据的权利和此类数据自由移动的指令）。全面监管指的是制定专门的要求网络安全合规的法律、法案或指令（如美国 2002 联邦信息安全管理法案）。请列出法律和规则的类型，并将其标注为“无”、“部分”或“全面”。

技术措施

技术是抵御网络威胁和恶意在线代理的第一道防线。如果没有恰如其分的侦测和应对网络攻击的技术措施和能力，那么这个国家及其相关实体将很容易受到网络威胁的破坏。要想继续促进 ICT 的创新和成功，必须提供一种信任安全的环境。各国有必要制定相关的战略，规定可接受的最低安全标准，并出台软件应用系统的认证方案。这些工作必须由国家层面致力于处理网络事件的国家实体负责（最低限度是负责的政府机构），而且必须制定应对网络安全的国家框架，以推动开展监控、预警和应急响应工作。

技术措施的衡量可以基于是否具有以及有多少政府支持或创建的技术机构和框架来处理网络安全事件。子类别由以下绩效指标组成：

A. CERT/CIRT/CSIRT

建立国家性 CIRT（计算机事件响应组），CERT（计算机应急响应组）或 CSIRT（计算机安全事件响应组），这些组织应能够发现、防御、应对和管理网络威胁，并能增强该国网络空间的安全度。此外，还应具备自己收集情报的能力，而非依赖 CIRT 社区或其他来源的次级网络安全事件报告。请列出经官方批准的国家性或部门性 CERT 或 CSIRT 小组的名字和数量，并指出其职责是否由法律授权。发展程度将基于是否有国家团队以及其职责是否由法律授权等进行排序。

B. 标准

该指标衡量是否存在一个经政府批准（或支持）的框架（或多个框架），用以实施国际公认的公共部门（政府机构）及关键基础设施（即使是私营部门运营的）的网络安全标准。这些标准包括但不限于由以下机构制定的标准：ISO、ITU、IETF、IEEE、ATIS、OASIS、3GPP、3GPP2、IAB、ISOC、ISG、ISI、ETSI、ISF、RFC、ISA、IEC、NERC、NIST、FIPS、PCI DSS 等。请列出任何经官方批准的用于实施国际公认网络安全标准的国家性（或部门性）框架。

C. 认证

该指标衡量是否存在一个经政府批准（或支持）的框架（或多个框架），该框架根据国际公认的安全标准来开展国家（政府）机构和公共部门技术人员的认证和鉴定工作。这些认证、鉴定和标准包括但不限于以下各项：云安全知识（云安全联盟），CISSP、SSCP、CSSLP CBK 网络安全取证分析师(ISC²)、GIAC、GIAC GSSP (SANS)、CISM、CISA、CRISC (ISACA)、CompTIA、C|CISO、CEH、ECSA、CHFI (EC 理事会)、OSSTMM (ISECOM)、PCIP/CCISP (关键基础设施研究所)、(无建议)认证、Q/ISP、软件安全工程师证书 (安全大学)、CPP、PSP、PCI (ASIS)、LPQ、LPC (丢失防护研究所)、CFE (欺诈审查师认证协会)、CERT-计算机安全时间处理机构认证 (SEI)、CITRMS (消费者金融教育研究所)、CSFA (网络安全研究所)、CIPP (IAPP)、ABCP、CBCP、MBCP (DRI)、BCCP、BCCS、BCCE、DRCS、DRCE (BCM)、CIA、CCSA (内部审计研究所)、(专业风险管理师国际协会)、PMP (项目管理研究所)等。请累出任何由官方批准的对国家机构和公共部门专业人员进行认证和鉴定的国家性（或部门性）框架。

组织措施

组织和程序措施对于实施任何类型的国家举措都是必需的。各个国家政府都有必要制定具有实施、提供和衡量措施等全面规划的宏观战略目标。组织架构（如国家机构）必须到位，以便将战略付诸实施，并衡量规划的成功或失败。如果没有国家战略、治理模式和监管机构，不同部门和产业界的努力都会变得分散和互不关联，这将不利于实现该国网络安全能力发展的一致协调性。

组织架构可以基于在国家层面上是否存在以及有多少个负责网络安全发展的机构和战略。建立有效的组织架构有利于促进网络安全、打击网络犯罪和进一步发挥监控、预警和事件响应的作用，并确保在机构内部、跨部门和跨边界对新出现的或现有举措进行协调。子类别包括以下绩效指标：

A. 政策

制定促进网络安全的政策应置于最高优先级的位置。国家层面网络和信息系统安全战略应能够确保信息基础实施的稳定和可靠，并确保公民的安全；保护公民、组织和国家的材料和智力财产；防止关键基础设施受到网络攻击的破坏；能够在受到网络攻击后将损失降低到最小限度，并能实现最快程度的恢复。有关保护信息基础设施的国家层面网络安全战略或国家性规划必须由一个国家官方定义和支持，且可以包括以下承诺：为政府（地方、区域和联邦或国家）各个层面规定明确的职责，其中要清晰定义作用和责任；就网络安全做出明确承诺，这个承诺应该是公开和透明的；鼓励私营部门参与政府牵头的举措，并建立合作关系来推动网络安全。请列出任何由官方认可的国家性或部门性网络安全战略。

B. 治理路线图

网络安全治理路线图通常由国家网络安全战略/政策来制定，其中要指出起关键作用的利益攸关方。对于高级别网络安全治理来说、制定国家政策框架是最高优先级的任务。国家政策框架必须考虑对国家关键信息基础设施的保护。该框架也应寻求促进公共部门内部以及公共部门和私营部门之间的信息共享。网络安全治理应基于国家性框架。该框架应在国家层面上处理信息安全和网络安全挑战及其他问题，主要内容可包括：国家战略和政策；将安全相关的法律转化为网络及在线环境的法律基础；建设网络安全文化；处理 ICT 安全泄漏和事件的程序（报告、信息共享、警报管理，司法和警界合作）；国家安全政策的有效实施；网络安全项目控制、评估、验证和优化。请列出任何经官方认可的国家性或部门性网络安全治理路线图。

C. 负责机构

负责机构指的是实施国家网络安全战略/政策的机构，可以包括常设委员会、官方工作组、咨询理事会或跨部门中心。大多数国家机构直接负责开展监控、预警系统以及事件响应工作，并制定用以协调网络攻击响应的组织架构。请累出任何经官方认可的国家性或部门性网络安全机构。

D. 国家基准

该指标衡量是否存在官方认可的国家性或部门性设立基准的活动或衡量网络安全发展程度的参考基线。例如，基于 ISO/IEC 27002-2005 的国家安全标准（NCSec 参考框架）有助于国家确定网络安全要求。该参考框架分为五个部分：NCSec 战略和政策；NCSec 组织架构；NCSec 实施；国家层面协调；网络安全宣传活动。请列出任何经官方认可的国家性或部门性设立基准的活动或衡量网络安全发展程度的参考框架。

能力建设

能力建设与前三个措施（法律、技术和组织）内在密切相关。对技术、风险及其影响具备充分的了解，能够帮助制定更好的立法、更好的政策和战略以及更好的涉及各种不同职责和职能的组织架构。网络安全是一个相对全新的领域，其历史并不比互联网长多少。对这一领域的研究通常从技术角度出发；但该领域对社会经济和政治产生的影响却很大。人力和机制能力建设对于提高各个部门的知识和技能非常重要，能够推动采用最佳的解决方案，并促进最优竞争力技术人员的发展。

网络安全能力建设框架应包括宣传活动，并具备可用资源。能力建设可以基于是否存以及有多少研发、教育和培训项目以及认证专业人员和公共部门机构等进行衡量。子类别由以下绩效指标组成；

A. 标准制定

标准化是衡量技术成熟度的很好指标。通常在关键领域会出现新的标准，这显示出标准的极端重要性。虽然网络安全一直被认为是国家安全问题，且不同国家采取的应对措施也不一样，但公认的标准还是支持共同的做法。这其中包括但不限于以下机构制定的标准：ISO、ITU、IETF、IEEE、ATIS、OASIS、3GPP、3GPP2、IAB、ISOC、ISG、ISI、ETSI、ISF、RFC、ISA、IEC、NERC、NIST、FIPS、PCI DSS 等。请列出任何经官方认可的在网络安全标准、最佳实践和指导原则（既适用于私营部门也适用于公共部门）方面开展的的国家性或部门性研究和开发（R&D）计划/项目。

B. 人力开发

人力开发指的是各国利用 NGO、研究所、组织、ISP、图书馆、本地贸易组织、社区中心、计算机商店、社区学院和承认教育项目、学校和家长教师会等开展的涉及尽可能多人的宣传安全上网行为信息的公众宣传活动。这些行动包括建立门户网站和网页来开展宣传，传播教育机构支持材料，并设立（或鼓励）专业培训课程和教育项目。请列出任何经官方认可的国家性或部门性教育和职业培训项目，这些项目旨在提高公众的认识程度（如国家网络安全宣传日、周或月），推动在高等教育（技术、社会科学等）开设网络安全课程，并推动公众或私营部门的专业人员认证工作。

C. 专业认证

该绩效指标可通过根据国际认可证书项目标准开展的公共部门专业认证的数量进行衡量，其中标准包括但不限于：云安全知识（云安全联盟），CISSP、SSCP、CSSLP CBK,网络安全取证分析师 (ISC²)、GIAC、GIAC GSSP (SANS)、CISM、CISA、CRISC (ISACA)、CompTIA、C|CISO、CEH、ECSA、CHFI (EC 理事会)、OSSTMM (ISECOM)、PCIP/CCISP (关键基础设施研究所)、(无建议)认证、Q/ISP、软件安全工程师证书 (安全大学)、CPP、PSP、PCI (ASIS)、LPQ、LPC (丢失防护研究所)、CFE (欺诈审查师认证协会)、CERT-计算机安全时间处理机构认证 (SEI)、CITRMS (消费者金融教育研究所)、CSFA (网络安全研究所)、CIPP (IAPP)、ABCP、CBCP、MBCP (DRI)、BCCP、BCCS、BCCE、DRCS、DRCE (BCM)、CIA、CCSA (内部审计研究所)、(专业风险管理师国际协会)、PMP (项目管理研究所)等。请列出根据国际认可证书项目开展的公众领域专业认证项目的数量。

D. 机构认证

该绩效指标可通过根据国际认可标准认证的认证政府和公共部门机构的数量进行衡量。其中标准包括但不限于以下机构制定的标准：ISO、ITU、IETF、IEEE、ATIS、OASIS、3GPP、3GPP2、IAB、ISOC、ISG、ISI、ETSI、ISF、RFC、ISA、IEC、NERC、NIST、FIPS、PCI DSS 等。请列出获得国际认可标准认证的政府和公共部门机构的数量。

合作

网络安全需要各部门、各领域的参与贡献，因此有必要采取多利益攸关方原则。加强合作有利于对话和协调，有利于创造更为全面的网络安全应用领域。在不同部门之间以及在私营部门运营商内部，开展信息共享是最为困难的。这在国际层面尤为突出。但网络犯罪是全球性问题，超越了国家边境或部门界限的限制。加强合作有助于促进共享威胁信息、攻击情景以及应对和防卫最佳实践。开展更多更有意义的合作举措将确保发展更强大的网络安全能力，有助于阻击反复顽固的在线威胁，并确保对恶意代理进行更有效的调查、逮捕和起诉。

国家和国际合作指标可以根据是否存在以及有多少合作伙伴、合作框架和信息共享网络来进行衡量。其子类别由以下绩效指标组成：

A. 国内合作

国内合作指的是任何经官方认可的国家性或部门性合作伙伴关系，用于共享跨国境边界的网络安全资产（比如签署双边或多边合作伙伴关系，开展信息、专业知识、技术和/或资源的合作或交换）。国家合作也包括区域性层面的举措，比如（但不限于）由欧盟、欧洲理事会、八国集团、亚太经合组织（APEC）、美洲国家组织（OAS）、东南亚国家联盟（ASEAN）、阿拉伯联盟、非洲联盟、上海合作组织（SCO）以及网络运营组织（NOG）等开展的活动。请列出与其他国家开展跨边境网络安全资产分享的国家层面或部门层面的合作伙伴关系。

B. 机构内合作

机构内合作指的是任何经官方认可的公共部门内部分享网络安全资产（人员、程序、工具）的国家性或部门性项目（如在不同部门和机构之间开展合作或交换信息、专业知识、技术和/或资源的官方合作伙伴关系）。这一项目包括不同部门（执法、军队、医疗、交通、能源、水和水管理等）之间以及在司局/部委（联邦/地方政府，人力资源，IT 服务台，公共关系等）内部开展的举措或项目。请列出任何经官方认可的用于在公共部门内部分享网络安全资产的国家性或部门性项目。

C. 公私伙伴关系

公私伙伴关系（PPP）指的是在公共和私营部门之间开展的项目。该绩效指标可以通过官方认可的在公共部门和私营部门之间分享网络安全资产（人员、程序、工具）的国家性或区域性项目（如用于合作或交换信息、专业知识、技术和/或资源的官方伙伴关系）的数量来进行衡量。请列出任何经官方认可的在公共部门和私营部门之间分享网络安全资产的国家性和部门性项目。

D. 国际合作

该绩效指标指的是任何经官方认可的参与国际网络安全平台和论坛的活动。此类合作举措包括（但不限于）那些由以下国际组织开展的活动：联合国大会；国际电信联盟（ITU）；国际刑警组织/欧洲刑警组织；经济合作与发展组织（OECD）；联合国 毒 品和犯罪 问题办公室（UNODC）；联合国区域间犯罪和司法研究所（UNICRI）；互联网名称与数字地址分配机构（ICANN）；国际标准化组织（ISO）；国际电工委员会（IEC）；互联网工程任务组；FIRST（事件响应和安全团队论坛）。请列出任何经官方认可的参与区域和/或国际网络安全平台和论坛活动的情况。

方法

本指数采用的统计模型基于多标准分析方法（MCA）。MAC 在不同选项之间选定偏好的选项，其方法是通过参考具有确定目标的明确集合。对于这些目标来说，有明确的可衡量的标准来评估这些目标能在多大程度上得到实现。这里采用的是简单线性叠加评估模型。MCA 性能矩阵对不同选项进行描述，每一列描述不同选项在各个标准之下的表现。每个绩效评估以数值形式表示。

基准计分将基于以下指标得分，每个指标具有相同权重（但子类别指标的权重将比其他指标稍高，因为一些指标包含多个子类别）。无任何活动的情况得 0 分；部分行动得 1 分；更为全面的行动得 2 分。分配给每个类别的总得分点分别为：

1. 法律措施	**4**
A. 刑事立法	2
B. 监管和合规。	2
2. 技术措施	**6**
A. CERT/CIRT/CSIRT	2
B. 标准	2
C. 认证	2
3. 组织措施	**8**
A. 政策	2
B. 治理路线图	2
C. 负责机构	2
D. 国家性基准	2
4. 能力建设	**8**
A. 标准制定	2
B. 人力开发	2
C. 专业认证	2
D. 机构认证	2
5. 合作	**8**
A. 国内合作	2
B. 机构内合作	2
C. 公私伙伴关系	2
D. 国际合作	2

符号:

x_{qc} 国家 c 的单个指标 q 的值， 其中，q=1,…、Q，且 c=1,…、M.

I_{qc} 国家 c 的单个指标 q 的归一化值

CI_c 国家 c 的复合指标值

这里采用的基准是假定一个国家在各个就绪点上都能够得到最大值（34 分）。由此得出的复合指数将在 0（可能的最差就绪情况）和 1（基准）之间变化：

$$CI_c = \frac{I_{qc}}{34}$$

归一化方法将基于排名方法：

$$I_{qc} = Rank\,(x_{qc})$$

影响

GCI 的长期目标是要推动在全球范围进一步采取网络安全措施，并将网络安全整合进入各国战略。对各国网络安全战略进行比较，将凸显那些在具体领域具有较高排名的国家，同时也将曝光那些目前为止仍未制定网络安全战略的国家。这能够有效推动这些处于不同发展阶段的国家在部署网络安全时更多地分享有关信息。通过开展对各个领域网络安全措施到位程度的衡量工作，该指数将使各国有机会评估其发展规模，了解在哪些方面尚需进一步改进，同时明晓其距离可接受的网络安全基准还有多远。当前，各国都在向更加数字化和更加互联的环境积极迈进。在此过程中，越早采取网络安全措施，就越能够确保建立长期的更为安全可靠的基础设施。

附件 2: 问卷样本

调查问卷

全球网络安全指数

回复本份问卷的国家 (包括联系人信息):	
问题	**回答**
1A. 请列出任何有关网络安全的刑事立法 包括法律/法案/条款的网址、标题和/或措辞	
1B. 请列出任何有关网络安全的监管和合规要求 包括法律/法案/条款的网址、标题和/或措辞	
2A. 请列出任何经官方批准的国家性或部门性 CERT、CIRT 或 CSIRT 组织，以及它们是否经法律授权 包括网址、官方名称和详细联系方式	
2B. 请列出任何经官方批准的用于实施国际公认网络安全标准的国家性（和部门性）网络安全框架 包括框架的网址、官方名称、负责机构（及详细联系方式）和简要描述	
2C. 请列出任何经官方批准的用于对国家机构和公众部门专业人员进行认证和鉴定的国家性（和部门性）网络安全框架 包括框架的网址、官方名称、负责机构（及详细联系方式）和简要描述	
3A. 请列出任何经官方认可的国家性或部门性网络安全战略和/或政策 包括战略/政策的网址、官方名称、负责机构（及详细联系方式）和简要描述	
3B.请列出任何经官方认可的国家性或部门性网络安全治理路线图 包括路线图的网址、官方名称、负责机构（及详细联系方式）和简要描述	
3C. 请列出任何经官方认可的负责实施国家网络安全战略/政策/路线图的国家或部门机构 包括负责 机构的网址、官方名称（及详细联系方式）及其职责的简要描述	
3D. 请列出任何经官方认可的用于衡量网络安全发展程度的国家性或部门性设定基准的活动或参考框架 包括基准活动的网址、官方名称、负责机构（及详细联系方式）和简要描述	
4a. 请列出任何经官方认可的旨在开发用于私营或公共部门的网络安全标准、良好实践和指导原则的国家性或部门性科研开发(R&D)计划/项目 包括计划/项目/良好实践/标准/指导原则的网址、官方名称、负责机构（及详细联系方式）和简要描述	
4B. 请列出任何经官方认可的旨在提高公众认识程度、推动在高等教育中纳入网络安全课程以及促进为公众或私营部门专业人员开展认证工作的国家性或部门性教育和专业培训项目 包括计划/项目的网址、官方名称、负责机构（及详细联系方式）和简要描述	

4C. 请列出通过网络安全国际认可认证项目认证的公共部门专业人员的数量 包括认证类型和认证机构	
4D. 请列出通过国际认可网络安全认证项目认证的政府和公共部门机构的数量 包括认证类型和认证机构	
5A. 请列出任何经官方认可的用于与其他国家开展跨边境网络安全资产共享的国家性或部门性伙伴关系 包括伙伴关系的网址、官方名称、负责国家机构（及详细联系方式）、参与国家以及简要描述	
5B. 请列出任何经官方认可的用于在公共部门内部分享网络安全资产的国家性或部门性项目 包括项目的网址、官方名称、负责机构（及详细联系方式）、参与组织以及简要描述	
5C. 请列出任何经官方认可的用于在公共部门和私营部门之间开展网络安全资产共享的国家性或部门性项目 包括项目的网址、官方名称、负责国家机构（及详细联系方式）、参与组织以及简要描述	
5D. 请列出任何经官方认可的对区域性和/或国际性网络安全平台及论坛的参与活动 包括平台/论坛的网址、官方名称、负责国家机构（及详细联系方式）、参与国家以及简要描述	
感谢！	

Annex 3: Cyberwellness country profiles A-Z

The profiles in this annex were updated in December 2014. For more up to date information, kindly consult our online profiles on ITU website at http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx

TABLE OF CONTENT

CYBERWELLNESS PROFILE

AFGHANISTAN

BACKGROUND

Total Population: : 33 397 000

data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 5.90%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Afghanistan does not have any officially recognized criminal legislation pertaining to cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Afghanistan does not have any officially recognized regulation pertaining to data protection, breach notification and certification requirement.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU completed a CIRT readiness assessment for Afghanistan at Maldives in August 2010 (3-5th August 2010). Afghanistan has an officially recognized national CIRT (AFCERT). AFCERT is under the Information and Cyber Security Directorate (ICSD). The role of AFCERT is to actively work with law enforcement to combat cybercrimes in the country.

1.2.2 STANDARDS

Afghanistan does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Afghanistan Root Certificate Authority (ARCA) has an officially approved national (and sector specific) cybersecurity framework for the certification and accreditation of Public Key Infrastructure (PKI) and Certificate Authority (CA).

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Afghanistan has a draft of the national cybersecurity strategy which will be presented to National ICT Council for endorsement in August 2014.

1.3.2 ROADMAP FOR GOVERNANCE

Information and Cyber Security Directorate (ICSD) is responsible for providing a national governance roadmap for cybersecurity in Afghanistan.

1.3.3 RESPONSIBLE AGENCY

ICSD, in coordination with the National ICT Council, is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Afghanistan does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Afghanistan does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Afghanistan has officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors. The Ministry of Communication and Information Technology (MCIT) has organized a series of trainings for the government employees and academia, so far more than 900 people are trained. Currently the second phase of the training for 750 people is underway for 4 months. This program runs until 2016.

1.4.3 PROFESSIONAL CERTIFICATION

Afghanistan does not have the exact numbers of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Afghanistan does not have any government or public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Afghanistan does not have any officially recognized national framework for sharing cybersecurity asset across with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Afghanistan does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Afghanistan does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Afghanistan is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

ICSD, e-Gov, Technology and innovation directorates along with Afghan Telecommunications Regulatory Authority (ATRA) have been taking part in international cybersecurity workshops, conferences and forums.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Afghanistan does not have any officially recognized national legislation pertaining to child online protection.

2.2 UN CONVENTION AND PROTOCOL

Afghanistan has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Afghanistan has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Afghanistan does not have any officially recognized agency that offers intuitional support on child online protection.

2.4 REPORTING MECHANISM

Afghanistan does not have any officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
ALBANIA

BACKGROUND

Total Population: 3 227 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 60.10%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation pertaining to cybercrime is mandated through the following legal instruments:

- Albanian penal code
- Electronic communications law.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation to cybersecurity has been enacted through the following instruments:

-Law on Protection of personal Data

-Law on copyright and other related rights.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU completed a CIRT readiness assessment for Albania at Belgrade in 2010. Albania has an officially recognized national CIRT (ALCIRT).

1.2.2 STANDARDS

Albania does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Albania does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Albania does not yet have any officially recognized national cybersecurity strategy. However ALCIRT together with an interagency working group is working on drafting a policy paper for cybersecurity.

1.3.2 ROADMAP FOR GOVERNANCE

Albania does not yet have any national governance roadmap for cybersecurity. However it will be included in the policy paper for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The officially recognized CIRT (ALCIRT) is the legal mandated Agency created by Decision of Council of Ministers to implement a national cybersecurity policy-paper strategy.

1.3.4 NATIONAL BENCHMARKING

Albania does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Albania does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

The officially recognized CIRT (ALCIRT) is the legal mandated Agency created by Decision of Council of Ministers to organize awareness campaigns, trainings, publish informative materials either for the private or public sector.

1.4.3 PROFESSIONAL CERTIFICATION

Albania does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Albania does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Albania does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Albania does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Albania does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Albania is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Albania participated in the ITU Regional Forum on Cybersecurity for Europe and CIS in October 2012 at Sofia, Bulgaria. Albania participated in the International Cyber Shield Exercise 2014 in Turkey (ICSE 2014).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION AND STRATEGY

Specific legislation on child protection has been enacted through the following instruments:

-Article 117 of the Criminal Code

-Law N. 23/201231.

Objectives 4.2 and 5.2 of the National Child Strategy of Albania refer to the protection from inappropriate and harmful content and establishment of helplines.

2.2 UN CONVENTION AND PROTOCOL

Albania has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Albania has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Albania does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Albanian National Child Helpline (ALO 116 ANCH) is a free service available to children and youth 24/7, website under construction as of 05.05.14.

CYBERWELLNESS PROFILE
ALGERIA

BACKGROUND

Total Population: 36 486 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 16.50%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Penal Code

-Law for Post and Telecommunications

-Law to prevent and combat ICT crime.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Law on Electronic Signature

-Executive Decree 07-162.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Algeria does not have an officially recognized national CIRT. United States Agency for International Development (USAID) is assisting the Algerian government in developing its own national CIRT capability.

1.2.2 STANDARDS

Algeria does not have an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Algeria does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals. However an inter-ministerial committee has been established and is working on it.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Algeria does not have an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Algeria does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Algeria does not have an officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap. However a National Prevention and Control Body will be set up.

1.3.4 NATIONAL BENCHMARKING

Algeria does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Algeria does not have any officially recognized national or sector-specific research and development programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Algeria does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

However there are several academic clubs in Algeria that are active in this field such as student clubs of the National Superior School of Computer Science (ENSI).

1.4.3 PROFESSIONAL CERTIFICATION

Algeria does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Algeria does not have any government or public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Algeria have official recognized partnerships with the following organizations:

-France cooperation for Information Society -Bilateral Agreement with United States.

1.5.2 INTRA-AGENCY COOPERATION

Algeria does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Algeria does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Algeria is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Algeria participated in the 2012 ITU-IMPACT Workshop on Cyber Drill in Jordan and in the ITU RCC Regional cybersecurity Forum Cyber Drill 2013 in Oman.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-The Criminal Code (Article 303, 324-344 and 347)

-Law to prevent and combat ICT crime (Article 12).

2.2 UN CONVENTION AND PROTOCOL

Algeria has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Algeria has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography

2.3 INSTITUTIONAL SUPPORT

Algeria does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Algeria does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
PRINCIPALITY OF ANDORRA

BACKGROUND

Total Population: 79 300

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 94.00%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Penal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Data Protection

- Electronic Signature.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Andorra does not have any officially recognized national CIRT.

1.2.2 STANDARDS

Andorra does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Andorra.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Andorra does not have any officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Andorra.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Andorra.

1.3.4 NATIONAL BENCHMARKING

Andorra does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Andorra does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Andorra.

1.4.3 PROFESSIONAL CERTIFICATION

Andorra does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Andorra does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Andorra does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Andorra does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Andorra.

1.5.4 INTERNATIONAL COOPERATION

Andorra is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Articles 155-157 of the Criminal Code. [Article 155 modified by the Law 15/2008].

2.2 UN CONVENTION AND PROTOCOL

Andorra has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Andorra has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Andorra.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Andorra.

CYBERWELLNESS PROFILE
REPUBLIC OF ANGOLA

BACKGROUND

Total Population: 20 163 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 19.10%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Penal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Law on Electronic Signature

- Law on Data Protection.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Angola does not have an officially recognized national CIRT. A CIRT readiness assessment was conducted for Angola in 2014 by ITU.

1.2.2 STANDARDS

Angola does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Angola.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Angola does not have any officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Angola.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Angola.

1.3.4 NATIONAL BENCHMARKING

Angola does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Angola does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Angola.

1.4.3 PROFESSIONAL CERTIFICATION

Angola does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Angola does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Angola does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states

1.5.2 INTRA-AGENCY COOPERATION

Angola does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Angola.

1.5.4 INTERNATIONAL COOPERATION

Angola is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Article 184* of the Criminal Code

- Articles 12, 13, 16 and 17* of the Law to Combat Crime in the Field of ICT and Information Society.

2.2 UN CONVENTION AND PROTOCOL

Angola has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Angola has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Angola.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Angola.

CYBERWELLNESS PROFILE
ANTIGUA AND BARBUDA

BACKGROUND

Total Population: 90, 800

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 63.40%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- The Computer Misuse Act

- The Telecommunications Act

- The Electronic Transactions Bill

- The Electronic Transfer of Funds Crimes Act.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Electronic Transactions Bill

- Electronic Evidence Act

- Electronic Crimes Act

- Data Protection Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Antigua and Barbuda does not have any officially recognized national CIRT.

1.2.2 STANDARDS

Antigua and Barbuda does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Antigua and Barbuda.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Antigua and Barbuda has the Information and Communication technologies (ICTs) draft policy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Antigua and Barbuda.

1.3.3 RESPONSIBLE AGENCY

The Telecommunications Division, Ministry of Information, Broadcasting and Telecommunications and the Royal Police Force of Antigua and Barbuda are the agencies responsible for cybersecurity.

1.3.4 NATIONAL BENCHMARKING

Antigua and Barbuda does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Antigua and Barbuda does not have any officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

Antigua and Barbuda held the First National Workshop on Cyber Security and Incident Response. The workshop's objectives, and the objectives of the government of Antigua and Barbuda, were to conduct a national security self-assessment in order to identify vulnerabilities particular to the cyber domain, and to create a governmental Cyber Security Incident Response Team. Antigua and Barbuda is already home to a Regional Cyber Forensics Lab that assists in regional cyber law enforcement, and has started training police officers in cybercrime investigation.

1.4.3 PROFESSIONAL CERTIFICATION

Antigua and Barbuda does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Antigua and Barbuda does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Antigua and Barbuda does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Antigua and Barbuda.

1.5.4 INTERNATIONAL COOPERATION

Antigua and Barbuda is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:
- Section 15 of the Computer Misuse Act.

2.2 UN CONVENTION AND PROTOCOL

Antigua and Barbuda has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Antigua and Barbuda has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Antigua and Barbuda.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to reporting incidents in Antigua and Barbuda.

CYBERWELLNESS PROFILE
ARGENTINE REPUBLIC

BACKGROUND

Total Population: 41 119 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 59.90%

(data source: ITU Statistics, December 2013)

1. **CYBERSECURITY**

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Criminal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Law on Digital Signatures
- Law on Internet Providers
- Law on Personal Data Protection.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Argentina has an officially recognized national CIRT known as the Computer Emergency Response Team of the Argentine, ArCERT.

1.2.2 STANDARDS

There is no information on any officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards in Argentina.

1.2.3 CERTIFICATION

There is no information on any cybersecurity framework for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

The Oficina Nacional de Tecnologías de Información ONTI is currently working on the second draft of the National Cyber Security and Critical Infrastructure Protection Plan 2013–2015. This Plan is based on four pillars: awareness raising, securing digital assets, promoting judicial and academic understanding of information security, and critical information infrastructure.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national or sector-specific governance roadmap for cybersecurity in Argentina.

1.3.3 RESPONSIBLE AGENCY

The following agencies are responsible for implementing a national cybersecurity strategy, policy and roadmap by respective agencies:

- ONTI - ArCERT

- Argentine Federal Police

- Argentine National Gendarmerie ANG

- Programa Nacional de Infrastructuras Criticas ICIC.

1.3.4 NATIONAL BENCHMARKING

There is no national benching exercises or referential to measure cybersecurity development in Argentina.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

ICIC *GAP conducts research and preventative actions to reduce security incidents. This is the officially* recognized national research and development (R&D) program/project for cybersecurity standards, best practices and guidelines to be applied in the public sector.

1.4.2 MANPOWER DEVELOPMENT

The ICIC has also developed an initiative referred to as Internet Sano ("healthy" or "sound" Internet), which aims to promote responsible use of ICTs and the internet. A second awareness raising program called "With you on the web" has been developed by the National Directorate for the Protection of Personal Information, under the Ministry of Justice and Human Rights. Several institutions of higher learning in Argentina currently offer certification and degree programs in a wide range of aspects of cybersecurity, including digital forensics. The National Institute for Public Administration (INAP) also reportedly offers training and coursework on cybersecurity-related topics. The Argentine Federal Police Cyber Crimes Unit organizes seminars to train staff and the general public and works with NGOs, prosecutors and judges.

1.4.3 PROFESSIONAL CERTIFICATION

Argentina does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Argentina does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no information about any framework for sharing cybersecurity assets across borders with other nation states in Argentina.

1.5.2 INTRA-AGENCY COOPERATION

Argentina does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Argentina does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Argentina is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Argentina hosted the OAS Crisis Management Exercise on Cybersecurity.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Article 128* of the Criminal Code

- Law for the Protection of Children and Adolescents* there is not specifically pertaining to the internet.

2.2 UN CONVENTION AND PROTOCOL

Argentina has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Argentina has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

ICIC provides information on general cybersecurity and a link to the governmental initiative aiming to promote safety on internet. The Internet Sano initiative provides information* on child online protection for children, parents and educators.

2.4 REPORTING MECHANISM

InternetSano initiative provides a practical guide to report computer-facilitated offenses. The federal police receives complaints about computer incidents through the email address delitostecnologicos@policiafederal.gov.ar.

CYBERWELLNESS PROFILE
ARMENIA

BACKGROUND

Total Population: 3 109 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 46.30%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Penal Code -Law on Electronic Communication.

1.1.2 REGULATION AND COMPLIANCE

Armenia does not have specific regulation and compliance requirement pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU completed a CIRT readiness assessment in October 2011. Armenia has an officially recognized national CIRT (CERT AM).

1.2.2 STANDARDS

Armenia does not have an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Armenia does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Armenia does not have an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Armenia does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Armenia does not have an officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Armenia does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Armenia does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Armenia does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Armenia does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity

1.4.4 AGENCY CERTIFICATION

Armenia does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Armenia does not have official recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Armenia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Armenia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Armenia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-The Criminal Code (Article 263).

2.2 UN CONVENTION AND PROTOCOL

Armenia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Armenia has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Armenia does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Armenia Computer Incident Response Team (CERT AM) is the officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

AUSTRALIA

BACKGROUND

Total Population: 22 919 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 83.00%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Cybercrime Legislation Amendment Act 2012.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- National Plan to Combat Cybercrime
- Australian Communications and Media Authority (ACMA) enforces the Spam Act.
- Australian Cybercrime Online Reporting Network
- Data breach notification

1.2 TECHNICAL MEASURES

1.2.1 CIRT

CERT Australia is the officially recognized national computer emergency response team (CERT). In addition the Cyber Security Operations Centre (CSOC) is also responsible for coordinating and assisting operational responses to cyber events of national importance across government and systems of national importance.

1.2.2 STANDARDS

The ASD is responsible for producing ICT security policy and standards for the government and publishes these in the Australian Government Information Security Manual.

1.2.3 CERTIFICATION

The Emanation Security Program is responsible for the framework for certification and accreditation of national agencies and public sector professionals, and sets out the requirements for government and industry agencies to be formally recognised by the national authority. ASD conducts emanation security practices to national standards.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Australia has officially recognized the National Plan to Combat Cybercrime and the Cyber Security Strategy as the national strategy.

1.3.2 ROADMAP FOR GOVERNANCE

The national governance roadmap for cybersecurity is elaborated in the National Security Information Environment Roadmap: 2020 Vision.

1.3.3 RESPONSIBLE AGENCY

The following are the officially recognized agencies responsible for cybersecurity in Australia:

- The Cyber Policy and Intelligence Division - The Attorney-General's Department

- The Department of Prime Minister and Cabinet - The Australian Signals Directorate.

1.3.4 NATIONAL BENCHMARKING

In Australia the Federal Government entities subject to the Public Governance, Performance and Accountability Act 2013 participate in annual benchmarking of their ICT activities.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Currently Australia does not have any national or sector-specific recognized body or framework responsible for Research and development (R&D) of cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

The following programs have been put in place fostering educational and professional programs for raising awareness, higher education:- Cybersmart - Stay Smart Online - Budd:e Cybersecurity builder.

1.4.3 PROFESSIONAL CERTIFICATION

Australia does not have a recognized national or sector-specific body for certifying professionals in cybersecurity. Currently there is no record showing the number of public sector professionals who are certified in the area of cybersecurity.

1.4.4 AGENCY CERTIFICATION

In Australia there is no recognized national or sector-specific body for certifying agencies in the area of cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Australia has officially recognized the following partnerships:

- Statement of Intent regarding the Cooperation on Cybersecurity and Cyber Incident Response between the United States Department of Homeland Security (DHS) and the Attorney-General's Department (AGD) of the Commonwealth of Australia.

- CERT Australia has direct working relationships and a range of bilateral and multilateral agreements with government and business computer emergency response teams around the world.

1.5.2 INTRA-AGENCY COOPERATION

Through the Govdex and Govshare platforms, agencies are encouraged and supported to share knowledge, skills, and resources in the pursuit of more effective, efficient and innovative solutions. These are the nationally recognized platforms for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

The Trusted Information Sharing Network (TISN) is the framework for sharing cybersecurity assets between the public and private sectors in Australia.

1.5.4 INTERNATIONAL COOPERATION

Australia participates in the following:

- UN GGE - ASEAN

CERT Australia is a member of APCERT and FIRST.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

-Divisions 273 and 474 (subdivisions D-F) of the Criminal code.

2.2 UN CONVENTION AND PROTOCOL

Australia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Australia has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Australian Communications and Media Authority ACMA and Stay smart online are the institutions responsible for child online protection.

2.4 REPORTING MECHANISM

Inappropriate and offensive content can be reported directly to the CERT Australia on the number: 1300 172 499 (24 hours) and by the e-mail info@cert.gov.au. Also online content complaints can be directed to ACMA.

CYBERWELLNESS PROFILE
AUSTRIA

BACKGROUND

Total Population: 8 429 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 80.62%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Penal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- E-Commerce Act
- The Austrian E-Government Act
- Federal Electronic Signature Law
- Federal Act on the Protection of Personal Data
- Austrian Signature Ordinance.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Austria has an officially recognized government CIRT (GovCERT.AT) and a military CERT (milCERT) operated by the Defence Agency (Abwehramt) and the Command Support Centre (Führungsunterstützungszentrum) of the Federal Ministry of Defense and Sports (BMVLS).

1.2.2 STANDARDS

There is no available information regarding any officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no available information regarding any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Austria has officially recognized a National ICT Security Strategy in 2012 and an Austrian cybersecurity strategy in 2013.

1.3.2 ROADMAP FOR GOVERNANCE

The implementation of the measures adopted by the federal government in March 2013 in order to increase national cyber security are monitored by the Cyber Security Steering Group (consisting of members liaising with the National Security Council as well as the cyber security experts of all ministries) which provides the national governance roadmap for cybersecurity in Austria.

1.3.3 RESPONSIBLE AGENCY

The Cybersecurity Steering Group and the Cyber Crime Competence Center (C4) of the Federal Ministry of the Interior (BM.I) are the national coordination and reporting bodies for combating cybercrime and the officially recognized agencies responsible for implementing a national cybersecurity strategy, policy and roadmap in Austria.

1.3.4 NATIONAL BENCHMARKING

Every year the government publishes a cybersecurity report used to measure cybersecurity development in Austria.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

The Austrian IT Security Handbook contributes to the research and development (R&D) program/project for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector. Also the Austrian security research funding program (KIRAS) is a national program to promote safety research in Austria. KIRAS supports national research projects with the aim of increasing the security of Austria and its people.

1.4.2 MANPOWER DEVELOPMENT

The European Cybersecurity Month in Austria provides educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

There is no available information regarding the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

The number of certificates accredited by national accredited bodies against ISO/IEC 27001 was 28 in 2012.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Austria has officially recognized partnerships with the following organizations:

-Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX) - The exercise held in Poland in June 2013 provided an opportunity to perform technical and operational tests with deployment-oriented systems, services and applications. Cybersecurity Platform (CECSP) was founded in May 2013 on the initiative of Austria and the Czech Republic and aims to enable the information, best practices, lessons learned and know-how sharing about cyber threats and potential or (un)successfully carried out cyber-attacks.

1.5.2 INTRA-AGENCY COOPERATION

The ICT Security Portal is a measure defined in the Austrian Cybersecurity Strategy and is officially recognized as the national or sector-specific program for sharing cybersecurity assets within the public sector. It was launched as an inter-ministerial initiative in cooperation with the Austrian economy. The aim of the Web platform, which went online in 2013, is to raise awareness and it serves as a valuable source for information and communication for different target groups.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Austria has officially recognized the following national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

- The Private Public Partnership Program for Critical Infrastructure Protection (APCIP) with the objective to develop a comprehensive strategy and detailed measures and to bring all relevant public and private organizations and infrastructure operators under one common conceptual roof.

-The CERT Alliance which enhances cooperation of Austrian CERTs in the public as well as the private sector. Its aim is to bundle available resources and to use the joint know-how optimally in order to ensure maximum ICT security.

- The Austrian Trust Circle (ATC) founded in 2010 is an initiative of GovCERT.AT and the Federal Chancellery in order to build confidence between the responsible persons and organizations in individual sectors of strategic infrastructures so as to facilitate the exchange of security-related experience and ensure that swift and joint action will be taken in concrete cases.

1.5.4 INTERNATIONAL COOPERATION

Austria is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. To facilitate sharing of cybersecurity assets across borders or with other nation states, Austria has officially recognized partnerships with the following organizations:

- UN - NATO - EU - OSCE - ENISA - FIRST

- Trusted Introducer - The European Forum for Member States (EFMS)

- Participation in NATO exercise Cyber Coalition 2013.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION AND STRATEGY

Specific legislation on child online protection has been enacted through the following instruments:

- §64(1)4a and §207a* of the Criminal Code.

- Law on Obscene Publications and on the fight to protect the youth against moral hazard*.

The National ICT Strategy Austria considers campaigning on a social media guide for parent in its objective of awareness-raising.

2.2 UN CONVENTION AND PROTOCOL

Austria has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Austria has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Computer Emergency Response Team of Austria (CERT.at (*)) does not provide specific information on child online protection.

2.4 REPORTING MECHANISM

Illegal online content can be reported at www.stopline.at(*).

CYBERWELLNESS PROFILE

AZERBAIJAN

BACKGROUND

Total Population: 9 421 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 58.70%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

-Criminal Code .

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

-Law on Protection of Information.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Azerbaijan officially recognized national CIRTs are AZ-CERT and ScienceCERT. AZ-CERT is under the Ministry of Communications while ScienceCERT is under the National Academy of Science and is an information security incident responding group in Internet network which aim is to maintain the information security risk at an accepted level.

1.2.2 STANDARDS

Azerbaijan has an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards through the Standardization, Metrology and Patents Committee of the Republic of Azerbaijan.

1.2.3 CERTIFICATION

Azerbaijan does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals. However it provides the ISO/IEC 27001:2013 Training course through the Standardization, Metrology and Patents Committee of the Republic of Azerbaijan

1.2 ORGANIZATION MEASURES

1.3.1 POLICY

Azerbaijan has an officially recognized national cybersecurity strategy (National Strategy of the Republic of Azerbaijan on the Development of the İnformation Society for the years 2014-2020)

1.3.2 ROADMAP FOR GOVERNANCE

Azerbaijan does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The AZ-CERT and ScienceCERT are the officially recognized agencies responsible for implementing a national cybersecurity strategy, policy and roadmap in Azerbaijan.

1.3.4 NATIONAL BENCHMARKING

Azerbaijan does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.3 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Azerbaijan Ministry of Communications and High Technologies has officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector. The Technical Committee is to implement the preparation of national standards on the basis of international (regional) and interstate standards

1.4.2 MANPOWER DEVELOPMENT

Azerbaijan conducts short training courses on E-government and information security. In addition, the AZ-CERT organizes capture-the-flag competitions to enhance professional competence in information security.

1.4.3 PROFESSIONAL CERTIFICATION

Azerbaijan has numerous public sector professionals certified under internationally recognized certification programs in cybersecurity. However it did not have the exact statistic.

1.4.4 AGENCY CERTIFICATION

The IT and Communications Department of the State Oil Company of *Azerbaijan* Republic (SOCAR) is certified under ISO 27001:2005.

1.4 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Azerbaijan has officially recognized partnerships with Japan, Russia, Ukraine, Republic of Latvia and Republic of Slovakia.

1.5.2 INTRA-AGENCY COOPERATION

Azerbaijan AZ-CERT has an officially recognized national program (knowledge base) for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Azerbaijan AZ-CERT has an officially recognized national program for public-private sector partnership. The purpose is to share information on the latest cybersecurity landscape.

1.5.4 INTERNATIONAL COOPERATION

Azerbaijan is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Azerbaijan hosted an IT security conference in December 2012 with ITU.

Azerbaijan also participated in the following cybersecurity activities:

-International Cyber Shield Exercise 2014

-Security Conference Israel 2014

-HP Discover 2013

-Global Cybersecurity Cooperation: Challenges and Visions

-The Ninth Advanced International Conference on Telecommunications AICT 2013

-Applied Learning for Emergency Response Team (ALERT) 2012 on Regional Forum on cybersecurity

AZ-CERT is a member of FIRST.

2. CHILD ONLINE PROTECTION

2.2 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Article 242* of the Criminal Code.

-Article 10 (*) of the Law on Mass Media.

2.3 UN CONVENTION AND PROTOCOL

Azerbaijan has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Azerbaijan has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography

2.4 INSTITUTIONAL SUPPORT

Azerbaijan does not have an officially recognized agency that offers institutional support on child online protection.

2.5 REPORTING MECHANISM

Azerbaijan does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection. However there is a 24/7 helpline service.

CYBERWELLNESS PROFILE COMMONWEALTH OF THE BAHAMAS

BACKGROUND

Total Population: 351 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 72.00%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.2 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Computer Misuse Act.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Data Protection Act

- Electronic Communications and Transactions Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

The Bahamas does not have officially recognized national CIRT.

1.2.2 STANDARDS

The Bahamas does not have officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in The Bahamas.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

The Bahamas does not have an officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in The Bahamas.

1.3.3 RESPONSIBLE AGENCY

There is no officially recognized agency responsible for cybersecurity in The Bahamas.

1.3.4 NATIONAL BENCHMARKING

The Bahamas does not have any officially recognized national benchmarking or referential for measuring cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines in The Bahamas.

1.4.2 MANPOWER DEVELOPMENT

The Inter-American Committee against Terrorism (CICTE) of OAS conducted a two-day cybersecurity workshop in The Bahamas, as part of the technical assistance to be provided to the Government of The Bahamas for the development of its National Cyber Security Strategy, through an initiative that will be coordinated by the OAS Cyber Security Program together with the Ministry of National Security of The Bahamas. There is the ICA Advanced Certificate in Cyber Security at the Bahamas Institute of Financial Services.

1.4.3 PROFESSIONAL CERTIFICATION

The Bahamas does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

The Bahamas does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

The Bahamas does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in The Bahamas.

1.5.4 INTERNATIONAL COOPERATION

The Bahamas participates in the inter-American Committee against Terrorism (CICTE) of the OAS.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:
-Sections 5A and 16A of the “The Sexual Offences and Domestic Violence Act, January 2006, amended by the Act n. 29, December 2008.

2.2 UN CONVENTION AND PROTOCOL

The Bahamas has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. The Bahamas has not acceded to Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for the child online protection in the Bahamas.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to receiving reports of incidents.

CYBERWELLNESS PROFILE
BAHRAIN

BACKGROUND

Total Population: 1 359 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 90.00%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Law No. 60 of 2014 concerning Information Technology Crimes

- Law No. 16 of 2014 concerning Protection of State Information and Documents.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:
- Regulation 9 of 2009 concerning Lawful Access.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Bahrain has an officially recognized national CERT (CERT.bh) mandated by Bahrain's the Supreme Council for Information and Communication Technology via Resolution No. 37-2/2013. However CERT.bh is currently under formation.

1.2.2 STANDARDS

Bahrain does not have an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Bahrain does not have an officially approved national (and sector specific) cybersecurity framework for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Bahrain is currently in the process of drafting the national cybersecurity policy.

1.3.2 ROADMAP FOR GOVERNANCE

The "National Trust Programme", which is currently under development, will provide a framework for the Government sector to improve cybersecurity governance and operations.

1.3.3 RESPONSIBLE AGENCY

The General Directorate of Information Security from the Central Informatics Organization is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Bahrain does not currently have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Bahrain does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Bahrain has officially recognized through SafeSurf Programme an educational and professional training program for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors. The SafeSurf Bahrain offers tutorials to help parents and carers to enjoy all the best aspects of the online world and to facilitate learning of the dangers their children could face online – so they can use these new technologies safely and responsibly.

1.4.3 PROFESSIONAL CERTIFICATION

Bahrain's information security team at the Central Informatics Organization, which is responsible for overall government security, is certified under more than 50 internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Bahrain has numerous public sector agencies that are certified in accordance with ISO 27001 certification. Furthermore, the national PKI implementation is currently undergoing ETSI certification for qualified digital signatures, encryption, and authentication.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Bahrain does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5.2 INTRA-AGENCY COOPERATION

Bahrain CERT (CERT.bh) which is currently under formation will be the official certified government and public sector agency certified under internationally recognized standards in cybersecurity.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Bahrain does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5.4 INTERNATIONAL COOPERATION

Bahrain is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Bahrain is also is a member of the Gulf Cooperation Council CERT committee (GCC-CERT).

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Bahrain has not enacted any specific legislation on child online protection.

2.2 UN CONVENTION AND PROTOCOL

Bahrain has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Bahrain has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The National Centre for Child Protection (*), under the Ministry of Social Development, is the governmental organ responsible assessing and following up children's rights together with other governmental organs. It has no specific policy on online protection.

The Telecommunications Regulatory Authority(*) provides information for child online protection on its space for Safe Surf. It has launched a Report on the state of internet safety in the Kingdom. It also organizes lectures in schools to help parents and teachers understand the online safety issues which affect children.

2.4 REPORTING MECHANISM

Bahrain Telecommunications Regulatory Authority provides a space for complaints and enquiries on its website.

CYBERWELLNESS PROFILE
BANGLADESH

BACKGROUND

Total Population: 152 490 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 6.50%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Information and Communication Technology Act

-Bangladesh Telecommunication Regulation Act.

-Penal Code

1.1.2 REGULATION AND COMPLIANCE

Bangladesh does not have specific regulation and compliance requirement pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU completed a CIRT assessment for Bangladesh at Dhaka, Bangladesh from November to May 2010, and at Maldives in August 2010.

Bangladesh has an officially recognized CIRT (BDCERT).

1.2.2 STANDARDS

Bangladesh does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Bangladesh does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Bangladesh does not have an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Bangladesh does not have a national governance roadmap for cybersecurity in Bangladesh. However there are efforts from the Honorable Prime Minister's office, Bangladesh Computer Council and the Telecommunication Regulatory Commission (BTRC) to finalize a roadmap to ensure cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Bangladesh does have an officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Bangladesh does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Bangladesh does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

BDCERT organises educational and professional training every year to raise awareness and capabilities for combating cyber incidents. In addition there are also organised programs to raise awareness in general public, e.g. SMS circulation throughout the country.

1.4.3 PROFESSIONAL CERTIFICATION

Bangladesh has numerous public sector professionals certified under internationally recognized certification programs in cybersecurity. However it did not conduct a survey to gather the exact statistic.

1.4.4 AGENCY CERTIFICATION

Bangladesh does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Bangladesh has official recognized partnerships with the following organizations:

-ITU -APCERT -OIC-CERT.

1.5.2 INTRA-AGENCY COOPERATION

Bangladesh does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector

1.5.3 PUBLIC SECTOR PARTNERSHIP

Bangladesh does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector. However BDCERT organizes events to share knowledge with the law enforcing agencies, industry and academia.

1.5.4 INTERNATIONAL COOPERATION

Bangladesh is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.
In addition, BDCERT has joined Asia Pacific CIRT (APCERT) Cyber Security Drills for the last 5 years. It also attends regional events organized by other CERTs like Japan CIRT (JPCERT) and Korean CIRT (KRCERT).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-The Criminal Code (Article 292 and 294)

-Information Technology and Communication Act (Article 57).

2.3 UN CONVENTION AND PROTOCOL

Bangladesh has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Bangladesh has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.4 INSTITUTIONAL SUPPORT

Bangladesh does not have an officially recognized agency that offers institutional support on child online protection.

2.5 REPORTING MECHANISM

Bangladesh does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection. However Arapajeyo Bangladesh provides a helpline at the number: 1098 and can be contacted by email: info@arapajeyo.org.

CYBERWELLNESS PROFILE

BARBADOS

BACKGROUND

Total Population: 275 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 75%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Telecommunications Act -Computer Misuse Act -Privacy and Data Protection Act(Draft Stage).

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Privacy and Data Protection Act (Draft Stage).

1.2 TECHNICAL MEASURES

1.2.1 CIRT

A CIRT readiness assessment was conducted for Barbados in August 2012 during the Regional Workshop on establishing National Computer Incident Response Team (CIRT), Caribbean Region at St. Georges, Grenada. Barbados is currently in the process of implementing a National CERT with the assistance of ITU.

1.2.2 STANDARDS

Barbados does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

However Barbados, in collaboration with the Caribbean Governments, the Caribbean Telecommunication Union (CTU) and Commonwealth Telecommunications Organization (CTO) are currently organising discussions on "Consultation on a Commonwealth Cyber Governance Model" to be implemented by the Commonwealth countries. This includes a framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Barbados does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

However the "Consultation on a Commonwealth Cyber Governance Model" mentioned earlier will include a framework for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Barbados does not have any officially recognized national cybersecurity strategy. However the "Consultation on a Commonwealth Cyber Governance Model" mentioned earlier will include a national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Barbados does not have any official recognized national or sector specific governance for cybersecurity. However a National Cyber Security Strategic Plan is in the pipeline.

1.3.3 RESPONSIBLE AGENCY

The Telecommunications Unit is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

The Telecommunications Unit is collecting data on cyber-attacks across government departments. This data will enable critical analysis of the types of attacks, frequency and mitigation techniques currently being implemented.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Barbados does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector. However a National Cyber Security Strategic Plan is in the pipeline.

1.4.2 MANPOWER DEVELOPMENT

The Telecommunications Unit has endeavored in a campaign since 2010 to raise awareness in the area of protecting kids in Cyberspace. Since then the unit has partnered with the Caribbean Cyber Security Centre to assist in promoting the "Think Click Surf" campaign.

1.4.3 PROFESSIONAL CERTIFICATION

Caribbean Cybersecurity Center has numerous public sector professionals who are certified under internationally recognized certification programs in cyber security. However it has not conducted a survey to gather the exact statistic.

1.4.4 AGENCY CERTIFICATION

Barbados does not have any government and public sector agencies certified under internationally recognized standards in cybersecurity. However the National Cyber Security Strategic Plan, which is in the pipeline, will provide a national program to enable certification of professionals in the government and public sector.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Barbados does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states. However this is expected to change after the development of the national CIRT.

1.5.2 INTRA-AGENCY COOPERATION

Barbados does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector. However this is expected to change after the development of the national CIRT.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Barbados does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector. However this is expected to change after the development of the national CIRT.

1.5.4 INTERNATIONAL COOPERATION

Barbados is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. In addition, the Government of Barbados participates in CTU, ITU, and Organization of American States (OAS) platforms and forums.

Barbados is among the beneficiary countries of the EU/ITU co-funded project "Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures" (HIPCAR). Barbados participated in the ITU-IMPACT Applied Learning for Emergency Response Teams (ALERT- 2013) in Montevideo, Uruguay.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:
-Computer Misuse Act.

2.2 UN CONVENTION AND PROTOCOL

Barbados has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

2.3 INSTITUTIONAL SUPPORT

Barbados does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Barbados does not have any officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE REPUBLIC OF BELARUS

BACKGROUND

Total Population: 9 527 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 54.17%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Penal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Law on information, Informatization and Protection of Information.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Belarus has an officially recognized national CIRT known as CERT.BY which is under the Operational and Analytical Center under the Aegis of the President of the Republic of Belarus (OAC).

1.2.2 STANDARDS

Belarus does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Belarus.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

There is no national or sector-specific cybersecurity strategy in Belarus.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Belarus.

1.3.3 RESPONSIBLE AGENCY

There is no information on any agency responsible for cybersecurity in Belarus.

1.3.4 NATIONAL BENCHMARKING

Belarus does not have an officially recognized national benchmarking or referential for measuring cybersecurity development in Belarus.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines in the Belarus.

1.4.2 MANPOWER DEVELOPMENT

There is no program or project for cybersecurity standards in educational and professional training programs for raising awareness, higher education and certification in Belarus.

1.4.3 PROFESSIONAL CERTIFICATION

Belarus does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Belarus does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Belarus does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Belarus.

1.5.4 INTERNATIONAL COOPERATION

Belarus is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Belarus also participates in the following cybersecurity activities:

-FIRST -OSCE -NATO.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Articles 343 and 343.1* of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Belarus has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Belarus has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Belarus.

2.4 REPORTING MECHANISM

There is a helpline and website where incidents can be reported.

CYBERWELLNESS PROFILE
BELGIUM

BACKGROUND

Total Population: 10 788 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 82.17%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Penal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Electronic Communications Act
- Law on Electronic Signatures and certification services
- Law on Certain legal aspects of the Information Society
- Law on the protection of private life with regard to the processing of personal data.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Belgium has an officially recognized national CIRT known as CERT.be formerly Belnet CERT (both CERTs have since merged) and it is operated by Belnet, the Belgian national research network, on behalf of Fedict.

1.2.2 STANDARDS

Belgium has officially approved national and sector specific cybersecurity frameworks for implementing internationally recognized cybersecurity standards through the Federal Public Service for Information and Communication Technology Fedict.

1.2.3 CERTIFICATION

There is no information about any framework for certification and accreditation of national agencies and public sector professionals in Belgium.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Belgium has an officially recognized national cybersecurity strategy known as Belgian Cyber Security Strategy Guide.

1.3.2 ROADMAP FOR GOVERNANCE

There is no information on any national or sector-specific governance roadmap for cybersecurity strategy in Belgium.

1.3.3 RESPONSIBLE AGENCY

The CERT.be, Fedict and the Centre Cyber Security Belgique (CCSB) monitor and coordinate the implementation of the national cybersecurity strategy and policy.

1.3.4 NATIONAL BENCHMARKING

Belgium does not have any national benchmarking exercises or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

The Belgian Cybersecurity Guide makes provision for the national research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

The European Cyber Security Month for Belgium has had over 5 events which are programs for raising awareness for higher education, professional training and certification.

1.4.3 PROFESSIONAL CERTIFICATION

Belgium does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Belgium does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, B-CCENTRE coordinates and collaborates beyond the Belgian borders and partners in the Netherlands (UVT, WODC) and European collaboration and coordination via the 2CENTRE network with a.o. national centres in Ireland and France.

1.5.2 INTRA-AGENCY COOPERATION

Belgium has an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector through the B-CCENTRE.

1.5.3 PUBLIC SECTOR PARTNERSHIP

The B-CCENTRE is the main platform for collaboration; it provides officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sectors.

1.5.4 INTERNATIONAL COOPERATION

To facilitate sharing of cybersecurity assets and for participation in regional and international cybersecurity platforms Belgium, through Belnet CERT, is a member of FIRST.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Articles 383, 383bis, 385, 386 and 387* of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Belgium has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Belgium has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no information on any institution that supports child online protection in Belgium.

2.4 REPORTING MECHANISM

Online child abuse images can be reported www.stopchildporno.be.

CYBERWELLNESS PROFILE

BELIZE

BACKGROUND

Total Population: 324 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 31.70%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-None.

1.1.2EGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Electronic Transactions Act
- Electronic Evidence Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Belize does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Belize does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

The Ministry of National Security – specifically the focal point for CICTE-OAS is presently working on establishing an ICT Steering Committee within the Ministry, with the dual aims of developing a national cybersecurity strategy and reviewing and strengthening the legislative framework regarding cybercrime.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Belize.

1.3.3 RESPONSIBLE AGENCY

The Ministry of National Security and the Belize Police Department (BPD) are the agencies responsible for cybersecurity in Belize.

1.3.4 NATIONAL BENCHMARKING

There is no benchmarking or referential to measure cybersecurity development in Belize.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines in Belize.

1.4.2 MANPOWER DEVELOPMENT

The BPD's IT Unit undertakes an annual countrywide "ICT Road Show" to promote increased awareness of internet and cybersecurity-related issues among the general public.

1.4.3 PROFESSIONAL CERTIFICATION

Belize does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Belize does not have any government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no framework for sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Belize does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Private sector institutions are not legally required to report cyber incidents to national authorities; the BPD has worked to establish cooperative relationships with many private sector entities, and has provided support and assistance when it has been requested.

1.5.4 INTERNATIONAL COOPERATION

Belize is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Belize participates in the CICTE-OAS.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:
-None.

2.2 UN CONVENTION AND PROTOCOL

Belize has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Belize has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency that is responsible for child online protection in Belize.

2.4 REPORTING MECHANISM

There is no website or hotline to report incidents in Belize.

CYBERWELLNESS PROFILE
REPUBLIC OF BENIN

BACKGROUND

Total Population: 9 352 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 4.90%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Decree No. 200/MISP/DC/SGM/DGPN/SERCT/DER/SA related to the creation of a division in charge of the fight against internet crime. This decree stipulates that victims of internet crime can approach Interpol or the BEF with their complaints.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

- Loi 9 of 27 Apr 2009 (protection of personal information in databases).

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Benin does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Benin does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Benin does not have a cybersecurity framework for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Benin does not have a national or sector-specific cybersecurity strategy. However the Telecoms Regulatory Authority has presented a plan to combat cybercrime to the president in November 2012.

1.3.2 ROADMAP FOR GOVERNANCE

There is no governance roadmap for cybersecurity in Benin.

1.3.3 RESPONSIBLE AGENCY

The Economic and Financial Crimes Commission (EFCC) is responsible for cybersecurity in Benin.

1.3.4 NATIONAL BENCHMARKING

Benin does not have any benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines in Benin.

1.4.2 MANPOWER DEVELOPMENT

The CNF of the AUF at Cotonou, in association with the Abomey-Calavi University, The Lawyer Order of Benin and the Union of Media Professionals of Benin organize a training seminar on the topic Cyber-criminality: New threats to privacy, companies, banks and administrations.

1.4.3 PROFESSIONAL CERTIFICATION

Benin does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Benin does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Benin does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Benin.

1.5.4 INTERNATIONAL COOPERATION

Benin is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:
- None.

2.2 UN CONVENTION AND PROTOCOL

Benin has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Benin has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Benin.

2.4 REPORTING MECHANISM

There is no website or hotline to report incidence in Benin.

CYBERWELLNESS PROFILE
BHUTAN

BACKGROUND

Total Population: 750 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 29.9%

(data source: ITU Statistics 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation pertaining to cybercrime is mandated through the following legal instrument:

-Information Communications & Media Act.

1.1.2 REGULATION AND COMPLIANCE

Bhutan does not have any officially recognised regulation pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU completed a CIRT readiness assessment for Bhutan at Maldives in August 2010. Bhutan does not have an officially recognized national CIRT. However there are plans to build one in the near future.

1.2.2 STANDARDS

Bhutan does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Bhutan does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Bhutan does not have any officially recognized national cybersecurity strategy. However Bhutan is going to develop the e-Gov Policy (2014) where cybersecurity will be one of the key components.

1.3.2 ROADMAP FOR GOVERNANCE

Bhutan does not have any national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The Ministry of Information and Communication is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Bhutan does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Bhutan does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Bhutan does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Bhutan does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Bhutan does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Bhutan does not any official recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Bhutan does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Bhutan does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Bhutan is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child protection has been enacted through the following instruments:

-The Criminal Code (Article 225 and 476)
-Information Communications & Media Act (Article 160 and 179).

2.2 UN CONVENTION AND PROTOCOL

Bhutan has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Bhutan has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Bhutan does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Bhutan does not have any officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE PLURINATIONAL STATE OF BOLIVIA

BACKGROUND

Total Population: 10 248 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 39.50%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- None.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

- Draft law on E-Documents, E-Signatures and E-Commerce.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

There is not yet an official national CIRT; however the Agency for the Development of an Information Society in Bolivia, ADSIB, is in the process of creating a national incident response capability utilizing its existing team of trained and competent personnel. A CIRT readiness assessment was conducted for Bolivia by the ITU in 2014.

1.2.2 STANDARDS

Bolivia does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Bolivia.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Bolivia does not have any officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Bolivia.

1.3.3 RESPONSIBLE AGENCY

The Scientific Technical Research Institute of the Police University (IITCUP) and ADSIB are the agencies responsible for cybersecurity in Bolivia.

1.3.4 NATIONAL BENCHMARKING

Bolivia does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Bolivia does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

World Telecommunication and Information Society Day is held annually on May 17. To coincide with Bolivia's celebrations, the Autonomous Municipal Act No. 067 of the Internet in the Municipality of La Paz came into effect, requiring Internet cafes in the La Paz region to filter Internet content to protect children. EducaBolivia is a portal operated by the Ministry of Education and contains information aimed at parents, teachers and students on a wide range of topics, including online safety. ADSIB has also organized a training seminar on protecting web sites from cyberattacks. IITCUP reports that many universities in Bolivia offer cybersecurity-related coursework, including in digital forensics, and that appropriate personnel from IITCUP often utilize these courses for training. However, most of the coursework offered is general in scope and theory-based, and incorporates little in the way of hands-on practical training. Authorities report that to date, very little has been done to raise cybersecurity awareness within government, the private sector, or society at large.

1.4.3 PROFESSIONAL CERTIFICATION

Bolivia does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Bolivia does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Sharing of cybersecurity assets across borders or with other nation states between ADSIB and its counterpart entities in other countries is limited. However one particular reported security incident resulted in direct coordination with the national CIRT of Argentina, ArCERT, in responding to and resolving a situation involving phishing and the targeting of an enterprise deemed critical to Bolivia’s national interests. The successful management of this incident was considered a major success for the government.

1.5.2 INTRA-AGENCY COOPERATION

Bolivia does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Bolivia.

1.5.4 INTERNATIONAL COOPERATION

Bolivia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Bolivia is a member of the OAS.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Article 318 and 319 of the Criminal Code.

- Article 281(quarter) of Law 3325 on Trafficking in human beings and related crimes.

2.2 UN CONVENTION AND PROTOCOL

Bolivia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Bolivia has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Bolivia.

2.4 REPORTING MECHANISM

There is no website or hotline where incidents can be reported in Bolivia.

CYBERWELLNESS PROFILE
BOSNIA AND HERZEGOVINA

BACKGROUND

Total Population: 3 744 000
(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 67.90%
(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Council of Europe's Convention on Cybercrime
- Penal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Legal Interception and Data Collection
- Children Protection.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Bosnia and Herzegovina has a strategy and establishment of a national CERT.

1.2.2 STANDARDS

There is no available information concerning any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no available information concerning any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Bosnia and Herzegovina has an officially recognized national cybersecurity strategy through the establishment of a national CERT and an action Plan on Protection of Children and Prevention of Violence against Children through ICT 2014-2015, in accordance with the Strategy on Combating Trafficking in Human Beings in Bosnia and Herzegovina (2013 – 2015).

1.3.2 ROADMAP FOR GOVERNANCE

There is no available information concerning a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

There is no available information concerning an officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

There is no available information concerning any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no available information concerning any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Bosnia and Herzegovina began the implementation of the EU funded project "EU Support to Law Enforcement" the objectives of which are to enhance information exchange by more efficient usage of existing and new communication and IT systems and procedures. However there is no available information concerning an officially recognized national or sector-specific educational and professional training program for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

There is no available information concerning any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

There is no available information concerning any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no available information concerning any official recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

There is no available information concerning any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no available information concerning any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Bosnia and Herzegovina is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Bosnia and Herzegovina participated in the International Cyber Shield Exercise 2014 in Turkey (ICSE 2014)

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- The Federal Criminal Code Articles 211 and 212.

2.2 UN CONVENTION AND PROTOCOL

Bosnia and Herzegovina has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Bosnia and Herzegovina has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Bosnia and Herzegovina does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

2.5 International Forum of Solidarity offers space in its website (*) for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

BOTSWANA

BACKGROUND

Total Population: 2 053 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 15%

(data source: ITU Statistics, 2013)

1 CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Cybercrime and Computer Related Crimes Act.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Law on Data Protection (Under Review)

-Electronic Commerce and Signatures Bill

-Electronic (Evidence) Records ACT 2014.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU conducted a CIRT readiness assessment for Botswana at Maseru, Lesotho in October 2012. Botswana does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Botswana does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Botswana does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Botswana does not have an officially recognized national cybersecurity strategy. However the Maitlamo National ICT policy provides provisions for cybersecurity.

1.3.2 ROADMAP FOR GOVERNANCE

Botswana does not have a national governance roadmap for cybersecurity. However the Maitlamo National ICT policy provides provisions for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The Telecommunication Authority is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Botswana does not have any officially recognized national benchmarking and referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Botswana does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Botswana does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Botswana does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Botswana does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Botswana does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Botswana does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Botswana does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Botswana is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Bostwana is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-The Criminal Code (Section 178)

-Cybercrime and Computer Related Crimes (Section 16).

2.2 UN CONVENTION AND PROTOCOL

Botswana has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Botswana has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Botswana does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Botswana does not have any officially recognized agency that offers an avenue for the reporting of incidents related to child online protection. However Childline Botswana, a non for profit organization, has a helpline available.

CYBERWELLNESS PROFILE
BRAZIL

BACKGROUND

Total Population: 198 361 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 51.60%

(data source: ITU Statistics, December 2012)

1 CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Law 8,137/1990, Art. 2
- Law 8,069/1990, Art. 241
- Law 9,100/1995, Art. 67
- Law 9,296/1996, Art. 10
- Law 9,504/1997
- Law 9,983/2000
- Law 11,829/2008
- Law 12,735/2012, Art.4
- Law 12,737/2012.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Administrative Rule no. 35/2009
- Administrative Rule no. 45/2009
- Administrative Rule no. 34/2009
- Decree 3,505/2000
- Decree 7,845/2012
- Resolution No. 614/2013, Art. 53
- Resolution No. 617/2013, Art. 47.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Bazil has officially recognized a national CERT, a government CSIRT and a sector specific SCIRT.

1.2.2 STANDARDS

Brazil has officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards through three instruments:

-Normative Instruction GSI no 1/2008 which organizes the Management of Information and Communications Security in the Federal Public Administration, direct and indirect, among other provisions.

-Normative Instruction GSI no 2/2008 which provides for accreditation on security for the treatment of classified information at any level of confidentiality in the under the Federal Executive Branch.

-Normative Instruction GSI no 3/2008 that defines minimum parameters and standards for cryptographic algorithms for encryption of classified information under the Federal Executive Branch.

1.2.3 CERTIFICATION

The Complementary Standards offer a cybersecurity framework for the certification and accreditation of national agencies and public sector professionals.

Complementary Standard no. nº 17 establishes guidelines for the certification and accreditation for information and communication security professionals of the direct and indirect Federal Public Administration.

Complementary Standard no. nº 18 establishes guidelines for training of the information and communication security professionals of the direct and indirect Federal Public Administration.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Brazil has an officially recognized national cybersecurity policy through the following instruments:

- Decree 6703/2008 - National Defense Strategy
- Information Technology Strategy, 2013-2015

- Anatel - Public Consultation no. 21, on a regulation for critical telecommunication infrastructure protection. This regulation establishes measures to be undertaken by telecom operators to promote risk management processes related to security and performance of network and telecommunication services. It also promotes coordination among telecom operators for disaster relief.
- Administrative Normative Rule no. 3,389 of the Ministry of Defense, which establishes the Cyber Defence Policy
- Critical Information and Communication Infrastructure protection.

1.3.2 ROADMAP FOR GOVERNANCE

Brazil does not currently have any national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Brazil does not have an officially recognised national or sector-specific agency responsible for implementing a national cybersecurity strategy, policy and roadmap since responsibilities are shared among the following several entities:

- National Defense Council in charge of planning and conducting the policy and strategy for national defence
- Cabinet of Institutional Security of the Presidency of the Republic which proposes guidelines and strategies for the cybersecurity in the scope of the Federal Public Administration, by means of the Communication and Information Safety Department
- Cyber defense Centre of the Brazilian Army
- Brazilian Intelligency Agency
- Ministry of Justice – Department of Federal Police.

1.3.4 NATIONAL BENCHMARKING

Brazil has officially recognized the following national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

- TIC Kids Online 2012 - Survey on Internet Use by Children in Brazil
- ICT Households and Enterprises - Survey on the Use of Information and Communication Technologies in Brazil
- Survey on the Use of Information and Communication Technologies in Brazil
- The Bureau of Information Technology Audit (Sefti/TCU) conducts benchmark exercises periodically to measure cybersecurity development in government sector.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Brazil has officially recognized the following national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

-ABNT which defines the Brazilian versions of ISO IEC standards (e.g. ABNT NBR ISO/IEC 27000 series)

-CEPESC - Research and Development Center for the Security of Communication – that develops scientific and technological research applied to projects related to the security of communications including technology transfer.

-CAIS RNP – Security Incident Response Team – which acts in the detection, solution and prevention of security incidents in the Brazilian academic network, besides creating, promoting and spreading security practices in networks.

1.4.2 MANPOWER DEVELOPMENT

The Brazilian Internet Steering Committee (CGI.br) is responsible for recommending technical standards and best practices related to the Internet, and promoting security best practices. In order to perform its activities the CGI.br created the Brazilian Network Information Center (NIC.br) which implements these efforts through:

- Brazilian national (CERT.br) which offers professional training programs.
- Best practices Portal BCP.nic.br - a portal to promote Current Best Practices (BCPs) for system administrators.
- Antispam.br - a portal for awareness about spam, with contents to both end users and system administrators.

- InternetSegura.br - a portal with links to all currently known awareness materials developed by Brazilian organizations.
- SaferNet Brazil works with prevention, providing information to the users and organizing awareness campaigns, but it also functions as an internet complaint center for crimes against human rights.

- CEGSIC which offers specialization course in Management of Information Security and Communications.

1.4.3 PROFESSIONAL CERTIFICATION

Brazil has numerous public sector professionals certified under internationally recognized certification programs in cybersecurity. However it did not conduct a survey to gather the exact statistic.

1.4.4 AGENCY CERTIFICATION

Brazil has numerous certified government and public sector agencies under internationally recognized standards in cybersecurity. However it did not conduct a survey to gather the exact statistic.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets access borders and with other nation states, Brazil has officially recognized a partnership with the Inter-American Committee Against Terrorism (CICTE) by enhancing the exchange of information via the competent national authorities.

1.5.2 INTRA-AGENCY COOPERATION

The SegInfo blog is the officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector since it offers to its readers the main news related to information security, and frequent articles by renowned professionals in the information security area. The site aims to collect, catalog and spray events, news, vulnerability warnings and most relevant projects in the information security area, among countless other aspects.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Brazilian national CERT (CERT.br) participates in several initiatives for sharing cybersecurity assets within the public and private sector.

- SpamPots Project which gathers data related to the abuse of Internet infrastructure by spammers in order to identify malware botnets etc.
- Distributed Honeypots Project which objective is to increase the capacity of incident detection and trend analysis in the Brazilian Internet Space.

- Tentacles Project : a Cooperation Agreement between the Brazilian Federal Police Department and FEBRABAN (Brazil´s Bank Federation) in which the Brazilian Federal Police Department receives on line information on almost the entire electronic frauds committed inside Brazil borders, allowing the continuous feeding of the National Electronic Frauds Database and the quick generation of statistics, crime analysis and strategic planning, among other means known to be effective in combating this type of illicit act.

1.5.4 INTERNATIONAL COOPERATION

Brazil is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Brazil participated in the following cybersecurity activities.
- Latin American and Caribbean Regional CSIRTs Meeting organized by LACNIC.
- Brazilian Federal Police participates in the I-24/7 global police communications system developed by Interpol to connect law enforcement officers, including cybercrimes:

CERT.br is a member of FIRST.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Articles 218, 218A, 218B* of the Criminal Code, amended and included by the Law n. 12015/2009

-Articles 240* and 241A-E* of the Law n. 8069/1990, amended by the law n. 11829/2008.

2.2 UN CONVENTION AND PROTOCOL

Brazil has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Brazil has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Brazilian national CERT (CERT-BR*) provides for information* on internet security in its website. Also there is a Website* gathering Brazilian initiatives on internet security, built by the Brazilian Internet Steering Committee*.

2.4 REPORTING MECHANISM

Online illegal content can be reported in the helpline on child and adolescent pornography in internet created by the government: www.disque100.gov.br* Available as a telephone number in: 100.

SaferNet Brasil provides information on internet safety and space for complaints in its website.

The Federal Police* has a dedicated space to receive denouncements at its website, which can also be made by its email address denuncia.ddh@dpf.gov.br.

CYBERWELLNESS PROFILE
BRUNEI

BACKGROUND

Total Population: 413 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 64.50%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Computer Misuse Act -Penal Code -Copyright Act.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Broadcasting (Class License) Notification -Internet Code of Practice Notification -Electronic Transaction Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Brunei has an officially recognized national CIRT (BruCERT).

1.2.2 STANDARDS

Brunei does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards. However the E-Government National Centre (EGNC) is in progress in developing the Brunei National Cyber Security Framework.

1.2.3 CERTIFICATION

Brunei does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Brunei has an officially recognized national cybersecurity strategy through the E-Government Strategic Plan 2009-2014.

1.3.2 ROADMAP FOR GOVERNANCE

Brunei does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Brunei does not have an officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Brunei does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Brunei does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Brunei Ministry of Education incorporates cybersecurity awareness to their education curriculum. In Year 3, there is one syllabus about risk/dangers/responsible internet and email safety rules. BruCERT conduct awareness training programs for Civil Servants since 2005, Awareness Outreach Programs for Schools. It also disseminates information through printed and digital media, and roadshows so as to raise youth and citizens' awareness.

1.4.3 PROFESSIONAL CERTIFICATION

Brunei has 30 public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Brunei does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Brunei has officially recognized partnerships with the following organizations:

-ITU -APCERT -ASEAN

-FIRST -OIC-CERT

BruCERT is a member of FIRST.

1.5.2 INTRA-AGENCY COOPERATION

Brunei has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector through the E-Government National Center.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Brunei has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector through the Information Technology Protective Security Services.

1.5.4 INTERNATIONAL COOPERATION

Brunei is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services and has participated in the ASEAN-Japan Information Security Meetings since 2009.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Sections 292-294 of the Criminal Code

-Section 3 of the Undesirable Publications Act.

2.2 UN CONVENTION AND PROTOCOL

Brunei has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Brunei has acceded, with no declarations or reservations to articles 2 and 3, to the Optional

Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Brunei does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Brunei BruCERT is the officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
BULGARIA

BACKGROUND

Total Population: 7 398 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 53.06%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

-The Criminal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Electronic Communication Act -E-Governance Act -State National Security Agency Act

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Bulgaria has an officially recognized national CIRT (CERT Bulgaria).

1.2.2 STANDARDS

Bulgaria has officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards through the Electronic Communications Act and E-governance Act.

1.2.3 CERTIFICATION

Bulgaria has officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals through the E-governance Act.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Bulgaria is currently developing a national cybersecurity strategy with an inter-departmental working group. It is expected to be completed by the end of 2014.

1.3.2 ROADMAP FOR GOVERNANCE

Bulgaria does not have a national governance roadmap for cybersecurity currently. The roadmap will be included in the national cybersecurity strategy which is expected to be completed by end of 2014.

1.3.3 RESPONSIBLE AGENCY

The Ministry of Transport, information Technology and Communications, State Agency "National Security" and the Ministry of Defense are the officially recognized agencies responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Bulgaria has the following official benchmark exercise to measure cybersecurity development:

- 2011 – Computer-Aided Exercise “Cyber-Winter” within the Ministry of Transport, Information Technology and Communications;
- 2012 – Cyber-drill during the Regional Cybersecurity Forum, Sofia, Bulgaria

- 2013 – Operational Program Administrative Capacity Directorate (OPAC) project on development of plan, scenarios, assessment methodology, questionnaires for conducting national exercise for critical information infrastructure protection

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

The National Laboratory of Computer Virology is a research unit within the Bulgarian Academy of Sciences and has officially recognized national research and development (R&D) programs/projects on cybersecurity.

1.4.2 MANPOWER DEVELOPMENT

The State National Security Agency is involved in an OPAC national project to conduct professional cybersecurity training.

1.4.3 PROFESSIONAL CERTIFICATION

Bulgaria does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Bulgaria does not have the exact number of government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Bulgaria does not have officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Bulgaria does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector

1.5.3 PUBLIC SECTOR PARTNERSHIP

Bulgaria does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Bulgaria is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services and also collaborates with the European Commission and ENISA for cybersecurity issues. Bulgaria hosted and participated in the Applied Learning for Emergency Response Team (ALERT) for Europe and CIS countries in October 2012. Bulgaria participated in the International Cyber Shield Exercise 2014 in Turkey (ICSE 2014).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-The Criminal Code (Article 159).

2.2 UN CONVENTION AND PROTOCOL

Bulgaria has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Bulgaria has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Bulgaria does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Report of online illegal content pertaining to child online protection can be made at safenet.bg (*).

CYBERWELLNESS PROFILE
BURKINA-FASO

BACKGROUND

Total Population: 17 482 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 4.40%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

-Law on Network and Electronic communication services.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

-Law on Services and Electronic Transaction.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU conducted a CIRT readiness assessment for Burkina Faso in Ouagadougou, Burkina-Faso in May 2010. The ITU-IMPACT established the national CIRT of Burkina-Faso, CIRT.BF which will be part of the National Agency for Information Systems Security (ANSSI).

1.2.2 STANDARDS

The National CIRT (CIRT.BF) has officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Burkina-Faso does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

ANSSI is currently developing an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

The National Cybersecurity Plan provides a national governance roadmap for cybersecurity in Burkina-Faso. It is designed as a global reference that will help build all the actions in the sector of cybersecurity. This plan contains major actions that must be taken into account in order to build a sustainable protection against all the types of attacks coming from Internet.

1.3.3 RESPONSIBLE AGENCY

The National Agency for Information Systems Security (ANSSI) is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap. ANSSI will be in charge of the Internet ecosystem of Burkina Faso, in terms of information systems security. ANSSI will have also the power of an Auditor Agency for Information security. ANSSI will only be fully operational at the end of 2014.

1.3.4 NATIONAL BENCHMARKING

The regulatory authority for electronic communication of Burkina Faso (ARCEP), with the assistance of ITU, has conducted in 2010 a global study in Burkina Faso. This study set the benchmark for the level of cybersecurity protection in Burkina-Faso.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Burkina-Faso does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Burkina-Faso does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Burkina-Faso does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Burkina-Faso does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Burkina-Faso does not have any official recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Burkina-Faso has an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector, through the national CIRT (CIRT.BF).

1.5.3 PUBLIC SECTOR PARTNERSHIP

Burkina-Faso does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Burkina-Faso is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Burkina Faso is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA).

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Burkina-Faso does not have any national legislation pertaining to child online protection.

2.2 UN CONVENTION AND PROTOCOL

Burkina-Faso has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Burkina-Faso has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Burkina-Faso does not have any officially recognized agency that offers intuitional support on child online protection.

2.4 REPORTING MECHANISM

Burkina-Faso does not have any officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
BURUNDI

BACKGROUND

Total Population: 8 749 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 1.30%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

-Penal Code (Article 467-470).

1.1.2 REGULATION AND COMPLIANCE

Burundi does not have officially recognised regulations and compliance requirement pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU is currently cooperating with Burundi to implement the national CIRT project.

1.2.2 STANDARDS

Burundi does not have officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Burundi does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Burundi does not have an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Burundi does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The Agency for Regulation and Control of Telecommunications (ARCT) is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Burundi does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Burundi does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Burundi does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Burundi does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Burundi does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Burundi has officially recognized partnerships with Common Market for Eastern and Southern Africa (COMESA) and East African Communications Organisation (EACO) for intra-state cooperation.

1.5.2 INTRA-AGENCY COOPERATION

Burundi does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Burundi does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Burundi is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Burundi is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-The Criminal Code (Article 519, 523).

2.2 UN CONVENTION AND PROTOCOL

Burundi has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Burundi has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Burundi does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Burundi does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
CAMBODIA

BACKGROUND

Total Population: 14 478 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 6.00%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation pertaining to cybercrime is mandated through the following legal instrument:

- Criminal Court of the Kingdom of Cambodia: Articles 317-320 and Articles 427-432.

1.1.2 REGULATION AND COMPLIANCE

Cambodia does not have any officially recognised regulation pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU completed a CIRT readiness assessment for Cambodia at Yangon, Myanmar in October 2011. Cambodia has an officially recognized national CIRT (CamCERT).

1.2.2 STANDARDS

Cambodia does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Cambodia does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Cambodia does not have any officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Cambodia does not have any national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The Department of ICT Security, Ministry of Posts and Telecommunications is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Cambodia does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Cambodia does not have any officially recognized national or sector-specific research and development programs or projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Cambodia does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Cambodia does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Cambodia does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Cambodia does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Cambodia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Cambodia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Cambodia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Cambodia participated in the Applied Learning for Emergency Response Team (ALERT) in December 2011, held in Yangon, Myanmar. Cambodia also participated in the ALERT at Vientiane, Lao P.D.R., in December 2013 (9-11th December 2013).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child protection has been enacted through the following instrument:

-Article 349 of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Cambodia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Cambodia has signed and ratified, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Cambodia does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Computer incidents can be reported to the National Cambodia Computer Emergency Response Team (CamCERT) on the phone number (855) 92 335 536 and by the email incident@camcert.gov.kh

CYBERWELLNESS PROFILE
CAMEROON

BACKGROUND

Total Population: 20 469 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 6.40%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

-Law on Cybersecurity and Cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Decree on IT Security Audit -Decree on Electronic Certification -Cybersecurity Standard.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU conducted a CIRT Assessment for Cameroon at Yaoundé, Cameroon in December 2010. Cameroon has established an officially recognized National CIRT.

1.2.2 STANDARDS

Cameroon has an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards. The framework is developed by the National Information Technology Agency (ANTIC) for government agencies.

1.2.3 CERTIFICATION

Cameroon does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Cameroon does not have an officially recognized national cybersecurity strategy. However it has developed a cybersecurity policy for government agencies.

1.3.2 ROADMAP FOR GOVERNANCE

Cameroon ICT/Telecomm roadmap includes a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

ANTIC is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Cameroon does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development. However in the ICT/Telecom roadmap, there are studies planned on to measure the impact of cybercrime in Cameroon.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Cameroon does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards. ANTIC has developed best practices and guidelines to be applied in the public sector.

1.4.2 MANPOWER DEVELOPMENT

Cameroon has dedicated a budget for public awareness program. Two awareness programs will be organized in Yaoundé and Douala which are the two major cities of our country. ANTIC also raises awareness on cybersecurity through a radio program every fortnight.

ANTIC is now working with the tertiary institution to develop programs related to cybersecurity in its engineering schools and universities.

Two cybersecurity seminars have also been organized in partnership with IMPACT in 2010 and 2013. Topics like penetration testing, security audit and forensic investigation were taught.

1.4.3 PROFESSIONAL CERTIFICATION

Cameroon has 3 public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Cameroon does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Cameroon does not have officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states. However Central Africa's countries are finalizing the development of a cybersecurity framework for intra-state cooperation.

1.5.2 INTRA-AGENCY COOPERATION

Cameroon does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Cameroon does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Cameroon is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Cameroon is among the beneficiaries of the EU/ITU co-funded project "Support for Harmonization of the ICT Policies in Sub-Sahara Africa" (HIPSSA).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

-Law on Cybersecurity and Cybercrime (Article 43, 76 and 80-82).

2.2 UN CONVENTION AND PROTOCOL

Cameroon has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Cameroon has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Cameroon does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Cameroon does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
CANADA

BACKGROUND

Total Population**:** 36 675 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 85.80%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

-Criminal Code (1985).

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Anti-Spam Act

-Secure Electronic Signature Regulations

-Electronic Commerce Protection Regulations

-Personal Information Protection and Electronic Documents Act

-Draft Bill C-12: An Act to Amend the Personal Information Protection and Electronic Documents Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

The Canadian Cyber Incident Response Centre (CCIRC) is the officially recognized CIRT. The Cyber Threat Evaluation Centre (CTEC) is another establishment responsible for the detection, analysis, and assessment of cyber threat activity on nationally important networks.

1.2.2 STANDARDS

In Canada the Management of Information Technology Security (MITS) is the body responsible for operational security standards. *The government has a* security policy *that states the requirements for protecting information and it directs the federal departments and agencies to which it applies to have an IT security strategy. The* Operational Standard for the Security of Information Act *is the nationally recognised instrument for cybersecurity standards.*

1.2.3 CERTIFICATION

Canada does not have a national or sector-specific framework for certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

The officially recognized national and sector-specific strategy for cybersecurity is the Canada's Cyber Security Strategy.

1.3.2 ROADMAP FOR GOVERNANCE

The Action Plan 2010-2015 for Canada's Cyber Security Strategy is the national roadmap for governance of cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The following agencies are the officially recognised national and sector-specific agencies responsible for cybersecurity in Canada:

-Royal Canadian Mounted Police (RCMP)
-Canadian Cyber Incident Response Centre (CCIRC)

-Office of the Privacy Commissioner of Canada (OPC)
-Office of the Critical Infrastructure Protection and Emergency Preparedness (OCIPEP).

1.3.4 NATIONAL BENCHMARKING

Canada does not currently have any national benchmarking exercise or referential to measure cybersecurity.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

The following are the national and sector-specific organizations responsible for R&D in Canada:

-Defence Research and Development Canada (DRDC) -Canadian Cyber Incident Response Centre (CCIRC)

-The Communications Security Establishment Canada (CSEC) -Information Technology Incident Management Plan

-Cyber Security Self-Assessment Guidance for Federally Regulated Financial Institutions.

1.4.2 MANPOWER DEVELOPMENT

Canada has recognized various types of awareness programs on cybersecurity, for the general public as well as for public and private sector employees through the following:

- CCIRC - OCIPEP -The Canadian Anti-Fraud Centre (CAFC)

- Public Safety Canada's Industrial Control Systems (ICS)

1.4.3 PROFESSIONAL CERTIFICATION

Canada does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Canada does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets between Canada and other nation states, Canada officially recognized the Canada-US Action plan on cybersecurity under the Beyond Border Action Plan. Additionally the CCIRC works closely with its international counterparts such as US-CERT, GovCert UK, CERT Australia, New Zealand CCIP to help mitigate cyber threats and to share information on best practices for protecting critical infrastructure.

1.5.2 INTRA-AGENCY COOPERATION

The OCIPEP and Shared Services Canada (SSC) facilitate communication and networking amongst Canadian organisations and businesses; these serve as a Framework for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Canada has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector: The SSC streamlines and consolidates information and communications technologies between various government departments. The CCIRC works closely with Internet Service Providers and security companies to help identify threats and develop effective countermeasures in cybersecurity.

1.5.4 INTERNATIONAL COOPERATION

Canada is a member of the following cybersecurity activities:
-FIRST -OAS -OSCE.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Section 163, 163.1, 172.1 and 172.2 of the Criminal Code.

-Bill C-22 an Act respecting the mandatory reporting of internet child pornography by persons who provide an internet service.

2.2 UN CONVENTION AND PROTOCOL

Canada has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Canada has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The following institutions are responsible for the activities preventing online child abuse:

- (CCIRC) -Public Safety Canada

-Contribution Program to Combat Child Sexual Exploitation and Human Trafficking (CPCCSEHT)

-The Royal Canadian Mounted Police through the National Child Exploitation Coordination Centre and the National Missing Children Service.

2.4 REPORTING MECHANISM

Cybertip.ca, Canada's national tip line for reporting the online sexual exploitation of children, provides an online form.

CYBERWELLNESS PROFILE
CAPE-VERDE

BACKGROUND

Total Population: 505 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 37.50%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Cape-Verde does not have currently any officially recognized national criminal legislation pertaining to cybercrime but there is a work in progress.

1.1.2 REGULATION AND COMPLIANCE

Cape-Verde does not have currently any officially recognized national regulation pertaining to cybersecurity but there is a work in progress.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Cape-Verde does not have currently any officially recognized national CIRT but there is a work in progress.

1.2.2 STANDARDS

Cape-Verde does not have currently any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity but there is a work in progress.

1.2.3 CERTIFICATION

Cape-Verde does not have currently any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals but there is a work in progress.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Cape-Verde does not have currently an officially recognized national cybersecurity strategy but there is a work in progress.

1.3.2 ROADMAP FOR GOVERNANCE

Cape-Verde does not have currently an officially recognized national governance roadmap for cybersecurity but there is a work in progress.

1.3.3 RESPONSIBLE AGENCY

Cape-Verde does not have any officially recognized agencies responsible for implementing a national cybersecurity strategy, policy and roadmap. However there is a committee working on cybersecurity strategy.

1.3.4 NATIONAL BENCHMARKING

Cape-Verde does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Cape-Verde does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Cape-Verde does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Cape-Verde does not have the exact numbers of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Cape-Verde does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Cape-Verde does not have officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Cape-Verde does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Cape-Verde does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Cape-Verde is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Cape-Verde is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-The Criminal Code (Article 150).

2.2 UN CONVENTION AND PROTOCOL

Cape-Verde has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Cape-Verde has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Cape-Verde does not have any officially recognized agencies that offer institutional support on child online protection.

2.4 REPORTING MECHANISM

Cape-Verde does not have any officially recognized agencies that offer an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
CENTRAL AFRICAN REPUBLIC

BACKGROUND

Total Population: 4 576 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 3.50%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- None.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- None.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Central African Republic does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Central African Republic does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Central African Republic.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Central African Republic does not have an officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Central African Republic.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Central African Republic.

1.3.4 NATIONAL BENCHMARKING

Central African Republic does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Central African Republic does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Central African Republic.

1.4.3 PROFESSIONAL CERTIFICATION

Central African Republic does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Central African Republic does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Central African Republic does not have a framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Central African Republic does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Central African Republic.

1.5.4 INTERNATIONAL COOPERATION

There is no information that Central African Republic currently participates in any international cybersecurity cooperation initiative.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Articles 85, 86, 110 and 111* of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Central African Republic has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Central African Republic has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for the child online protection in Central African Republic.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Central African Republic.

CYBERWELLNESS PROFILE
REPUBLIC OF CHAD

BACKGROUND

Total Population: 11 831 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 2.30%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- None.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- None.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Chad does not have an officially recognized national CIRT. ITU conducted a CIRT assessment for Chad in 2010.

1.2.2 STANDARDS

Chad does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Chad.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Chad does not have an officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Chad.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Chad.

1.3.4 NATIONAL BENCHMARKING

Chad does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Chad does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Chad.

1.4.3 PROFESSIONAL CERTIFICATION

Chad does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Chad does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Chad does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Chad does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Chad.

1.5.4 INTERNATIONAL COOPERATION

Chad is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- None.

2.2 UN CONVENTION AND PROTOCOL

Chad has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Chad has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Chad.

CYBERWELLNESS PROFILE
REPUBLIC OF CHILE

BACKGROUND

Total Population: 17 423 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 66.50%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Law on Cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Law on Personal Data Protection
- Law on Electronic Documents and Digital Signature.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Chile has an officially recognized national CIRT, CLCERT. CLCERT-CL has existed and functioned within the government but it is not a formal institutional entity so much as an operational capacity and structure maintained by the Ministry of the Interior and Public Safety.

1.2.2 STANDARDS

Chile has officially approved the Supreme Decree No. 1299, Program for the Improvement of Information Security Systems Management as the national framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no information on any framework for certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

While there is no official national cybersecurity strategy or policy document, Chilean authorities have been working for a number of years to develop a strong national capacity for cyber incident response and management. Emphasis has been placed on developing standardized procedures and best practices for incident management and cybersecurity more broadly.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national or sector-specific governance roadmap for cybersecurity in Chile.

1.3.3 RESPONSIBLE AGENCY

The Ministry of the Interior and Public Safety, Cyber Crime Investigation Unit (BRICIB), the General Secretariat of the Presidency and the Sub-Secretariat of Telecommunications all play key roles in cybersecurity.

1.3.4 NATIONAL BENCHMARKING

There is no national benchmarking and referential to measure cybersecurity development in Chile.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Regular risk assessments and trainings for staff are also carried out occasionally as a means of research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in the public sector.

1.4.2 MANPOWER DEVELOPMENT

Personnel from CLCERT -CL receive technical training in aspects of cyber investigations and incident management from experts in the field. Cybersecurity and cybercrime-related bachelors and masters degrees are offered by the University of Chile and other academic institutions. To raise awareness and promote a culture of cybersecurity the Ministry of Education has developed and is implementing, in partnership with several private sector entities, a long-term campaign called Internet Segura. Internet safety is taught in schools as part of the ethics competencies contained in the Technology curriculum.

1.4.3 PROFESSIONAL CERTIFICATION

Chile does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Chile does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, CLCERT-CL has actively collaborated with other national CSIRTs around the region in responding to incidents.

1.5.2 INTRA-AGENCY COOPERATION

Chile does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Private companies are able and encouraged by the government to also provide incident management-related services, both to other private enterprises as well as public institutions in Chile.

1.5.4 INTERNATIONAL COOPERATION

To facilitate participation in regional/international cybersecurity platforms and forums:

CLCERT is a member of the FIRST.

CLCERT-CL has participated in initiatives to train personnel in other OAS Member States.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

-Article 366quater and 366quinquies of the Criminal Code, included by Law n. 19.927/2004, January 2004.

-Articles 374 to 374ter of the Criminal Code, included by the Law n.19.617, July 1999, 19.806, May 2002 and 19.927, January 2004.

2.2 UN CONVENTION AND PROTOCOL

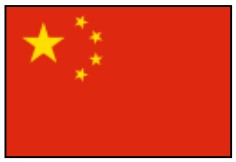
Chile has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Chile has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The website of the Chilean Computer Emergency Response Team CLCERT has general information on cybersecurity and specific information on child online protection.

2.4 REPORTING MECHANISM

Computer incidents can be reported to the National Chile Computer Emergency Response Team CLCERT by the email clcert@clcert.cl. The Integra Foundation provides a helpline.



CYBERWELLNESS PROFILE

CHINA

BACKGROUND

Total Population: 1 353 601 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 45.80%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Art 285,286 & 287 Criminal Law, 1997
- Art 285, Criminal Law, 2009.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Regulations on Safeguarding Computer Information Systems 1996
- Measures on Management of Internet Information Services 2000
- Decision of the Standing Committee of the National People's Congress on Preserving Computer Network Security 2000.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

There is an officially recognized National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT).

1.2.2 STANDARDS

Through China's Information Security Standardization Technical committee 18 standards were issued in 2010.

1.2.3 CERTIFICATION

Currently China does not have any officially recognized national or sector specific certification body for cybersecurity.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

China has an officially recognized national cybersecurity policy through the following instrument:

- The National Medium- and Long-Term Program for Science and Technology Development (2006-2020).

1.3.2 ROADMAP FOR GOVERNANCE

China does not currently have any national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

In China the officially recognised national or sector-specific agency responsible for implementing a national cybersecurity strategy and policy are:

- Ministry of Industry and Information Technology (MIIT)
- National Network & Information Security Coordination Team
- The Central Internet Security and Informatization Leading Group.
- State Internet information Office
- Ministry of Science and Technology

1.3.4 NATIONAL BENCHMARKING

China does not have an officially recognized national or sector-specific benchmarking exercise or body.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

A blue paper "China's Protection for Critical Information Infrastructure" issued by the Information Security Law Research Centre which identifies priority sectors such as Government affairs information system, educational and government research institutes, public communications such as radio and television, suffices as the national and sector-specific (R&D) of cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

The CNCERT produces reports that are used for educational and professional training purposes.

1.4.3 PROFESSIONAL CERTIFICATION

China does not have any officially recognized certified public sector professionals.

1.4.4 AGENCY CERTIFICATION

There are no certified government and public sector bodies recognized for certification of agencies in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Currently there are no officially recognized national or sector-specific partnerships for sharing cybersecurity assets across borders in China.

1.5.2 INTRA-AGENCY COOPERATION

The Annual Chinese Conference on Computer and Network Security by the Office of the Cyber Affairs is the officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector. The Central Internet Security and Information Leading Group increases the coordination between different government department sectors.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is massive cooperation between the Internet Society of China, China mobile, China Telecom, China Unicom, China Internet Network Information Center and CNCERT/CC.

1.5.4 INTERNATIONAL COOPERATION

China is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. China is also a member of the following organizations:

- FIRST -APCERT -ASEAN -Anti-Phishing Working Group.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Chapter VI, Section 9 of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

China has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

China has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no specific institution recognized for child online protection as The National Computer Network Emergency Response Technical Team Coordination Center of China (CNCERT (*)) does not provide specific information on this.

2.4 REPORTING MECHANISM

Online illegal or harmful content can be reported by filling the form on the (CNCERT) website.

China Internet Network Information Center (CNNIC (*)) accepts complaints by the number 8610-58813000 and by the email address supervise@cnnic.cn .

CYBERWELLNESS PROFILE
COLOMBIA

BACKGROUND

Total Population: 47 551 500

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 51.70%

(data source: ITU Statistics, 2013)

1.**CYBERSECURITY**

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

-The Criminal Code (Protection of Information and Data).

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Statutory Law 1266

-Statutory Law 1581

-Decree 1377 of 2013

-External Circular 042 of 2012 of the Financial Superintendence of Colombia.

-External Circular 042 of 2012

-Statutory Law 1621

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Colombia has the following National and sector-specific CIRT:

-ColCERT (group Cyber Emergency Response of Colombia), under the Ministry of Defense.

-CSIRT-Ponal (headquarters of the National Police telematics).

-CSIRT-CCIT (Computer Security Incident Response Team of the Colombian Chamber Informatics and Telecommunications).

CSIRT-ETB (Computer Security Incident Response Team - Empresa de Telecomunicaciones de Bogota SA ESP).

DigiCSIRT (DigiSOC Computer Security Incident Response Team).

SOC-CCOC (Security Operations Center - Cyber Operations Command Joint)

1.2.2 STANDARDS

Colombia has an officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards through the Model of information security for government online strategy and Conpes 3701 (National Planning Policy guidelines for cyber security and defense) .

1.2.3 CERTIFICATION

Colombia does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Colombia has an officially recognized national cybersecurity strategy through the Conpes 3701 (National Planning Policy guidelines for cyber security and defense).

1.3.2 ROADMAP FOR GOVERNANCE

The Conpes 3701 (National Planning Policy guidelines for cyber security and defense) provides a national governance roadmap for cybersecurity in Colombia.

1.3.3 RESPONSIBLE AGENCY

The National Planning Department and the Ministry of Information Technologies and Communications (MINTIC) are the officially recognized agencies responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Colombia does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Colombia has an officially recognized national or sector-specific research and development (R&D) program (through the MINTIC) for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Colombia does not have any officially recognized national educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

However Colombia has different sector initiatives that address these issues. There are 113 companies nationwide that provide specialized courses which address cybersecurity fronts. Also it has 11 academic programs offered by security institutions nationwide.

1.4.3 PROFESSIONAL CERTIFICATION

Colombia has numerous public sector professionals certified under internationally recognized certification programs in cybersecurity. However Colombia did not carry out a survey to gather the exact statistic.

1.4.4 AGENCY CERTIFICATION

Colombia does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Colombia is able to facilitate sharing of cybersecurity assets across borders or with other nation states through the ColCERT and CSIRTPonal.

1.5.2 INTRA-AGENCY COOPERATION

Colombia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Colombia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Colombia cooperated as a member in the Anti-Phishing Working Group (APWG). ColCERT, CSIRT-ETB, CSIRTPonal, DigiCSIRT ,CSIRT-CCIT and SOC-CCOC are members of FIRST.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-The Criminal Code (Article 218 and 219A)

-Law n. 679*.

2.2 UN CONVENTION AND PROTOCOL

Colombia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Colombia has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Police Cybernetic Centre*is the officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

The Police Cybernetic Centre* is the officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
COMOROS

BACKGROUND

Total Population: 773 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 6.50%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Comoros does not have any officially recognized national criminal legislation pertaining to cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Comoros does not have any officially recognized national regulation pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Comoros does not have any officially recognized national CIRT. ITU conducted a CIRT readiness assessment for Comoros in 2014.

1.2.2 STANDARDS

Comoros does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Comoros does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Comoros does not have an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Comoros does not have an officially recognized national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Comoros does not have any officially recognized agencies responsible for implementing a national cybersecurity strategy, policy and roadmap. However there is a committee working on cybersecurity strategy.

1.3.4 NATIONAL BENCHMARKING

Comoros does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Comoros does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Comoros does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Comoros does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Comoros does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Comoros does not have officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Comoros does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Comoros does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Comoros is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-The Criminal Code (Article 247,317 and 318).

2.2 UN CONVENTION AND PROTOCOL

Comoros has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Comoros has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Comoros does not have any officially recognized agencies that offer institutional support on child online protection.

2.4 REPORTING MECHANISM

Comoros does not have any officially recognized agencies that offer an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

DEMOCRATIC REPUBLIC OF CONGO

BACKGROUND

Total Population: 69 575 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 2.20%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

DRC does not have any officially recognized national legislation pertaining to cybercrime.

1.1.2 REGULATION AND COMPLIANCE

DRC does not have any officially recognised regulation pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

A CIRT Assessment was conducted by ITU in December 2010. DRC does not have an officially recognized national CIRT currently.

1.2.2 STANDARDS

DRC does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

DRC does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

DRC does not have any officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

DRC does not have any national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

DRC does not have an officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

DRC does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

DRC does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

DRC does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

DRC does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

DRC does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

DRC does not any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

DRC does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

DRC does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

DRC is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. DRC is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA).

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child protection has been enacted through the following instruments:

-The Criminal Code (Article 172, 175-177)

-Child Protection Law (Article 160, 169, 173 and 179-180).

2.2 UN CONVENTION AND PROTOCOL

DRC has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. DRC has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

DRC does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

DRC does not have any officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

CONGO

BACKGROUND

Total Population: 4 233 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 6.60%

(data source: ITU Statistics, 2013)

1 CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Draft Law on the Fight against Cybercrime

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Draft Law on Cybersecurity

-Draft Law on Electronic Transaction

-Draft Law on Protection of Personal Data.

-Draft Law on Copyright and neighbouring Right

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Congo does not have an officially recognized national CIRT. ITU is currently conducting a CIRT readiness assessment for Congo.

1.2.2 STANDARDS

Congo does not have officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Congo does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Congo does not have an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Congo does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Congo does not have an officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap. However Congo is planning to establish the Congolese Agency for ICT.

1.3.4 NATIONAL BENCHMARKING

Congo does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Congo does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Congo does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Congo does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Congo does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Congo does not have officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Congo does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Congo does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Congo is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Congo is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Article 66* of the Law on Child Protection.

2.2 UN CONVENTION AND PROTOCOL

Congo has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Congo has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Congo does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Congo does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE REPUBLIC OF COSTA RICA

BACKGROUND

Total Population: 4 794 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 45.96%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Penal Code amended by the Costa Rican Cybercrime Offence Law 9048.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Law on Protecting Individual Personal Information
- Law on the Certificates, Digital Signatures and Electronic Documents
- Law on Registration, Seizure and Examination of Private Documents and Intervention in Communications.

1.2 MEASURES

1.2.1 CIRT

Costa Rica has an officially recognized national CIRT known as CSIRT-CR established under the Ministry of Science, Technology and Telecommunications.

1.2.2 STANDARDS

Cost Rica does not have any framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Costa Rica does not have any framework for certification and accreditation of national agencies and public sectors professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

A National Digital Strategy has been adopted by the government. Its primary focus is on defining a vision for the integrated use of technologies by the State, and it does not go much beyond identifying cybersecurity as a priority. There is presently no national cybersecurity strategy or policy guiding the related efforts of national authorities.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national or sector-specific governance roadmap for cybersecurity in Costa Rica.

1.3.3 RESPONSIBLE AGENCY

The following agencies are responsible for cybersecurity in Costa Rica:

-CSIRT-CR

-Digital Government / Digital Secretariat

-Directorate for Digital Signatures

-The Superintendency for Telecommunications

-The Computer Crimes Section of the Judiciary -Ministry of Science, Technology and Telecommunications

-The Computer Crime Section of the Investigative Branch of the Judiciary.

1.3.4 NATIONAL BENCHMARKING

Costa Rica does not have any national benchmarking and referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no information on any programs for research and development of cybersecurity standards, best practices and guidelines in Costa Rica.

1.4.2 MANPOWER DEVELOPMENT

The Centre for the Formation of ICTs (CENFOTEC) offers a specialization in cyber security; the Latin American Science and Technology University (ULACIT) offers a specialization in information Security. Other institutions in Costa Rica offer cybersecurity and cybercrime relevant courses.

1.4.3 PROFESSIONAL CERTIFICATION

Costa Rica does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Costa Rica does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states Costa Rica has participated in various training programs by the OAS. Personnel of the computer crime section have received training in the United States and Canada.

1.5.2 INTRA-AGENCY COOPERATION

CSIRT-CR is mandated to coordinate among entities of the State and autonomous institutions to identify threats, minimize risks, and improve cooperation and information-sharing on relevant cybersecurity-related matters.

1.5.3 PUBLIC SECTOR PARTNERSHIP

CSIRT-CR is also mandated to coordinate not just among entities of the State and autonomous institutions, but also companies and banks to identify threats, minimize risks, and improve cooperation and information-sharing on relevant cybersecurity-related matters. There is no legal obligation for private sector entities to share information with national authorities in the event of an incident and the links and mechanisms necessary for facilitating such cooperation are limited and informal.

1.5.4 INTERNATIONAL COOPERATION

Costa Rica is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Article 173* of the Criminal Code, amended by the law n. 8590, July 2007

- Article 173bis* of the Criminal Code, added by the law n. 8590, July 2007

- Article 13* of Law n. 7739, Code for Childhood and Adolescence

- Article 174* of the Criminal Code, reformed by the law 7899, August 1999
- Law n. 8934*Protection of Children and Young from Harmful Content on the Internet and other Electronic Media, March 2011.

2.2 UN CONVENTION AND PROTOCOL

Costa Rica has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Costa Rica has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

A National Committee on the commercial sexual exploitation of children was created under the National Plan against Commercial Sexual Exploitation, 2002- Plan Nacional contra la Exploitación Sexual Comercial de Niñas, Niõs y Adolescentes. A National Committee for Online Security was created in December 2010-Comisión Nacional de Seguridad en Línea (Decree n.36274).

2.4 REPORTING MECHANISM

The Patronato Nacional de la Infancia (PANI) provides a space for online reporting on its Website.

CYBERWELLNESS PROFILE
CÔTE D'IVOIRE

BACKGROUND

Total Population: 20 595 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 2.60%

(data source: ITU Statistics, 2013)

1 CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

-Law No. 2013-451.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Electronic Transaction Act -Protection of Personal Data Act -Decree No. 2011-476.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

The national computer incident response team is the CI-CERT. ITU completed an auditing exercise in May 2010. An exercise to improve and enhance CI-CERT's performance was carried out in 2013.

1.2.2 STANDARDS

Côte d'Ivoire does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Côte d'Ivoire does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Côte d'Ivoire does not have any officially recognized national cybersecurity strategy and policy.

1.3.2 ROADMAP FOR GOVERNANCE

Côte d'Ivoire does not have any national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The Telecommunication Regulatory is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap for data protection and audit of information systems.

1.3.4 NATIONAL BENCHMARKING

Côte d'Ivoire does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Côte d'Ivoire does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Côte d'Ivoire does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

However the Training Center Computer Security CI-CERT (CFSI) will be set up. This organization will be responsible to provide programs at school and university as well as certification programs in cybersecurity.

1.4.3 PROFESSIONAL CERTIFICATION

Côte d'Ivoire has 12 public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Côte d'Ivoire does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Côte d'Ivoire does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Côte d'Ivoire does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Côte d'Ivoire has 12 officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Côte d'Ivoire is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. As a member of the African CERT, Côte d'Ivoire is involved in the promoting of preventive measures and coordinating of cyber security response in the event of cyber incidents. Côte d'Ivoire is among the beneficiaries of the EU/ITU co-funded project "Support for Harmonization of the ICT Policies in Sub-Sahara Africa" (HIPSSA).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

-The Criminal Code (Article 334, 337 and 338).

2.2 UN CONVENTION AND PROTOCOL

Côte d'Ivoire has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Côte d'Ivoire has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Côte d'Ivoire Computer Incident Response Team (CI-CERT) is the officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Côte d'Ivoire does not have any officially recognized agency that offers an avenue for the reporting of incidents related to child online protection. However there is a helpline "SOS enfant en détresse": 800 800 80.

CYBERWELLNESS PROFILE

CROATIA

BACKGROUND

Total Population: 4 387 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 66.75%

(data source: ITU Statistics, December 2012)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Croatian Criminal Law (January 2013).

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Law on Information Security 2007
- Law on Protection of Personal Data 2003
- Law on Ratification of conventions on cybercrime 2002
- Law on Electronic Document
- Law on the Security and Intelligence System 2006
- Law on Security validation
- Ordinance on the manner and deadlines for the implementation of measures for protection safety and integrity of networks and services 2012
- Regulation on Information Security Measures 2008.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Croatia has an officially recognized national CERT in accordance with the Information security law and its main task is processing of incidents on the Internet. Croatia has also a government CERT ZSIS which is responsible for state authorities, local and territorial (regional) governments, legal personnel with public authorities and legal and physical person who have access to, or handle classified and unclassified information.

1.2.2 STANDARDS

Croatia has officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards. They can be found under the guidelines set by Information Systems Security Bureau and by Office of the National Security Council.

1.2.3 CERTIFICATION

Croatia has officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals. They can be found under the guidelines set by Information Systems Security Bureau and by Office of the National Security Council.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Croatia is currently in progress for adoption of a national strategy on cybersecurity. The Office of the National Security Council is responsible for the preparation of this document. Other bodies involved in the preparation of this document are: Information Systems Security Bureau, Croatian Regulatory Authority for Network Industries, Ministry of Interior, Ministry of Foreign and European Affairs, Croatian national computer emergency response team, Croatian National Bank, Ministry of Maritime Affairs, Transport and Infrastructure, Ministry of Public Administration, Security and Intelligence Agency, Ministry of Defence of the Republic of Croatia.

1.3.2 ROADMAP FOR GOVERNANCE

Croatia does not currently have any national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The Office of the National Security Council is the officially recognized institution responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Croatia does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Croatia does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Croatian national CERT provides a national or sector-specific research and development (R&D) program through many presentations and easily accessible documents. It also informs people about threats on Internet, gives them statistics about the most common problems concerning cybercrime and also give them advice about how to protect themselves. Center for Information Security (CIS) also creates documents on topics in information security that will be useful to the public, develops educational materials intended for the public, organizes events to raise awareness of information security for the public and for specific groups, cooperates with all the media to raise awareness about information security, brings together young people interested in information security and educates them and also prepares them for professional engagement in the field of information security.

1.4.3 PROFESSIONAL CERTIFICATION

The Information Systems Security Bureau (ZSIS) and the national CERT are public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

The Information Systems Security Bureau (ZSIS) is the central state authority responsible for the technical areas of information security of the state certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

The authorities in Croatia work closely with European Network and Information Security Agency (ENISA), as a body of expertise, whose main task is to help the European Commission, the Member States and the business community to address, respond and especially to prevent network and information security problems and thus Republic of Croatia works with other European countries regarding security incidents.

1.5.2 INTRA-AGENCY COOPERATION

Croatia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Croatia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Croatia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Croatia also participated at conference on Strategic Priorities on Cybercrime (Dubrovnik, February, 15th 2013) also participating were Albania, Bosnia and Herzegovina, Montenegro, Serbia, Macedonia, Turkey and Kosovo in cooperation with the Council of Europe and the European Union.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

- Articles 163-165* of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Croatia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Croatia has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Croatian national CERT provides specific information for parents in its guide about online safety.

2.4 REPORTING MECHANISM

The Croatian national CERT provides the following email address to report computer incidents: ncert@cert.hr

The Center for Missing and Exploited Children provides an online form to report illegal content.

CYBERWELLNESS PROFILE
REPUBLIC OF CUBA

BACKGROUND

Total Population: 11 249 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 25.71%

(data source: ITU Statistics, December 2013)

1 CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- None.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- None.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Chad does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Cuba does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Cuba.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Cuba does not have any officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Cuba.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Cuba.

1.3.4 NATIONAL BENCHMARKING

Cuba does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Cuba does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Cuba.

1.4.3 PROFESSIONAL CERTIFICATION

Cuba does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Cuba does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Cuba does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Cuba does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Cuba.

1.5.4 INTERNATIONAL COOPERATION

Cuba is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Article 310.1* and 311(c)* of the Criminal Code, modified by the Decree 175, June 1997, and the Law 87, February 1999.

2.2 UN CONVENTION AND PROTOCOL

Cuba has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Cuba has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for the child online protection in Cuba.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Cuba.

CYBERWELLNESS PROFILE
CYPRUS

BACKGROUND

Total Population: 1 129 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 65.45%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Law Ratifying the Cybercrime Convention of 2001 (22(III)/2004).

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Processing of Personal Data Law
- Electronic Commerce Law (156(I)/2004)
- Law for the Protection of Confidentiality of Private Communications
- Law Regulating Electronic Communications and Postal Services of 2004
- Legal Framework for Electronic Signatures and for Relevant Matters Law.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Cyprus has an officially recognized research and education CSIRT known as Cyprus Research & Academic Network. ITU conducted a CIRT readiness assessment for Cyprus in 2014.

1.2.2 STANDARDS

Cyprus does not have an officially recognized national or sector specific cybersecurity framework for implementing internationally recognized standard.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Cyprus.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Cyprus has officially recognised the Cyprus Cybersecurity Strategy Document as its national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Cyprus.

1.3.3 RESPONSIBLE AGENCY

The Ministry of Communications & Works and the Office of the Commissioner of Electronic Communications and Postal Regulation (OCECPR) are responsible for cybersecurity coordination in Cyprus.

1.3.4 NATIONAL BENCHMARKING

There is no benchmarking or referential to measure cybersecurity development in Cyprus.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no officially recognized national or sector-specific program or project for the research and development of cybersecurity standards, best practices and guidelines in Cyprus.

1.4.2 MANPOWER DEVELOPMENT

SafenetCY and Simssafety are the projects that promote the safe use of Internet in Cyprus.

1.4.3 PROFESSIONAL CERTIFICATION

Cyprus does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Cyprus does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no information of any framework for sharing cybersecurity assets across borders with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Cyprus does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

CyberEthics is the officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Cyprus is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Cyprus also participates in activities of the ENISA.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

- Law for Combating Trafficking, Exploitation of Human Beings and for the Protection of Victim.

2.2 UN CONVENTION AND PROTOCOL

Cyprus has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Cyprus has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Pedagogical Institute of Cyprus* develops support material* for the integration of ICTs in the learning process.

2.4 REPORTING MECHANISM

Complaints can be addressed to the Cyprian Police on the number 1460. CyberEthics (*) website, sponsored by the Safer Internet Program of the European Union, provides a form to submit complaints as well as the number 26 67 47 47. CyberEthics is a project of The Cyprus Safer Internet Center.

CYBERWELLNESS PROFILE
CZECH REPUBLIC

BACKGROUND

Total Population: 10 566 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 74.11%

(data source: ITU Statistics, December 2012)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Czech Republic does not have any specific legislation pertaining to cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

- Act on Cybersecurity and Change of Related Acts which has been recently adopted and will become effective on 1st January 2015.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Czech Republic has an officially recognized and legally mandated a government CERT (GovCert.CZ) and a national CSIRT (CSIRT.CZ).

1.2.2 STANDARDS

Czech Republic has officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards through the Act on Cybersecurity and Change of Related Acts.

1.2.3 CERTIFICATION

Czech Republic does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

The Czech government has officially recognized the National cybersecurity strategy and Action Plan which is valid through 2015. This strategy is still in force and it is the basic document for the creation of legal acts, security policies of information and communication systems, standards, rules, operation measures, maintenance plans, recommendations and other tools for cyber security of the Czech Republic.

1.3.2 ROADMAP FOR GOVERNANCE

Czech Republic does not have an officially recognized national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The National Security Authority is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap in Czech Republic and for this purpose it has recently established a specialized department, the National Cybersecurity Centre.

1.3.4 NATIONAL BENCHMARKING

Czech Republic does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Czech Republic does not yet have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Czech Republic does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Czech Republic has numerous public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

The governmental CERT (GovCert.CZ), an accredited member of Terena-Trusted, is the only public agency certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Czech Republic has officially recognized partnerships with the following organizations:

- FIRST
- TRUSTED INTRODUCER
- NATO
- EUROPOL
- TERENA
- ENISA
- CCDCOE.

1.5.2 INTRA-AGENCY COOPERATION

Czech Republic does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Czech Republic does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Czech Republic participated in the Central European Cyber Security Platform (CECSP) which was founded in May 2013 on the initiative of Austria and the Czech Republic and whose aim is to enable the sharing of information, best practices, lesson learned and know-how about cyber threats and potential or (un)successfully carried out cyber-attacks.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION AND STRATEGY

Specific legislation on child protection has been enacted through the following instruments:

- §192 and §193* of the Criminal Code.

The Cyber security Strategy of the Czech Republic talks about raising cybersecurity awareness, but does not have specific provision for child online protection.

2.2 UN CONVENTION AND PROTOCOL

Czech Republic has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Czech Republic has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The InternetHotline* website, under the national police in cooperation with non-governmental organizations, provides information on child online protection for children, parents and educators.

The National Computer Security Incident Response Team (CSIRT*) does not provide specific information on child online protection.

2.4 REPORTING MECHANISM

Illegal online content can be reported in the website of InternetHotline*.

Illegal and harmful content can be reported by the filling of a form in the Czech Saferinternet (*) website.

CYBERWELLNESS PROFILE

DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA

BACKGROUND

Total Population: 34 554 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: Unknown%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- None.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- None.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

North Korea does not have an officially recognized national CIRT.

1.2.2 STANDARDS

North Korea does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in North Korea.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

North Korea does not have any officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in North Korea.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in North Korea.

1.3.4 NATIONAL BENCHMARKING

North Korea does not have an officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

North Korea does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in North Korea.

1.4.3 PROFESSIONAL CERTIFICATION

North Korea does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

North Korea does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

North Korea does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

North Korea does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in North Korea.

1.5.4 INTERNATIONAL COOPERATION

There is no information that North Korea participates in any international cybersecurity cooperation initiative.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- None.

2.2 UN CONVENTION AND PROTOCOL

North Korea has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Guinea-Bissau has not acceded to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in North Korea.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in North Korea.

CYBERWELLNESS PROFILE
DENMARK

BACKGROUND

Total Population: 5 593 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 94.6297%

(data source: ITU Statistics, December 2013)

1 CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Penal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Ecommerce Act
- Law on Electronic Signatures
- Act on Processing of Personal Data
- Law on Electronic Communications Networks and Services
- Act on Processing of Personal Data by the Operation of the Government.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Denmark has an officially recognized national CIRT known as GovCERT.DK. There is an ISP customer base CIRT known as CSIRT.DK and an educational and research CIRT known as DKCERT.

1.2.2 STANDARDS

Denmark does not have any officially approved national cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Denmark is a member of the CCRA which provides officially approved national cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Danish cyber strategy is defensive and focused on protecting military computer systems from exploitation or disruption, without an explicit focus on developing offensive or response mechanisms. Denmark is preparing a new cyber security strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Denmark does not currently have any national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The GovCERT.DK and the Center for Cyber Security are the officially recognized institutions responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

In Denmark the Center for Cyber Security produces an officially recognized national benchmarking report used to measure cybersecurity development. The Danish Defense Intelligence Service also makes an annual intelligence assessment of conditions abroad affecting Danish security, referring to the appropriate risk assessment.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Center for Cyber Security's publications include guides, forms and templates that are relevant to authorities and the telecommunications industry. This is the *officially* recognized national or sector-specific research and development (R&D) program/project for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Computer Security is a new DTU programme which will benefit public and private sectors alike. The programme comprises—among other things—a special competence course in cyber security, which the Danish Defense Intelligence Service's Cyber Security Center, Copenhagen Finance IT Region (CFIR) and IBM have helped to realize.

1.4.3 PROFESSIONAL CERTIFICATION

There is no information on the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity for Denmark.

1.4.4 AGENCY CERTIFICATION

There is no information of any government and public sector agencies that are certified under internationally recognized standards in cybersecurity in Denmark.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Center for Cyber Security collaborates with private and public stakeholders at home and abroad to facilitate sharing of cybersecurity assets across borders, working with various CIRTS of different countries and intelligence agencies amongst others. Also participates in: - EU - NATO.

1.5.2 INTRA-AGENCY COOPERATION

Center for Cyber Security establishes a contact with representatives of relevant ministries and authorities to dialogue on the identification of critical ICT infrastructure and to ensure coordination of cyber security in Denmark. There is also in place an MoU between the members of the ISP Security Forum, DK-CERT and GovCERT to combat botnets.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Center for Cyber Security has established a forum for cooperation with public and private owners and providers of ICT infrastructure. The Forum will contribute to the dialogue on security of critical ICT infrastructure and support this work.

1.5.4 INTERNATIONAL COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Denmark has officially recognized partnerships with the following organizations: -DKCERT is a member of:

- FIRST - EU - NATO - ENISA.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

-S235 of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Denmark has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Denmark has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no information on the institutional support in for online child protection in Denmark.

2.4 REPORTING MECHANISM

Child pornography on the internet can be reported by a form filled in the National Police (*) website. Save the Children Denmark also provides a space to report child abuse images on the internet.

CYBERWELLNESS PROFILE

DJIBOUTI

BACKGROUND

Total Population: 467 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 9.50%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Penal Code

-Law on Protection of Copyright

-Law on Information Technology and Communication Sector

-Law on Postal and Telecommunication Sector.

1.1.2 REGULATION AND COMPLIANCE

Djibouti does not have officially recognised regulation pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU conducted a CIRT readiness assessment for Djibouti at Djibouti City, Djibouti in December 2012. Djibouti does not have an officially recognized National CIRT.

1.2.2 STANDARDS

Djibouti does not have officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Djibouti does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Djibouti does not have an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Djibouti does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Djibouti does not have an officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Djibouti does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Djibouti does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Djibouti does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Djibouti does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Djibouti does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Djibouti does not have officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Djibouti does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Djibouti does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Djibouti is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Djibouti participated in the 2012 ITU-IMPACT Workshop on Cyber Drill in Jordan.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-The Penal Code (Article 352,353 and 463).

2.2 UN CONVENTION AND PROTOCOL

Djibouti has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Djibouti has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Djibouti does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Djibouti does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

THE COMMONWEALTH OF DOMINICA

BACKGROUND

Total Population: 71 300

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 59.00%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Electronic Crimes Bill.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Data Protection Bill

- Electronic Evidence Act

- Electronic Transactions Bill.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Dominica does not have any officially recognized national CIRT. Dominica is working towards establishing a national CIRT.

1.2.2 STANDARDS

Dominica does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Dominica.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Dominica does not have any officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Dominica.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Dominica.

1.3.4 NATIONAL BENCHMARKING

Dominica does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Dominica does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Dominica.

1.4.3 PROFESSIONAL CERTIFICATION

Dominica does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Dominica does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Dominica does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Dominica does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Dominica.

1.5.4 INTERNATIONAL COOPERATION

Dominica is a member of the OAS-CICTE.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- None.

2.2 UN CONVENTION AND PROTOCOL

Dominica has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Dominica has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Dominica.

CYBERWELLNESS PROFILE
DOMINICAN REPUBLIC

BACKGROUND

Total Population: 1 359 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 45.90%

(data source: ITU Statistics, December 2012)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-High Technology Crimes Law No. 53/07

-Electronic Commerce, Documents and Digital Signatures Law.

1.1.2 REGULATION AND COMPLIANCE

Dominican Republic does not have specific legislation and regulation related to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU conducted a CIRT readiness assessment for Dominican Republic at Santo Domingo, Dominican Republic in April 2012 (23-27th April 2012). Dominican Republic does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Dominican Republic does not have officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Dominican Republic does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Dominican Republic does not have an officially recognized national cybersecurity strategy or policy.

1.3.2 ROADMAP FOR GOVERNANCE

Dominican Republic does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The Interagency Commission against Crimes and High Tech Crime is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Dominican Republic does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Dominican Republic does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

The National Commission for Information Society and Knowledge (CNSIC) has an officially recognized national awareness program that promotes norms, values and social behaviors that contribute to integrity, creativity and innovation in navigating cyberspace.

1.4.3 PROFESSIONAL CERTIFICATION

Dominican Republic does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Dominican Republic does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Dominican Republic does not have officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Dominican Republic does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Dominican Republic does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Dominican Republic is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Dominican Republic also cooperated with the Cybercrime Convention Committee (T-CY) of the Council of Europe, Inter-American Committee contra el Terrorismo (CICTE) of the OAS and INTERPOL.

Dominican Republic is among the beneficiary countries of the EU/ITU co-funded project “Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures” (HIPCAR).

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific national legislations pertaining to child online protection are enacted through the following legal instrument:

- Law against High Technology Crimes and Offences (Article 24).

2.2 UN CONVENTION AND PROTOCOL

Dominican Republic has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Dominican Republic has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The High Technology Investigation Department (Departamento de Investigación de Crímenes de Alta Tecnología) has produced a presentation on online safety for children.

The National Commission for the Information and Knowledge Society (CNSIC*) maintains together with the Dominican Telecommunications Institute (INDOTEL*) a website* dedicated to prevent the risk of using internet for young people. The website also has information for parents and teachers.

2.4 REPORTING MECHANISM

Complaints can be made by the telephone of the Attorney-General 1-809-200-7393, or by filling the form available in the website www.internetsano.do.

CYBERWELLNESS PROFILE
ECUADOR

BACKGROUND

Total Population: 14 865 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 40.35%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:
- Draft Penal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Electronic commerce Law. -Electronic signatures -Messages of information

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU conducted a CIRT Assessment for Ecuador in 2013. Ecuador has an officially recognized national CIRT (EcuCERT).

1.2.2 STANDARDS

Ecuador has officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards through the following instruments:

-The “Comite Tecnico de Ciberseguidad”, a local working group, dealing with cybersecurity, which gathers together many public and private organizations.

- Decree 166 of the National Secretariat of Public Administration establishes that all entities of the Central Public Administration must comply with technical standards for information security.

1.2.3 CERTIFICATION

Ecuador has officially approved INEN, the national (and sector specific) cybersecurity framework for the certification and accreditation of national agencies and public sector professionals which helps to ensure compliance with citizens' rights relating to security and works on technical standards which are applied at the national level.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

There is no available information regarding any officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no information available regarding any recognized national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Ecuador has officially recognized the following agencies responsible for implementing a national cybersecurity strategy, policy and roadmap in Ecuador:

-EcuCERT

- The National Secretariat of Public Administration, through its Directorate for Technological Architecture and Information Security.

- The Ministry of Intelligence through its Counter-intelligence and Info-communications Section and its Strategic Technological Operations Centre.

1.3.4 NATIONAL BENCHMARKING

There is no information available regarding any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

The Technological Crimes Investigations Unit and the National Police receive relevant technical training from higher education institutions within the country, as well as international organizations and are the officially recognized national and sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Ecuador's private and public institutions provide various types of awareness programs, industry talks, conferences, training programs and workshops on cybersecurity, for the general public as well as for public and private sector employees.

CEDIA is a National Research and Education Network whose mission is "to promote, coordinate and develop advanced computer and telecommunications networks to boost technology in innovative scientific research and education." Its members are: Universities, Polytechnics, research centers, public and private organizations.

The ESPOL offers a Master's degree in Applied Computer Security (MSIA) which is a new academic option considered by the ESPOL of high national priority and which represents the efforts of a group of senior specialists. The Judicial Police of Ecuador has created a Facebook page in order to promote awareness raising and prevention of cybercrimes through publication of complaints, security alerts, information campaigns, technical assistance, and cybersecurity tips for citizens.

The Ministry of Intelligence has also created a project called "Promoting a culture of intelligence", which aims to do precisely that through democratization and more robust citizen participation.

1.4.3 PROFESSIONAL CERTIFICATION

Ecuador has numerous public sector professionals certified under internationally recognized certification programs in cybersecurity. However it did not conduct a survey to gather the exact statistic.

1.4.4 AGENCY CERTIFICATION

Ecuador has one certified government and public sector agencies certified under internationally recognized standards in cybersecurity (ISO 270001).

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no information available regarding any officially recognized national or sector-specific partnerships for sharing cybersecurity assets across borders with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

There is no information available regarding any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Ecuador's Technological Crimes Investigations Unit has begun to create spaces for increased inter-institutional cooperation between public and private sector entities, both within the country as well as at the international level. Emphasis has been placed on promoting the exchange of information and cooperation, particularly in the investigation of electronic fraud and child pornography.

1.5.4 INTERNATIONAL COOPERATION

Ecuador is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services and has participated in the following cybersecurity activities:

-Participation in the Latin American Working Group on Cybercrime of INTERPOL

- FIRST -LACNIC -CERT CC.

2. CHILD ONLINE PROTECTION

Please note that in Ecuador a child is a person under 14

2.1 NATIONAL LEGISLATION

- Article 528.6* of the Criminal Code.

-Articles 52, 69* and 72* of the Childhood and Adolescence Code, January 2003.

2.2 UN CONVENTION AND PROTOCOL

Ecuador has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Ecuador has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The National Council on Childhood and Adolescence is the responsible organ for the protection of children but it has no current project on online protection.

2.4 REPORTING MECHANISM

Ecuador does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

EGYPT

BACKGROUND

Total Population: 83 958 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 49.56%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-The Penal Code
-Intellectual Property Law
-Telecom Act
-E-Signature Law
-Child Act.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

-E-Signature Regulation.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Egypt has an officially recognized national CIRT (EG-CERT). EG-CERT has expanded to reach 26 cybersecurity professionals working in four departments: incident handling, cyber forensics, malware analysis and reverse engineering, and penetration testing. EG-CERT has moved to a separate facility and is currently upgrading its labs in the four key operational departments. Additional labs are being planned for mobile cyber security and Industrial control systems cyber security.

1.2.2 STANDARDS

Egypt is currently drafting an officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

Cybersecurity-based regulations for the banking sector are issued by the Central Bank of Egypt (CBE), in relation to internet banking and mobile money and by the Egyptian Financial Supervisory Authority (EFSA) in relation to electronic stock trading.

1.2.3 CERTIFICATION

The e-Signature Law requires ISO 27000 certification for (private sector) Digital Certificates Service Providers (CSPs). The ISO 27000 certification is a prerequisite for CSPs licensing by IT Industry Development Agency (ITIDA).

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

A joint expert group from Government and (private) Industry were commissioned by the Minister of Communications and Information Technology to prepare a Cybersecurity Strategic Business Plan (SBP) at the

national level. The 6 months efforts resulted in a SBP that has become part of the national ICT strategic plan from 2014 to 2020.

1.3.2 ROADMAP FOR GOVERNANCE

A national committee headed by the minister of Communications and Information Technology with participation from key governmental stakeholders prepared a roadmap for cybersecurity governance and high level strategic policy and operational recommendations that was forwarded to the Cabinet of Ministers in September 2014.

1.3.3 RESPONSIBLE AGENCY

The Ministry of Communications and Information Technology (MCIT) is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

EG-CERT participates regularly in regional and international cyberdrills. EG-CERT successfully participated in (Asia Pacific - APCERT) cyberdrill (2012 & 2013), (Organization of Islamic Countries - OIC-CERT) cyberdrill (2012 & 2013), and ITU-Impact Arab region cyberdrill (2012). In 2014, EG-CERT participated both in APCERT cyberdrills as well as the OIC-CERT cyberdrills.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

The IT Academia Collaboration (ITAC) Program at ITIDA recognizes cybersecurity as a priority R&D domain. Since 2005, ITAC has provided several grants for cybersecurity related R&D projects carried out jointly by partners from the academic sector and ICT companies. ITAC R&D grants are valued between $15K and $280K each. (An example of the ITAC funded R&D cybersecurity related projects is a project that successfully developed a smart PKI token for e-signature.)

In addition, EG-CERT has on-going R&D activities in the area of cybersecurity.

1.4.2 MANPOWER DEVELOPMENT

In 2009 and 2010, the National Telecommunications Regulatory Authority (NTRA) organized and sponsored an advanced cybersecurity training program for professionals, training 220 professionals in 38 organizations within the governmental/public sector, banking sector, education sector, as well as from ICT private sector companies (Telecom companies, mobile operators, CSPs, etc.). As a result, 179 of those professionals obtained international certificates from SANS.
In 2008, MCIT established a national Child Online Protection (COP) Committee, and launched a program called Amanak for public awareness, especially targeting youth, educators, and families. In 2013, the national COP Committee was given the mandate to develop a comprehensive national COP strategy.

1.4.3 PROFESSIONAL CERTIFICATION

Egypt has over 1000 certified professionals (public and private sector) with international certificates from SANS (through SANS-EGYPT) and EC Council (through 16 EC Council certified centers that are based and operating in Egypt).

1.4.4 AGENCY CERTIFICATION

Egypt has 17 entities certified under internationally recognized standards in cybersecurity precisely ISO/IEC 27001 certification in 2013.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Egypt has officially recognized partnerships with the following organizations:

-ITU	-OMAN CERT	-TUNISIA CERT
-FIRST	-CyberSecurity Malaysia	-Indian CERT
-South Korea KISA	-Uganda CERT.	

In addition to the listed partnerships, EG CERT has partnership with US CERT and Tanzania CERT (TZ-CERT).

1.5.2 INTRA-AGENCY COOPERATION

EG-CERT organizes workshops and disseminates cybersecurity related reports within the ICT sector, governmental sector, public sector, and with the banking and financial sectors.

1.5.3 PUBLIC SECTOR PARTNERSHIP

EG-CERT organizes workshops and disseminates cybersecurity related reports within the ICT sector, governmental sector, public sector, and with the banking and financial sectors.

1.5.4 INTERNATIONAL COOPERATION

Egypt is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

Egypt is a member of the United Nations Group of Government Experts (UN GGE) on the Developments in the Field of Information and Telecommunications in the Context of International Security (Aug'12-Jun'13). The UN GGE is a high level group of 15 international experts who prepared a report that addresses emerging cybersecurity threats, forwarded to the UN General Assembly in Oct 2013.

The UNGGE report that Egyptian Expert participated in preparing (the only expert from Africa and Middle East) was adopted by United Nations' General Assembly in October/November 2013. A new UN GGE has been formed to follow up on the work of the 2012/13 UN GGE, and Egypt continues to be a member of that Group in 2014/15. Egypt has led the efforts to establish and currently chairs the ITU Council Working Group for Child Online Protection (CWG-COP) since 2010. Egypt is a member of MERIDIAN conference since 2009. Egypt is an observer of the OECD's Committee for Information, Computer and Communications Policy (ICCP), including the working party on Information Security and Privacy (WPISP).
EG-CERT is a full member of FIRST (2012), has participated in its annual conference since 2009, and has served on the program committee of the annual FIRST Conference in 2012 and 2013.
EG-CERT is a member of the Organization of Islamic Countries-CERT (OIC-CERT), and has participated in OIC-CERT annual general meeting since 2009.

NTRA (EG-CERT) hosted an ITU Arab Regional cybersecurity Forum attended by over 120 professionals from 8 countries, in Dec 2011, and an Egypt-US R&D cybersecurity Workshop attended by over 200 professionals, in May 2013.
Egypt participated in the 2012 ITU-IMPACT Workshop on cyber Drill in Jordan and in the ITU RCC Regional cybersecurity Forum cyber Drill 2013 in Oman.

Egypt was the chair of the Program Committee of the Annual meeting of the national CERTs held in Boston – June 2014.

Egypt is also supporting Africa CERT and participated in its annual meeting in Djibouti – May 2014.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

Child Act (Article 96 and 116).

2.2 UN CONVENTION AND PROTOCOL

Egypt has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Egypt has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

TEDate (*) was established in 2001 by Egypt Telecom (*) and is Egypt's largest IP based data communications vehicle. Its service is supervised by the National Telecommunication Regulatory Agency (NTRA). TEData launched the "Family Internet" service to protect children from inappropriate content exposure on the web.

Egypt has led efforts to establish and currently chairs the ITU Council Working Group for Child Online Protection (CWG-COP) since 2010. At the national level, a national COP Committee was established in May 2013, with representatives from key stakeholders from governmental entities, private sector, academia and professional

associations. Three national COP competitions were organized in 2013/14, in addition to several awareness workshops, seminars, and training of trainers sessions.

2.4 REPORTING MECHANISM

Complaints can be addresses to the Child helpline using the number: 16000.

CYBERWELLNESS PROFILE REPUBLIC OF EL SALVADOR

BACKGROUND

Total Population: 6 264 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 23.11%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

-The proposed Special Law against Cybercrime is currently being considered by the presidency.

1.1.2 REGULATION AND COMPLIANCE

No specific legislation and regulation related to cybersecurity has been enacted.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

El Salvador has an officially recognized national CIRT known as SALCERT.

1.2.2 STANDARDS

Although there is not yet an established national strategy or policy for cybersecurity, one is presently being developed.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in El Salvador.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Although there is not yet an established national strategy or policy for cybersecurity in El Salvador, one is presently being developed.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in El Salvador.

1.3.3 RESPONSIBLE AGENCY

The following agencies are responsible for cybersecurity in El Salvador:

- The Ministry of Justice
- Computer Crime Investigations Group of the National Civil Police
- Ministry for Public Security.

1.3.4 NATIONAL BENCHMARKING

El Salvador does not have any benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

In El Salvador individual users are provided a cybersecurity policy manual which provides explicit instructions about authorized and responsible use of government-run information systems.

1.4.2 MANPOWER DEVELOPMENT

There is no information on any educational and professional programs or projects in El Salvador.

1.4.3 PROFESSIONAL CERTIFICATION

El Salvador does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

El Salvador does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no framework to facilitate sharing of cybersecurity assets across borders with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

In El Salvador there is no framework for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no framework for sharing cybersecurity assets between the public and private sector in El Salvador.

1.5.4 INTERNATIONAL COOPERATION

El Salvador is currently formalizing a partnership with the UNODC to receive cybercrime related training to bolster its existing capabilities.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Article 351(12)* of the Family Code, 1993

- Articles 172, 173* and 173-A* from the Criminal Code, respectively modified and added by Law n.210, December 2003.

2.2 UN CONVENTION AND PROTOCOL

El Salvador has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. El Salvador has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no information about any agency responsible for the protection of children online.

2.4 REPORTING MECHANISM

There is no information about any website or hotline where incidents can be reported to.

CYBERWELLNESS PROFILE

REPUBLIC OF EQUATORIAL GUINEA

BACKGROUND

Total Population: 740 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 16.40%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- None.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- None.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Equatorial Guinea does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Equatorial Guinea does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Equatorial Guinea.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Equatorial Guinea does not have an officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Equatorial Guinea.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Equatorial Guinea.

1.3.4 NATIONAL BENCHMARKING

Equatorial Guinea does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Equatorial Guinea does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Equatorial Guinea.

1.4.3 PROFESSIONAL CERTIFICATION

Equatorial Guinea does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Equatorial Guinea does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Equatorial Guinea does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Equatorial Guinea does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Equatorial Guinea.

1.5.4 INTERNATIONAL COOPERATION

Equatorial Guinea does not currently participate in any international cybersecurity cooperation initiative.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- None.

2.2 UN CONVENTION AND PROTOCOL

Equatorial Guinea has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Equatorial Guinea has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Equatorial Guinea.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Equatorial Guinea.

CYBERWELLNESS PROFILE
STATE OF ERITREA

BACKGROUND

Total Population: 5 581 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 0.90%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments: None.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments: None.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Eritrea does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Eritrea does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Eritrea.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Eritrea does not have an officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Eritrea.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Eritrea.

1.3.4 NATIONAL BENCHMARKING

Eritrea does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Eritrea does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Eritrea.

1.4.3 PROFESSIONAL CERTIFICATION

Eritrea does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Eritrea does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Eritrea does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Eritrea does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Eritrea.

1.5.4 INTERNATIONAL COOPERATION

Eritrea is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments: None.

2.2 UN CONVENTION AND PROTOCOL

Eritrea has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Eritrea has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Eritrea.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Eritrea.

CYBERWELLNESS PROFILE
REPUBLIC OF ESTONIA

BACKGROUND

Total Population: 1 340 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 80.00%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Penal Code.

1.1.2 REGULATION AND COMPLIANCE

Estonia has the following specific legislation related to cybersecurity and compliance:

- Digital Signatures Act
- Electronic Communications Act
- Public Information Act
- Personal Data Protection Act
- Payment and E-money institution Act
- Information Society Services Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Estonia has an officially recognized national CERT known as CERT-EE.

1.2.2 STANDARDS

In Estonia the ISKE is the officially approved national cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Estonia does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

The Estonian Cyber Security Strategy is the officially recognised national policy for cybersecurity.

1.3.2 ROADMAP FOR GOVERNANCE

The Cyber Security Strategy provides specific actions regarding the implementation of the objectives of the strategy.

1.3.4 NATIONAL BENCHMARKING

The RIA inspects the security of the information systems of state and local government agencies and providers of vital services. It also cooperates with the CERT Estonia and CIIP for the better performance of these functions. There is also Annual Report Cyber Security Branch that serves as the officially recognized national or sector-specific benchmarking exercise or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

RIA organizes the protection of the critical information infrastructure, among other things by preparing risk analyses and developing the security measures needed for the protection of the critical information infrastructure.

1.4.2 MANPOWER DEVELOPMENT

The Information Security Interoperability Framework and 'Raising Public Awareness about the Information Society' programme are the *officially* recognized national research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.3 PROFESSIONAL CERTIFICATION

CERT-EE team currently includes one Head Officer and five information security experts, one of them acting as a GovCERT officer. Four team members are located in Tallinn (the capital of Estonia) and two in Tartu (second largest city).

1.4.4 AGENCY CERTIFICATION

Estonia does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

The cooperation initiative was launched in August 2013, at the meeting of the heads of state of Estonia, Latvia and Lithuania with US President Barack Obama in Washington. The goal of the meeting was primarily to enhance cyber security dialogue between the Nordic-Baltic regions and the US and to share experiences.

1.5.2 INTRA-AGENCY COOPERATION

The X-Road is the officially recognized national platform for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

X-Road is the officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Estonia is a member of NATO CCDCOE, TERENA and TI TF-CSIRT.

CERT-EE is affiliated to FIRST.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- §178, §178(1) and §179 of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Estonia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Estonia has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The institution that supports the protection of children online is the Estonian Union for Child Welfare.

2.4 REPORTING MECHANISM

Illegal content can be reported by a form filled on the website of Estonian Union for Child Welfare.

CYBERWELLNESS PROFILE

FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA

BACKGROUND

Total Population: 86 539 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 1.90%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- None.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- None.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Ethiopia does not have an officially recognized national CIRT. A CIRT Assessment is currently being carried out by ITU.

1.2.2 STANDARDS

Ethiopia does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Ethiopia.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Ethiopia does not have an officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Ethiopia.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Ethiopia.

1.3.4 NATIONAL BENCHMARKING

Ethiopia does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Ethiopia does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Ethiopia.

1.4.3 PROFESSIONAL CERTIFICATION

Ethiopia does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Ethiopia does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Ethiopia does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Ethiopia does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Ethiopia.

1.5.4 INTERNATIONAL COOPERATION

Ethiopia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Articles 613, 640, 643 and 644 of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Ethiopia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Ethiopia has not acceded to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Ethiopia.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Ethiopia.

CYBERWELLNESS PROFILE

FIJI

BACKGROUND

Total Population: 876 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 37.10%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- CRIMES DECREE 2009 : Division 6 - Computer Offences.

1.1.2 REGULATION AND COMPLIANCE

Fiji does not have specific legislation and regulation related to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Fiji does not have an officially recognized National CIRT. However it is a member of the Pacific Regional CIRT (PacCERT). ITU conducted a CIRT assessment for Fiji in 2014

1.2.2 STANDARDS

Fiji does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Fiji does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Fiji does not have an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Fiji does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Fiji does not have an officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Fiji does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Fiji does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Fiji does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Fiji does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Fiji does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Fiji does not have official recognized partnerships with any organizations to facilitate the sharing of cybersecurity assets across borders.

1.5.2 INTRA-AGENCY COOPERATION

Fiji does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Fiji does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Fiji is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Fiji also takes part in the Asia Pacific CIRT cybersecurity forums. Fiji is among the beneficiary countries of the EU/ITU co-funded project “Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries” (ICB4PAC).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Fiji does not have specific legislation on child online protection.

2.2 UN CONVENTION AND PROTOCOL

Fiji has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Fiji has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Fiji does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Fiji does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

FINLAND

BACKGROUND

Total Population: 5 403 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 91.51%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

-Criminal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

-Act on the Protection of Privacy in Electronic Communications.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Finland has an officially recognized national CIRT (CERT-FI).

1.2.2 STANDARDS

Finland's National Security Auditing Criteria the main goal of which is to harmonise official measures when an authority conducts an audit in a company or in another organisation to verify their security level. KATAKRI is used as a tool when checking the fulfilment of security requirements (e.g. EU and NATO security requirements for classified information).

1.2.3 CERTIFICATION

The Accreditation of information security inspection bodies in Finland is regulated in the act on information security inspection bodies. An Inspection body may be a private organization or public agency/body. Accreditation framework is based on ISO 17021 and ISO 27006 standards with sector specific regulations. The responsible agency is the national accreditation body FINAS.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Finland has an officially recognized national cybersecurity strategy since 2013 (Finland cybersecurity strategy). It defines the key goals and guidelines which are used in responding to the threats against the cyber domain and which ensure its functioning. By following the Cyber Security Strategy's guidelines and the measures required, Finland can manage deliberate or inadvertent disturbances in the cyber domain as well as respond to and recover from them.

1.3.2 ROADMAP FOR GOVERNANCE

The Information Society Program provides a national governance roadmap for cybersecurity in Finland.

1.3.3 RESPONSIBLE AGENCY

The Security Committee (yet to be established) monitors and coordinates the implementation of a national cybersecurity strategy, policy and roadmap by respective agencies.

1.3.4 NATIONAL BENCHMARKING

The National Emergency Supply Agency is involved in organizing sector-specific preparedness exercises on some critical infrastructure sectors. They also have a self-assessment tool CIP organizations can use to measure and benchmark their level of preparedness to their peers.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Finland does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Cyber security education is supported by the modern data network laboratory which focuses on the use of the ICT education as well as projects. Laboratory for cyber security development and research will be built to increase versatile knowledge of field. The Tekes – the Finnish Funding Agency for Technology and Innovation- is the main agency responsible for these efforts.

1.4.3 PROFESSIONAL CERTIFICATION

Finland does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Finland does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Finland has officially recognized partnerships with the following organizations:

-ITU -FIRST -European Government Certs group.

1.5.2 INTRA-AGENCY COOPERATION

Finland has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector through its national CIRT.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Finland does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Finland participated in cybersecurity activities by FIRST and European Government CERTs group.

CERT-FI is a member of FIRST.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Chapter 17, §18, §18(a), §18(b) and §19-§21* of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Finland has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Finland has acceded, with no declarations or reservations to articles 2 and 3, to the

Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Finish Communications Regulation Authority maintains the Safe on the internet (*) website which provides information on internet safety for parents, children and educators.

2.4 REPORTING MECHANISM

Online Illegal content can be reported in the website (*) maintained by the organization Save the Children.

CYBERWELLNESS PROFILE

FRANCE

BACKGROUND

Total Population: 63 458 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 81.92%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Amended as Law no.2004-575 of June 21 2004,
- Ratification of the Council of Europe Convention on Cybercrime was made on January 10, 2006 (art 323).

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Law n° 78-17 of January 1976 relating to computer, files and freedoms
- Civil Code Law n° 2000-230 on Electronic Evidence and Electronic Signature
- Order of November 2011 and the interdepartmental Policy Statement No. 1300 on the protection of the confidentiality of national defense which is attached
- Recommendation n° 600 of March 1993 for the protection of sensitive information outside the scope of defense secrets Recommendations for computer workstations
- Law n° 2004-575 of June 2004 pour la confiance dans l'économie numérique
- Decree n° 2009-834 of July that creates the national security agency
- Recommendation n°901 of March 1994 for the protection of information systems dealing with non-classified sensitive information defense.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

France has an officially recognized national CIRT (CERT-FR) and many others CIRT such as the commercial CIRT (CERT-DEVOTEAM) and CERT LA POSTE etc.

1.2.2 STANDARDS

France has officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards through the following instruments:

- ANSSI (National agency of IT security)
- General security referential created by the decree n° 2005-1516 of December 2005 relating electronic exchange.
- Interdepartmental Instruction n°300 of 23 June 2014 on protection against compromising emanations.
- Order n° 485 of November 2013 relating to the installation requirements.

- Order n° 495 of November 2013 concerning the TEMPEST zoning concept.

1.2.3 CERTIFICATION

The national agency of IT security (ANSSI) offers a cybersecurity framework for the certification and accreditation of national agencies and public sector professionals. ANSSI has signed various mutual recognition agreements on certificates. The certificates issued by the PKI enable official identification of the certification authorities of the French administration. They also attest to the quality of public key management practices implemented by these authorities.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

France has officially recognized an information systems defence and security policy through the national agency of IT security (ANSSI).

1.3.2 ROADMAP FOR GOVERNANCE

There is no information available regarding any national governance roadmap for cybersecurity in France.

1.3.3 RESPONSIBLE AGENCY

The national agency of IT security (ANSSI) is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap in France.

1.3.4 NATIONAL BENCHMARKING

The Observatory of internet security and resilience is the officially recognized national and sector-specific benchmarking exercise or referential used to measure cybersecurity development in France.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

The laboratories of the national agency of IT security (ANSSI) contribute to research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

The training center in the security of information systems (CFSSI) is involved in the definition and implementation of the training policy, provides training for the benefit of state's staff, and is the main contact to ANSSI for agencies in charge of training.

1.4.3 PROFESSIONAL CERTIFICATION

There is no available information regarding the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

The national CERT (CERT-FR) is the officially recognized certified government and public sector agency certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, the national agency of IT security (ANSSI) has officially recognized partnerships with the following organizations:

-German BSI

-Netherlands NLNCSA

-Agreement with Estonia on cooperation on cyberdefense

-ENISA .

-United Kingdom CESG

-United States NSA & DHS

-Franco-British agreement on defense and security cooperation.

1.5.2 INTRA-AGENCY COOPERATION

The public sector portal for the prevention of major risk is the officially recognized the following national or sector-specific program for sharing cybersecurity assets within the public sector. The portal aims to explain how to behave in different crisis situations and presents the threats to information and communication systems.

1.5.3 PUBLIC SECTOR PARTNERSHIP

The national agency of IT security (ANSSI) is the officially recognized the following national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

France is a member of:

- FIRST - NATO - EU - OSCE.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

- Article 222-32, 222-33, 226-1, 227-22 until 227-27* of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

France has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. France has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The official portal on reporting illegal content in the internet (internet-signalement.gouv.fr*) furnishes advices on internet safety for youth and parents.

2.4 REPORTING MECHANISM

Online illegal content can be reported in the website internet-signalement.gouv.fr*

Online illegal content can be reported in the website pointdecontact.net*.

CYBERWELLNESS PROFILE
GABON

BACKGROUND

Total Population: 1 564 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 9.20%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

-Draft Law on Cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

-Draft Law on Cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Gabon is currently establishing an officially recognized national CIRT. ITU conducted a CIRT assessment for Gabon in 2010.

1.2.2 STANDARDS

Gabon has an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards through the security policy of information systems.

1.2.3 CERTIFICATION

Gabon does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Gabon has an officially recognized information system security policy managed by the National Agency for Digital Infrastructure and Frequencies (ANINF).

1.3.2 ROADMAP FOR GOVERNANCE

Gabon is currently establishing a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The National Agency for Digital Infrastructure and Frequencies (ANINF) is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Gabon has officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Gabon does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Gabon does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Gabon does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Gabon does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Gabon does not have officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Gabon has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector through the AINF.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Gabon does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Gabon is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Gabon is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA).

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Articles 255 and 263* of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Gabon has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Gabon has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Gabon does not have officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Gabon does not have officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
THE GAMBIA

BACKGROUND

Total Population: 1 825 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 14.00%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation pertaining to cybercrime has been mandated through the following legal instrument:

-Information and Communications Act.

1.1.2 REGULATION AND COMPLIANCE

Gambia does not have any officially recognised regulation pertaining to cyber security.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU conducted a CIRT readiness assessment for Gambia at Dakar, Senegal in November 2011 (14-18th November 2011). Gambia does not have an officially recognized national CIRT currently.

1.2.2 STANDARDS

Gambia does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Gambia does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Gambia does not have any officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Gambia does not have any national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Gambia does not have an officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Gambia does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Gambia does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Gambia does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Gambia does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Gambia does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Gambia does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Gambia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Gambia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Gambia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Gambia is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child protection has been enacted through the following instruments:
-Information and Communications Act (Section 170 and174)

2.2 UN CONVENTION AND PROTOCOL

Gambia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Gambia has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Gambia does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Gambia does not have any officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
GEORGIA

BACKGROUND

Total Population: 4 304 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 43.10%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

-Georgia Computer System Protection Act.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

-Law on Information Security.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

The national computer incident response teams are the CERT-GOV-GE and CERT-MOD-GOV.

1.2.2 STANDARDS

Georgia has an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards through the Law on Information Security which is based on ISO 27000.

1.2.3 CERTIFICATION

The Data Exchange Agency has an officially approved national cybersecurity framework for the certification and accreditation of public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Georgia has an officially recognized national cybersecurity strategy (Cyber security strategy 2012-2015)

1.3.2 ROADMAP FOR GOVERNANCE

The Cybersecurity strategy 2012-2015 provides a national governance roadmap for cybersecurity in Georgia.

1.3.3 RESPONSIBLE AGENCY

The Data Exchange Agency is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

The Data Exchange Agency is currently working to measure the cybersecurity readiness of Georgia.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Georgia does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

The Data Exchange Agency has officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals.

1.4.3 PROFESSIONAL CERTIFICATION

Georgia has 11 public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Georgia does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Georgia does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Georgia has an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector through the Data Exchange Agency.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Georgia has an officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector through the Data Exchange Agency.

1.5.4 INTERNATIONAL COOPERATION

Georgia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. CERT-GOV-GE is a member of FIRST. Georgia also participated in the International Cyber Shield Exercise 2014 in Turkey (ICSE 2014).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

-The Criminal Code (Article 255 and 256).

2.2 UN CONVENTION AND PROTOCOL

Georgia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Georgia has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Georgia does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Georgia Computer Incident Response Team (CERT-GOV-GE) is the officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE GERMANY

BACKGROUND

Total Population: 81 991 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 83.96%

(data source: ITU Statistics 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Germany has a specific legislation pertaining to cybercrime. It is mandated through the following legal instrument:

-German Criminal Code 1998.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Electronic Signature Act 2001

-Freedom of Information Act 2013

-Act on the Federal Office for Information Security 2009

-Federal Data Protection Act 2009

-Act to Strengthen the Security of Federal Information Technology of 14 August 2009.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Germany has an officially recognized and legally mandated government CERT (CERT Bund).

1.2.2 STANDARDS

There are BSI Technical Guidelines for implementing international recognized cybersecurity standards in Germany.

1.2.3 CERTIFICATION

The approved national certification and accreditation body in Germany is the IT-Grundschutz.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

There is a Cyber Security Strategy. Also in place is the National Plan for Information Infrastructure Protection (NPSI)- these are the officially recognized national and sector-specific cybersecurity strategy in place Germany.

1.3.2 ROADMAP FOR GOVERNANCE

There is no officially recognized national or sector-specific governance roadmap for cybersecurity in Germany.

1.3.3 RESPONSIBLE AGENCY

The Federal Office for Information Security (BSI) is the officially recognized agency responsible for implementing a national cybersecurity strategy and policy.

1.3.4 NATIONAL BENCHMARKING

The BSI Annual Report is responsible for national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

The BSI has published several documents with information on topics of cybersecurity for research and development (R&D) programs/projects. Also BSI has standards for Internet security (ISi-series).

1.4.2 MANPOWER DEVELOPMENT

The officially recognized national or sector-specific educational and professional training program for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors is the IT -Grundschutz training , Germany.

1.4.3 PROFESSIONAL CERTIFICATION

Germany does not have any body responsible for educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sector.

1.4.4 AGENCY CERTIFICATION

Germany does not have any certified government or public sector agencies certified under internationally recognized standards.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is a U.S.-Germany Cyber Bilateral Meeting. This serves as a recognized partnership to facilitate sharing of cybersecurity assets across borders.

1.5.2 INTRA-AGENCY COOPERATION

There is a joint initiative between the Federal Office of Civil Protection, Disaster Assistance (BBK) and the Federal Office for Information Security (BSI) forming the Internet platform on Critical Infrastructure Protection as a framework for sharing cybersecurity assets between agencies.

1.5.3 PUBLIC SECTOR PARTNERSHIP

The BSI, Federal Association for Information Technology, Telecommunications and New Media launched a voluntary program called Alliance for Cybersecurity to inform and report on cyber incidents. The CERT-Verbund is an alliance of German security and computer emergency response teams.

1.5.4 INTERNATIONAL COOPERATION

Germany is part of the -EGC -TERENA -ENISA -FIRST -APCERT.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child protection has been enacted through the following instrument:

- Criminal Code (SS 183a, SS184b & SS238).

2.2 UN CONVENTION AND PROTOCOL

Germany has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Germany has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Germany has an officially recognized and legally mandated government CERT (CERT Bund).

2.4 REPORTING MECHANISM

Online illegal content located in Germany can be reported in the website of the Voluntary Self-Monitoring of Multimedia and Service Providers (FSM e. V. (*)).

Information on the Violation of the protection of minors can be reported in the Website of the Jugendschutz Program, founded by the Youth Ministers of all states.

The Internet Complaint Office provides online forms to file complaints.

CYBERWELLNESS PROFILE
GHANA

BACKGROUND

Total Population: 25 546 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 12.30%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Criminal Code
- Regulation of Interception of Communication Act (RICA).

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Electronic Signature Act
- Telecommunications Act
- Federal Data Protection Act
- Electronic Transactions Act
- Act on the Federal Office for Information Security.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Ghana has two national CIRTs NITA CERT under the Ministry of Communication and CERT-GH which was established by the ITU-IMPACT.

1.2.2 STANDARDS

Ghana does not have an officially recognized national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Ghana.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Ghana does not have an officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Ghana.

1.3.3 RESPONSIBLE AGENCY

The Ministry of Communication, National Information Technology Agency and Commercial Crime Unit, Criminal Investigation Department of the Ghana Police Force coordinate cybersecurity in Ghana

1.3.4 NATIONAL BENCHMARKING

There is no benchmarking or referential to measure cybersecurity development in Ghana.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no officially recognized national or sector-specific research and development program/project for cybersecurity standards, best practices and guidelines in Ghana.

1.4.2 MANPOWER DEVELOPMENT

NITA CERT trainings create security awareness within the ministries, departments and agencies and other government institutions and educate them in the area of Information Security with the latest security threats, needs and developments and deployment of techniques and tools in order to minimize security risk.

1.4.3 PROFESSIONAL CERTIFICATION

Ghana does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Ghana does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no information on any framework for sharing cybersecurity assets across borders with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Ghana does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Ghana.

1.5.4 INTERNATIONAL COOPERATION

Ghana is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Ghana participated in the:

- CCI, where the government of Ghana formalized a relationship with the Commonwealth Secretariat, adopting a Cybersecurity Strategy and signing a Memorandum of Understanding focusing on child online protection and cybersecurity schemes.

- ACCP - UNCTAD - ISS

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

-Section 124 of Children's Act, 1998 provides only a definition of child abuse.

2.2 UN CONVENTION AND PROTOCOL

Ghana has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Ghana has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Domestic Violence & Victims Support Unit, under the Ghana Police, is mandated to handle child related crimes but does not have any clear definition of online offences related to child protection.

2.4 REPORTING MECHANISM

NITA CERT provides the following email address to report computer incidents: incident@nitacert.gov.gh.

CYBERWELLNESS PROFILE

GREECE

BACKGROUND

Total Population: 11 419 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 59.87%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Penal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:
-Presidential Decree 131/2003 on eCommerce
- Law 3431/2006 on Electronic Communications
- Presidential Decree 150/2001 on Electronic Signatures

-PREFECTURE 3649/2008 National Intelligence Agency and other provisions

-PRESIDENTIAL DECREE 126/2009 Agency of the National Intelligence Service (NIS)" (Official Gazette A '173)

-Legislative Act 13 OCT 2009 Entry of National Intelligence Service (NIS) to the Minister of Citizen Protection (Official Gazette A '215)

-PREFECTURE 2225/1994 for the protection of freedom and connection and communication and other provisions

-PREFECTURE 2472/1997 Protection of Individuals with regard to the processing of personal data

-PREFECTURE 3115/2003 Assurance of confidentiality of communications

-PRESIDENTIAL DECREE 47/2005 Procedures and technical and organizational safeguards to lift the secrecy of communications and the security of

-PREFECTURE 3471/2006 Protection of personal data and privacy in the electronic communications sector and amending Law. 2472/1997.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Greece has an officially recognized national CERT known as the National Authority against Electronic Attacks (NAAEA).

1.2.2 STANDARDS

Greece does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Greece.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Greece does not have any officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Greece.

1.3.3 RESPONSIBLE AGENCY

The National Intelligence Service (EYP) is the agency responsible for cybersecurity in Greece.

1.3.4 NATIONAL BENCHMARKING

Greece does not have any benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines in Greece.

1.4.2 MANPOWER DEVELOPMENT

The Greek Cybercrime Centre (GCC) is part of an emerging coordinated European effort which has the capacity to significantly improve education and research in the newly growing area of cybercrime. As a national project, GCC seamlessly complements transnational projects such as 2CENTRE (The Cybercrime Centres of Excellence Network), and B-CCENTRE.

On a national level, GCC directly benefits the local LEAs to fight cybercrime. Greece ranks very high in reported metrics related to cybercrime infrastructure support. Thus the local LEAs are often called first to deal with cybercrime incidents and any advances in cybercrime training, research, and education provide significant benefit to them.

1.4.3 PROFESSIONAL CERTIFICATION

Greece does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Greece does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no framework in Greece to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Greece does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Greece.

1.5.4 INTERNATIONAL COOPERATION

Greece is a member of the NATO and ENISA.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Article 348A of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Greece has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Greece has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency that supports child online protection in Greece.

2.4 REPORTING MECHANISM

Online illegal content can be reported in the website of SafeLine (*).

CYBERWELLNESS PROFILE

GRENADA

BACKGROUND

Total Population: 105 000 (data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population:35.00% (data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

-Electronic Crime Act.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Electronic Transaction Act

-Interception of Communication Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU completed a CIRT assessment for Grenada in August 2012. Grenada does not have an officially recognized National CIRT.

1.2.2 STANDARDS

Grenada does not have officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Grenada does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Grenada does not have an officially recognized national cybersecurity strategy or policy.

1.3.2 ROADMAP FOR GOVERNANCE

Grenada does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The National Telecommunications Regulatory Commission (NTRC) is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Grenada does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Grenada does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Grenada does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Grenada does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Grenada has one public agency (National Defense University) certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Grenada does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Grenada does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Grenada does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Grenada is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

Grenada is among the beneficiary countries of the EU/ITU co-funded project “Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures” (HIPCAR).

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-The Criminal Code (Section 133(e) and 203A).

2.2 UN CONVENTION AND PROTOCOL

Grenada has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Grenada has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Grenada does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Grenada does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE GUATEMALA

BACKGROUND

Total Population: 15 138 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 19.70%

(data source: ITU Statistics, 2013)

1 CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Guatemala does not have specific legislation on cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Guatemala does not have specific legislation and regulation related to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Guatemala has an officially recognized national CIRT (CSIRT-GT).

1.2.2 STANDARDS

Guatemala does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Guatemala does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Guatemala does not have an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Guatemala does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Guatemala does not have an officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Guatemala has officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development. In 2014, with the support of OAS, CSIRT-GT organized a benchmarking exercise on multiple sectors.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Guatemala has officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector. This is mandated through the 4055 bill which was passed in the congress.

1.4.2 MANPOWER DEVELOPMENT

Guatemala does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

However CSIRT-GT has promoted training course with the support of OAS, public sector professionals.

1.4.3 PROFESSIONAL CERTIFICATION

Guatemala has 4 public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Guatemala does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Guatemala does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Guatemala does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Guatemala does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Guatemala is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Guatemala also participated in multiple cybersecurity events promoted by the OAS (CICTE) and Council of Europe.

CSIRT-GT is a member of FIRST.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

Articles 188-192, 194, 195bis, 195ter, 195quinquies* of the Criminal Code, reformed and added by the Decree n. 9*, February 2009

Article 56* of the Decree n. 27 - Law for the Comprehensive Protection of Childhood and Adolescence, June 2003.

2.2 UN CONVENTION AND PROTOCOL

Guatemala has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Guatemala has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Guatemala does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Guatemala does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

GUINEA

BACKGROUND

Total Population: 10 481 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 1.60%

(data source: ITU Statistics, 2013)

1 CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

The ECOWAS legislation is being transposed into Guinean legal system. However specific legislation pertaining to cybercrime has already been mandated through the following legal instrument:

-The Penal Code.

1.1.2 REGULATION AND COMPLIANCE

Guinea does not have any officially recognized national regulation pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Guinea does not have any officially recognized national CIRT.

1.2.2 STANDARDS

Guinea does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity.

1.2.3 CERTIFICATION

Guinea does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Guinea is in the process of drafting an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Guinea is in the process of drafting an officially recognized national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The Agence Nationale de la Gouvernance Electronique et de l'Informatisation de l'Etat (ANGEIE) is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap. However there is a committee working on cybersecurity strategy.

1.3.4 NATIONAL BENCHMARKING

Guinea does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Guinea does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Guinea does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Guinea does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Guinea does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Guinea does not have officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Guinea does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Guinea does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Guinea is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Guinea is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Guinea does not have any national legislation pertaining to child online protection.

2.2 UN CONVENTION AND PROTOCOL

Guinea has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Guinea has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Guinea does not have any officially recognized agencies that offer institutional support on child online protection.

2.4 REPORTING MECHANISM

Guinea does not have any officially recognized agencies that offer an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
REPUBLIC OF GUINEA-BISSAU

BACKGROUND

Total Population: 1 580 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 3.10%

(data source: ITU Statistics, December 2013)

1 CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- None.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- None.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Guinea-Bissau does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Guinea-Bissau does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Guinea-Bissau.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Guinea-Bissau does not have an officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Guinea-Bissau.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Guinea-Bissau.

1.3.4 NATIONAL BENCHMARKING

Guinea-Bissau does not have an officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Guinea-Bissau does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Guinea-Bissau.

1.4.3 PROFESSIONAL CERTIFICATION

Guinea-Bissau does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Guinea-Bissau does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Guinea-Bissau does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Guinea-Bissau does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Guinea-Bissau.

1.5.4 INTERNATIONAL COOPERATION

Guinea-Bissau is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- None

2.2 UN CONVENTION AND PROTOCOL

Guinea-Bissau has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Guinea-Bissau has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Guinea-Bissau.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Guinea-Bissau.

CYBERWELLNESS PROFILE

CO-OPERATIVE REPUBLIC OF GUYANA

BACKGROUND

Total Population: 758 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 33.00%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-None.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-None.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Guyana has an officially recognized national CIRT known as GNCIRT.

1.2.2 STANDARDS

Guyana does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Guyana.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Guyana does not have any officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Guyana.

1.3.3 RESPONSIBLE AGENCY

GNCIRT and the Criminal Investigations Department of the Guyana Police Force are the agencies responsible for cybersecurity in Guyana.

1.3.4 NATIONAL BENCHMARKING

Guyana does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Guyana does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Guyana.

1.4.3 PROFESSIONAL CERTIFICATION

Guyana does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Guyana does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Guyana does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Guyana does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Guyana.

1.5.4 INTERNATIONAL COOPERATION

Guyana is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Guyana is also a member of the OAS-CICTE.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Section 351 of the Criminal Law Offences Act – *does not explicitly criminalize child pornography but only indecent or obscene material.*

- Sections 11 to 13 and 21 of the Sexual Offences Act of 2010.

2.2 UN CONVENTION AND PROTOCOL

Guyana has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Guyana has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Child Care and Protection Agency was created by the government, under the Ministry of Labor, Human Services and Social Security, and is responsible for child protection.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Guyana.

CYBERWELLNESS PROFILE
REPUBLIC OF HAITI

BACKGROUND

Total Population: 10 256 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 10.60%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- None.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- None.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Haiti does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Haiti does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Haiti.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Haiti does not have an officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Haiti.

1.3.3 RESPONSIBLE AGENCY

The central Directorate of the Judicial Police (Direction Centrale de la Police Judiciaire –DCPJ) takes the lead on investigating identified cyberattacks.

1.3.4 NATIONAL BENCHMARKING

Haiti does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Haiti does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

Some Haitian academic institutions offer course work in cybersecurity or related topics. In conjunction with the national e-Governance Coordinator, the telecommunication authority CONATEL has undertaken an awareness raising campaign consisting of a series of events to inform decision-makers and other national stakeholders and assess opportunities to combat cyber and IT related vulnerabilities and crime.

1.4.3 PROFESSIONAL CERTIFICATION

Haiti does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Haiti does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Haiti does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Haiti does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Haiti. There is some degree of informal and unofficial cooperation between the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Haiti is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Haiti is also a member of the OAS-CICTE.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

- Article 282 of the Criminal Code – forbids molestation not pornography, for people under 21.

2.2 UN CONVENTION AND PROTOCOL

Haiti has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Haiti has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Haiti.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Haiti.

CYBERWELLNESS PROFILE
REPUBLIC OF HONDURAS

BACKGROUND

Total Population: 7 912 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 17.80%

(data source: ITU Statistics, December 2013)

1.**CYBERSECURITY**

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- None.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- None.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Honduras does not have an officially recognized national CIRT. A CIRT readiness assessment was conducted for Honduras by ITU in 2012.

1.2.2 STANDARDS

Honduras does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Honduras.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Honduras does not have an officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Honduras.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Honduras.

1.3.4 NATIONAL BENCHMARKING

Honduras does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Honduras does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Honduras.

1.4.3 PROFESSIONAL CERTIFICATION

Honduras does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Honduras does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Honduras does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Honduras does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Honduras.

1.5.4 INTERNATIONAL COOPERATION

Honduras is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Articles 148, 149, 149B, 149D* of the Criminal Code

- Article 134(c)* of the Decree n. 73 – Code for Childhood and Adolescence, September 1996.

2.2 UN CONVENTION AND PROTOCOL

Honduras has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Honduras has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Center for Investigation of Cybercrimes, under the Public Ministry, is responsible for the investigation of sexual commercial exploitation of children.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Honduras.

CYBERWELLNESS PROFILE
HONG KONG

BACKGROUND

Total Population: 7 155 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 74.20%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Crime Ordinance -Theft Ordinance

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Personal Data (Privacy) Ordinance -Electronic Transactions Ordinance

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Hong Kong has an officially recognized CIRT (HKCERT).

1.2.2 STANDARDS

The Baseline IT Security Policy (S17) is an officially-approved cybersecurity framework for all government departments in Hong Kong. The Policy was developed by making reference to International security standards such as ISO 27001. In addition, the Hong Kong Monetary Authority (HKMA) has officially issued the Supervisory Policy Manual on "Supervision of e-banking". In developing the manual, HKMA has taken into consideration supervisory approach and guidance of the international regulatory community, particularly those recommended by the Basel Committee on Banking Supervision.

1.2.3 CERTIFICATION

The Hong Kong Certification Body Accreditation Scheme (HKCAS), operated under the auspices of the Hong Kong Accreditation Service (HKAS), offers accreditation to certification bodies for information security management system (ISMS) certification.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Hong Kong has an officially recognized national cybersecurity policy (Baseline IT Security Policy)

1.3.2 ROADMAP FOR GOVERNANCE

Hong Kong has a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The Information Security Management Committee is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Hong Kong does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development. However HKCERT is producing statistics on number of incident reports received and number of alerts issued annually so as to provide a reference on the local trend on cybersecurity.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

The OGCIO continues to review and enhance the Government IT security related requirements to ensure that they tie in with the advancement of technology, the local and global security trends and the development of international/industry practices in information security management such as the ISO27001, ISO27002, COBIT, etc., as well as changes in Government's information security development.

Cybersecurity best practices and guidelines are published on the one-stop portal INFOSEC for reference by the public

1.4.2 MANPOWER DEVELOPMENT

To raise public awareness on information security and strengthen the protection of their computers from cyber-attacks, annual campaigns covering contemporary topics have been organized in Hong Kong since 2005. Every year, Hong Kong organizes seminars, conferences, competition events to raise public awareness to protect their computer assets and be mindful on suspicious cyber-attacks with a view to "Build a Secure Cyber Space". Hong Kong also disseminates security alerts, news and tips through the one-stop portal INFOSEC website, as well as promotes security awareness through posters, leaflets and radio clips.

1.4.3 PROFESSIONAL CERTIFICATION

Hong Kong has 1434 professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Hong Kong has 32 certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Hong Kong have officially recognized partnerships with the following organizations:

-ITU -APCERT -APEC

-Interpol.

1.5.2 INTRA-AGENCY COOPERATION

The Internet Infrastructure Liaison Group (IILG) was established by the OGCIO in 2005 to maintain close liaison with Internet infrastructure stakeholders and strive in collaboration with the stakeholders to the healthy operation of the Internet infrastructures of Hong Kong. The IILG is chaired by Deputy Government Chief Information Officer (Consulting and Operations). Members of the IILG including OGCIO, HKCERT, Hong Kong Internet Registration Corporation Limited (HKIRC), Hong Kong Internet Service Providers Association (HKISPA), Hong Kong Police Force (HKPF), and Office of the Communications Authority (OFCA).

The cybersecurity Security Centre (CSC) under the Technology Crime Division of Commercial Crime Bureau of the Hong Kong Police Force has started its operation since 7 December 2012. The CSC was for enhancing the protection of critical infrastructures and strengthening the resilience against cyber- attacks in Hong Kong.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Hong Kong has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector through the Internet Infrastructure Liaison Group (described above).

Furthermore, an Expert Group on Cloud Computing Services and Standards (EGCCSS) was established by the OGCIO in 2012. The objectives of the EGCCSS are to draw expertise from the industry, academia, community and Government to facilitate and drive cloud computing adoption and deployment in Hong Kong, as well as facilitate expert exchanges among cloud experts. EGCCSS includes three working groups, namely Working Group on Cloud Computing Interoperability Standards (WGCCIS), Working Group on Cloud Security and Privacy (WGCSP) and Working Group on Provision and Use of Cloud Services (WGPUCS).

1.5.4 INTERNATIONAL COOPERATION

Hong Kong, China participates in various meetings under APEC, including APEC TEL (Telecommunications and Information Working Group). Under APEC TEL, our delegates participate in meetings and activities of the Security and Prosperity Steering Group (SPSG).

HKCERT is a member of FIRST. Since 1990, its members have resolved an almost continuous stream of security-related attacks and incidents including handling thousands of security vulnerabilities affecting nearly all of the millions of computer systems and networks throughout the world connected by the ever growing Internet.

HKCERT is a member of FIRST

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Hong Kong does not have specific legislation on child online protection.

2.2 UN CONVENTION AND PROTOCOL

Hong Kong has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Hong Kong has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Hong Kong Computer Incident Response Team (CIRTHong Kong) is the officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Hong Kong Computer Incident Response Team (CIRTHong Kong) is the officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
HUNGARY

BACKGROUND

Total Population: 9 950 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 72.64%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Criminal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Act No CVIII/2001 on Electronic Commerce and Information Society Services

-Act No C/2003 on Electronic Communications

-Act No. XC/2005 on the Freedom of Information by Electronic means

-Act No. LXIII of 1992 on the Protection of Personal Data and Disclosure of Data of Public Interest Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary

-Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies

-Act No. XXXV/2001 on Electronic Signatures.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Hungary has an officially recognized national government CERT (GovCERT-Hungary) and other specialized CERTs such as CIP CERT (operated by General Directorate for National Catastrophe Management).

1.2.2 STANDARDS

Hungary has an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standard through the Infosec and Crypto Division that performs official approval, monitoring and control functions regarding electronic systems handling classified information, operated and managed by governmental organizations and companies.

1.2.3 CERTIFICATION

Hungary has officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals through the Product Certification Division. The Division has been working on the establishment of the legal framework of the certification authority related activities, such as information and physical security assessments, certification of hardware and software components applied during classified information handling - in close cooperation with professionals of the security protection industry.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Hungary has an officially recognized National Cybersecurity Strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Hungary has a national governance roadmap for cybersecurity through the National cybersecurity Action Plan.

1.3.3 RESPONSIBLE AGENCY

Hungary has officially recognized the following agencies responsible for implementing a national cybersecurity strategy, policy and roadmap.

- National Cybersecurity Coordination Council (Prime Minister's Office, national coordination)

- Cybersecurity Authority (Ministry of National Development, assessment and supervision)

- National Security Office (Ministry of Public Administration and Justice, vulnerability handling by request)

- National Electronic Information Security Authority (NEISA).

1.3.4 NATIONAL BENCHMARKING

The National Electronic Information Security Authority (NEISA) is the officially recognized national or sector-specific benchmarking exercise or referential used to measure cybersecurity development. NEISA works on the annual audit plan, annual and ad-hoc reports to the Government on IT system security and critical infrastructure cybersecurity.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

The National Electronic Information Security Authority (NEISA) is the officially recognized national or sector-specific research and development (R&D) program/project for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

The International Children's Safety Service (ICSS) coordinates the project and serves as its national awareness center; the Kék Vonal Child Crisis Foundation manages Hungary's national helpline and the Theodore Puskas Foundation hosts the National Cyber Security Centre, CERT-Hungary and, since 2011, runs the Biztonsagosinternet hotline.

The national Electronic Information Security Authority (NEISA) participates in certain National Cybersecurity Coordination Council workgroups, especially in those informing IT system users, aimed at students of primary and secondary education by collecting, merging and re-publishing related materials.

1.4.3 PROFESSIONAL CERTIFICATION

The national government CERT (GovCERT-Hungary)'s team is certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

The national government CERT (GovCERT-Hungary) is officially the government and public sector agency certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Hungary has officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states through the NSA HU division which is responsible for preparing and coordinating negotiations about bi- and multilateral agreements on the exchange and mutual protection of classified information, as well as organizing international events. The division is initiating the national security inspection of persons resident in Hungary at the request of foreign authorities.

1.5.2 INTRA-AGENCY COOPERATION

Hungary has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector through the national Electronic Information Security Authority (NEISA).

1.5.3 PUBLIC SECTOR PARTNERSHIP

Hungary has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector through the Information and Cyber Security conference (ISCD). The fourth ISCD Information and Cyber Security conference organized by the Hungarian National Security Authority was held in Budapest on 8-9 September 2014. The conference touched upon the current issues of cyber security and discussed the means of cooperation between NGOs and the State.

1.5.4 INTERNATIONAL COOPERATION

Hungary is signatory to Council of Europe Convention on Cybercrime and is part of the following organizations:

- EU - NATO - OSCE - UN.

The NSA HU is representing the national interests by an active and persistent attendance at various NATO and EU committees and working groups. The division is responsible for coordinating this international attendance.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

- Section 208 of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Hungary has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Hungary has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Hungary does not have any officially recognized agency that offers intuitional support on child online protection.

2.4 REPORTING MECHANISM

The National Media and Infocommunications Authority (*) has developed the Internet Hotline website (*) where online content which is unlawful or detrimental to minors can be reported.

Illegal and harmful online content can be reported at the website (*) created by the Theodore Puskas Foundation

Computer incidents can be reported to the following email address of the National Cybersecurity Center (*): cert@cert-hungary.hu.

CYBERWELLNESS PROFILE

ICELAND

BACKGROUND

Total Population: 328 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 96.55%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Penal Code
- Cybercrime Law.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Information Act
- Data Protection Act
- Act on Electronic Signatures
- Electronic Communications Act
- Act on Electronic Commerce and other Electronic Services
- Regulation on the Protection of Information on Public Communications Networks
- Regulation on Protection, Functionality, and Quality of IP Communications Services.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Iceland has an officially recognized national CIRT known as CERT-IS.

1.2.2 STANDARDS

There is no officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Iceland does not have an officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Iceland.

1.3.3 RESPONSIBLE AGENCY

The following organizations are responsible for cybersecurity in Iceland:

- Ministry of Interior
- The Post
- Telecom Administration
- The Icelandic Police
- The Data Protection Authority.

1.3.4 NATIONAL BENCHMARKING

Iceland does not have an officially recognized national benchmarking or referential to measure cybersecurity.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no *officially* recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines in Iceland.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Iceland.

1.4.3 PROFESSIONAL CERTIFICATION

Iceland does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Iceland does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Iceland participates in the Nordic defense cooperation (NORDEFCO).

1.5.2 INTRA-AGENCY COOPERATION

Iceland does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Iceland.

1.5.4 INTERNATIONAL COOPERATION

Iceland participates in the following international cybersecurity platforms:

- NATO CCDCOE - OECD - Council of Europe Convention on Cybercrime.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Article 210 of the Criminal Code

- Article 1(5) of the Act on the Monitoring of Children's Access to Films and Computer Games.

2.2 UN CONVENTION AND PROTOCOL

Iceland has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Iceland has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no institution responsible for the protection of children online in Iceland.

2.4 REPORTING MECHANISM

The website of Save the Children Iceland provides an online form to report illegal content.

CYBERWELLNESS PROFILE

INDIA

BACKGROUND

Total Population: 1 258 351 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 15.1%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- The Indian Penal Code
- Information Technology Act.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Information Technology Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

The officially recognized national CIRT is known as CERT-IN.

1.2.2 STANDARDS

In India to enable comprehensive cyber security policy compliance, the government mandated implementation of security policy within government agencies in accordance with the Information Security Management System (ISMS) Standard ISO 27001. Computer Security Guidelines have been issued for compliance within government and are being circulated to all departments and ministries. Cyber security drills are being conducted to assess preparedness for critical organisations. The Five Year Plan on Information Security also states guides on standards.

1.2.3 CERTIFICATION

India does not have any officially approved national or sector specific cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals. However it has in place the Information Security Management System (ISMS) Standard ISO 27001.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

India has an officially recognized National Cyber Security Policy (NCSP).

1.3.2 ROADMAP FOR GOVERNANCE

India has a national governance roadmap for cybersecurity through the Five Year Plan on Information Security.

1.3.3 RESPONSIBLE AGENCY

The Department of Electronics and Information Technology and Ministry of Communications and Information Technology are the officially recognized agencies responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

As a means of benchmarking and referential to measure cybersecurity development, security auditors have been empanelled to conduct security audits including vulnerability assessment, penetration testing of computer systems and networks of various organizations of the government, critical infrastructure organizations and those in other sectors of the Indian economy.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Nation-wide Information Security Education and Awareness Programmes have been implemented to create necessary cyber security awareness through formal and informal programmes. This is the officially recognized national or sector-specific research and development (R&D) program/project for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector. A number of other R&D projects have been supported at premier academic and R&D institutions in the identified Thrust Areas like cryptography and cryptanalysis, steganography, network and systems security assurance, network monitoring, cyber forensics and capacity development in the area of cyber security.

1.4.2 MANPOWER DEVELOPMENT

Cyber security training facilities have been set up to provide training for law enforcement agencies and facilitate cyber-crime investigation. CERT-IN in collaboration with CII, NASSCOM and Microsoft has created PortalSecureYourPc.in to educate consumers on cyber security issues. Training centers have been set up at CBI, Ghaziabad and Kerala Police to facilitate advanced training in cyber-crime investigation. 94 training programs have been conducted by CERT-IN on specialized Cyber Security topics in which 3392 people have been trained.

1.4.3 PROFESSIONAL CERTIFICATION

There is no statistics showing how many professionals in India are certified under internationally recognized certification.

1.4.4 AGENCY CERTIFICATION

Controller of Certifying Authority (CCA) has licensed seven Certifying Authorities (CA).

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, specific cyber security cooperation agreements were signed with US, Japan and South Korea. India participated in cyber security drills of US (Cyber Storm III). CERT-IN experts helped in establishment of CERT-Mauritius.

1.5.2 INTRA-AGENCY COOPERATION

There is no officially recognized national program that supports the sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

As part of national level cooperation, cyber security awareness programs were organized in cooperation with industry associations – CII, NASSCOM-DSCI.

1.5.4 INTERNATIONAL COOPERATION

India is a member of the ITU-IMPACT initiative and has access to its relevant cybersecurity services. India is also a member of the UN Committee of Group of Experts as well as in the Council of Security Cooperation in Asia-Pacific (CSCAP) for enhancing cooperation in the area of Cyber Security.

India participates in the following:

- APCERT -FIRST -APWG

CERT-IN is a member of FIRST.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Sections 67, 67A and 67B of the Information Technology (Amendment) Act.

-Section 20 of the Protection of Children from Sexual Offences Bill.

2.2 UN CONVENTION AND PROTOCOL

India has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. India has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography

2.3 INSTITUTIONAL SUPPORT

India does not have an officially recognized agency that offers institutional support to child online protection.

2.4 REPORTING MECHANISM

A security incident report can be filled in the website of CERT-IN which also makes available the phone number (+91) 1800 11 4949 and the email address incident@cert-in.org.in.

CYBERWELLNESS PROFILE

INDONESIA

BACKGROUND

Total Population: 2 44 769 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 15.82%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:
-Law of The Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transaction (Articles 29-37)

1.1.2 REGULATION AND COMPLIANCE

Indonesia has officially recognized regulations regarding cybersecurity and compliance requirements through the following instruments:

- Government Regulation of The Republic of Indonesia Number 82 of 2012 concerning Implementation of Electronic Systems and Transactions

- SNI/ISO/EIC 27001: 2013, Information Security Management System

- National Information Security Index (Index KAMI)

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Indonesia has officially recognized national and sector specific CIRT such as:

Gov-CERT
ID-SIRTII
ID-CERT
Academic CERT.

1.2.2 STANDARDS

Indonesia has not yet officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Indonesia does not currently have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Indonesia does not currently have an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Indonesia does not currently have an officially recognized national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The Directorate of Information Security, the Directorate General of Informatics Applications and the Ministry of Communication and Information Security are the officially recognized agencies responsible for implementing a national cybersecurity strategy, policy and roadmap in Indonesia.

1.3.4 NATIONAL BENCHMARKING

Indonesia does not currently have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development. However the current measurement is based on the National Information Security Index (Index KAMI).

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Indonesia does not currently have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

The Directorate of Information Security and Ministry of Communication & Information Technology conducts awareness-raising and technical assistance programs that provide educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Indonesia has approximatively 500 public sector professionals certified under internationally recognized certification programs in cybersecurity such as ISO270001, CEH, CISA, CISM and CISSP.

1.4.4 AGENCY CERTIFICATION

Indonesia has six certified government institutions certified under internationally recognized standards in cybersecurity such as ISO270001.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders with other nation states Indonesia has officially recognized partnerships with the National Information Security Council (NISC) of Japan.

1.5.2 INTRA-AGENCY COOPERATION

Indonesia is in the process of recognizing national or sector-specific programs for sharing cybersecurity assets within the public sector as they are developing national government security monitoring center.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Indonesia is in the process of recognizing national or sector-specific programs for sharing cybersecurity assets within the public and private sector as they are developing national government security monitoring center.

1.5.4 INTERNATIONAL COOPERATION

Indonesia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Indonesia participated in several cybersecurity activities with the following organizations/forums:

-FIRST -AP-CERT -ASEAN-Japan expert cybersecurity Forum,

-Indonesia-JAPAN Bilateral Cybersecurity Forum -Internet Governance Forum

-ASEAN Network Security Council (ANSAC) Working Group

-World Conference on International Communication.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child protection has been enacted through the following instruments:

-Article 295(1)2nd of the Criminal Code.

-Articles 4, 5, 8-11, 18, 19, 29-32, 37 and 38* of the Law number 44 of 2008 about Pornography.

2.2 UN CONVENTION AND PROTOCOL

Indonesia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Indonesia has signed and ratified, with no declarations or reservations to articles 2 and 3, the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Indonesia does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Indonesia does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

IRAN

BACKGROUND

Total Population: 75 612 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 31.40%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Computer Crimes Law.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

- Electronic Commerce Law of Islamic Republic of Iran.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Iran has an officially recognized national CIRT known as CERTCC MAHER.

1.2.2 STANDARDS

Iran does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Iran does not have any cybersecurity framework for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Iran has a comprehensive cybersecurity strategy that includes the creation of what it calls a “national information network” that could disconnect most of Iran from the global internet.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Iran.

1.3.3 RESPONSIBLE AGENCY

There following agencies are responsible for overseeing cybersecurity activities in Iran:

- BASIJ
- IRGC
- Ministry of ICT
- Iran’s Passive Defense Organization
- Information Technology Organization of Iran.

1.3.4 NATIONAL BENCHMARKING

Iran does not have any officially recognized national benchmarking or referential for measuring cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no information on any program or project for research and development of cybersecurity standards, best practices and guidelines in Iran.

1.4.2 MANPOWER DEVELOPMENT

ASIS Cyber Security Contest was created to raise cybersecurity awareness in Iran.

1.4.3 PROFESSIONAL CERTIFICATION

Iran does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Iran does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no information on any framework for sharing cybersecurity assets across borders with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Iran does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Iran.

1.5.4 INTERNATIONAL COOPERATION

Iran is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Iran is also a member of the OIC-CERT.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

No specific legislation on child online protection has been enacted.

2.2 UN CONVENTION AND PROTOCOL

Iran has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Iran has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Information Technology and Digital Media Development Center, under the Ministry of Culture and Islamic Guidance (*), is responsible for online safety at the government level. In 2010, the Information Technology and Digital Media Development Center has produced two publications regarding online safety (available in Farsi): one directed at parents*, another directed at children*.

2.4 REPORTING MECHANISM

CERTCC MAHER displays a space for reporting an incident, but it was not working as of 05th May 2014. The child helpline SPRC Sedaye Yara can be contacted at the number: 88531109**. The Helping Voice helpline can also be contacted: +98-21-850 1414 or +98-21-850 1415.**

CYBERWELLNESS PROFILE
REPUBLIC OF IRAQ

BACKGROUND

Total Population: 33 703 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 9.20%

(data source: ITU Statistics, December 2013)

1 CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Cyber Crime law in Iraq revoked.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-None.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Iraqi ministry of communications attended a four-day comprehensive capacity building programme (a security core and CIRT training) with ITU-IMPACT. There is still no nationally recognized CERT in Iraq.

1.2.2 STANDARDS

Iraq does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Iraq.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Iraq has made some effort to form a higher committee for cybersecurity.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Iraq.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Iraq.

1.3.4 NATIONAL BENCHMARKING

Iraq does not have any benchmarking or referential for measuring cybersecurity.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There is no educational and professional training program for raising awareness, higher education and certification.

1.4.3 PROFESSIONAL CERTIFICATION

Iraq does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Iraq does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Iraq does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Iraq.

1.5.4 INTERNATIONAL COOPERATION

Iraq is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:
-None.

2.2 UN CONVENTION AND PROTOCOL

Iraq has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Iraq has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Iraq.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to receiving reports of incidents.

CYBERWELLNESS PROFILE
IRELAND

BACKGROUND

Total Population: 4 579 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 78.25%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Criminal Justice (Theft and Fraud Offences) Act 2001.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Data Protection Act
- Electronic Commerce Act
- Freedom of Information Act
- Freedom of Information (Amendment) Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Ireland has an officially recognized national CIRT known as IRISS-CERT.

1.2.2 STANDARDS

Ireland does not have an officially recognized national and sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Ireland.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Ireland does not have any officially recognized national and sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Ireland.

1.3.3 RESPONSIBLE AGENCY

There is no information about any agency responsible for cybersecurity in Ireland.

1.3.4 NATIONAL BENCHMARKING

Ireland does not have any officially recognized national benchmarking or referential for cybersecurity.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

IRISS-CERT organizes conferences such as the Cyber Crime Conference annually. IRISS-CERT also hosts Ireland's Premier Cyber Security Challenge. UCD Centre for Cybersecurity and Cybercrime Investigation (CCI) is a unique, world-class education and research Centre with strong and well-established collaborative relationships with law enforcement and industry.

1.4.3 PROFESSIONAL CERTIFICATION

Ireland does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Ireland does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no framework for sharing cybersecurity assets across borders with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Ireland does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Ireland.

1.5.4 INTERNATIONAL COOPERATION

There is no record of Ireland being involved in any international cooperation.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

- Section 4-6 of the Child Trafficking and Pornography Act.

2.2 UN CONVENTION AND PROTOCOL

Ireland has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Ireland has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Irish Office for Internet Safety provides information on internet safety for parents and children.

2.4 REPORTING MECHANISM

Suspected online illegal content can be reported to the website of Irish internet Hotline. Online illegal content can be reported in the website of the Irish Office for Internet Safety.

CYBERWELLNESS PROFILE
ISRAEL

BACKGROUND

Total Population: 7 695 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 70.80%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Computer Law 1995.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Electronic Signature Law
- E-commerce Bill
- The 'Regulation of Security in Public Bodies Act of 1998'
- Communications Bill (Amendment - Duty to filter harmful websites)
- Communications Bill (Amendment - Sites and harmful content on the Internet)
- Israel resolved (in Resolution 84/b) to determine the areas of responsibility for protecting computerized systems
- Resolution 3611 "Advancing the national capacity in cyberspace" of August 2011 adopted the recommendations of the "National Cyber Initiative.
- Special Resolution B/84 on 'The responsibility for protecting computerized systems in Israel.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Israel has an officially recognized national CIRT (CERT GOVIL) and an academic network CERT (IUCC-CERT).

1.2.2 STANDARDS

There is no available information regarding any officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

The Standards Institution of Israel offers a cybersecurity framework for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Israel has officially recognized a cybersecurity policy based on two major official milestones. The first of two has been the 2010 "National Cyber Initiative", aiming for Israel to become global cyber superpower by 2015. The second milestone is the Government of Israel's Government Resolution No. 3611 as of August 7, 2011 adopting recommendations for the "National Cyber Initiative".

1.3.2 ROADMAP FOR GOVERNANCE

The Israel's government Resolution No. 3611 provides the national governance roadmap for cybersecurity in the Israel.

1.3.3 RESPONSIBLE AGENCY

There are two regulators that monitor and coordinate the implementation of a national cybersecurity strategy, policy and roadmap in Israel: 'The top steering committee for the protection of computerized systems in the State of Israel,' and 'the national unit for the protection of vital computerized systems.' While the steering committee has a policy perspective, the 'national unit' - National Information Security Authority (NISA) - has the professional authority.

1.3.4 NATIONAL BENCHMARKING

The Israel National Cyber Bureau (INCB) is the officially recognized national or sector-specific benchmarking exercise or referential used to measure cybersecurity development as it is working towards the establishment of a national cyber situation assessment and the definition of the national cyber threat reference.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

The Israel National Cyber Bureau (INCB) is the officially recognized national or sector-specific research and development (R&D) program/project for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector as it publishes various "warnings" and "preventive practices" and programs to prioritize the cyber defense industry, in cooperation with the Chief Scientist of the Ministry of Industry, Trade and Labor.

1.4.2 MANPOWER DEVELOPMENT

The Israel National Cyber Bureau (INCB) will provide various types of educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors such as the "national education plans", commonly aimed at "increasing public awareness" to cyber threats. The INCB also established a committee for the definition of the cyber professions.

1.4.3 PROFESSIONAL CERTIFICATION

There is no available information regarding the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Israeli national CIRT (CERT GOVIL) and the academic network CERT (IUCC-CERT) are the officially recognized certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

The INCB coordinates national and international exercises as well as cooperation with parallel bodies abroad. The Bureau acts to develop foreign relations in the cyber field with friendly countries for various purposes such as information sharing, mutual R&D and more.

1.5.2 INTRA-AGENCY COOPERATION

The Israel National Cyber Bureau (INCB) is the officially recognized national program for sharing cybersecurity assets within the public sector. The INCB advances coordination and cooperation between governmental bodies, the defense community, academia, industrial bodies, business and other bodies relevant to the cyber field.

1.5.3 PUBLIC SECTOR PARTNERSHIP

The Israel National Cyber Bureau (INCB) is the officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector. The INCB promotes cybersecurity within the civilian and private sectors, in cooperation with other government offices.

1.5.4 INTERNATIONAL COOPERATION

Israel is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Also the Israel National Cyber Bureau (INCB) coordinates national and international exercises as well as cooperation with parallel bodies abroad.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

-Article 214 of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Israel has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Israel has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The following supports provide information on internet safety for parents, children and educators:

- The Ministry of Education (*) offers different tools for parents, teachers and children about online safety.

- The website http://safe.org.il/ provides information on safe internet for parents, children and educators.

- The IUCC Computer Emergency Response Team (IUCC CERT) is responsible for Israeli cybersecurity in higher education. It has no specific information on child online protection.

2.4 REPORTING MECHANISM

The academic network CERT (IUCC-CERT) provides the following email address to report a computer incident: cert@cert.ac.il.

Also the website ISOC-IL provides an online reporting form.

CYBERWELLNESS PROFILE

ITALY

BACKGROUND

Total Population: 60 964 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 58.46%

(data source: ITU Statistics, 2013)

1 CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

-Penal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Law on Electronic Commerce -Law on Electronic Communications -Law on Electronic Signatures.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

The Ministry of Economic Development has been mandated by the Legislative Decree n.70, May 28th 2012, which transposes the 2009/140/EC Directive, to implement the national CERT (CERT-SPC).

1.2.2 STANDARDS

Italy does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Italy does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Italy has an officially recognized national cybersecurity strategy through the National Strategic Framework for Cyberspace Security.

1.3.2 ROADMAP FOR GOVERNANCE

The National Plan for Cyberspace Protection and ICT Security provides a national governance roadmap for cybersecurity in Italy.

1.3.3 RESPONSIBLE AGENCY

The Presidency of the Council of the Ministers is the officially recognized organization responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Italy does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Italy has officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines through the National Plan for Cyberspace Protection and ICT Security.

1.4.2 MANPOWER DEVELOPMENT

Italy has officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals through the National CERT(CERT-SPC-C) and CNAIPIC (National Anti-Crime Computer Centre for Critical Infrastructure Protection).

1.4.3 PROFESSIONAL CERTIFICATION

Italy does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

The Body of Information Security Certification (OCSI) certifies government and public sector agencies under internationally recognized standards in cybersecurity. However they are no exact numbers of public agencies being certified.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Italy has an officially recognized partnership with Israel to facilitate sharing of cybersecurity assets across borders.

1.5.2 INTRA-AGENCY COOPERATION

The Guideline for National Cybersecurity mandates the sharing of cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Italy has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector through the National Plan for Cyberspace Protection and ICT Security.

1.5.4 INTERNATIONAL COOPERATION

Italy is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Italy also participates in the Network and Information Security Platform (NIS Platform), established by the European Commission. The output of the platform will feed into the Commission recommendations on cybersecurity. Italy participated in the International Cyber Shield Exercise 2014 in Turkey (ICSE 2014).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-The Criminal Code (Article 600 and 609).

2.2 UN CONVENTION AND PROTOCOL

Italy has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Italy has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Italy Computer Incident Response Team (CERT-SPC-C) is the officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

The Stop-it website provides links to report child online pornography. Telefono Azzuro also provides forms to report illegal content.

CYBERWELLNESS PROFILE

JAMAICA

BACKGROUND

Total Population: 2 761 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 37.80%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Cybercrimes Act.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

- Electronic Transactions Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

The Jamaican government in collaboration with ITU is in the process of establishing a national CIRT to assist in the protection of Jamaica's online cyber infrastructure.

1.2.2 STANDARDS

There is no officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards in Jamaica.

1.2.3 CERTIFICATION

There is no framework for the certification and accreditation of national agencies and public sector professionals in Jamaica.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

There is a draft National Cybersecurity Strategy to be launched soon.

1.3.2 ROADMAP FOR GOVERNANCE

There is no governance roadmap for cybersecurity in Jamaica.

1.3.3 RESPONSIBLE AGENCY

The following agencies are responsible for the cybersecurity in Jamaica:

- Constabulary Force (JCF)
- The Ministry of Science, Technology, Energy and Mining (MSTEM)
- Communication Forensic and Cybercrime Unit (CFCU) of the Jamaica.

1.3.4 NATIONAL BENCHMARKING

There is no benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no *officially* recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines in Jamaica.

1.4.2 MANPOWER DEVELOPMENT

The National Cybersecurity Task Force (NCSTF) is tasked with assisting in creating a framework to build confidence in the use of cyberspace and the protection and security of related assets; establishing a public education and awareness program; and formulating a strategy to develop, grow and retain high quality cyber talent for the national workforce. Two of the major universities (Northern Caribbean University and the University of the West Indies) offer degrees in computer science with some degree of specialization in information security and network security, as well as more advanced coursework in cryptography.

1.4.3 PROFESSIONAL CERTIFICATION

Jamaica does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Jamaica does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no framework for sharing cybersecurity assets across borders with other nation states in Jamaica.

1.5.2 INTRA-AGENCY COOPERATION

Jamaica has officially recognized the NCSTF as responsible for the national program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

The NCSTF is tasked with promoting collaboration amongst all stakeholders.

1.5.4 INTERNATIONAL COOPERATION

Jamaica is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Jamaica also participates in the OAS.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Section 9 of the Sexual Offences Act

- The Child Pornography (Prevention) Act.

2.2 UN CONVENTION AND PROTOCOL

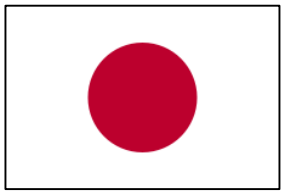
Jamaica has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Jamaica has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no information about any agency that is responsible for the protection of children online.

2.4 REPORTING MECHANISM

There is no information about any website or hotline to which incidents can be reported.



CYBERWELLNESS PROFILE
JAPAN

BACKGROUND

Total Population: 126 435 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 86.25%

(data source: ITU Statistics 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Japan has a specific legislation pertaining to cybercrime. It is mandated through the following legal instrument:

-Unauthorized Computer Access Law 2000.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Electronically Recorded Monetary Claims Act -Telecommunications Business Law

-Act on Regulation of Transmission of Specified Electronic Mail -Act on the Protection of Personal Information

-Law Concerning Electronic Signatures and Certification Business

-Basic Act on the Formation of an Advanced Information and Telecommunications Network Society.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Japan has an officially recognized and legally mandated government CERT (JPCERT/CC).

1.2.2 STANDARDS

Japan has an officially approved national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards through the following instrument:

-Technical Standards for Information Security Measures for the Central Government Computer Systems (April 2012).

1.2.3 CERTIFICATION

The Management Standards for Information Security Measures for the Central Government Computer Systems is the framework for certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

The Basic Policy of Critical Information Infrastructure Protection and Information Security Strategy for Protecting the Nation in Japan are the officially recognized national and sector-specific cybersecurity policy and strategy in Japan.

1.3.2 ROADMAP FOR GOVERNANCE

The Information Security 2012 Annual Plan is the officially recognized national or sector-specific governance roadmap for cybersecurity in Japan.

1.3.3 RESPONSIBLE AGENCY

In Japan the National Information Security Center (NISC) is the officially recognized agency responsible for implementing a national cybersecurity strategy and policy.

Other agencies include the following:

-Information Security Policy Council (ISPC)
-National Policy Agency
-Ministry of Economy, Trade and Industry (METI)
-Ministry of Internal Affairs and Communications (MIC)
-Ministry of Defense.

1.3.4 NATIONAL BENCHMARKING

Japan does not have any national benchmarking and referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Japan has in place an Information Security Research and Development Strategy for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

The officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors are:

-Information Security Human Resource Development Program
-NISC Information Security Awareness Month
-Information Security Outreach and Awareness Program
-JPCERT/CC.

1.4.3 PROFESSIONAL CERTIFICATION

Although Japan is home to 22 members of FIRST it does not have an officially recognized national or sector-specific body responsible for certification of professionals.

1.4.4 AGENCY CERTIFICATION

Japan does not have any officially recognized national or sector-specific body responsible for certifying agencies.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Japan currently partners with the US, Israel and the UK on cybersecurity matters.

1.5.2 INTRA-AGENCY COOPERATION

The Ministry of Defense Information sharing programs and the METI Cybersecurity Information Sharing Partnership Japan (J-CSIP) serve as a framework for sharing cybersecurity assets between agencies.

1.5.3 PUBLIC SECTOR PARTNERSHIP

The officially recognized body for information sharing between the public and private sector is (JPCERT/CC) which shares information with domestic vendors particularly of the private sector. The METI Cybersecurity Information Sharing Partnership Japan (J-CSIP) is also responsible for sharing cybersecurity assets between the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Japan is part of the ASEAN and APCERT. In place also is an International Strategy on Cybersecurity.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child protection has been enacted through the following instruments:

-Articles 174 and 175 of the Criminal Code.

-Article 7 of the Act on Punishment of Activities relating to Child Prostitution and Child Pornography, and the Protection of Children.
-The Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People.

2.2 UN CONVENTION AND PROTOCOL

Japan has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Japan has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The following are the officially recognized and legally mandated support institutions in Japan:

- NISC - EMA - JISPA -JPCERTCC.

2.4 REPORTING MECHANISM

Harmful and illegal content online can be filled and reported at the Internet Report Centre in Japan.

CYBERWELLNESS PROFILE
JORDAN

BACKGROUND

Total Population: 6 457 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 44.20%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

-Law on Information System and Cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

-Electronic Transaction Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Jordan does not have an officially recognized CIRT Team; however they are currently working on it. A CIRT readiness assessment was conducted for Jordan in 2014 by ITU.

1.2.2 STANDARDS

Jordan does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards. However the National Information Technology Center (NITC) maintains some audits on governmental entities using ISO 27001 standard.

1.2.3 CERTIFICATION

Jordan does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Jordan has an officially recognized national cybersecurity strategy (National Information Assurance and Cyber Security Strategy).

1.3.2 ROADMAP FOR GOVERNANCE

Jordan does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The National Information Technology Center (NITC) is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Jordan does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Jordan does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Jordan does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Jordan has 14 public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Jordan does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Jordan does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Jordan's National Information Technology Center has an officially recognized national program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Jordan does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector. However according to the CERT roadmap, they will handle this role.

1.5.4 INTERNATIONAL COOPERATION

Jordan is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Jordan is also a member of the OIC-CERT Team. The goal of OIC-CERT is to provide a platform for member countries to explore and to develop collaborative initiatives and possible partnerships in matters pertaining to cybersecurity that shall strengthen their self-reliance in the cyberspace. Jordan hosted and participated in the ITU-IMPACT Applied Learning for Emergency Response Teams (ALERT) at Jordan, in July 2012. Jordan participated in the International Cyber Shield Exercise 2014 in Turkey (ICSE 2014).

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Jordan does not have any national legislation pertaining to child online protection.

2.2 UN CONVENTION AND PROTOCOL

Jordan has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Jordan has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Jordan does not have any officially recognized agency that offers intuitional support on child online protection.

2.4 REPORTING MECHANISM

Jordan does not have any officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE REPUBLIC OF KAZAKHSTAN

BACKGROUND

Total Population: 16 381 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 54.00%

(data source: ITU Statistics, December 2013)

1.**CYBERSECURITY**

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Penal Code

- Kazakhstan's Criminal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Law on Informatization

- Law on Communications

- Draft Law on Personal Data Protection

- Law on Electronic Documents and Digital Signatures

- Laws on the Protection of State Secrets of the Republic of Kazakhstan

- Amendments and additions to some legislative acts of the Republic of Kazakhstan on Information and Communication Networks.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Kazakhstan has an officially recognized national CERT known as KZ-CERT.

1.2.2 STANDARDS

Kazakhstan does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Kazakhstan.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Kazakhstan has an officially recognized Military Doctrine and Policy which is the national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Kazakhstan.

1.3.3 RESPONSIBLE AGENCY

There is no information about any agency that is responsible for cybersecurity in Kazakhstan.

1.3.4 NATIONAL BENCHMARKING

Kazakhstan does not have any benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no officially recognized national or sector-specific research and development (R&D) program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Kazakhstan.

1.4.3 PROFESSIONAL CERTIFICATION

Kazakhstan does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Kazakhstan does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

India and Kazakhstan adopted a Road map for 2011-2014 to strengthen the strategic partnership.

1.5.2 INTRA-AGENCY COOPERATION

Kazakhstan does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Kazakhstan.

1.5.4 INTERNATIONAL COOPERATION

KZ-CERT is a member of FIRST.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

- Article 273.1* of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Kazakhstan has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Kazakhstan has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Kazakhstan.

2.4 REPORTING MECHANISM

Illegal content can be reported to the hotline for prevention and response to illegal content in Kazakhstan.

CYBERWELLNESS PROFILE

KENYA

BACKGROUND

Total Population: 42 749 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 39.00%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

-Information and Communication Act.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

-Information and Communication Act (Amended).

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU-IMPACT completed a CIRT Implementation in the country in October 2012 and the national computer incident response team is the KE-CIRT/CC.

1.2.2 STANDARDS

Kenya does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Kenya does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Kenya is in the process of developing an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Kenya is in the process of developing a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Ministry for Information, Communications and Technology is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Kenya has officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development through collaboration with ITU.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Kenya does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Kenya has officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals through the national CIRT (KE-CIRT/CC).

1.4.3 PROFESSIONAL CERTIFICATION

Kenya does not have the exact numbers of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Kenya Competition Authority is currently in the process of being certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Kenya has officially recognized partnerships with EACO Working Group 5 on IP Networks, Standards and Cybersecurity.

1.5.2 INTRA-AGENCY COOPERATION

Kenya has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector through the Industry Computer Security Incident Response Team (iCSIRT).

1.5.3 PUBLIC SECTOR PARTNERSHIP

Kenya has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector through the national CIRT (KE-CIRT/CC).

1.5.4 INTERNATIONAL COOPERATION

Kenya is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Kenya is also a member of the EACO Working Group 5 on IP Networks, Standards and Cybersecurity. Kenya is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA).

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Sexual Offense Act

-Children Act
-Information and Communication Act.

2.2 UN CONVENTION AND PROTOCOL

Kenya has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Kenya has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Kenya does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Kenya does not have any officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

KIRIBATI

BACKGROUND

Total Population: 103 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 11.50%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Kiribati does not have any specific legislation on cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

-Telecommunication Act

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Kiribati does not have an officially recognized national CIRT. However it is a member of the Pacific Island Regional CIRT (PacCERT).

1.2.2 STANDARDS

Kiribati does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Kiribati does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Kiribati does not have an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Kiribati does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The ICT unit in the Ministry of Communication, Transport and Tourism Development is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Kiribati does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Kiribati does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Kiribati does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Kiribati does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Kiribati does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Kiribati has an officially recognized partnership with PacCERT to facilitate sharing of cybersecurity asset across border.

1.5.2 INTRA-AGENCY COOPERATION

Kiribati does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Kiribati does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Kiribati is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Kiribati also participated in cybersecurity training and forums organized by PacCERT.

Kiribati is among the beneficiary countries of the EU/ITU co-funded project “Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries” (ICB4PAC).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Kiribati does not have specific legislation on child online protection.

2.2 UN CONVENTION AND PROTOCOL

Kiribati has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

2.3 INSTITUTIONAL SUPPORT

Kiribati does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Kiribati does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
REPUBLIC OF KOREA

BACKROUND

Total Population: 48 588 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 84.77%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Criminal Act (Art. 316(2), Art. 366, Art, 314(2), Art. 347(2), Art. 227(2), Art. 323(2), Art. 140(3), Art 141(1))
- Act on Promotion of Information and Communications Network Utilization and Information Protection
- Personal Information Protection Act
- Act on the Protection of Information and communications Infrastructure.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Act on Promotion of Information and Communications Network Utilization and Information Protection
- Personal Information Protection Act
- Use and Protection of Credit Information Act
- Electronic Financial Transactions Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Republic of Korea has an officially recognized national CIRT (KrCERT/CC) and a private CERT (CONCERT) that is promoting secure operation of information and communications network by preventing incidents in the domestic information and communications network.

1.2.2 STANDARDS

The Information Security Management system (ISMS) is the officially approved national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

The Korea Internet Security Agency (KISA) provides cybersecurity frameworks in order to foster professionals equipped with information security technology and practical abilities, national qualification. Also SIS (Specialist for Information Security), an accredited private qualification, was promoted to national technical qualification (information security engineer/ industrial information security engineer) in 2013.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Republic of Korea has an officially recognized national cybersecurity strategy National Cybersecurity Measures in order to ensure a systematic government-level response to various cyber threats to national security.

1.3.2 ROADMAP FOR GOVERNANCE

The Personal information protection normalization plan (five plans) provides a national governance roadmap for cybersecurity in Republic of Korea.

1.3.3 RESPONSIBLE AGENCY

The Ministry of Science, ICT and Future Planning establishes, supervises, adjusts and evaluates scientific and technological policies, such as on information security, information culture, ICT convergence promotion and radio wave management. It also monitors and coordinates the implementation of a national cybersecurity strategy, policy and roadmap in Republic of Korea.

1.3.4 NATIONAL BENCHMARKING

The National Information Security Index is a measure for assessing the information security level of the private sector (enterprises and individual internet users) in Republic of Korea and is the officially recognized national benchmarking referential to measure cybersecurity development. The Ministry of Science, ICT and Future Planning also organizes joint workshops and shares information with countries, agencies and companies holding excellent technologies by concluding MoU with them .

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

The Korea Internet Security Agency (KISA) provides various guidelines regarding personal information protection on Internet, VOIP information security and biometric information. It is also the officially recognized national or sector-specific research and development (R&D) program/project for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

The ICIS (International Conference on Information Security) share latest information about information security, such as domestic and international advanced security technologies, success cases and government policies, and to highlight the importance of security industry as the next-generation growth power.

The Korea Internet Security Agency (KISA) also provides various educational and professional training programs in order to raise awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in both public and private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Republic of Korea has numerous public sector professionals certified under internationally recognized certification programs in cybersecurity such as CISA, CISSP etc. However it did not conduct a survey to gather the exact statistic.

1.4.4 AGENCY CERTIFICATION

The Korea Internet Security Agency (KISA) is the only public agency certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Korea Internet Security Agency (KISA) has signed MoU and has officially recognized partnerships with the following organizations:

- Office of cybersecurity and Information Assurance (OCSIA UK)
- Israël National Cyber Bureau (INCB)
- Checkpoint Israel
- MacAfee
- Microsoft
- CERT Australia
- CERT Romania (CERT-RO)
- Japan CERT (JP CERT)
- Chinse CERT (CN CERT)
- Cybersecurity Institute (STS) of Kazakhstan.

1.5.2 INTRA-AGENCY COOPERATION

Republic of Korea has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector through the Information Communication Infrastructure Protection Committee which is

part of Ministry of Science, ICT and Future Planning and which aims to coordinate policies on critical ICT infrastructure and improve institution on protection of critical ICT infrastructure.

1.5.3 PUBLIC SECTOR PARTNERSHIP

The National Cyber Security Conference is held on a regular basis in order to share information about key cyber security threats occurring in public and private sector in which governmental departments, key CERTs, security companies (vaccine, monitoring) and ISP are the participating organizations.

Republic of Korea has also has a Private – Public – Military Joint Response Team created by the Ministry of Science, ICT and Future Planning organized and operated for decision-making on cyber threats, situation monitoring, analysing of threats and joint investigation.

1.5.4 INTERNATIONAL COOPERATION

Republic of Korea participated in several cybersecurity activities with APCERT and FIRST, of which the Korean CERT KrCERT/CC is a member.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Articles 243-245 o the Criminal Code.

- Article 8 of the Act on the Protection of Children and Juveniles from Sexual Abuse.

2.2 UN CONVENTION AND PROTOCOL

Republic of Korea has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Republic of Korea has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Illegal and Harmful Information Report Center (*), under the Korean Communications Standards Commission (KCSC (*)), works on the protection of internet users with the Korean National Police Agency, the Commission on Youth Protection, NGOs and ISPs.

The SafeNet (*) website, under KCSC (*) introduced a rating system that allows content providers to rate and filter content according a selection made by parents and educators.

The Korean Computer Emergency Response Team (KrCERT/CC*) provides information on general cyber-threats.

2.4 REPORTING MECHANISM

The Illegal and Harmful Information Report Center, a channel of the Korean Internet Safety Commission, receives report on illegal and harmful information.

CYBERWELLNESS PROFILE

STATE OF KUWAIT

BACKGROUND

Total Population: 2 892 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 75.46%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- None.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- None.

1.2. TECHNICAL MEASURES

1.2.1 CIRT

Kuwait does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Kuwait does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Kuwait.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Kuwait does not have an officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Kuwait.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Kuwait.

1.3.4 NATIONAL BENCHMARKING

Kuwait does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Kuwait does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

Kuwait has an Information Security forum which is nationally recognized as a program for creating awareness for cybersecurity.

1.4.3 PROFESSIONAL CERTIFICATION

Kuwait does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Kuwait does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Kuwait has a security program with the UK.

1.5.2 INTRA-AGENCY COOPERATION

Kuwait does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Kuwait.

1.5.4 INTERNATIONAL COOPERATION

Kuwait is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- None.

2.2 UN CONVENTION AND PROTOCOL

Kuwait has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Kuwait has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Central Agency for Information Technology (*) launched a National Awareness Program in 2008 and maintains a weekly broadcast in Kuwait Satellite Channel on a variety of IT topics including internet safety.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Kuwait.

CYBERWELLNESS PROFILE
KYRGYZ REPUBLIC

BACKGROUND

Total Population: 5 448 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 23.40%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Criminal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

- Law on Protection of Software and Databases.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Kyrgyzstan does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Kyrgyzstan does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Kyrgyzstan.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Kyrgyzstan does not have any officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Kyrgyzstan.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Kyrgyzstan.

1.3.4 NATIONAL BENCHMARKING

Kyrgyzstan does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Kyrgyzstan does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Kyrgyzstan.

1.4.3 PROFESSIONAL CERTIFICATION

Kyrgyzstan does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Kyrgyzstan does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Kyrgyzstan does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Kyrgyzstan does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Kyrgyzstan.

1.5.4 INTERNATIONAL COOPERATION

Kyrgyzstan is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- None.

2.2 UN CONVENTION AND PROTOCOL

Kyrgyzstan has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Kyrgyzstan has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Kyrgyzstan.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Kyrgyzstan.

CYBERWELLNESS PROFILE

LAO PEOPLE'S DEMOCRATIC REPUBLIC

BACKROUND

Total Population: 6 374 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 12.50%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Lao PDR does not have specific legislation on cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Lao PDR does not have specific regulation and compliance requirement pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Lao PDR has an officially recognized national CIRT, LaoCERT. ITU conducted a CIRT assessment for Lao PDR in 2011.

1.2.2 STANDARDS

Lao PDR does not have officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Lao PDR does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Lao PDR does not have an officially recognized national cybersecurity strategy or policy.

1.3.2 ROADMAP FOR GOVERNANCE

Lao PDR does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Lao PDR does not have an officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Lao PDR does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Lao PDR does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Lao PDR does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Lao PDR does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Lao PDR does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Lao PDR has officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Lao PDR does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Lao PDR does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Lao PDR is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Lao PDR participated in the Applied Learning for Emergency Response Team (ALERT) in December 2011, held in Yangon, Myanmar.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Article 138 (*) of the Criminal Code.

-Article 86 (*) of the Law on the Protection of the Rights and Interests of Children.

2.2 UN CONVENTION AND PROTOCOL

Lao PDR has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Lao PDR has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Lao PDR does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Lao PDR does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
REPUBLIC OF LATVIA

BACKGROUND

Total Population: 2 235 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 75.2344%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Penal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- National Information System Law
- The Electronic Communications Law
- Information Technology Security Law.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Latvia has an officially recognized national CIRT known as CERT.LV.

1.2.2 STANDARDS

There are officially approved national and sector specific cybersecurity frameworks for implementing internationally recognized cybersecurity standards:

- ISO 27000
- ITIL, ISO 20000
- COBIT
- ISO 13335
- IT Safety Guidelines
- Online collection system certification
- ISF Standard of Good Practice for Information Security.

1.2.3 CERTIFICATION

Latvia does not have any nationally recognized cybersecurity framework for certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Latvia has officially recognized National Security Concept and Cyber Security Strategy of Latvia 2014-2018 as its national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

The Cybersecurity Policy in Latvia Coordination, Strategy & Priorities presented by the Ministry of Defense provides the national governance roadmap for cybersecurity in the Latvia.

1.3.3 RESPONSIBLE AGENCY

The National IT Security Council and the Ministry of Defense oversee cybersecurity strategy, policy and roadmap in Latvia.

1.3.4 NATIONAL BENCHMARKING

Currently there are no national or sector-specific benchmarking exercises or referential used to measure cybersecurity development in Latvia.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

CERT.LV has developed information technology security recommendations for state and local government authorities; it also has produced some activity reports which suffice as the officially recognized national or sector-specific research and development (R&D) programs/projecst for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

CERT.LV produces training for IT security issues at the national and local government institutions.

1.4.3 PROFESSIONAL CERTIFICATION

There is no available information regarding the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

CERT.LV is the officially recognized certified government and public sector agency certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

CERT.LV partners with its counterparts around Europe, sharing cybersecurity assets. Latvia is an accredited member state of the TI TF-CSIRT. TF-CSIRT holds regular security incident response team meetings to better get to know colleagues from other countries, as well as to work together in different areas of research and to improve incident resolution options.

1.5.2 INTRA-AGENCY COOPERATION

The CERT.LV cooperates with state and local authorities encouraging them to make the security of their electronic information space a priority. CERT.LV has prepared a brief overview of the legal frame of cooperation with state and local authorities.

1.5.3 PUBLIC SECTOR PARTNERSHIP

CERT.LV cooperates with the Internet Service providers as a framework for sharing cybersecurity assets between the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

CERT.LV is a member of FIRST and TERENA. The government of Latvia has recognized the danger of increased cyber threats and is working together with NATO, the European Union, the Baltic States, Nordic states, and the United States to strengthen its cybersecurity. The United States supports Latvia's efforts through visits by U.S. experts and Latvian participation in EUCOM and NATO sponsored events and U.S.-based training. The government of Latvia is also a partner in the Freedom Online Coalition, a group of governments collaborating to advance Internet freedom.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

- Section 166 of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Latvia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Latvia has acceded, with no declarations or reservations to articles 2 and 3, to the Optional

Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Watchmen website, under the Latvian national police provides information on internet safety for children and youth.

2.4 REPORTING MECHANISM

Illegal online content can be reported in the website of the Latvian Safer Internet Centre or by the phone number: 11611.

CYBERWELLNESS PROFILE
LEBANON

BACKGROUND

Total Population: 4 292 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 70.50%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Lebanon does not have specific criminal legislation pertaining to cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Lebanon does not have specific regulation and compliance requirements on cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU-IMPACT conducted a CIRT readiness assessment for Lebanon at Beirut, Lebanon in October 2012.

Lebanon does not have an officially recognized national CIRT currently.

1.2.2 STANDARDS

Lebanon does not have officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Lebanon does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Lebanon does not have an officially recognized national cybersecurity strategy or policy.

1.3.2 ROADMAP FOR GOVERNANCE

Lebanon does have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The Telecommunication Regulatory Authority (TRA) is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Lebanon does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Lebanon does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

There are a number of cybersecurity research initiatives in Lebanon conducted under the American University of Beyrouth.

Currently Lebanon relies on its service providers, Cybercrime Bureau and individual experts to provide support and knowledge sharing on best practices and security awareness. In addition, the Ministry of Telecommunications (MOT) and the Telecommunications Regulatory Authority (TRA) hosted the "Responsible Citizen in Cyberspace" event on April 15, 2013 at the MOT premises.

1.4.3 PROFESSIONAL CERTIFICATION

Lebanon does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Lebanon does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Lebanon has an officially recognized partnership with the following organization:

-Pan Arab Observatory for Cybersecurity.

1.5.2 INTRA-AGENCY COOPERATION

Lebanon does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Lebanon does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Lebanon is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Lebanon does not have any national legislation pertaining to child online protection.

2.2 UN CONVENTION AND PROTOCOL

Lebanon has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Lebanon has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Lebanese Telecommunication Regulatory Authority (*) presents information (*) on child online protection, (link to National Safety Website by TRA www.e-aman.com) and leads an intense awareness program for Child Online Protection

2.4 REPORTING MECHANISM

Lebanon does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
LESOTHO

BACKGROUND

Total Population: 2 217 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 5.00%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Lesotho does not have any officially recognized national legislation pertaining to cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Lesotho does not have any officially recognised regulation pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU-IMPACT conducted a CIRT readiness assessment for Lesotho at Maseru, Lesotho during November 2012 (19 - 23rd November 2012). Lesotho does not have yet an officially recognized national CIRT.

1.2.2 STANDARDS

Lesotho does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Lesotho does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Lesotho does not have an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Lesotho does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The Ministry of Communication, Science and Technology is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Lesotho does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Lesotho does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Lesotho does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Lesotho does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Lesotho does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Lesotho does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Lesotho does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Lesotho does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Lesotho is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Lesotho is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA).

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child protection has been enacted through the following instruments:

-Sexual Offense Act.

2.2 UN CONVENTION AND PROTOCOL

Lesotho has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Lesotho has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Lesotho does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Lesotho does not have any officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

LIBERIA

BACKGROUND

Total Population: 4 245 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 4.60%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Liberia does not have any officially recognized national legislation pertaining to cybercrime. However it has transposed the Economic Community of West African States (ECOWAS) Directive on Cybercrime into local Telecommunications law, which is currently awaiting legislative approval.

1.1.2 REGULATION AND COMPLIANCE

Liberia does not have any officially recognized regulation pertaining to cyber security. However it has transposed the Economic Community of West African States (ECOWAS) Directive on Cybercrime into our local Telecommunications law, which is currently awaiting legislative approval.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU conducted a CIRT readiness assessment for Liberia at Addis Ababa, Ethiopia in March 2014 (10-14th March 2014). Currently, Liberia does not have any officially recognized national CIRT. However it is in the process of developing such a body with technical expertise from ITU.

1.2.2 STANDARDS

Liberia does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Liberia does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Liberia does not have an officially recognized national cybersecurity strategy. Her current ICT policy minimally addresses cybersecurity.

1.3.2 ROADMAP FOR GOVERNANCE

Liberia does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The Government of Liberia CIO program is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Liberia does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Liberia have officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector. However these initiatives are currently in their infant stages under the Government of Liberia CIO Program. There are various assessments being conducted which would consummate into a full Enterprise Architecture (EA) framework for the Government. The EA framework would address such issues as cybersecurity standards, best practices etc.

1.4.2 MANPOWER DEVELOPMENT

Liberia has a number of Universities which provide computer security related programs. It has also developed a professional program that certifies CIOs, which includes security related programs among others.

1.4.3 PROFESSIONAL CERTIFICATION

Liberia does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Liberia does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Liberia does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Liberia Chief Information Officer (CIO) has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector

1.5.3 PUBLIC SECTOR PARTNERSHIP

Liberia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Liberia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Liberia is also a member of ECOWAS. Liberia is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

-Children Law (Section 18.16).

2.2 UN CONVENTION AND PROTOCOL

Liberia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Liberia has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Liberia does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Liberia does not have any officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

LIBYA

BACKGROUND

Total Population: 6 469 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 16.50%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Libya does not have specific legislation pertaining to cybercrime. However Libya is currently embarking in drafting new legislations on cyber-activities e.g. Cybercrime Law, Data Protection Law, Cyber-IPR Law, e-Transactions Law, e-Commerce Law.

1.1.2 REGULATION AND COMPLIANCE

Libya does not have specific regulation and compliance requirements pertaining to cybersecurity. However, NISSA is mandated to carry out the needed steps for such cybersecurity compliance process at the national level.

1.2 TECHNICAL MEASURE

1.2.1 CIRT

Libya requested assistance from ITU for establishing a national CIRT. As a result, Libya-CERT is up and running since February 2013 providing some basic services under the umbrella of the National Information Security and Safety Authority (NISSA). The webpage of Libya-CERT is under construction.

1.2.2 STANDARDS

Libya does not have officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards. However, NISSA is mandated to carry out the needed steps for such cybersecurity framework at the national level including governmental agencies.

1.2.3 CERTIFICATION

Libya does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Libya does not have an officially recognized national cybersecurity strategy. However NISSA is currently developing a national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Libya does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The NISSA and the Ministry of Communications and Informatics are the officially recognized agencies responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Libya does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Libya does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

NISSA is running a national program in raising the awareness and promoting cybersecurity specific educational program among the public and private sectors. NISSA has organized the first International Cybersecurity Days Conference (CDC) during the period 27-29 August 2013 in Libya with participation from international organizations.

1.4.3 PROFESSIONAL CERTIFICATION

Libya does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Libya does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Libya has officially recognized partnerships with the following organizations:

-United States Trade and Development Agency

-National US-Arab Chamber of Commerce

-OMAN-CERT

-TUN-CERT

-Alcatel-Lucent France CERT and SOC

1.5.2 INTRA-AGENCY COOPERATION

NISSA is currently implementing an officially recognized national program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Libya does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Libya participated in the 2012 ITU-IMPACT Applied Learning for Emergency Response Teams (ALERT) from 15-17 July in Amman, Jordan.

Libya also participated in Africa-CERT, OIC-CERT, SANS and EC-Council activities

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-The Criminal Code (Article 421)

2.2 UN CONVENTION AND PROTOCOL

Libya has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Libya has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Libya does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Libya does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
PRINCIPALITY OF LIECHTENSTEIN

BACKGROUND

Total Population: 36 500

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 93.80%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Criminal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Data Protection Act

- Law on E-commerce

- Law on Electronic Signatures

- Law on Electronic Communication

- Law on the Re-use of Public Sector Information.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Liechtenstein does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Liechtenstein does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Liechtenstein.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Liechtenstein does not have an officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Liechtenstein.

1.3.3 RESPONSIBLE AGENCY

There is no nationally recognized agency for the cybersecurity in Liechtenstein.

1.3.4 NATIONAL BENCHMARKING

Liechtenstein does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Liechtenstein does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Liechtenstein.

1.4.3 PROFESSIONAL CERTIFICATION

Liechtenstein does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Liechtenstein does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Liechtenstein does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Liechtenstein does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Liechtenstein.

1.5.4 INTERNATIONAL COOPERATION

Liechtenstein is a member of the CoE.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- §218(a) and §219* of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Liechtenstein has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Liechtenstein has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Liechtenstein.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Liechtenstein.

CYBERWELLNESS PROFILE

LITHUANIA

BACKGROUND

Total Population: 3 292 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 68.45%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Criminal Code of the Republic of Lithuania (chapter on crimes against security of electronic Data and Information Systems).

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

- Law in Electronic Communication (Article 42 & 62).

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Lithuani a has an officially recognized national CIRT (CERT-LT) established within the Communications Regulatory Authority dealing with network and information security incidents in Lithuanian public electronic communications networks.

Concerning sector-specific CERT; LITNET CERT is the Computer Emergency Response Team of the Lithuanian academic and research network LITNET. SVDPT-CERT is a computer emergency response team of Secure State Data Communication Network of the Lithuanian state institutions and municipalities and LTU MOD CIRT is a computer incident response team of the Lithuanian Ministry of Defence.

1.2.2 STANDARDS

There is no available information concerning any officially approved national or sector specific cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no available information concerning any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

The Programme for the Development of Electronic Information Security for 2011–2019 approved by Government of the Republic of Lithuania and carried out by the Ministry of the Interior is the officially recognized national cybersecurity policy.

The purpose of the Programme is in one hand to determine the objectives and tasks for the development of electronic information in order to ensure the confidentiality, integrity and accessibility of electronic information and services provided in cyberspace, safeguarding of electronic communication networks, information systems and critical information infrastructure against incidents and cyberattacks, protection of personal data and privacy, as well as to set the tasks, implementation of which would allow total security of cyberspace and entities operating in this medium. On the other hand the programme ensures the security of state-owned information resources, an efficient functioning of critical information infrastructure.

1.3.2 ROADMAP FOR GOVERNANCE

The Programme for the Development of Electronic Information Security for 2011–2019 provides a national governance roadmap for cybersecurity in Lithuania.

1.3.3 RESPONSIBLE AGENCY

The coordination of the national cybersecurity strategy (Programme for the Development of Electronic Information Security for 2011–2019 implementations) is carried out by the Ministry of the Interior of the Republic of Lithuania. Also, an inter-institutional Electronic Information Security (Cybersecurity) Coordination Commission is in operation, chaired by the representative of the Ministry of the Interior.

1.3.4 NATIONAL BENCHMARKING

There is no available information concerning any officially recognized national of sector-specific benchmarking exercises or referential used to measure cybersecurity development in Lithuania.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no available information concerning any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

There is no available information concerning any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

There is no available information concerning any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Lithuanian CERT-LT, LITNET CERT, SVDPT-CERT are all accredited teams by Trusted Introducer which address common needs and build a service infrastructure providing vital support for all security and incident responses teams.

LITNET is a member of the Trans-European Research and Education Networking Association TERENA which offers a forum to collaborate, innovate and share knowledge in order to foster the development of Internet technology.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Lithuania has officially recognized national or sector-specific partnerships with the following organizations:

-The Communication Regulatory Authority (RTT) which is an independent national institution regulating communication sector in Lithuania that implements the European Union Safer Internet programme and, in cooperation with the Centre of Information Technologies in Education (ITC) and other partners executes **the Safer Internet project**.

- Association INHOPE which is a hotline established by RRT to report illegal or harmful content on the Internet

- Council of Europe -ENISA

CERT-LT has signed Memorandums of Understanding with CERTs of other countries (e.g., KZ-CERT).

1.5.2 INTRA-AGENCY COOPERATION

There is no available information concerning any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no available information concerning any officially recognized national or sector-specific programs for sharing cybersecurity assets between the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Lithuania is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

Lithuania participated in the cybersecurity activities of ENISA. Lithuania, represented by the Communications Regulatory Authority, is a member of the Government Advisory Committee (GAC), an advisory body to the Board of Directors of the Internet Corporation for Assigned Names and Numbers (ICANN), the organization which performs the administration of the Internet protocol addresses, domain name system and Internet root servers. The main function of GAC is to advise ICANN on public policy issues.

Lithuania also participated in the International Cyber Shield Exercise 2014 in Turkey (ICSE 2014).

CERT-LT, LITNET CERT, LTU MOD CIRT are members of FIRST and are all listed teams by Trusted Introducer of TERENA .

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

- Article 309* of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Lithuania has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Lithuania has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The website of the Lithuanian Communications Regulatory Authority (CRA (*)) has information on internet security for consumers and provides a link to Safer Internet.

2.4 REPORTING MECHANISM

Online information with pedophilic or pornographic character or information inciting racial and ethnic hatred can be reported in the website (*) of Safer Internet Lithuania.

Online harmful content can be reported at the website of the Lithuanian Computer Emergency Response Team (cert-lt (*)).

CYBERWELLNESS PROFILE
LUXEMBOURG

BACKGROUND

Total Population: 523 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 93.77%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Penal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Law on Data Protection on Electronic Communications- Law on Electronic Communications and Radio Waves
- Law on Electronic Commerce - Law on Electronic Signature and Cryptography
- Law on the Protection of Individuals with regard to the Processing of Personal Data.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Luxembourg has an officially recognized national CIRT GOVCERT.LU and the Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to gather, review, report and respond to computer security threats and incidents.

1.2.2 STANDARDS

There is no information on any framework for implementing internationally recognized cybersecurity standards in Luxembourg.

1.2.3 CERTIFICATION

There is no information on any framework for certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Luxembourg has an officially recognized Stratégie Nationale en Matière de Cyber Sécurité as its National Cybersecurity Strategy.

1.3.2 ROADMAP FOR GOVERNANCE

The Plan Directeur de la Mise en Œuvre des Technologies de l'Information au Sein de l'Etat provides a national governance roadmap for cybersecurity in Luxembourg.

1.3.3 RESPONSIBLE AGENCY

The GOVCERT.LU and Le Cyber Security Board (CSB) monitor and coordinate the implementation of a national cybersecurity strategy, policy and roadmap by respective agencies.

1.3.4 NATIONAL BENCHMARKING

There is no information on any national benchmarking exercises or referential used to measure cybersecurity development in Luxembourg.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no information on any program or exercise available for research and development (R&D) of cybersecurity standards, best practices and guidelines in Luxembourg.

1.4.2 MANPOWER DEVELOPMENT

CIRCL offers courses to its members and organizations based in Luxembourg to improve information security. CIRCL is sharing its field experience through a set of training or technical courses.

1.4.3 PROFESSIONAL CERTIFICATION

CIRCL team member are certified public sector professionals.

1.4.4 AGENCY CERTIFICATION

CIRCL is RIPE member and an accredited CERT of TF-CSIRT Trusted Introducer.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, CIRCL cooperates with CERTs from various countries.

1.5.2 INTRA-AGENCY COOPERATION

Luxembourg has an officially recognized Malware Information Sharing Platform. MISP acts as a platform for sharing threat indicators within private and public sectors.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Private organizations in Luxembourg or accredited CERTs can request an access to their respective MISP platform. MISP acts as a platform for sharing threat indicators within private and public sectors. This is the officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Luxembourg participates in the following international cooperation activities through CIRCL:
- FIRST - EU - TI.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Articles 327, 383-385, 385-1 and 385b of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Luxembourg has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Luxembourg has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no information showing any agency that provides support for online child protection in Luxembourg.

2.4 REPORTING MECHANISM

Online illegal content can be reported at the website BEE SECURE Stopline (*). Also computer incidents can be reported in the website of the CIRCL, by the email address info@circl.lu or by the phone number (+352) 247 88444.

CYBERWELLNESS PROFILE REPUBLIC OF MACEDONIA

BACKGROUND

Total Population: 2 067 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 61.20%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Criminal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Law on Personal Data
- Law on Electronic Commerce
- Law on Electronic communications
- Law on Interception of Communications
- Law on free Access to public Information
- Law on Data in Electronic Form and Electronic Signature.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Macedonia has an officially recognized national CIRT known as MARNet-CERT. ITU conducted a CIRT readiness assessment for Macedonia in 2012.

1.2.2 STANDARDS

Macedonia does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Macedonia.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Macedonia does not have any officially recognized national or sector-specific cybersecurity strategy. But it has a strategy for personal data protection followed by an Action Plan.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Macedonia.

1.3.3 RESPONSIBLE AGENCY

There is no information about any agency responsible for cybersecurity in Macedonia.

1.3.4 NATIONAL BENCHMARKING

Macedonia does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Macedonia does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Macedonia.

1.4.3 PROFESSIONAL CERTIFICATION

Macedonia does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Macedonia does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Macedonia does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Macedonia does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Macedonia.

1.5.4 INTERNATIONAL COOPERATION

Macedonia is a member of the NATO and CoE.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:
- Articles 193 and 193a of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Macedonia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Macedonia has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Macedonia.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Macedonia.

CYBERWELLNESS PROFILE
MADAGASCAR

BACKGROUND

Total Population: 21 929 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 2.20%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Act 2014-006 on the fight against Cybercrime

1.1.2 REGULATION AND COMPLIANCE

Madagascar does not have specific regulation and compliance requirement related to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Madagascar does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Madagascar does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Madagascar does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Madagascar does not have an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Madagascar does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Madagascar does not have an officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Madagascar does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Madagascar does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Madagascar does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Madagascar does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Madagascar does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Madagascar does not have official recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Madagascar does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Madagascar does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Madagascar is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Madagascar is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Articles 330, 346 and 347 of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Madagascar has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Madagascar has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Madagascar does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Madagascar does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

MALAWI

BACKGROUND

Total Population: 15 883 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 5.40%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Malawi does not have specific criminal legislation pertaining to cybercrime. However a legislation bill is being drafted and is expected to be passed by parliament shortly.

1.1.2 REGULATION AND COMPLIANCE

Malawi does not have specific regulation and compliance requirement pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Malawi does not have officially recognized national CIRT.

1.2.2 STANDARDS

Malawi does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Malawi does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Malawi has an officially recognized national cybersecurity policy (National ICT Policy 2013). The Policy recognises the importance of the cyber security and aims at promoting the use of ICTs to mitigate crimes and enhance public security and cooperate with international security agencies.

1.3.2 ROADMAP FOR GOVERNANCE

Malawi does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Malawi Communication Regulatory Authority is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Malawi does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Malawi has an officially recognized national research and development (R&D) project (HIPSSA PROJECT) for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

There is an educational program **(**MSc. Information Theory, Coding & Cryptography**) that** provides skills in Coding and **Cryptography for the public and private sector professionals.**

1.4.3 PROFESSIONAL CERTIFICATION

Malawi does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Malawi does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Malawi has an officially recognized partnership with ITU-IMPACT.

1.5.2 INTRA-AGENCY COOPERATION

Malawi does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Malawi does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector. However BD CERT organizes events to share knowledge with the law enforcing agencies, industry and academia.

1.5.4 INTERNATIONAL COOPERATION

Malawi is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Malawi participated in the ITU-IMPACT meeting within the African Forum on Best Practices in ICT, Ouagadougou, Burkina Faso, October 10-12, 2013.

Furthermore, Malawi participated in the COMESA Cyber Security Validation Workshop (24th to 28th July 2011) and the COMESA Cyber Security and Public Key Infrastructure Meeting (25th to 28th November 2013). Malawi is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-The Criminal Code (Section 179).

2.2 UN CONVENTION AND PROTOCOL

Malawi has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Malawi has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Malawi does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Malawi does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

MALAYSIA

BACKGROUND

Total Population: 29.82 million

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 66.97%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Communications and Multimedia Act 1998 [Act 588]
- Computer Crime Act 1997 [Act 563]
- Personal Data Protection Act 2010 [Act 709]
- Penal Code [Act 574]
- Copyright Act 1987
- Digital Signature Act 1997[Act 562]
- Financial Services Act 2013
- Electronic Commerce Act 2006 [Act 658].

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Communications and Multimedia Act 1998
- Financial Services Act 2013
- Digital Signature Act 1997.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Malaysia has an officially recognized national CIRT (MyCERT) operated by the office of Cybersecurity Malaysia. Malaysia has also a Government CERT (GCERT) which coordinates knowledge sharing and exchanges programs between MyCERT, Internet Service Providers and enforcement agencies.

1.2.2 STANDARDS

Malaysia has officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards through the following instruments:

- National Cybersecurity Policy (NCSP)
- National Security Council directive No. 24 “Arahan 24”
- The Cabinet’s Decision in 2010
- Arahan Keselamatan under Chief Government Security Office (CGSO).

1.2.3 CERTIFICATION

The Policy Thrust 3 Cybersecurity Technology Framework from the National Cybersecurity policy (NCSP) offers a cybersecurity framework for the certifications and accreditations of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Malaysia has an officially recognized National Cybersecurity Policy (NCSP) which was initiated by the Ministry of Science Technology and Innovation, to harness national effort to enhance the security of Malaysia’s Critical National Information Infrastructure (CNII).The Policy was formulated based on a National Cybersecurity

Framework that comprises legislation and regulatory, technology, public-private cooperation, institutional, and international aspects.

1.3.2 ROADMAP FOR GOVERNANCE

The Policy Thrust 1 "Effective Governance" from the National Cybersecurity Policy (NCSP) provides a national governance roadmap for cybersecurity in Malaysia.

1.3.3 RESPONSIBLE AGENCY

The Ministry of Communications and Multimedia (KKMM) and the Ministry of Science, Technology and Innovation (MOSTI) monitor and coordinate the implementation of a national cybersecurity strategy, policy and roadmap by respective agencies.

1.3.4 NATIONAL BENCHMARKING

Malaysia has officially recognized national benchmarking for the national cyber crisis management plan. Malaysia conducted on 2007 by Cybersecurity Malaysia a Malaysian Incident Handling Drill. Cybersecurity Malaysia coordinated the first National Cyber Crisis Exercise Cyber Drill codenamed X-Maya in collaboration with the National Security Council in 2008.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Standards Malaysia *is* the national standards Body and the national accreditation body, providing confidence to various stakeholders, through credible standardization and accreditation services for global competitiveness and has officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Malaysian Communications and Multimedia Commission provides various types of awareness programs, industry talks, conferences, training programs and workshops on cybersecurity, for the general public as well as for public and private sector employees. CyberSAFE, short for Cybersecurity Awareness for Everyone, is Cybersecurity Malaysia's initiative to educate and enhance the awareness for the general public on the technological and social issues facing internet users, particularly on the dangers of getting online.

1.4.3 PROFESSIONAL CERTIFICATION

Malaysia does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Malaysia does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Malaysian Communications and Multimedia Commission has officially recognized partnerships with the following organizations:

- ASEAN – Japan Partnership -APT Cybersecurity -ASEAN Cyber Drill.

1.5.2 INTRA-AGENCY COOPERATION

Malaysia has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector through the national X-MAYA and the National Security Council directive No. 24 named Arahan 24.

1.5.3 PUBLIC SECTOR PARTNERSHIP

The Policy Thrust 7 "Cybersecurity Emergency Readiness" from the National Cybersecurity Policy (NCSP) provides officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Malaysia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Malaysia participated in the International Cyber Shield Exercise 2014 in Turkey (ICSE 2014).

Malaysia participated in the following cybersecurity activities:

- ASEAN JAPAN Information Security
- APT Cybersecurity Forum
- Meridian Conference
- Octopus Conference (Cooperation against cybercrime)
- JTC 1/SC 27 Meeting

MyCERT is a member of FIRST.

2. CHILD ONLINE PROTECTION

2.2 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Child Act 2001 (Act 611)
- Section 293, Penal Code (Act 574)
- Sections 211 and 233, Communications and Multimedia Act 1998.

2.3 UN CONVENTION AND PROTOCOL

Malaysia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.Malaysia has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.4 INSTITUTIONAL SUPPORT

Ministry of Women, Family and Community Development (MWFCD), Malaysian Communications and Multimedia Commission (MCMC) and the Ministry of Education (MOE) provide information on internet safety for parents, children and educators.

2.5 REPORTING MECHANISM

Online Illegal content can be reported on the Child line 15999. NUR Alert is responsible for spreading information as fast as possible to help trace missing children (below 12 years of age) who could be victims of crime or abuse. NUR Alert comes under the National Child Protection Policy and Action Plan.

CYBERWELLNESS PROFILE

MALDIVES

BACKGROUND

Total Population: 324 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 44.10%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Maldives does not have any officially recognized national legislation pertaining to cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Maldives does not have any officially recognised regulation pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU conducted a CIRT readiness assessment for Maldives, at Maldives, in August 2010. Maldives does not have an officially recognized national CIRT currently.

1.2.2 STANDARDS

Maldives does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Maldives does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Maldives does not have any officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Maldives does not have any national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The Communication Authority of Maldives is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Maldives does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Maldives does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Maldives does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Maldives does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Maldives does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Maldives has signed a Memorandum of Collaboration against Malicious Activities in Cyberspace with Japan Ministry of Information and Communication.

1.5.2 INTRA-AGENCY COOPERATION

Maldives does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Maldives does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Maldives is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Maldives participates in regular forums held by APT and ITU.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Maldives does not have any officially recognized legislation pertaining to child online protection.

2.2 UN CONVENTION AND PROTOCOL

Maldives has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Maldives has acceded, with no declarations or reservations to articles 2 and 3, the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Maldives does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Maldives does not have any officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

MALI

BACKGROUND

Total Population: 16 319 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 2.30%

(data source: ITU Statistics, 2013)

1 CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1. CRIMINAL LEGISLATION

Specific legislations on cybercrime have been enacted through the following legal instrument:

-Criminal Code (Article 264,271)

1.1.2 REGULATION AND COMPLIANCE

Mali does not have specific regulation and compliance requirement pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Mali does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Mali does not have officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Mali does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Mali does not have an officially recognized national cybersecurity strategy or policy.

1.3.2 ROADMAP FOR GOVERNANCE

Mali does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Mali does not have an officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Mali does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Mali does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Mali does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Mali does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Mali does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Mali has officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Mali does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Mali does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Mali is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Mali also cooperates with CEDEAO and Africa Union on cybersecurity issues. Mali is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:
-The Criminal Code (Articles 224-225 and 228)

2.2 UN CONVENTION AND PROTOCOL

Mali has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Mali has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Mali does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Mali does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

MALTA

BACKGROUND

Total Population: 419 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 68.91%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Criminal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Electronic Commerce Act
- Electronic Communications (regulation) Act
- Processing of Personal Data (Electronic Communications Sector) Regulations.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Malta has an officially recognized national CIRT known as mtCERT.

1.2.2 STANDARDS

There is no officially recognized framework for implementing internationally recognized cybersecurity standards in Malta.

1.2.3 CERTIFICATION

Malta information Technology Agency (MITA) Security Governance Unit is responsible for ISO27001 implementation and enterprise risk management. This is the recognised cybersecurity framework for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Malta has an officially recognized National Digital Strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national or sector-specific governance roadmap for cybersecurity in Malta.

1.3.3 RESPONSIBLE AGENCY

The following agencies are responsible for cybersecurity in Malta:

- MITA

- Malta Police Cyber Crime Unit.

1.3.4 NATIONAL BENCHMARKING

In Malta there is no national benching marking and referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

The MITA Security Policy is responsible for the research and development of cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are various programs in Malta to facilitate educational and professional training programs for raising awareness, higher education and certification. These programs are:

- The Malta Be Smart Online!
- MITA Security Awareness Campaign
- MCAST – student awareness programme
- Malta Cyber Crime Unit Task Force – 'Child Abuse over the Internet'.

1.4.3 PROFESSIONAL CERTIFICATION

Malta does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

MITA is the certified government and public sector agency for cybersecurity in Malta; it is ISO27001 certified.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Malta Cyber Crime Unit collaborates with international law agencies.

1.5.2 INTRA-AGENCY COOPERATION

Malta does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Malta does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Malta is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Malta participates in the following cybersecurity activities:

- EU - ENISA

MtCERT is a member of FIRST.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Articles 208A, 208AA, 208AB and 209 of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Malta has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Malta has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no information about the institution responsible for online child protection in Malta.

2.4 REPORTING MECHANISM

Child abuse over the internet can be reported through the website of the Foundation for Social and Welfare Services.

CYBERWELLNESS PROFILE
MARSHALL ISLANDS

BACKGROUND

Total Population: 55 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 11.70%

(data source: ITU Statistics, 2013)

1 CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Marshall Islands does not have any officially recognized national legislation pertaining to cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Marshall Islands does not have any officially recognised regulation pertaining to cyber security.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Marshall Islands does not have an officially recognized national CIRT. However it is a member of the Pacific Island's Regional CIRT, PacCERT.

1.2.2 STANDARDS

Marshall Islands does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Marshall Islands does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Marshall Islands does not have any officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Marshall Islands does not have any national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The Ministry of Transportation and Communication is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Marshall Islands does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Marshall Islands does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Marshall Islands does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Marshall Islands does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Marshall Islands does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Marshall Islands does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Marshall Islands does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Marshall Islands does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Marshall Islands is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Marshall Islands is among the beneficiary countries of the EU/ITU co-funded project “Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries” (ICB4PAC).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Marshall Islands does not have any officially recognized legislation pertaining to child online protection.

2.2 UN CONVENTION AND PROTOCOL

Marshall Islands has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

2.3 INSTITUTIONAL SUPPORT

Marshall Islands does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Marshall Islands does not have any officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

MAURITANIA

BACKGROUND

Total Population: 3 623 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 6.20%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Mauritania does not have any officially recognized criminal legislation pertaining to cybercrime. However it has an ICT Legal framework.

1.1.2 REGULATION AND COMPLIANCE

Mauritania does not have currently any officially recognised regulation and compliance requirement pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Mauritania does not currently have an officially recognized national CIRT but there is a project to create a National Cybersecurity Agency after the successful CIRT assessment conducted by ITU in 2012. Also there is a team of unofficial CERT not yet legally mandated.

1.2.2 STANDARDS

Mauritania does not have any officially recognized national or sector specific cybersecurity frameworks for implementing internationally recognized cybersecurity standards. The cybersecurity vision is still considered as a part of national ICT strategy but Mauritania is considering implementing a specific cybersecurity strategy.

1.2.3 CERTIFICATION

Mauritania does not have currently any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Mauritania has an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Mauritania has a national governance roadmap for cybersecurity under the national cybersecurity strategy.

1.3.3 RESPONSIBLE AGENCY

Mauritania does not have an officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Mauritania performs annual security audit on existing infrastructure (administration intranet platform) as part of a national benchmarking program.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Mauritania does not have currently any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied

in either the private or the public sector but it will be considered with the collaboration of the University of Nouakchott.

1.4.2 MANPOWER DEVELOPMENT

Mauritania does not have currently any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Mauritania does not have currently any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Mauritania does not have currently any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Mauritania does not have currently officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Mauritania does not have currently any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Mauritania does not have currently any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Mauritania is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Mauritania participated in the 2012 ITU-IMPACT Applied Learning for Emergency Response Teams (ALERT) from 15-17 July in Amman, Jordan.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Article 306* of the Criminal Code

Articles 47 and 48* of the Protection Code for Children.

2.2 UN CONVENTION AND PROTOCOL

Mauritania has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Mauritania has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Mauritania does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Mauritania does not have officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

MAURITIUS

BACKGROUND

Total Population: 1 314 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 39.00%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through four IT legislations:

-ICT Act 2001

-Computer Misuse and Cybercrime Act 2003

-Electronic Transaction Act 2000

-Data Protection Act 2004

- Unsolicited Commercial Electronic Bill is being drafted in collaboration with the Council of Europe.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Data Protection Act 2004 which deals with the protection of individuals with regard to the processing of personal data
- ICT Act 2001.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Mauritius has a National CERT known as Computer Emergency Response Team of Mauritius (CERT-MU). CERT-MU operates under the National Computer Board, a statutory body under the aegis of Ministry of Technology, Communication and Innovation. IT Security Unit (ITSU) acts as the Computer Security Incident Response Team (CSIRT) for the Civil Service.

1.2.2 STANDARDS

Mauritius has officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards. As part of National Information and Communication Technology Strategic Plan (NICTSP) of 2007-2011 and 2011-2014, the promotion and adoption of international information cybersecurity standard (ISO 27001) is one of the high priority projects and is already implemented. Also a risk assessment methodology has been defined for the Civil Service. IT Security Unit is reviewing the following standards for adoption:

-PAS 555:2013 – Cyber security risk – Governance and management – Specification

-ISO/IEC 27032 – Information technology – Security techniques – Guidelines for cybersecurity

1.2.3 CERTIFICATION

As per the NICTSP 2007-2011, the ISO 27001 is the recommended standard for the adoption within the public sector. The accreditation of the ISO 27001 standard is done through the Mauritius Standards Bureau. The Framework for CIIP that covers critical sectors is being drafted and will be completed by June 2014.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Cybersecurity strategy is included in NICTSP 2007-2011 and 2011-2014. A new national cybersecurity Strategy and Action Plan has been developed. The IT Security Unit will be responsible for carrying out information security risk assessment exercises, to perform IT security audit based on information security standards and industry best

practices in order to provide an overall assessment of the IT security level as well as for complex and critical Information Systems in Civil Service and to manage ICT incidents in the Civil Service through the establishment of an effective incident handling mechanism for government information systems.

1.3.2 ROADMAP FOR GOVERNANCE

National Information Assurance and Critical Information Infrastructure Protection Policy provide a national governance roadmap for cybersecurity in Mauritius and is in the finalization stage.

1.3.3 RESPONSIBLE AGENCY

The Agency responsible for implementing national cybersecurity strategy policy and roadmap in Mauritius is the CERT Mauritius (CERT-MU) of the National Computer Board and for IT Security Unit for the Civil Service.

1.3.4 NATIONAL BENCHMARKING

A survey has been carried out to measure the state of Information Security in Businesses in Mauritius in 2013 December by NCB (CERT-MU). So far, this is the first exercise.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

CERT-MU of the national Computer Board publishes regularly best practice and guidelines on different themes relevant for industry and for general public on information security. IT Security Unit conducts research on ISO 27000 set of standards for information security and issues security guidelines for the Civil Service.

1.4.2 MANPOWER DEVELOPMENT

CERT-MU of the national Computer Board organizes regular trainings to train local ICT professionals on information security. Certification courses are also organized for both public and private sectors. Postgraduate courses on cyber security are offered at tertiary institutions such as the Ministry of Education and Human Resources, Tertiary Education and Scientific Research or the Tertiary Education Commission.

1.4.3 PROFESSIONAL CERTIFICATION

As part of the capacity building exercise, the National Computer Board has organized the following internationally recognized certification programs. There are more than 100 public sector professionals certified.

1. BS25999 from BSI
2. ISO 27001 Lead Auditor from IRCA

There are public sector professionals also certified on the following internationally recognized certification programs.

Officers of the IT Security Unit currently hold the following certifications:

-Certified Ethical Hacker (CEH)

-Certified Information Systems Security Professional (CISSP)

- Certified Information System Auditor (CISA)

-Certified in Risk and Information System Control (CRISC)

-Certified Information Security Manager (CISM)

1.4.4 AGENCY CERTIFICATION

There are 2 public sector agencies (Passport and Immigration Office and Mauritius Planters Association) who are ISO 27001 certified as of date. The certified government and public sector agency certified under internationally recognized standards in cybersecurity in Mauritius is the Mauritius Standards Bureau.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Mauritius national CERT, CERT-MU has officially recognized partnerships with the following organizations:

- FIRST

-IMPACT.

1.5.2 INTRA-AGENCY COOPERATION

Mauritius has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector through the following instruments:

- CERT-MU that disseminates information security news to the public sector on a daily basis regarding vulnerability note, advisory and virus alerts.

- The 'National Information Security Strategy' of the National ICT Strategic Plan (NICTSP) 2011-2014, which plans for the setting up of a National IT Security Committee with many agencies.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Mauritius has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector through information sharing between ISPs (Internet Service Providers) and ICTA regarding Online Child Sexual Abuse. Information sharing is done in all the Sectors.

1.5.4 INTERNATIONAL COOPERATION

Mauritius is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Mauritius has been a party to the Budapest Convention on Cybercrime since November 2013.

The CERT-MU is a member of FIRST and participates in the FIRST Conference.

Mauritius is among the beneficiaries of the EU/ITU co-funded project "Support for Harmonization of the ICT Policies in Sub-Sahara Africa" (HIPSSA). Mauritius has participated in the following Conferences:

Cyber Security Forum organized by the Commonwealth Telecommunication Organisation and the Forum of the Council of Europe including the Conferences organized under the GLACY (Global Action on Cybercrime) Project funded by Council of Europe.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION AND STRATEGY

Specific legislation on child online protection has been enacted through the following instruments:

- Sections 248, 251 and 288 of the Criminal Code.
- Section 18(m) and 46(h)(i) of the Information and Communication Technologies Act, 2001.
- Sections 13A and 15 of the Child Protection Act, 1995 (not available in pdf or html).
- Section 22 of the Computer Misuse and Cybercrime Act, 2003 (Amends the Child Protection Act.)

Mauritius has adopted the Child Safety Online Action Plan.

2.2 UN CONVENTION AND PROTOCOL

Mauritius has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Mauritius has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Mauritian ICT Authority is responsible for regulating harmful and illegal online content. It has a procedure of content-filtering related to child sexual abuse websites.

The National Computer Board (NCB), operating under the Ministry of Technology, Communication and Innovation and part of the Cybersecurity Emergency Response Team (CERT-MU), has issued a Child Safety Online Action Plan.

The NCB maintains a website dedicated to promote child safety online.

The CERT-MU has a dedicated space to the information of young people and parents.

2.4 REPORTING MECHANISM

The Mauritian ICT Authority provides an online form to report child sexual abuse images. The NCB also provides an online form to report cases related to children issues at Child Development Unit.

CYBERWELLNESS PROFILE

MEXICO

BACKGROUND

Total Population: 116 147 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 43.46%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Federal Criminal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Law on Advanced Electronic Signatures.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Mexico has an officially recognized national CIRT known as CERT-MX.

1.2.2 STANDARDS

In Mexico compliance with ISO standard 207001's requirements for an information security management system is required of all key government institutions. This is the nationally recognized framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Mexico.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

The Specialized Information Security Committee (CESI) was created to develop a National Strategy for Information Security (ENSI), which guides all actions to be undertaken by entities of the federal government to prevent, identify, neutralize or counteract risks and threats to information security.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Mexico.

1.3.3 RESPONSIBLE AGENCY

The Federal Police of Mexico of a national cybersecurity strategy, policy and roadmap by respective agencies.

1.3.4 NATIONAL BENCHMARKING

No data available.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There are no projects or programs for research and development of cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

Personnel at the Scientific Division have received and continue to participate in specialized training from the Police Development System of Mexico (SIDEPOL), as well as from numerous other security and law enforcement organizations in countries including Colombia, the US, Holland and Japan. Government-led efforts to promote increased cybersecurity awareness have included the organization of various conferences for both government institutions and educational institutions.

1.4.3 PROFESSIONAL CERTIFICATION

Mexico does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Mexico does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no information about any framework for sharing cybersecurity assets across borders with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Mexico has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector through CESI authorities have also developed a collaboration protocol between CERT-MX and the various dependencies of the Mexican central government to address and respond to cyber incidents.

1.5.3 PUBLIC SECTOR PARTNERSHIP

CERT-MX also communicates and cooperates directly with private institutions. The ENSI has as one of its primary aims further increasing and institutionalizing cooperation and information-sharing between all sectors of the society-public and private- in a more integrated fashion.

1.5.4 INTERNATIONAL COOPERATION

To facilitate participation in regional/international cybersecurity platforms and forum Mexico is a member of:

-FIRST -OAS/CICTE.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Law for the Protection of Children and Adolescents* -nothing regarding internet.

2.2 UN CONVENTION AND PROTOCOL

Mexico has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Mexico has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Department of Public Safety has issued a document from a cyber-crime workshop containing information on cyber-threats. The national system eMexico works on internet security and presents information on security of internet for children.

2.4 REPORTING MECHANISM

Complaints can be made to The Crimes against Children and Cyber Police Unity by the number 5241-0420 or 01800 440 3690 or by the email policia_cibernetica@ssp.gob.mx. Security Alliance in Mexico provides space for complaints in its website.

CYBERWELLNESS PROFILE

FEDERATED STATES OF MICRONESIA

BACKGROUND

Total Population: 112 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 27.80%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Micronesia does not have officially recognized national legislations on cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Micronesia does not have officially recognised regulations and compliance requirements on cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Micronesia does not have an officially recognized National CIRT.

1.2.2 STANDARDS

Micronesia does not have officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Micronesia does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Micronesia has an officially recognized national cybersecurity strategy (FSM National ICT and Telecommunication Policy (2012).

1.3.2 ROADMAP FOR GOVERNANCE

Micronesia does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The Division of Communication under the Department of Transportation, Communication and Infrastructure is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Micronesia does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Micronesia does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Micronesia does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors. However two workshops were conducted by ITU under ICB4PAC.

1.4.3 PROFESSIONAL CERTIFICATION

Micronesia does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Micronesia does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Micronesia does not have officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Micronesia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Micronesia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Micronesia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

Micronesia also takes part in the Asia Pacific CIRT cybersecurity forums. Micronesia is among the beneficiary countries of the EU/ITU co-funded project “Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries” (ICB4PAC).

Micronesia also participated in several workshops/trainings provided by ITU and APT.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Micronesia does not have specific legislation on child online protection.

2.2 UN CONVENTION AND PROTOCOL

Micronesia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Micronesia has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Micronesia does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Micronesia does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

MOLDOVA

BACKGROUND

Total Population: 3 519 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 48.80%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Penal Code, Law on Preventing and Combating cybercrime

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Law on Informatics
- Law on Access to Information
- Law on Electronic Communications
- Law on Information and State Information Resources
- Law on Electronic Document and Digital Signature
- Law on Personal Data Protection
- Law on E-Commerce

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Moldova has an officially recognized governmental CERT (CERT-GOV-MD).

1.2.2 STANDARDS

There is no available information regarding any officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Moldova has officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals through the Special Telecommunications Center that also operates the second level Public Key Certification Authority (CA). The Special Telecommunications Center is the first and unique CA accredited in Moldova and provides certification services (including Mobile Signature) for public administration authorities and third parties.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Moldova has an officially recognized national strategy for information society development called "Digital Moldova 2020".

1.3.2 ROADMAP FOR GOVERNANCE

There is no available information regarding any national governance roadmap for cybersecurity in Moldova.

1.3.3 RESPONSIBLE AGENCY

The national governmental CERT (CERT-GOV-MD) is the officially recognized institution responsible for implementing a national cybersecurity strategy, policy and roadmap in Moldova.

1.3.4 NATIONAL BENCHMARKING

There is no available information regarding any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development in Moldova.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no information available regarding any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Moldova's Government annually organizes awareness events on cybersecurity. Also The European Cybersecurity Month in Moldova provides educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

There is no available information regarding the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

The national governmental CERT (CERT-GOV-MD) is the only certified government and public sector agency certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Moldova has officially recognized partnerships with the following organizations:

- Romania CERT (CERT-RO)
- Israel CERT (CERT GOVIL)
- United Kingdom CERT (CSIRTUK, and GovCertUK)
- Ukraine CERT (CERT-UA)

Also, in 2013, the e-Governance Academy of Estonia and the e-Government Center of the Republic of Moldova implemented a cybersecurity project.

1.5.2 INTRA-AGENCY COOPERATION

The national governmental CERT (CERT-GOV-MD) has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector with the following organizations:

- Intelligence and Security Service
- Ministry of Information Technology and Communications
- Internet service providers in Moldova

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no information available regarding any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Moldova is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Moldova has also participated in cybersecurity activities with the following organizations:

- NATO
- EU
- Council of Europe
- USAID

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

- Article 208(1) of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Moldova has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Moldova has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Moldova does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Moldova does not have any officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
PRINCIPALITY OF MONACO

BACKGROUND

Total Population: 36 100

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 90.70%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Law on Digital Economy.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

- Law on the Protection of Personal Information.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Monaco does not have any officially recognized national CIRT. ITU conducted a CIRT readiness assessment for Monaco in 2013.

1.2.2 STANDARDS

Monaco does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Monaco.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Monaco does not have any officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Monaco.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Monaco.

1.3.4 NATIONAL BENCHMARKING

Monaco does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Monaco does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Monaco.

1.4.3 PROFESSIONAL CERTIFICATION

Monaco does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Monaco does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Monaco does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Monaco does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Monaco.

1.5.4 INTERNATIONAL COOPERATION

Monaco is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Monaco is a member of the EU and CoE.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

- Articles 294-3 to 294-7 of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Monaco has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Monaco has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible child online protection.

2.4 REPORTING MECHANISM

The government provides an online form to report child pornography content.

CYBERWELLNESS PROFILE

MONGOLIA

BACKGROUND

Total Population: 2 844 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 17.70%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

There is a draft legislation on cybercrime "Draft of Cyber Security ACT 2013" approved by the joint decree of the Minister of Justice and Internal Affairs and Chairman of the General Intelligence Authority.

1.1.2 REGULATION AND COMPLIANCE

Within the scope of the implementation of Government Resolution no. 312 of the year 2011 on "Some measures to ensure state information security", the risk assessment of information security for the state central organizations was conducted in 2012. Based on the assessment report, the preparation to organize trainings among the civil servants on how to prevent risks in the future is now going on.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Mongolia is currently in the process of creating the National CIRT (MNCIRT).

1.2.2 STANDARDS

Mongolia has officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards through the following instruments:

- ISO/IEC 2700x (5 standards)
-MNS ISO/IES 13335-1:2009
-MNS ISO/IES 17799:2007
-MNS 5969:2009 IT & information security techniques and risk management

1.2.3 CERTIFICATION

According to Government Decree no. 312 of the 9 November 2011, the State Communication Office under the auspices of the General Intelligence Authority was reorganized into the Office of Cyber Security to ensure the information security for state organizations and prevent cyber attacks. Also, the Department for Combating Cybercrime was established to combat cybercrime and cyber terrorism at the Criminal Police Office of the General Police Authority on July 2011.

The National Data Center operates the Department for Information Security, Encryption and Protection.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Mongolia is in the process of developing a national cybersecurity strategy. In 2010, the national programme on "Ensuring Information Security" was approved. The programme is to be implemented from 2010 to 2015.

1.3.2 ROADMAP FOR GOVERNANCE

Mongolia has an officially recognized national governance roadmap for cybersecurity that can be found in its national program in information security action plan.

1.3.3 RESPONSIBLE AGENCY

The National Cybersecurity Center is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap in Mongolia.

1.3.4 NATIONAL BENCHMARKING

Mongolia does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Mongolia does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

The National Program of Information Security plan provides educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Mongolia does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Mongolia does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Mongolia does not have any officially recognized national or sector-specific partnerships for sharing cybersecurity assets across borders with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Mongolia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Mongolia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Mongolia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Mongolia also participated in cybersecurity activities of APT cybersecurity forums.

2 CHILD ONLINE PROTECTION

Please note that in Mongolia a child is a person under 16

2.1 NATIONAL LEGISLATION

- Article 123 of the Criminal Code – does not criminalize simple possession.

2.2 UN CONVENTION AND PROTOCOL

Mongolia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

2.3 INSTITUTIONAL SUPPORT

Mongolia does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Mongolia does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE MONTENEGRO

BACKGROUND

Total Population: 633 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 56.80%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Law on Ratification of cybercrime convention

-The Criminal Procedure Code

-The Criminal Legislation Montenegro.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Law on Information Security

-Law on data confidentiality

-Regulation on Information Security Measures.

-Law on Electronic Communications

-Law on Electronic Commerce

-Law on Electronic Signatures

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU completed a CIRT assessment for Montenegro at Belgrade, Serbia from November to December 2010 (15th November-10th December 2010). In April 2012, ITU established the national CIRT of Montenegro, CIRTMontegro. The CIRT is under the Ministry for Information Society and Telecommunications.

1.2.2 STANDARDS

Montenegro has an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards through the Information Security Law and the Regulation on measures for information security.

1.2.3 CERTIFICATION

Montenegro does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Montenegro has an officially recognized national cybersecurity strategy (Cyber security strategy 2013-2017).

1.3.2 ROADMAP FOR GOVERNANCE

The law on information security and regulation of information security measures provides a national governance roadmap for cybersecurity in Montenegro.

1.3.3 RESPONSIBLE AGENCY

Ministry for Information Society and Telecommunications is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Montenegro does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Montenegro does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Montenegro does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Montenegro does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Montenegro does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Montenegro has officially recognized partnerships with the following organizations:

-ITU

-ENISA

-TRUSTED Introducer

-FIRST

-NATO

-CERT/CIRT Networks (Regional cooperation: Slovenian SI-CERT,i-Croatian CERT, Cooperation Agreement with CERT Japan)

-ACDC Project Europe (European center for advanced cyber defense and at the same time build a modern system of protection against botnet at EU level)

1.5.2 INTRA-AGENCY COOPERATION

Montenegro does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Montenegro does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Montenegro is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Montenegro participated in the Applied Learning for Emergency Response Team ALERT 2012 during the ITU Regional Forum on Cybersecurity for Europe and CIS, held in 2012, in Bulgaria.

CIRTMontegro is a member of FIRST.

Montenegro also participated cybersecurity training in Malaysia (ITU), Japan (JICA) and Turkey/Macedonia (NATO)

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-The Criminal Procedure Code.

2.2 UN CONVENTION AND PROTOCOL

Montenegro has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Montenegro has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Montenegro Computer Incident Response Team (CIRTMontenegro) is the officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Montenegro Computer Incident Response Team (CIRTMontenegro) is the officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
MOROCCO

BACKGROUND

Total Population: 32 599 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 56.00%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

-Penal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Law on Personal Data Protection

-Law on Online Consumer Protection

-Law on Electronic Transfer of Legal Information.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Morocco has established an official recognized national CIRT (maCERT).

1.2.2 STANDARDS

Morocco has an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards through the National Strategy for Information Society and Digital Economy and National Strategy of Cybersecurity.

1.2.3 CERTIFICATION

Morocco has an officially approved national (and sector specific) cybersecurity framework for the certification and accreditation of national agencies and public sector professionals. The framework is called the Project of professional master for training and certification of professionals in the public sector.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Morocco has an officially recognized national cybersecurity strategy through the National Strategy of Cybersecurity and National Strategy for Information Society and Digital Economy (Digital Morocco 2013).

1.3.2 ROADMAP FOR GOVERNANCE

The national cybersecurity strategy provides a national governance roadmap for cybersecurity in Morocco.

1.3.3 RESPONSIBLE AGENCY

The General Directorate of Information Security Systems under the Administration of National Defense is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Morocco has officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development. These include a project for identification and classification of national information systems and another project for measuring the level of maturity of these systems.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Morocco does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Actions 50 to 53 of the national strategy "Digital Morocco 2013" are related to cybersecurity trainings and awareness programs. Thus as part of the national cybersecurity strategy, most scientific and technical schools and universities in Morocco integrate into their curriculum, courses in cybersecurity to meet the growing demand for skills in systems information security at national level.

1.4.3 PROFESSIONAL CERTIFICATION

Morocco has 69 public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Morocco has 7 government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Morocco has officially recognized partnerships with the following organizations:

-ITU -South Korea -Cybersecurity Malaysia

-FIRST -France.

1.5.2 INTRA-AGENCY COOPERATION

Morocco does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector

1.5.3 PUBLIC SECTOR PARTNERSHIP

Morocco does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Morocco is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Morocco participated in the ITU-IMPACT Cyber Drill in Muscat, Oman in October, 2013. Morocco participated in the Applied Learning for Emergency Response Teams (ALERT) in Amman, Jordan in July, 2013 (15-17th October 2013). Morocco also participated in the ALERT in Muscat, Oman in October, 2013 (22-24th October 2013). maCERT is a member of FIRST.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-The Criminal Code (Article 483,497 and 503).

2.2 UN CONVENTION AND PROTOCOL

Morocco has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Morocco has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Morocco does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Morocco does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
REPUBLIC OF MOZAMBIQUE

BACKGROUND

Total Population:24 475 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 5.40%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- None.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

- Electronic transaction Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Mozambique does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Mozambique does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Mozambique.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Mozambique does not have an officially recognized national or sector-specific cybersecurity strategy. A National Cybersecurity management system is in the process of being implemented.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Mozambique.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Mozambique.

1.3.4 NATIONAL BENCHMARKING

Mozambique does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Mozambique does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Mozambique.

1.4.3 PROFESSIONAL CERTIFICATION

Mozambique does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Mozambique does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Mozambique does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Mozambique does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Mozambique.

1.5.4 INTERNATIONAL COOPERATION

Mozambique is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- None.

2.2 UN CONVENTION AND PROTOCOL

Mozambique has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Mozambique has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Mozambique.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Mozambique.

CYBERWELLNESS PROFILE

MYANMAR

BACKGROUND

Total Population: 48 724 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 1.20%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

-Electronic Transaction Act.

1.1.2 REGULATION AND COMPLIANCE

Myanmar does not have specific regulation and compliance requirement pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Myanmar has an officially recognized national CIRT (mmCERT). ITU conducted a CIRT for Myanmar in 2011.

1.2.2 STANDARDS

Myanmar does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Myanmar does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Myanmar does not have an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Myanmar does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The Ministry of Communications and Information Technology is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Myanmar does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Myanmar mmCERT cooperates with JPCERT to establish best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

There is the Asean - Japan Joint Cybersecurity Awareness Programs since 2012, which aim to raise awareness of cybersecurity in ASEAN region. In addition, there are some thesis programs of PhD student that are related to cybersecurity.

1.4.3 PROFESSIONAL CERTIFICATION

Myanmar does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Myanmar does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Myanmar has officially recognized partnerships with the following organizations:

-ITU -APCERT -ASEAN China

-FIRST -ASEAN-Japan

1.5.2 INTRA-AGENCY COOPERATION

Myanmar does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Myanmar does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Myanmar is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

Myanmar also participated in cybersecurity activities organized by APCERT, ASEAN-Japan, ASEAN-China and ITU. In 2011 Myanmar hosted the first ITU-IMPACT Applied Learning for Emergency Response Team (ALERT) in Yangon. Myanmar also participated in the ALERT at Vientiane in 2013.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Section 292-293 of the Criminal Code

2.2 UN CONVENTION AND PROTOCOL

Myanmar has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Myanmar has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Myanmar does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Myanmar Computer Incident Response Team (mmCERT) is the officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

NAMIBIA

BACKGROUND

Total Population: 2 364 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 13.90%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

The ECOWAS legislation is being transposed into Namibian legal system. However specific legislation pertaining to cybercrime has already been mandated through the following legal instruments:

-Use of Electronic Transaction and Communication Act

-Cybercrime bill (Draft)

1.1.2 REGULATION AND COMPLIANCE

Namibia does not have any officially recognized national regulation pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Namibia does not have any officially recognized national CIRT.

1.2.2 STANDARDS

Namibia does not have currently any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity but it has started working on it with the development of Cybercrime Bill.

1.2.3 CERTIFICATION

Namibia does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Namibia does not have an officially recognized national cybersecurity strategy but it has started working on it with the development of Cybercrime Bill.

1.3.2 ROADMAP FOR GOVERNANCE

Namibia does not have officially recognized national governance roadmaps for cybersecurity but it has started working on it with the development of Cybercrime Bill.

1.3.3 RESPONSIBLE AGENCY

Namibia does not have an officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap. However there is a committee working on cybersecurity strategy but it has started working on it with the development of Cybercrime Bill.

1.3.4 NATIONAL BENCHMARKING

Namibia does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development but it has started working in it with the development of Cybercrime Bill.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Namibia does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Namibia does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Namibia does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Namibia does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Namibia does not have officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Namibia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Namibia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Namibia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

Namibia is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Namibia does not have any national legislation pertaining to child online protection.

2.2 UN CONVENTION AND PROTOCOL

Namibia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Namibia has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Namibia does not have any officially recognized agencies that offer institutional support on child online protection.

2.4 REPORTING MECHANISM

Namibia does not have any officially recognized agencies that offer an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
NAURU

BACKGROUND

Total Population: 10 293

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: N/A

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Nauru does not have specific officially recognized national legislation pertaining to cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Nauru does not have specific regulations and compliance requirement pertaining to cyber security.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Nauru does not have an officially recognized national CIRT. However it is a member of the Pacific CERT (PACCERT).

1.2.2 STANDARDS

Nauru does not have officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Nauru does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Nauru does not have an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Nauru does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Nauru does not have an officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Nauru does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Nauru does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Nauru does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Nauru does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Nauru does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Nauru does not have officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Nauru does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Nauru does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Nauru is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Nauru is among the beneficiary countries of the EU/ITU co-funded project “Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries” (ICB4PAC).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Sections 227-229 of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Nauru has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Nauru signed but did not ratify articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Nauru does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Nauru does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

FEDERAL DEMOCRATIC REPUBLIC OF NEPAL

BACKGROUND

Total Population: 31 011 00

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 13.30%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- The Electronic Transactions Act.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

- The Electronic Transactions Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Nepal does not have an officially recognized national CIRT. ITU conducted a CIRT assessment for Nepal in 2010.

1.2.2 STANDARDS

Nepal does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Nepal.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Nepal does not have any officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Nepal.

1.3.3 RESPONSIBLE AGENCY

The Kathmandu Metropolitan Police Crime Division (KMPCD) is the agency responsible for cybersecurity in Nepal.

1.3.4 NATIONAL BENCHMARKING

Nepal does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Nepal does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Nepal.

1.4.3 PROFESSIONAL CERTIFICATION

Nepal does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Nepal does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Nepal does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Nepal does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Nepal.

1.5.4 INTERNATIONAL COOPERATION

Nepal is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Section 47 of the Electronic Transaction ordinance

- Section 2(c1) under Some Public (Crime and Punishment) Act

- Section 16(2) and (3) of the Children's Act, 2048 – only for children under 16.

2.2 UN CONVENTION AND PROTOCOL

Nepal has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Nepal has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Nepal.

CYBERWELLNESS PROFILE
KINGDOM OF THE NETHERLANDS

BACKGROUND

Total Population: 16 714 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 93.9564%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Penal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Electronic Signature Law - Decision on Electronic Signatures - Data Protection Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Until the National Cyber Security Centre was set up, GOVCERT.NL was the government organization dedicated to cyber security and incident response. The tasks and employees of GOVCERT.NL have all been transferred to the Center. This has ensured that the NCSC has had a sound foundation from the beginning. Therefore NCSC is the nationally recognized CIRT.

1.2.2 STANDARDS

There is no information on any internationally recognized standards used in The Netherlands. However, The Netherlands' iStrategy will make generic frameworks, services and products available to all Central Government organizations.

1.2.3 CERTIFICATION

The Netherlands does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

The Netherlands has adopted The National Cyber Security Strategy (NCSS), National Cyber Security Strategy 2 and The Defense Cyber Strategy as its national cybersecurity strategies.

1.3.2 ROADMAP FOR GOVERNANCE

The Netherlands has a nationally recognized governance roadmap for cybersecurity: 2014-2016 Action Programme Annex 1 to the NCSS 2.

1.3.3 RESPONSIBLE AGENCY

The following are the officially recognized agencies responsible for implementing the national cybersecurity strategy, policy and roadmap:

- National Coordinator for Security and Counterterrorism (NCTV) - NCSC.

1.3.4 NATIONAL BENCHMARKING

The Netherlands has officially recognized the Cybersecurity Assessment Netherlands (CSBN) as the body responsible for the national benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

The NCSC is the officially recognized national agency responsible for research and development (R&D) programs/projects for cybersecurity standards and best practices and guidelines to be applied in either the private or the public sector. It fulfils this function by collecting knowledge and expertise in the field of cybersecurity from all sectors of society, both practical knowledge and data from scientific research. The government, businesses and universities are able to pool their knowledge in the Center.

1.4.2 MANPOWER DEVELOPMENT

NCSC's Expertise & Advice and Sharing knowledge is recognized as the national program for raising awareness and promoting cybersecurity especially educational programs among the public and private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

There is no record of how many professionals are certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

NCSC is the certified government and public sector agency certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, the Netherlands has officially recognized partnerships with the following organizations:

- EGC
- CSIRT

1.5.2 INTRA-AGENCY COOPERATION

Various agencies are able to share cybersecurity assets in The Netherlands through the High-Tech Crime Unit of the Dutch Police Services Agency (KLPD) and through the NCSC.

1.5.3 PUBLIC SECTOR PARTNERSHIP

The Netherlands has an officially recognized national program for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

The NCSC is a member of the following:

- FIRST - TERENA - ENISA - EGC.

The Netherlands is involved in international cooperation with many other agencies.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

- Article 240b of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

The Netherlands has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. The Netherlands has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Government Computer Emergency Response Team of the Netherlands (GOVCERT.NL), merged with the NCSC, provides information on internet safety. The DigiAware Program, supported by the Ministry of Economic Affairs, Agriculture and Innovation, provides information about internet safety.

2.4 REPORTING MECHANISM

Online illegal content can be reported in the website of Meldpunt.

CYBERWELLNESS PROFILE

NEW ZEALAND

BACKROUND

Total Population: 44 610 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 82.78%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- 248-259 Crimes Act 1961.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Electronic Transaction Act
- Electronic Data Safety Bill
- Unsolicited Electronic Messages Act
- Electronic Identity Verification Bill
- Government Communications Security Bureau Act
- The Telecommunications (Interception Capability and Security) Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

The New Zealand National Cyber Security Centre (NCSC) is the national CIRT responsible for enhanced services to government agencies and critical infrastructure providers to assist them to defend against cyber-borne threats.

1.2.2 STANDARDS

Standards New Zealand is the nationally recognized agency responsible for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no nationally recognized body in New Zealand for certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

New Zealand's Cybersecurity Strategy is the officially recognised strategy document in place to ensure a systematic government-level response to various cyber threats to national security.

1.3.2 ROADMAP FOR GOVERNANCE

There is no officially recognised roadmap for cybersecurity in New Zealand.

1.3.3 RESPONSIBLE AGENCY

The agency responsible for overseeing the implementation of New Zealand's Cybersecurity Strategy is the Government Communications Security Bureau (GCSB).

1.3.4 NATIONAL BENCHMARKING

The GCSB Annual Report and Compliance Report are the nationally recognised benchmarks for cybersecurity in New Zealand.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Unitec is home to New Zealand's first Cybersecurity Centre which is the officially recognized national or sector-specific research and development (R&D) program/project for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector. The University of Waikato has a group known as Cyber Security Researchers of Waikato (CROW).

2.4.2 MANPOWER DEVELOPMENT

GCSB provides various educational and professional training programs in order to raise awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in both public and private sectors throughout New Zealand.

1.4.3 PROFESSIONAL CERTIFICATION

There is no record of the number of public officers that are certified in cybersecurity.

1.4.4 AGENCY CERTIFICATION

New Zealand does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

2.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, New Zealand (NCSC) partners with the following International organizations:

- CPNI - GovCertUK - US CERT - CCIRC - CERT Australia.

1.5.2 INTRA-AGENCY COOPERATION

New Zealand has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector through the (NCSC)'s partnership with the following:

- Department of Internal Affairs
- New Zealand Police
- Ministry of Business, Innovation and Employment
- Domain New Commission.

1.5.3 PUBLIC SECTOR PARTNERSHIP

The (NCSC) partners with a range of organisations from the private sector such as:

- Netsafe - InternetNZ - Connect Smart - New Zealand Internet Task force.

1.5.4 INTERNATIONAL COOPERATION

New Zealand participates in several cybersecurity activities with APCERT.

3 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Sections 124 and 131B of the Crime Act.
- Sections 3, 127 of the Films, Videos and Publications Classification Act.

2.2 UN CONVENTION AND PROTOCOL

New Zealand has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

New Zealand has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The following institutions are responsible for child online protection:

- (NCSC)
- The Privacy Commissioner
- The Police of New Zealand
- The Department of Internal Affairs.

2.4 REPORTING MECHANISM

NCSC provides the number (04) 498-7654 and a report to be completed in its website.

CYBERWELLNESS PROFILE
REPUBLIC OF NICARAGUA

BACKGROUND

Total Population: 5 955 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 15.50%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Criminal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Law on Electronic Signature

- Law on Personal Data Protection.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Nicaragua does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Nicaragua does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Nicaragua.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Nicaragua does not have an officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Nicaragua.

1.3.3 RESPONSIBLE AGENCY

Nicaraguan Committee on Science and Technology (CONICYT) and the Commission on Electronic Government in Nicaragua (GOBENIC) are the agencies responsible for cybersecurity in Nicaragua.

1.3.4 NATIONAL BENCHMARKING

Nicaragua does not have officially recognized national benchmarking or referential to measure cybersecurity.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

Academic institutions including the National University of Engineering, Central University, and National University of Managua offer coursework and specialized training in information security-related topics and computer forensics.

1.4.3 PROFESSIONAL CERTIFICATION

Nicaragua does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Nicaragua does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Nicaragua does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

There is no information about any international cooperation that Nicaragua participates in.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Articles 175 and 176* of the Criminal Code

- Article 5* of Law n. 287 – Code for Childhood and Adolescence.

2.2 UN CONVENTION AND PROTOCOL

Nicaragua has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Nicaragua has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency that is responsible for child online protection.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to receiving complaints of incidents in Nicaragua.

CYBERWELLNESS PROFILE

REPUBLIC OF NIGER

BACKGROUND

Total Population: 16 644 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 1.70%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Law on Offences in the Field of Computer.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- None.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Niger does not have any officially recognized national CIRT. Niger completed a CIRT assessment conducted by ITUin 2011.

1.2.2 STANDARDS

Niger does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Niger.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Niger does not have any officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Niger.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Niger.

1.3.4 NATIONAL BENCHMARKING

Niger does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Niger does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

Niger has a Parliamentary Day of Information Technology on Cybercrime: Equipping Parliament on the issue of cybercrime.

1.4.3 PROFESSIONAL CERTIFICATION

Niger does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Niger does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Niger does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Niger does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Niger.

1.5.4 INTERNATIONAL COOPERATION

Niger is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Niger is also a member of ECOWAS which has a mandate through a Directive to fight against cybercrime.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Articles 275, 276, 282 and 293 of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Niger has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Niger has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Niger.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Niger.

CYBERWELLNESS PROFILE
NIGERIA

BACKGROUND

Total Population: 166 629 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 38.00%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation pertaining to cybercrime is mandated through the following legal instruments:

-Money laundering (prohibition) Act 2011

- Advance Free Fraud & other related Offences Act 2006

- Evidence Act 2001

- Cybercrime Bill 2013 (in view).

1.1.2 REGULATION AND COMPLIANCE

There is no available information concerning any officially recognised regulation pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU-IMPACT completed a CIRT readiness assessment for Nigeria at Burkina Faso in May 2010. Nigeria has an officially recognized CIRT (CERRT.ng) by the Office of National Security Adviser. Nigeria is also in process of building another officially recognized national CIRT (NGCERT).

1.2.2 STANDARDS

The technical framework for cyber and information security (NCC) is the officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards. The Legal Framework for CIS Operational Procedure Manual for CIS is currently in view.

1.2.3 CERTIFICATION

The Computer Forensics Institute of Nigeria (CFIN) and the Association of Certified Cybersecurity Policy are the officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

The Office of the National Security Adviser (ONSA) has officially produced a draft on National cybersecurity policy and on National cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

The Office of the National Security Adviser (ONSA) provides a National cybersecurity roadmap.

1.3.3 RESPONSIBLE AGENCY

Nigeria has officially recognized the following agencies responsible for implementing a national cybersecurity strategy, policy and roadmap.

- Ministry of Communication Technology
- Office of the National Security Adviser
-Nigerian Communications Commission
-Economic and Financial Crimes Commission
-National Information and Technology Development Agency.

1.3.4 NATIONAL BENCHMARKING

Nigeria has officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development through the following instruments:

- Cybersecurity Strategy Bootcamp
- Cyber Security Stakeholder's Forum
- National Information and Technology Development Agency
- Office of the National Security Adviser.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Nigeria does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector. However, there is a review of the readiness of social media networks and its implications to telecommunications regulation and national security.

1.4.2 MANPOWER DEVELOPMENT

Nigeria does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors. However there is collaboration with the Department of Homeland Security on "Stop.Think.Act" Campaign for Nigeria. CERRT.NG is also engaged in promoting cybersecurity awareness campaigns.

1.4.3 PROFESSIONAL CERTIFICATION

Nigeria has 4 public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

The Central Bank of Nigeria is the only public agency certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Nigeria has officially recognized partnerships with the following organizations:

-FIRST
- Egypt (in progress).

1.5.2 INTRA-AGENCY COOPERATION

Nigeria has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector through the following instruments:

- Cybersecurity Forum
-Communication Channel among Nigerian CERT using PGP
-National Information and Technology Development Agency (in progress)
-Internet Governance Forum.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Nigeria has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector through the following instruments:

- Cybersecurity Forum
-Communication Channel among Nigerian CERT using PKI
-National Information and Technology Development Agency (in progress)
-Internet Governance Forum

1.5.4 INTERNATIONAL COOPERATION

Nigeria is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Nigeria is among the beneficiaries of the EU/ITU co-funded project "Support for Harmonization of the ICT Policies in Sub-Sahara Africa" (HIPSSA).

Nigeria also participated in the following cybersecurity activities:

-ITU Impact
-CTO – Commonwealth Telecommunications Organization
-ICANN
-AFRICACERT (Africacert.org).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child protection has been enacted through the following instrument:

- Chapter 21A of the Criminal Code – *does not explicitly criminalize child pornography but only obscene publications*.

2.2 UN CONVENTION AND PROTOCOL

Nigeria has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Nigeria has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Nigeria does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Nigeria does not have any officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

NORWAY

BACKGROUND

Total Population: 4 960 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 95.05%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Penal Code (Proposal)
- General Civil Penal Code (Penal Code).

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Electronic Commence Act
- Electronic Communication Act
- Personal Data Act
- Electronic Signature Act
- Act concerning Electronic Money Institutions
- Freedom of Information Act
- Act of 20 March 1998 relating to Protective Security Services.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Norway has an officially recognized national CIRT NorCERT operated by The Norwegian National Security Authority (NSM).

1.2.2 STANDARDS

Norway is a member of the ETSI standard organization and aligns with its standards for Cybersecurity.

1.2.3 CERTIFICATION

SERTIT offers a cybersecurity framework for the certifications and accreditations of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Norway has an officially recognized National Cybersecurity Policy National Strategy for Cyber Security . The NSM is currently developing the Norwegian Computer Network Defence (CND) strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no nationally recognized roadmap for Norway's cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The NSM, being a cross-sectoral professional and supervisory authority within the protective security services in Norway, is also responsible for matters of cybersecurity.

1.3.4 NATIONAL BENCHMARKING

There is no officially recognized national benchmarking exercise or program for cybersecurity in Norway.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Center for Cyber and Information Security (CCIS) provides training and study programs and Norway *has officially* recognized it as the national research and development (R&D) program/project for cybersecurity.

1.4.2 MANPOWER DEVELOPMENT

CCIS provides a wide range of organizations with a research and education centre in information. The CCIS also partners with the following:

- National Security Agency - Police Directorate - IBM

1.4.3 PROFESSIONAL CERTIFICATION

NSM-NorCERT team member are certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Norway's NSM-NorCERT is responsible for government and public sector agencies' certification under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states NSM-NorCERT partners with its counterparts worldwide.

1.5.2 INTRA-AGENCY COOPERATION

There is no record of any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no record of a framework for sharing cybersecurity assets between the public and private sector in Norway.

1.5.4 INTERNATIONAL COOPERATION

NSM-NorCERT is a member of FIRST.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- §204 and §204a* of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Norway has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Norway has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The following are the institutions responsible for the protection of children online:

- The Norwegian Media Authority - You Decide
- The Norwegian Communication Authority

2.4 REPORTING MECHANISM

Computer incidents can be reported to the NorCERT at the email address norcert@cert.no or by the phone number 02497.

CYBERWELLNESS PROFILE

OMAN

BACKGROUND

Total Population: 2 904 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 66.45%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Anti Cybercrime Act -E-Transaction Law -Telecom Act.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-General Security Policy -Internet and Email Policy -Web and e-services Policy -Oman e-Governance Framework (OeGAF).

1.2 TECHNICAL MEASURES

1.2.1 CIRT & RCC

Oman has an officially recognized national CIRT (OCERT). The national CIRT also hosts the first ITU Regional Cybersecurity Centre (RCC) established in 2013.

1.2.2 STANDARDS

Oman Information Technology Authority has an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards. The framework is based upon ISO 27001 standards.

1.2.3 CERTIFICATION

Through the cybersecurity professional development service Oman National CERT offers professional cybersecurity training in different security domains by providing information security competency and capability courses and certifications. The execution of the program is accomplished through strategic collaborations with reputable organisations in Oman and international accreditation institutions like (ISC), SANS and EC-council.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Oman has an officially recognized High Level Cyber Security Strategy and Master Plan.

1.3.2 ROADMAP FOR GOVERNANCE

Oman has a national governance roadmap for cybersecurity under the High Level Cybersecurity Strategy and Master Plan.

1.3.3 RESPONSIBLE AGENCY

Oman National CIRT (OCERT) is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

As part of its continuous effort in measuring the cybersecurity development in Oman OCERT is conducting a national cybersecurity survey at different levels. It also carries out cybersecurity audit and compliance against issued policies and framework. Oman also has an agreement with Ernest and Young to conduct a benchmark exercise under the Global Information Security Survey (GISS). The GISS provides organisation with an opportunity to compare themselves with others on important information security issues and gain insights for making key decisions through questions relates to security budget, investments, security governance, security effectiveness, maturity of security programs, security environment, and emerging technologies and trends.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

OCERT through its research and analysis team lead the development of national projects such as:

-National early warning Project -Intelligence gathering Project -National Cyber Clean Program

In addition, the Research Council is Oman's exclusive research funding body and leader of research development in the country. TRC serves as a focal point and hub dedicated to promoting and supporting research, scientific enquiry, and innovation in the Sultanate of Oman and Research and development in cyber security is one of the main areas focused by TRC.

1.4.2 MANPOWER DEVELOPMENT

The National CIRT (OCERT) has launched several cybersecurity training and awareness initiatives as below:

- National Awareness Campaign
- "Way Campaign" OCERT Unified Government Information Security Campaign
- Child Online Protection Campaign
- OCERT Ambassador Program

OCERT is working closely with Ministry of Education to introduce Information Security Curriculum in schools. In addition OCERT is an advisory member at Ministry of Manpower IT Committee reviewing IT and Security curriculums for the higher technical colleges. OCERT is also an advisory board member of private college.

1.4.3 PROFESSIONAL CERTIFICATION

Oman has about 350 public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Oman has 7 government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Oman has officially recognized partnerships with the following organizations:

-ITU	-APWG	-Malware Alliance
-FIRST	-HoneyNet Project	-GCC CERT/OIC CERT
-Estonia	-Singapore	-China (in progress)
-Malaysia (in progress)	Korea (in progress).	

1.5.2 INTRA-AGENCY COOPERATION

Oman has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector through the OCERT Ambassador Program that creates permanent links between OCERT and its constituents.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Oman has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector. For example, it has a Cybersecurity Information Exchange with private security center and the Cybersecurity Agreement with private security services providers' (Microsoft Security Cooperation Program).

1.5.4 INTERNATIONAL COOPERATION

Oman is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

OCERT is a member of FIRST.

Oman also participated in the following international cybersecurity activities:
- FIRST Conference and Annual Meetings Japan, Malta, Austria, US, Bangkok
- National CSIRT Meetings of CMU, Japan, Malta, Austria, US, Bangkok
- GCC CERT Continuous meetings, Saudi Arabia, QATAR, Muscat
- Working Group on Legal Framework for COP in the Arab region- June 2013 - Cairo
- Cyber Defence Summit 2012 & 2013, Muscat
- ITU-IMPACT Applied Learning for Emergency Response Teams (ALERT) from 15-17 July 2012 - Amman, Jordan
- 1st Cyber Security Forum for energy and utilities – Abu Dhabi 2012
- COP legal Framework for the Arab countries – Algeria 2012
- Arab Internet Governance Forum – October 2012 - Kuwait
- OIC –CERT Conference and Annual Meeting 2012 – Muscat
- Gulf Cyber Crime Conference 2011, Muscat
- ITU Regional Workshop on "Policy Advocacy & Capacity Building in Child Online Protection for the Arab Region" Muscat-Oman, 30-31 October 2011
- MIS – CISO Executive Summit 2010, Muscat
- OIC-CERT Conference, 2009, Kuala Lumpur, 2010 UAE, 2011 Muscat
- GOVCERT conference, 2008, Rotterdam, Holland
- CERT- Computer Emergency Response Centers workshop, 2008, Cairo, Egypt
- ITU cybersecurity working group meeting, 2007, Geneva, Switzerland

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Penal Code (Article 220)

-Cybercrime Law (Article 14 and 15)

2.2 UN CONVENTION AND PROTOCOL

Oman has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Oman has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Oman Computer Incident Response Team is the officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Oman Computer Incident Response Team is the officially recognized agency that offers an avenue for the reporting of incidents related to child online protection. Incidents can also be reported online on the Kids Online Security Website.

CYBERWELLNESS PROFILE ISLAMIC REPUBLIC OF PAKISTAN

BACKGROUND

Total Population: 179 951 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 10.90%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- None.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

- Electronic Transactions Ordinance.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Pakistan has an officially recognized national CERT known as PakCERT. PISA-CERT is Pakistan's first public CERT.

1.2.2 STANDARDS

Pakistan does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Pakistan.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Pakistan does not have an officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Pakistan.

1.3.3 RESPONSIBLE AGENCY

There is no recognized agency for cybersecurity in Pakistan.

1.3.4 NATIONAL BENCHMARKING

Pakistan does not have any officially recognized national benchmarking or referential for measuring cybersecurity.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

PakCERT has a Security Awareness Public Services. It also organizes seminars and presentations in different IT events.

1.4.3 PROFESSIONAL CERTIFICATION

Pakistan does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Pakistan does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Pakistan does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

PISA R3C is the newly formed collaborative project where multi-sector teams can join together to leverage each other's' skills set and resources to better address the needs of its partners. The core objective of the project is to bring experts, academia, the public sector and law enforcement closer.

1.5.4 INTERNATIONAL COOPERATION

Pakistan is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Pakistan participates in Asia Pacific Security Incident Response Coordination Working Group APSIRC-WG.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

- Section 293 of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

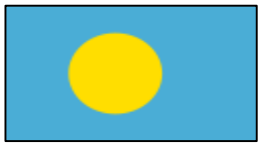
Pakistan has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Pakistan has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for online child protection.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to receiving reports of incidents.



CYBERWELLNESS PROFILE
REPUBLIC OF PALAU

BACKGROUND

Total Population: Unknown

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: Unknown%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- None.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- None.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Palau does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Palau does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Palau.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Palau does not have an officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Palau.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Palau.

1.3.4 NATIONAL BENCHMARKING

Palau does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Palau does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Palau.

1.4.3 PROFESSIONAL CERTIFICATION

Palau does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Palau does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Palau does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Palau does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Palau.

1.5.4 INTERNATIONAL COOPERATION

Palau participates in the PacCERT .

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- None.

2.2 UN CONVENTION AND PROTOCOL

There is no information on whether Palau has acceded to the Convention on the Rights of the Child.

There is no information on whether Palau has acceded to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Palau.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Palau.

CYBERWELLNESS PROFILE STATE OF PALESTINE

BACKGROUND

Total Population: unknown

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 46.60%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- None.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

- Electronic Transactions Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Palestine does not have any officially recognized national CIRT.

1.2.2 STANDARDS

Palestine does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Palestine.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Palestine has an officially recognized Information Security Policy and the National Strategy for Information and Communication Technology.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Palestine.

1.3.3 RESPONSIBLE AGENCY

The Ministry of Communication and Information Technology is the agency responsible for cybersecurity in Palestine.

1.3.4 NATIONAL BENCHMARKING

Palestine does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

The Information Security Bulletins serve as an educational tool and to promote professional cybersecurity awareness.

1.4.3 PROFESSIONAL CERTIFICATION

Palestine does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Palestine does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no framework to facilitate sharing of cybersecurity assets across borders or with other nation states in Palestine.

1.5.2 INTRA-AGENCY COOPERATION

Palestine does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Palestine.

1.5.4 INTERNATIONAL COOPERATION

There is no information on any international cooperation Palestine participates in.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:
- None.

2.2 UN CONVENTION AND PROTOCOL

Palestine has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Palestine has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Palestine.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Palestine.

CYBERWELLNESS PROFILE
PANAMA

BACKGROUND

Total Population: 3 625 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 42.90%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Penal Code

-Law on Electronic Signature

1.1.2 REGULATION AND COMPLIANCE

Panama does not have specific regulations and compliance requirements pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Panama has established an officially recognized National CIRT.

1.2.2 STANDARDS

Panama has an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards through the National Cybersecurity Strategy.

1.2.3 CERTIFICATION

Panama does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Panama has an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Panama is currently developing the national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The National Innovation Agency is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Panama does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Panama does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Panama has an officially recognised national cooperation agreement with STOP.THINK.CONNECT in 2013. The purpose of the agreement was to enable the public awareness program to reach people around the country and unite the hemisphere in the fight against cybercrime.

1.4.3 PROFESSIONAL CERTIFICATION

Panama does not know the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Panama does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Panama does not have officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Panama does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Panama does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Panama is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Panama also works very closely with the OAS/CICTE and with the OAS Member States in implementing a hemispheric cooperation web forum.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- The Criminal Code (Articles 184-188 and 190*)

-Law n. 16 – Contribution to the prevention and elimination of commercial sexual exploitation of children and adolescents in Central America, Panama and Dominican Republic (Chapter IV*)

2.2 UN CONVENTION AND PROTOCOL

Panama has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Panama has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Panama does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Panama Computer Incident Response Team (CSIRT Panama*) is the officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
PAPUA NEW GUINEA

BACKGROUND

Total Population: 7 171 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 6.50%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Papua New Guinea does not have specific legislation on cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Papua New Guinea does not have specific legislation and regulation related to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Papua New Guinea does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Papua New Guinea does not have officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Papua New Guinea does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Papua New Guinea does not have an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Papua New Guinea does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The National Information Communication and Technology Authority (NICTA) is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Papua New Guinea does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Papua New Guinea does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Papua New Guinea does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Papua New Guinea does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Papua New Guinea does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Papua New Guinea does not have officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Papua New Guinea does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Papua New Guinea does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Papua New Guinea is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Papua New Guinea is among the beneficiary countries of the EU/ITU co-funded project “Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries” (ICB4PAC).

Papa New Guinea is also a member of the APT and participates in APT organized Forum on cybersecurity.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Sections 229C and 229R-T of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Papua New Guinea has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

2.3 INSTITUTIONAL SUPPORT

Papua New Guinea does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Papua New Guinea does not have any officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

PARAGUAY

BACKGROUND

Total Population: 6 683 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 36.90%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Law No. 4439/2011 amending the Penal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-None.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Paraguay has an officially recognized national CIRT known as CERT-PY.

1.2.2 STANDARDS

Paraguay does not have an officially recognized national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Paraguay.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Paraguay does not have an officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Paraguay.

1.3.3 RESPONSIBLE AGENCY

CERT-PY and the National Secretariat for Information and Communication Technologies (SENATICs) are the lead authorities for cybersecurity in Paraguay. The Specialized Unit for Computer Crime, within the Office of the National Prosecutor, is the lead agency responsible for investigating and prosecuting cybercrimes.

1.3.4 NATIONAL BENCHMARKING

Paraguay does not have any officially recognized national benchmarking or referential to measure cybersecurity.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

The government currently works with key private sector entities to develop shared norms for information security, including cooperation and information sharing.

1.4.2 MANPOWER DEVELOPMENT

The government has undertaken a campaign called “Connect Yourself Safe PY [Paraguay]”, the principle objective of which is to increase the public’s consciousness about the dangers of posting sensitive personal information on social networking sites. SENATIC adopted a complementary initiative in 2013, STOPTHINKCONNECT, or PARAPIENSACONECTATE in Spanish, which is in the implementation phase.

1.4.3 PROFESSIONAL CERTIFICATION

Paraguay does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Paraguay does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Assistance has been received from numerous partners including the OAS, the US Department of State (DS/ATA), and other competent national authorities in the region. CERT-PY has been actively developing its cooperative ties with other national CSIRTs in the region, which it reported has enabled it to stay better informed of evolving cyber threats and techniques.

1.5.2 INTRA-AGENCY COOPERATION

Paraguay does not have any officially recognized national or sector-specific program for sharing cybersecurity assets.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Paraguay.

1.5.4 INTERNATIONAL COOPERATION

Paraguay is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Paraguay also hosted the Congress on Cybersecurity.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:
- Article 135* of the Criminal Code.
- Article 31* of the Law 1681/2001, Child and Adolescence Code, June 2003.
- Law n. 2861/2006*, “That restrain trade and commercial or noncommercial dissemination of pornographic material, using the image or other representation of minors or mental unable”, January 2006.

2.2 UN CONVENTION AND PROTOCOL

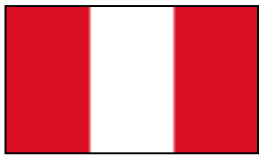
Paraguay has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Paraguay has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no institutional support for child online protection in Paraguay.

2.4 REPORTING MECHANISM

CERT-PY provides an email to report abuses: abuse@csirt.gov.py.



CYBERWELLNESS PROFILE
REPUBLIC OF PERU

BACKGROUND

Total Population: 29 734 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 39.20%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Penal Code
- Computer Crimes Act
- Incorporating Computer Crimes in the Criminal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Protection of Personal Data - Digital Signatures and Certificates Law.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Peru has an officially recognized national CIRT known as PeCERT.

1.2.2 STANDARDS

There is no officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Peru.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Peru has an officially recognized cybersecurity strategy known as Plan Estratégico en Seguridad Informática y de la Información.

1.3.2 ROADMAP FOR GOVERNANCE

Peru does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The PeCERT and the Division of High Technology Crimes (DIVINDAT) are responsible for cybersecurity in Peru.

1.3.4 NATIONAL BENCHMARKING

Peru does not have an officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no program or project for research and development of cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

DIVINDAT and PeCERT actively train their personnel to maintain and develop their capacity to perform their core functions. Internal awareness raising initiatives within their own institutions have entailed a full range of activities to ensure users' understanding of concepts not always associated with but key to cybersecurity such as physical security, security logic, and human security. External awareness raising activities have included media campaigns, and outreach and education for private sector entities including banks, payment processors, and other business and commercial interests. Awareness raising campaigns have also targeted citizens at large, emphasizing basic good practices for reducing vulnerability and protecting one's identity and information while using the Internet and ICTs.

1.4.3 PROFESSIONAL CERTIFICATION

Peru does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Peru does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states DIVINDAT actively seeks assistance from foreign entities where and when appropriate. It also maintains active partnerships with and supports the efforts of national and international NGOs working to combat cyber and other crimes that have utilized ICTs.

1.5.2 INTRA-AGENCY COOPERATION

Peru does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

PeCERT has initiated a dialogue to increase collaboration with the private sector, particularly ISPs and banks.

1.5.4 INTERNATIONAL COOPERATION

Peru is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Peru also participates in the OAS CICTE.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Articles 181-A* and 183-A* of the Criminal Code, added by the law n. 28.251 from April 1991.

2.2 UN CONVENTION AND PROTOCOL

Peru has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Peru has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no information about any agency responsible for child online protection in Peru.

2.4 REPORTING MECHANISM

PeCERT provides an email to report incident: pecert@pcm.gob.pe.

CYBERWELLNESS PROFILE

PHILIPPINES

BACKGROUND

Total Population: 96 471 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 37.00%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Cyber Crime Prevention Act - RA 10175.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Data privacy Act of 2012 RA 10173
- Electronic Act of 200 RA 8792
- Anti-Child Pornography Act of 2009 RA 9775.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Philippines has an officially recognized national CERT (PHCert).

1.2.2 STANDARDS

Philippines has an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards through iGovPhil services which include a single sign-on facility, a Public Key Infrastructure for secured online transactions.

1.2.3 CERTIFICATION

Philippines does not have an officially approved national (and sector specific) cybersecurity framework for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Philippine has an officially recognized national cybersecurity plan 2005.

1.3.2 ROADMAP FOR GOVERNANCE

Philippines does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Philippines has officially recognized the following agencies responsible for implementing a national cybersecurity strategy, policy and roadmap:

- Cyber Crime Unit and Cyber Crime Unit
- Computer Forensic Labs Computer Forensic Labs
- Zamboanga City Zamboanga City
- General Santos City General Santos City
- Davao City Davao City
- DOST-ICTO Cyber Security Section

1.3.4 NATIONAL BENCHMARKING

DOST-ICTO Cyber Security Section is responsible for benchmarking and measuring cybersecurity development in Philippines.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Philippines does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Philippines has officially recognized through ISACA a sector-specific educational and professional training program for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors. ISACA engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. It provides practical guidance and other effective tools for all enterprises that use information systems.

1.4.3 PROFESSIONAL CERTIFICATION

Philippines does not know the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Philippines does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Philippines does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5.2 INTRA-AGENCY COOPERATION

Philippines does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Philippines does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5.4 INTERNATIONAL COOPERATION

Philippines is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:
- Articles 201 and 355 of the Criminal Code.
- Section 4(c)(1) of the Cybercrime Act.

2.2 UN CONVENTION AND PROTOCOL

Philippines has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Philippines has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Philippines does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Philippines does not have any officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
REPUBLIC OF POLAND

BACKGROUND

Total Population: 38 317 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 62.8492%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Penal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Act on Electronic Signature
- Act on Electronic Payment Instruments
- The Act on the Protection of Personal Data
- Act on Providing Services by Electronic Means
- The Act on the Computerisation of the Operations of Entities Performing Public Tasks.

1.2 TECHNICAL MEASURES

1.2.1 CIRT & RCC

Poland has an officially recognized national CIRT called CERT.GOV.PL. The first CERT created in Poland was the CERT Polska followed by the PIONIERCERT and the TP CERT.

1.2.2 STANDARDS

There is no information available about any officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards in Poland.

1.2.3 CERTIFICATION

There is no information about any framework for certification and accreditation of national agencies and public sector professionals in Poland.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Poland has officially recognized national cybersecurity strategy and protection plans which are: National Security Strategy of the Republic of Poland and Cyberspace Protection Policy of the Republic of Poland.

1.3.2 ROADMAP FOR GOVERNANCE

Poland has a national governance roadmap for cybersecurity under the Cyberspace Protection Policy of the Republic of Poland.

1.3.3 RESPONSIBLE AGENCY

The Ministry of Administration and Digitization, The Ministry of National Defense and the Internal Security Service are the officially recognized agencies responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

There are reports on the activities of the CERT.GOV.PL and also reports on the state of cybersecurity in Poland.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

The National Cryptology Center is responsible for the research and development (R&D) of cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

The National CIRT CERT.GOV.PL conducts series of free training for administrators of IT systems of public administration. Courses are offered in cooperation with the Internal Security Agency Microsoft IT security SCP (Security Cooperation Program).

1.4.3 PROFESSIONAL CERTIFICATION

The CERT.GOV.PL members are certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

CERT.GOV.PL and TP CERT are certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

In facilitating sharing of cybersecurity assets across borders or with other nation states, Poland has officially recognized partnerships with the following through CERT.GOV.PL and CERT Polska:

- FIRST - TI.

1.5.2 INTRA-AGENCY COOPERATION

Poland has officially recognized ARAKIS-GOV as a national program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no information on any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector in Poland.

1.5.4 INTERNATIONAL COOPERATION

Poland is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

CERT Polska is a member of FIRST.

Poland also participates in international cybersecurity activities with the following:

- ENISA - NATO.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:
- Articles 197, 200a and 202 of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Poland has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Poland has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no information on any agencies in Poland that support child online protection.

2.4 REPORTING MECHANISM

Online illegal content can be reported on the website of Dyzurnet.

CYBERWELLNESS PROFILE PORTUGUESE REPUBLIC

BACKGROUND

Total Population: 10 699 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 62.10%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Penal Code
- Cybercrime Law.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Law on protection of Personal Data
- Law on Electronic Commerce
- Law on Electronic Signature
- Law on Electronic Communications
- Law on Legal protection of Computer Programs
- Law on Electronic Communications Infrastructure.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Portugal has an officially recognized national CIRT known as CER.PT.

1.2.2 STANDARDS

Portugal has an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Decree-Law 166-A/2006 creates the electronic certification system of the State-Public key infrastructure and also designates the national security authority as the national accrediting authority. The national security authority is competent to issue the accrediting certificate of the certifying entities exercising the accrediting competencies foreseen.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Through the Resolution of the Council of Ministers, there is a strategic plan to rationalize and reduce costs with the Information Technology and Communication, the task of coordinating with the relevant entities of the definition and implementation of a National Strategy for Information Security, which comprises, among other measures, the creation, installation and operation of a National Centre for Cybersecurity.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Portugal.

1.3.3 RESPONSIBLE AGENCY

The proposed National Cybersecurity Center will be responsible for cybersecurity.

1.3.4 NATIONAL BENCHMARKING

Portugal does not have an officially recognized national benchmarking or referential for measuring cybersecurity development

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no *officially* recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There is no known awareness program, training program or workshop on cybersecurity, for the general public or for public and private sector employees in Portugal.

1.4.3 PROFESSIONAL CERTIFICATION

Portugal does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

CER.PT has been certified since the 2004 under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no framework for sharing cybersecurity assets across borders with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Portugal does not have any framework for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no framework for sharing cybersecurity assets between the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Portugal participates in the EU/ENISA.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

- Article 172 of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Portugal has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Portugal has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Internet Segura* a public private partnership, gives information on online safety.

2.4 REPORTING MECHANISM

Online illegal content can be reported on the website of Linha Alerta (*).

CYBERWELLNESS PROFILE

QATAR

BACKGROUND

Total Population: 1 939 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 85.30%

(data source: ITU Statistics,2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Cybercrime Law (final draft phase)

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Information Privacy Law (final draft phase)

-Critical Information Infrastructure Protection Law (Final draft phase)

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Qatar has an officially recognized National CIRT (QCERT).

1.2.2 STANDARDS

Qatar has an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards through the National Information Assurance Framework (NIAF).

1.2.3 CERTIFICATION

Qatar recently endorsed the Accreditation & Certification Framework, anticipating to be enforced early 2014. The NIAF is an officially approved national (and sector specific) cybersecurity framework for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Qatar has finalized the National Cyber Security Strategy and it is currently under review by the Strategy Stakeholders.

1.3.2 ROADMAP FOR GOVERNANCE

The NIAF provides a national governance roadmap for cybersecurity in Qatar.

1.3.3 RESPONSIBLE AGENCY

The Cybersecurity Division at the Ministry of Information Communication & Technology is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Qatar does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

The Qatar Computing Research Institute (QCRI) has officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards.

1.4.2 MANPOWER DEVELOPMENT

Qatar national CIRT (QCERT) conducted several awareness programs on Cyber Safety and capacity building e.g. SANs institute to deliver security Technical courses for practitioners. The website is www.safespace.qa.

1.4.3 PROFESSIONAL CERTIFICATION

Qatar does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Qatar does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Qatar has official recognized partnerships with the following organizations:

-ITU
-Meridian Process
-OWASP
-FIRST
-APWG
-Cloud Security Alliance
-GCC CERT.

1.5.2 INTRA-AGENCY COOPERATION

Qatar has an officially recognized national program (National Incident Handling Framework) for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Qatar has an officially recognized national program for sharing cybersecurity assets within the public and private sector. An Information Risk Expert Committee will be set up for each industry sector.

1.5.4 INTERNATIONAL COOPERATION

Qatar is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Qatar also is a member of ICANN, FIRST, Meridian Process, OWASP, APWG, Cloud Security Alliance. In addition, it is a voting member in Industry System Automation and GCC CERT. Qatar participated in the 2012 ITU-IMPACT Workshop and the ITU RCC Regional cybersecurity Forum Cyber Drill 2013 in Oman. QCERT is a member of FIRST.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

-The Criminal Code (Article 292).

2.2 UN CONVENTION AND PROTOCOL

Qatar has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Qatar has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Qatar Computer Incident Response Team (QCERT) is the officially recognized agency that offers institutional support on child online protection. It monitors and restrains online threats, making available different information on Cybersecurity and Child Online Protection.

In addition the Government maintains Safe Space (*), a website dedicated to inform children, parents and educators about online threats, best practices, policies and tools for Cyber-safety. Furthermore the National Committee for Internet Safety, under ictQATAR, aggregates government representatives, law enforcement, academia, non-governmental organizations, parents and local youth.

2.4 REPORTING MECHANISM

Qatar Computer Incident Response Team (QCERT) is the officially recognized agency that offers an avenue for the reporting of incidents related to child online protection. Safe Space (*) also provides an avenue for the reporting of incidents.

CYBERWELLNESS PROFILE
ROMANIA

BACKROUND

Total Population: 1 314 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 49.76%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-The Budapest Convention, ratified by the Law no. 64/2004

-Law no. 161/2003 - Anti-Corruption Law – Title III - on preventing and fighting cybercrime (Art.42-51)

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Romania's Cyber Security Strategy and the National Action Plan on implementation of the national cyber security (2013) approved through GD 271/2013

-The Directive of the European Parliament and of the Council on attacks against information systems, to be transposed by 4 September 2015.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Romania has an officially recognized national CIRT (CERT-RO).

Romania has also few sectorial CERT:

- CERT-MIL (MoD) - CYBER-INT (Romanian Intelligence Service) - CORIS (Special Telecommunications Service)

1.2.2 STANDARDS

There is no available information concerning any officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no available information concerning any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Romania has an officially recognized national cybersecurity strategy (Romania's Cyber Security Strategy - national cybersecurity strategy (2013)).

1.3.2 ROADMAP FOR GOVERNANCE

The National Action Plan on implementation of the Romania's Cybersecurity Strategy provides a national governance roadmap for cybersecurity in Romania.

1.3.3 RESPONSIBLE AGENCY

The Ministry of Communication and Informational Society monitors and coordinates the implementation of a national cybersecurity strategy, policy and roadmap by respective agencies.

1.3.4 NATIONAL BENCHMARKING

Romania has not yet officially recognized national benchmarking for the national cyber crisis management plan. However, Romania participated in the annual exercise coordinated by ENISA in 2011 and 2013 and CERT-RO was the national actor.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Romania *does not have officially* recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector. However In the framework of European Cybersecurity Month, CERT-RO carried out, beside private sector partners, an awareness campaign regarding to cybersecurity issues. In this framework, were posted on the CERT-RO web site the cyber security standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Romania does not have yet any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors. However CERT-RO is currently implementing a European funded project, with the final goal to set up a National System for Countering Cybercrime.

1.4.3 PROFESSIONAL CERTIFICATION

Romania does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity since databases are operated by each responsible public institution.

1.4.4 AGENCY CERTIFICATION

There is no available information concerning any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, CERT-RO signed MoU for cooperation on network security and emergency response, with many other national or governmental CERTs team from different countries as follows:
-Hungary -Kazakhstan -Uzbekistan - South Korea - Japan - Republic of Moldova -P.R. of China
Also, another European project named Advanced Cyber Defence Centre (ACDC), carried out under FP7 European program by CERT-RO, has as a major objective, the establishment of the European antibotnet platform.

1.5.2 INTRA-AGENCY COOPERATION

Romania has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector through the national and sectorial CIRT: (CERT-RO, CERT-MIL, CORRIS). CERT-RO signed a Memorandum of Understanding (MoU) and Protocols with more than 20 public institutions in the cybersecurity field. Also, National System for Countering Cybercrime, could be considered the framework for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

CERT-RO signed Memorandum of Understanding (MoU) and Protocols with private entities in cybersecurity field from antivirus company as Bitdefender to bank CERT teams.

1.5.4 INTERNATIONAL COOPERATION

Romania is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Romania recognized participation in regional and international cybersecurity platforms and forums since it is affiliated with ENISA and TERENA. CERT-RO is a member of FIRST.

Romania participated in the International Cyber Shield Exercise 2014 in Turkey (ICSE 2014).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Articles 374 and 375* of the Criminal Code.
- Articles 7, 11, 13 and 14* of the Law on Preventing and Combating Pornography.
- Article 51* of the Anti-corruption Law.

2.2 UN CONVENTION AND PROTOCOL

Romania has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Romania has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Information on internet safety can be found in the website of the Romanian National Computer Security Incident Response Team (CERT-RO (*)).

2.4 REPORTING MECHANISM

Illegal content can be reported in the website of Focus Internet Hotline*.

CYBERWELLNESS PROFILE RUSSIAN FEDERATION

BACKGROUND

Total Population: 142 703 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 61.40%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Criminal code (art. 271-273).

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Federal Law 152 on Personal Data Protection - regulated by Roscomnadzor (Telecommunications Regulator)

-Federal Law 139 on Blacklisting and ISP control - regulated by Roscomnadzor (Telecommunications Regulator).

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Russia has an officially recognized governmental CERT (GOV-CERT), a joint government project CIRT (RU-CERT) and one based on Group IB, the leading Russian company in incident response business CIRT (CERT-GIB).

1.2.2 STANDARDS

Russia does not have an officially approved national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Russia does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Russia has officially recognized a National Security Concept of the Russian Federation (2000), a concept of the Foreign Policy of the Russian Federation (2013), an Information Security Doctrine of the Russian Federation (2000), basic Principles for State Policy of the Russian Federation in the Field of International Information Security (2013) and conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space (2011) .

However the draft of Russia's Cyber Security Strategy is underway.

1.3.2 ROADMAP FOR GOVERNANCE

Russia does not currently have any national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Russian Federal Security Service (FSB), Federal Protection Service (FSO), Federal Service for Technical and Export Control (FSTEC), Ministry of Internal Affairs (MVD), Ministry of Defence (MoD) and the Foreign Intelligence Service (SVR) are the officially recognized institutions responsible for implementing a national cybersecurity strategy, policy and roadmap in Russia.

1.3.4 NATIONAL BENCHMARKING

Each government entity in Russia performs an annual audit of its own networks and systems depending on the requirements of the information.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Russia has *officially* recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector through the ITU-T study group question 17 on security.

1.4.2 MANPOWER DEVELOPMENT

Russia does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Russia does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

There is no available information regarding any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, the Russian company in incident response business CIRT (CERT-GIB) has officially recognized partnerships with the League of Safer Internet and the National Coordination Centre.

1.5.2 INTRA-AGENCY COOPERATION

Russian Federal Security Service (FSB) has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector with the following organizations:

Federal Service for Technical and Export Control (FSTEC)	Ministry of Defence (MoD)
Ministry of Internal Affairs (MVD)	Financial Crimes Unit in Federal Tax Services.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Russia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Russia does not have any officially recognized participation in regional and/or international cyber security platforms and forums.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

- Article 242 of the Criminal Code – *does not criminalize simple possession*.

2.2 UN CONVENTION AND PROTOCOL

Russia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Russia has signed but not ratified (as of 14th December 2014), the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Russia does not have ant officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Cyber Security and Incident Response Team for the governmental networks of the Russian Federation (GOV-CERT.RU (*)) provides space in its website to report a computer incident.

Safer Internet Centre for Russia (*) provides space in its website to report online illegal content.

The Friendly RUNET Foundation (*) provides space (*) in its website to report online illegal content.

CYBERWELLNESS PROFILE

RWANDA

BACKGROUND

Total Population: 11 272 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 8.70%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Penal Code

-Law on Electronic Message, Signature and Transaction

-Draft ICT bill.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-National Standards for Cyber Security.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Rwanda has an officially recognized national CIRT Rw-CSIRT.

1.2.2 STANDARDS

Rwanda developed an Information Security Framework referred to as Government Security Architecture. This architecture provides information security policies, procedures and guidelines for the public and private sector.

1.2.3 CERTIFICATION

Rwanda does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals. However a draft national policy has been developed and submitted for cabinet approval. This allows the establishment of the organization in charge of cyber security, which will perform certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Rwanda does not yet have an officially recognized national cybersecurity policy. However there is a draft National Cyber Security Policy. This policy defines priority areas in the field of cyber security. It has been submitted to cabinet for approval and further dissemination.

1.3.2 ROADMAP FOR GOVERNANCE

Rwanda does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The Specialized Cyber Security Division in Rwanda Development Board (RDB) is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Rwanda has officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development. The last exercise was performed in 2013.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Research and Development (R&D) was defined as the most priority initiative in the National Information and Communication Infrastructure Plan (NICI III) and in the draft National Cyber Security Policy. In addition, a Unit in charge of R&D was established under the National CSIRT.

1.4.2 MANPOWER DEVELOPMENT

The Ministry of Education introduced different information security course modules in the overall IT or Computer engineering program in tertiary institutions. In the ICT skills development plan, IT security training and certification program was developed. For cyber security awareness, the Government of Rwanda developed a National Cyber Security Awareness and Training Program; this program promotes cyber security awareness for internet users in Rwanda and also promotes the development of security professional (i.e. cyber security workforce) in Rwanda that support the public and private institutions to protect their critical systems against cyber threats.

1.4.3 PROFESSIONAL CERTIFICATION

Rwanda has 80 public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Rwanda does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity. However Rwanda started the implementation of a Certification Authority (CA) which will be responsible of information certification with the usage of digital certificate. In addition, the draft National Cyber Security Policy defines the establishment of a cybersecurity agency, which will be in charge of information security compliance and certification.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Rwanda has officially recognized partnerships with the following organizations:

-ITU

-Korea KISA

1.5.2 INTRA-AGENCY COOPERATION

Rwanda has officially recognized national programs for sharing cybersecurity assets within the public sector through the national CIRT.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Rwanda has officially recognized programs for sharing cybersecurity assets within the public and private sector through the national CIRT.

1.5.4 INTERNATIONAL COOPERATION

Rwanda is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Rwanda participated in different regional cyber security fora. In East Africa Community (EAC) Rwanda was part of the forum which developed EAC framework for cyber security laws. Rwanda also participated in the forum to develop Africa Union Cyber Security Framework.

Rwanda is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Articles 211, 229 and 230 of the Organic Law Instituting the Penal Code

2.2 UN CONVENTION AND PROTOCOL

Rwanda has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Rwanda has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Rwanda does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Rwanda does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

SAINT LUCIA

BACKGROUND

Total Population: 178 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 35.20%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Criminal Code

- Electronics Crimes Bill.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Electronics Crimes Bill

- Interception of Communications Bill.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Saint Lucia does not have any officially recognized national CIRT.

1.2.2 STANDARDS

Saint Lucia does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Saint Lucia.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Saint Lucia does not have any officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Saint Lucia.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Saint Lucia.

1.3.4 NATIONAL BENCHMARKING

Saint Lucia does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Saint Lucia does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Saint Lucia.

1.4.3 PROFESSIONAL CERTIFICATION

Saint Lucia does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Saint Lucia does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Saint Lucia does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Saint Lucia does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Saint Lucia.

1.5.4 INTERNATIONAL COOPERATION

Saint Lucia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Saint Lucia hosted the eighth Caribbean Internet Governance Forum and Cyber Security Workshop from 29 to 30 August 2014 hosted in collaboration with the government of Saint Lucia, the Commonwealth Foundation for ICT and the Diplo Foundation.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- None.

2.2 UN CONVENTION AND PROTOCOL

Saint Lucia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Saint Lucia has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Saint Lucia.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Saint Lucia.

CYBERWELLNESS PROFILE

SAMOA

BACKGROUND

Total Population: 185 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 15.30%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Crimes Act 2013 (which deals with accessing electronic system without authorization; illegal remaining in an electronic system, illegal interception, damaging or interfering with electronic data, SPAM etc.)
- Criminal procedures Act 1972 (currently reviewing)

1.1.2 REGULATION AND COMPLIANCE

Aside from the Crimes Act 2013 aspects of cybersecurity are evident in particular enactments such as the Telecommunications Act 2005, Broadcasting Act 2010, Electronic Transactions Act 2008, Copyright Act 1998, Mutual Assistance in Criminal Matters Act 2007, Money Laundering Prevention Act 2007.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Samoa does not have currently have an officially recognized CIRT. But Samoa has sought through a proposal ITU assistance to establish its national CIRT entity. It must be noted however that Samoa is a member of PacCERT.

1.2.2 STANDARDS

Samoa does not have officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally standards.

1.2.3 CERTIFICATION

Samoa does not have an officially approved national (and sector specific) cybersecurity frameworks for certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Currently there is no national or sector-specific cyber security strategy and/ or policy on cybersecurity in Samoa but there are some initiatives under the National ICT Sector Plan which are in the pipeline.

However it is important note that on an official scale it is recognized under the National Information and Communication Technology policy 2012-2017 the need to create an enabling secure environment for the development and adoption of ICT through policy reform and improvements in legal frameworks, striving to put in place legislation to ensure the protection of children in relation to use of ICT and the security of information shared and access using ICT e.g. cybercrime laws.

1.3.2 ROADMAP FOR GOVERNANCE

Samoa does not have an officially recognized national or sector-specific governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The Office of the Regulator is at the forefront of implementing cybersecurity initiatives. However considering a holistic approach of promoting and having central focus on the implementation of cybersecurity strategy/policy/roadmap there is no national or sector-specific agency specifically responsible for implementing a national cybersecurity strategy/ policy/roadmap.

1.3.4 NATIONAL BENCHMARKING

Samoa does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Samoa does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

A workshop on Concepts and Techniques of Developing Cyber Crime Policy and Legislation was hosted by the Office of the Attorney General and the Office of the Regulator in partnership with ITUand European Commission under the ICB4PAC Project.

Also, the Ministry of Police conducted several safety campaigns against cybercrime activities in Samoa in collaboration with telecom service providers.

1.4.3 PROFESSIONAL CERTIFICATION

Samoa does not have an official record of any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Samoa does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Samoa has officially recognized partnerships with the following Organizations:

-Pacific ICT Regulatory Resource Center (“PIRRC”) -Pacific Computer Emergency Response Team (“PacCERT”)

-Pacific Transnational Crime Network - ITU

-Virtual Global Taskforce (Interpol is a member of Virtual Global Taskforce). - Interpol (Samoa is a member of Interpol)

1.5.2 INTRA-AGENCY COOPERATION

Samoa does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Samoa does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Samoa is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Samoa also participated in several cybersecurity activities with ITU and EU.

Samoa is among the beneficiary countries of the EU/ITU co-funded project “Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries” (ICB4PAC).

Samoa is also a participant in the following regional and international platforms and forums:

- Pacific Island Chapter of the Internet Society (“PICISOC”) -Asia Pacific Network Information Center (“APNIC”)

- Pacific Computer Emergency Response Team (“PacCERT”) - Asia Pacific Telecommunity (“APT”)

- Pacific ICT Regulatory Resource Center (“PIRRC”) - Cyber Safety Pasifika

-Virtual Global Taskforce -Interpol

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Sections 43 and 44 of the Crime Offences Act – provides only provision against distribution or exhibition of indecent matter but does not explicitly mention child pornography.

-Section 218 of Samoa Crimes Act 2013 – only criminalizes solicitation of children through the use of information and communication technology.

2.2 UN CONVENTION AND PROTOCOL

Samoa has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

2.3 INSTITUTIONAL SUPPORT

Samoa does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Samoa does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
REPUBLIC OF SAN MARINO

BACKGROUND

Total Population: 33 400

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 50.80%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Rules Concerning the Processing of Personal Data related to Information Technology Art. 17 of Law 23/05/1995 n.70

-Art 204, 403- Penal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:
-Law n.115 dated 20/07/2005 Digital document and digital signature
-Law n.58 dated 29/05/2013 Use of Electronic Communications and e-Commerce
-Law n.140 dated 26/11/1987 Procedure modality for the authorization of private databases
-Law n.71 dated 23/05/1995 Collection of statistic data and competences in the state information technology
-Art. 17 of Law 23/05/1995 n.70 Rules concerning the processing of personal data related to information technology
-Decree n.27 dated 13/03/1984 and decree n.67 dated 03/06/1986 The State Database and assign the maintenance management to private firms
-Decree n.156 dated 08/11/2005 Technical rules for the creation, transmission, preservation, duplication, reproduction and validation, of digital documents.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

San Marino does not have an officially recognized national CIRT.

1.2.2 STANDARDS

San Marino does not have an officially approved national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in San Marino.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

San Marino does not have an officially recognized national or sector-specific cybersecurity strategy or policy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no officially recognized national governance roadmap for cybersecurity in San Marino.

1.3.3 RESPONSIBLE AGENCY

The Information Technology Authority (Autorità per l'Informatica) is responsible for the information technology planning among the Public Administration.

The Information Technology Office (Ufficio Informatica, Tecnologia, Dati e Statistica) is the agency responsible for the technical support, operational and administrative authority for information technology in the preparation, management and development of the IT plan of the State.

1.3.4 NATIONAL BENCHMARKING

San Marino does not have an officially recognized national benchmarking exercise or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no officially recognized national or sector-specific research and development (R&D) program/project for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector in San Marino.

1.4.2 MANPOWER DEVELOPMENT

There is no officially recognized national or sector-specific educational and professional training program for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in San Marino.

1.4.3 PROFESSIONAL CERTIFICATION

San Marino does not have public sector professionals certified under internationally recognized certification program in cybersecurity.

1.4.4 AGENCY CERTIFICATION

San Marino does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states San Marino and the Italian Republic signed an agreement on mutual cooperation in cybercrime prevention and suppression. Cooperation takes place mainly through the NCB Interpol.

1.5.2 INTRA-AGENCY COOPERATION

San Marino does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in San Marino.

1.5.4 INTERNATIONAL COOPERATION

San Marino is a member of the ICPO-INTERPOL.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:
-Article 3* of the Law on the Repression of Sexual Exploitation of Minors.

2.2 UN CONVENTION AND PROTOCOL

San Marino has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

San Marino has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in San Marino.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to report of incidents in San Marino.

CYBERWELLNESS PROFILE
SAO TOME AND PRINCIPE

BACKGROUND

Total Population: 182 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 23.00%

(data source: ITU Statistics, 2013)

1 CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Sao Tome and Principe does not have any officially recognized national legislation pertaining to cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Sao Tome and Principe does not have any officially recognized regulation pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Sao Tome and Principe currently does not have any officially recognized national CIRT.

1.2.2 STANDARDS

Sao Tome and Principe does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Sao Tome and Principe does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Sao Tome and Principe does not have any officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Sao Tome and Principe does not have any officially recognized national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The General Regulatory Authority (AGER) is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Sao Tome and Principe does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Sao Tome and Principe does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Sao Tome and Principe does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Sao Tome and Principe does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Sao Tome and Principe does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Sao Tome and Principe does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Sao Tome and Principe does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Sao Tome and Principe does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Sao Tome is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Sao Tome is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA). Sao Tome and Principe is also a member of ARCTEL.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

-The Criminal Code (Article 180).

2.2 UN CONVENTION AND PROTOCOL

Sao Tome and Principe has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

2.3 INSTITUTIONAL SUPPORT

Sao Tome and Principe does not have any the officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Sao Tome and Principe does not have any the officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
KINGDOM OF SAUDI ARABIA

BACKGROUND

Total Population: 28 705 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 60:50%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Anti-Cyber Crime Law.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

- Electronic Transactions Law.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Saudi Arabia has an officially recognized national CIRT known as CERT SA.

1.2.2 STANDARDS

Saudi Arabia does not have an officially approved national or sector specific cybersecurity framework for Cybersecurity.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Saudi Arabia.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

There is no national or sector-specific cybersecurity policy in Saudi Arabia.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Saudi Arabia.

1.3.3 RESPONSIBLE AGENCY

CERT SA is the agency responsible for cybersecurity in Saudi Arabia.

1.3.4 NATIONAL BENCHMARKING

Saudi Arabia does not have an official national benchmarking and referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no *officially* recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

CERT SA security quality management is responsible for awareness building and education/training.

1.4.3 PROFESSIONAL CERTIFICATION

There is a certified professional statistics database where this information is stored.

1.4.4 AGENCY CERTIFICATION

Saudi Arabia does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no framework for sharing cybersecurity assets across borders with other nation states in Saudi Arabia.

1.5.2 INTRA-AGENCY COOPERATION

Saudi Arabia does not have an officially recognized national or sector-specific program for sharing cybersecurity assets.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Saudi Arabia.

1.5.4 INTERNATIONAL COOPERATION

Saudi Arabia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

Saudi Arabia participates in the following cybersecurity activities:

- APWG - OIC-CERT - The Honeynet Project.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Articles 6 and 8(3) of the Anti-Cybercrime Law (*).

2.2 UN CONVENTION AND PROTOCOL

Saudi Arabia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Saudi Arabia has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Computer Emergency Response Team of Saudi Arabia CERT.SA (*) provides specific information (*) on child online protection.

2.4 REPORTING MECHANISM

The website of CERT.SA provides space in its website for reporting a computer incident but requires a login to do so. It is still possible to contact the CERT through an online form or the mail: info@cert.gov.sa.

CYBERWELLNESS PROFILE REPUBLIC OF SENEGAL

BACKGROUND

Total Population: 13 108 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 20.90%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Senegal Law on Cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Cryptology Law

- Data Protection Law

- Electronic Transactions Law

- Law Guiding the Information Society.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU-IMPACT completed a CIRT assessment in Senegal in 2011. Senegal does have an official national CIRT.

1.2.2 STANDARDS

Senegal does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Senegal.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Senegal does not have an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Senegal.

1.3.3 RESPONSIBLE AGENCY

Senegal has proposed to establish a National Cybersecurity Centre to be funded by the EU.

1.3.4 NATIONAL BENCHMARKING

Senegal does not have an officially recognized national benchmarking or referential for measuring cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no officially recognized national or sector-specific research and development or program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There is no educational and professional training program for raising awareness, higher education and certification.

1.4.3 PROFESSIONAL CERTIFICATION

Senegal does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Senegal does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Senegal does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Senegal.

1.5.4 INTERNATIONAL COOPERATION

Senegal is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Senegal partners in a joint project of EU and Council of Europe on Global Action on Cybercrime (GLAY).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Articles 256, 318 and 320bis* of the Criminal Code.

- Articles 431(34)-431(37), 431(42), 431(58), 431(59) and 431(64)* of the Law on Cybercrime.

2.2 UN CONVENTION AND PROTOCOL

Senegal has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Senegal has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection.

2.4 REPORTING MECHANISM

There is no website or hotline to report incidents in Senegal.

CYBERWELLNESS PROFILE

SERBIA

BACKGROUND

Total Population: 9 847 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 51.50%

(data source: ITU Statistics, December 2012)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation pertaining to cybercrime is mandated through the following legal instrument:

- Criminal Code art. 298-304a.

1.1.2 REGULATION AND COMPLIANCE

Serbia does not have any specific legislation and regulation regarding cybersecurity and compliance requirements.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU conducted a CIRT readiness assessment for Serbia in 2010. Serbia has not yet established and legally mandated a national CERT. However the following institutions' tasks are connected to CERT functions.

- Administrative Agency for Joint Service of Government Authorities performs the tasks of managing security risks in information-communication systems of public administration bodies, protecting the public administration network and data, cooperation and coordination related to information security.

- The Academic Network of the Republic of Serbia (AMRES) is a public institution that performs the CERT activities for the educational and scientific-research institutions in the Republic of Serbia.

1.2.2 STANDARDS

Serbia does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Serbia does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Serbia does not have any officially recognized national cybersecurity strategy. However Serbia adopted a development strategy for Information Society in the Republic of Serbia by 2020 which has six priorities for development. One of the strategy priorities is Information Security, which will have to be developed by improving legal and institutional framework, critical infrastructure protection, fight against cybercrime and scientific, research and development work.

1.3.2 ROADMAP FOR GOVERNANCE

The Action plan (2013-2014) determines activities for the cybersecurity improvement in Serbia. The competent institution for proposing strategic and action plan documents in the area of information society is Ministry of Trade, Tourism and Telecommunications.

1.3.3 RESPONSIBLE AGENCY

The Ministry of Trade, Tourism and Telecommunications is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Serbia does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Serbia does not yet have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Serbia does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

The Academic Network of the Republic of Serbia (AMRES) team members are certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

The Academic Network of the Republic of Serbia (AMRES) is the official certified government and public sector agency certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Serbia does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Serbia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Serbia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Serbia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Serbia participated in the second conference of South-Eastern Europe National Security Authorities (SEENSA) and the Serbian NSA participated on the third conference about information security and cybernetic defence “ISCD 2013” in Hungary.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION AND STRATEGY

Specific legislation on child protection has been enacted through the following instruments:

-Article 185 of the Criminal Code.

-Articles 54 and 55 of the Law on Amendments and Additions to the Criminal Code, n. 72/09.

2.2 UN CONVENTION AND PROTOCOL

Serbia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Serbia has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Serbia does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

The Safer Internet Hotline “Net Patrol” provides an online form to report illegal content.

CYBERWELLNESS PROFILE
REPUBLIC OF SEYCHELLES

BACKGROUND

Total Population: 87 400

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 50.40%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Computer Misuse Act.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Electronic Transactions Act

- Data Protection Act (partial document).

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Seychelles does not have any officially recognized national CIRT.

1.2.2 STANDARDS

Seychelles does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Seychelles.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Seychelles does not have an officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Seychelles.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Seychelles.

1.3.4 NATIONAL BENCHMARKING

Seychelles does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Seychelles does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Seychelles.

1.4.3 PROFESSIONAL CERTIFICATION

Seychelles does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Seychelles does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Seychelles does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Seychelles does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Seychelles.

1.5.4 INTERNATIONAL COOPERATION

Seychelles is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

- Section 152 of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Seychelles has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Seychelles has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for the child online protection in Seychelles.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Seychelles.

CYBERWELLNESS PROFILE

SIERRA LEONE

BACKGROUND

Total Population: 6 126 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 1.70%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Sierra Leone does not have specific legislation on cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Sierra Leone does not have specific legislation and regulation related to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Sierra Leone does not have an officially recognized national CIRT. However ITU conducted the "Enhancing Cybersecurity for Least Developed Countries (LDC) Program" in Sierra Leone from 2 to 13 December 2013.

1.2.2 STANDARDS

Sierra Leone does not have officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Sierra Leone does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Sierra Leone does not have an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Sierra Leone does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The National Telecommunications Commission (NATCOM) is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Sierra Leone does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Sierra Leone does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Sierra Leone does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Sierra Leone does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Sierra Leone does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Sierra Leone does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Sierra Leone does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Sierra Leone does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Sierra Leone is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Sierra Leone is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

Sections 1 and 26-28 of the Sexual Offenses Act of Sierra Leone

2.2 UN CONVENTION AND PROTOCOL

Sierra Leone has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Sierra Leone has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Sierra Leone does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Sierra Leone does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

SINGAPORE

BACKGROUND

Total Population: 5 256 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 73.00%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Computer Misuse and Cybersecurity Act (Chapter 50A).

1.1.2 REGULATION AND COMPLIANCE

"Instruction Manual (IM) 8" specifies government policies, standards, regulations and codes of practice for IT security implemented by government agencies, that private vendors serving the government would also need to comply with. All IMs are mandatory for compliance by government agencies and subject to regular audit and assessment for enforcement purposes.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Singapore has an officially recognized national CIRT known as SingCERT. For the Government sector, the Government IT Security Incident Response (GITSIR) team co-ordinates with government agencies to perform investigations and supports agencies' response to the incident.

1.2.2 STANDARDS

Internationally recognised cybersecurity standards (such as ISO27000 series) are referenced in the development of Government security policies and standards. For the Telecommunications sector, internationally recognised cyber security standards (such as ISO27011) were referenced in the development of the Secure and Resilient Internet Infrastructure *Code of Practice.*

1.2.3 CERTIFICATION

Cybersecurity professionals are encouraged to obtain international certifications such as CISSP and the SANS series of certification. IDA's Critical Infocomm Technology Resource Programme (CITREP) provides support to offset the cost for people taking such certifications.

The Association of Information Security Professionals (AISP) aims to transform Infocomm security (IS) into a distinguished profession, with a recognised body, qualifications, established career paths and career development programmes.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Singapore has an officially recognized National Cyber Security Masterplan 2018 to further secure Singapore's cyber environment. As regulator of the financial services industry, the Monetary Authority of Singapore (MAS) uses a number of regulatory instruments to regulate and shape the conduct of financial institutions. While IDA does not have privileged access to MAS's cybersecurity strategy for the financial services industry, the publicly available 'Technology Risk Management Guidelines' and the Circular No. SRD TR01/2011: Information Technology Outsourcing sets out the risk management principles and standards to guide financial institutions in managing technology and IT outsourcing risks, including those relating to cybersecurity.

1.3.2 ROADMAP FOR GOVERNANCE

The National Cyber Security Masterplan 2018 launched to further secure Singapore's cyber environment and developed through a multi-agency effort led by IDA provides an overarching strategic direction to help Government and organisations in strengthening resilience against cyber threats.

1.3.3 RESPONSIBLE AGENCY

National Infocomm Security Committee is the national-level committee responsible for steering cybersecurity strategy in Singapore. Secretariat support is provided by Infocomm Development Authority.

1.3.4 NATIONAL BENCHMARKING

IDA's Infocomm Security Health Scorecard put in place to measure the level of security readiness, assesses the state of info-security health of government agencies in areas such as policies, standards, the security knowledge of public officers, as well as physical and environmental security. The scorecard is aimed at helping government agencies to improve their info-security strategies and processes.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

One of the research and development (R&D) themes under the National Cybersecurity R&D Programme is on 'cyberspace governance & policy research'. The Programme is currently undergoing grant call phase. iTrust is a multidisciplinary research centre located at the Singapore University of Technology and Design (SUTD), established collaboratively by SUTD and the Ministry of Defence, Singapore which focus is on cybersecurity.

1.4.2 MANPOWER DEVELOPMENT

Singapore has recognized various types of awareness programs on cybersecurity, for the general public as well as for public and private sector employees.

- National Infocomm Competency Framework (NICF) launched in 2008 serves as a reference for companies to use in their HR management of ICT professionals. Individuals (students and professionals) can also leverage on the framework to plan for their skills upgrading and career development.

-Critical Infocomm Technology Resource Programme (CITREP) established by the Infocomm Development Authority of Singapore (IDA) has the objective to accelerate the development of emerging, critical and specialised infocomm skills to meet Singapore's infocomm manpower needs.

-Company-Led training and Centres of Attachment aims to develop graduates and professionals through on-job-training and mentorship opportunities by leveraging local or overseas industry and education partners. These programs with focus on emerging skills will provide locals with structured quality learning and better career progression for the locals.

-Association of Information Security Professionals (AISP) aims to promote and enhance the information security profession in Singapore.

-National Cyber Security Masterplan 2018 aims to raise the awareness and adoption of cyber security best practices among the Public, Private and People sectors.
-There is collaboration between National Research Foundation (NRF) and IDA for Post-Grad Scholarship in Cybersecurity.

1.4.3 PROFESSIONAL CERTIFICATION

Singapore does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Singapore Prison service (SPS) has been certified for ISO/IEC 27001:2005 (Management and Operations of Data Centre Infrastructure Services). ISO/IEC 27001:2005 is a risk based information security standard and it is a requirement for organizations to have in place a risk management process based on the Plan-Do-Check-Act" (PDCA), Deming cycle approach. As part of maintaining the ISMS certification, organization needs to perform continual review on their information security program and ensuring effectiveness of security controls

Government Agencies comply with IM8 standards and ISD's Green book which has incorporated good practices but it is not an internationally recognised standard.

"Instruction Manual (IM) 8" specifies government policies, standards, regulations and codes of practice for IT security implemented by government agencies, that private vendors serving the government would also need to comply with.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Singapore, through SingCERT, actively engages international counterparts through platforms such as:

-APCERT - FIRST -ASEAN CERT Incident Drill (ACID)

Singapore is also a participant in Japan-led TSUBAME Working Group and PRACTICE (Proactive Response Against Cyber-attacks Through International Collaborative Exchange) Project.

1.5.2 INTRA-AGENCY COOPERATION

The National Infocomm Security Committee draws its members for senior ranks of relevant public sector stakeholders. NISC is a platform where national cybersecurity policies are deliberated, information is shared, and inter-agency action is coordinated.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Singapore has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector. Cybersecurity Awareness Alliance amalgamates efforts from its members by bringing together different strengths and resources, to build a culture of cybersecurity in Singapore and to promote and enhance awareness and adoption of essential infocomm security (IS) practices for the private and people sectors.

1.5.4 INTERNATIONAL COOPERATION

Singapore participated in the following cybersecurity activities:

- ASEAN CERT Incident Drill (ACID) -APCERT Incident Drill -ASEAN Japan Comms Check Drill

-APEC-TEL -ASEAN-Japan activities

SingCERT is a member of FIRST.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Sections 293 and 376E of the Criminal Code.

-Section 32 of the Films Act.

-Sections 11 and 12 of the Publications Act.

2.2 UN CONVENTION AND PROTOCOL

Singapore has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Singapore has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Singapore Computer Emergency Response Team (SingCERT) does not provide specific information on child online protection.

2.4 REPORTING MECHANISM

The CERT (SingCERT) provides an email to report incident: cert@singcert.org.sg and a hotline: 6211-0911.

CYBERWELLNESS PROFILE SLOVAKIA

BACKGROUND

Total Population: 5 480 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 77.88%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Criminal Law (Law 300/2005) Paragraphs § 247, § 283, § 196 and 197
- European Council Convention on Cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- For banks: Law 483/2001 & Law 747/2004
- For public administration : Law 275/2006
- For telecommunication sector: Law 351/2011
- For Personal identifiable information: Law 122/2013.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Slovakia has an officially recognized national CIRT (CSIRT Slovakia).

1.2.2 STANDARDS

Slovakia has officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards through the Standardization committee for Information Systems of public administration (ISVS). Standardization committee is responsible for setting standards for ISVS on security, technical standards, data standards and project management standards.

1.2.3 CERTIFICATION

The national cybersecurity framework for accreditation and certification of information systems is regulated by the National Security Authority which is the main body of the state administration for the protection of classified information, and electronic signature.

The officially approved national cybersecurity framework for the certification of information systems used for the protection of classified information is regulated in the Act on the protection of Classified Information.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Slovakia has an officially recognized national cybersecurity strategy through the National strategy for Information Security (*). It defines strategic goals for Slovak Republic in various sectors such as protection of CII, awareness raising and capabilities building, ensuring secure environment, technical, operational and strategic controls, effective management of information security, protection and defence of public administration information infrastructure and national and international cooperation.

1.3.2 ROADMAP FOR GOVERNANCE

The Action plan to the National Strategy for Information Security defines tasks for various agencies in the field of information security and provides a national governance roadmap for cybersecurity in Slovakia.

1.3.3 RESPONSIBLE AGENCY

The national agency responsible for implementing a national cybersecurity strategy is the Ministry of Finance of Slovak republic (information security and protection of sector information technology in critical infrastructure). Other Ministries/agencies responsible for implementing specific areas of a strategy are:

- Ministry of Interior -Ministry of Telecommunication (ISP)

- National Security Authority (NBU) (Protection of classified information, digital signature)

-Ministry of culture (authors' law) -Ministry of Justice (Fight against cybercrime).

1.3.4 NATIONAL BENCHMARKING

The national CIRT (CSIRT Slovakia) is the officially recognized national or sector-specific benchmarking exercise or referential used to measure cybersecurity development.
Slovakia has participated in cyber Slovak Information Security Exercise (SISE) on 2011, 2012 and 2013.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Slovakia has officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines through the workgroups created by the Ministry of Finance, under the Committee of Standardization for various tasks including cybersecurity.

1.4.2 MANPOWER DEVELOPMENT

Slovakia has officially recognized national educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals through the Ministry of Finance of Slovak Republic (MF SR) project on cybersecurity which consists of systematic education of non-professionals in IT, managers and security professionals in field of cybersecurity in public administration.

1.4.3 PROFESSIONAL CERTIFICATION

There is no available information concerning any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

There is no available information concerning any certified government and public sector agencies under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Slovakia has officially recognized partnerships with the following organizations:

-NATO -FIRST -OSCE -European Union.

1.5.2 INTRA-AGENCY COOPERATION

The Themis project is the officially recognized program for information sharing platform for connected organization from public administration. The national CIRT (CSIRT Slovakia) mandates the sharing of cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Slovakia has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector through the Themis project and the national CIRT (CSIRT Slovakia).

1.5.4 INTERNATIONAL COOPERATION

Slovakia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Slovakia also participated in the second Central European Cyber Security Platform (CECSP).

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-§132 and §368-370* of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Slovakia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Slovakia has signed and ratified with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no available information concerning any officially recognized agencies that offer institutional support in child online protection.

2.4 REPORTING MECHANISM

Online illegal content can be reported in the website of Stopline (*). Incidents can be reported in the website of the Computer Security Incident Response Team of Slovakia (CSIRT (*)).

CYBERWELLNESS PROFILE REPUBLIC OF SLOVENIA

BACKGROUND

Total Population: 2 040 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 72.68%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Penal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Telecommunications Law

- Personal Data Protection Act

- Electronic Communications Act

- Access to Public Information Act

- Electronic Commerce and Electronic Signature Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Slovenia has an officially recognized national CERT known as SI-CERT. It is a service of ARNES (Academic and Research Network of Slovenia).

1.2.2 STANDARDS

Slovenia does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Slovenia.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Slovenia is working out a cybersecurity strategy to upgrade its capability against cyber-attacks.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Slovenia.

1.3.3 RESPONSIBLE AGENCY

The agencies responsible for cybersecurity in Slovenia are:
- Criminal Police Directorate
- Ministry of Interior, Slovenia
- Head of Computer Investigation Centre.

1.3.4 NATIONAL BENCHMARKING

Slovenia does not have any benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

Slovenia participates in the European Cyber Security Month.

1.4.3 PROFESSIONAL CERTIFICATION

Slovenia does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Slovenia does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Slovenia does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Slovenia.

1.5.4 INTERNATIONAL COOPERATION

Slovenia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. SI-CERT also participates in the TF-CSIRT.

SI-CERT is a member of FIRST.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

- Article 176 of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Slovenia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Slovenia has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Information about online safety can be found in the website of Safe in Safe in Internet*, implemented by the SI-CERT.

2.4 REPORTING MECHANISM

Online illegal content can be reported in the website (*) of a Slovenian hotline co-sponsored by the EU.

CYBERWELLNESS PROFILE SOLOMON ISLANDS

BACKGROUND

Total Population: 566 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 8%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-None.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-None.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Solomon Islands does not have an officially recognized CIRT.

1.2.2 STANDARDS

Solomon Islands does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Solomon Islands.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Solomon Islands does not have any officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Solomon Islands.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Solomon Islands.

1.3.4 NATIONAL BENCHMARKING

Solomon Islands does not have any benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines in Solomon Islands.

1.4.2 MANPOWER DEVELOPMENT

There is no program or project for education and professional training, raising awareness or higher education and certification in Solomon Island.

1.4.3 PROFESSIONAL CERTIFICATION

Solomon Islands does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Solomon Islands does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no framework in Greece to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Solomon Islands does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Solomon Islands.

1.5.4 INTERNATIONAL COOPERATION

Solomon Islands is a member of the PacCERT.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-None.

2.2 UN CONVENTION AND PROTOCOL

Solomon Islands has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Solomon Islands has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency that supports child online protection in Solomon Islands.

2.4 REPORTING MECHANISM

There is no website or hotline where incident can be reported to in Solomon Islands.

CYBERWELLNESS PROFILE

SOMALIA

BACKGROUND

Total Population: 9 797 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 1.50%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Somalia does not currently have any officially recognized national legislation pertaining to cybercrime but there is a work in progress.

1.1.2 REGULATION AND COMPLIANCE

Somalia does not currently have any officially recognized regulation pertaining to cybersecurity but there is a work in progress.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Somalia does not have any officially recognized national CIRT currently but there is a work in progress.

1.2.2 STANDARDS

Somalia does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Somalia does not currently have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals but there is a work in progress.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Somalia does not currently have any officially recognized national cybersecurity strategy but there is a work in progress.

1.3.2 ROADMAP FOR GOVERNANCE

Somalia does not currently have any officially recognized national governance roadmap for cybersecurity but there is a work in progress.

1.3.3 RESPONSIBLE AGENCY

Somalia does not currently have any officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap but there is a work in progress.

1.3.4 NATIONAL BENCHMARKING

Somalia does not currently have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development but there is a work in progress.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Somalia does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector. There are some disjointed efforts.

1.4.2 MANPOWER DEVELOPMENT

Somalia does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors. However, Somalia proposes a few workshops and awareness campaign by the Internet Society Chapter of Somalia at an elementary level.

1.4.3 PROFESSIONAL CERTIFICATION

Somalia does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Somalia does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Somalia does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Somalia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Somalia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Somalia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Somalia participated in the 2012 ITU-IMPACT Applied Learning for Emergency Response Teams (ALERT) from 15-17 July in Amman, Jordan.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Somalia does not have any national legislation pertaining to child online protection.

2.2 UN CONVENTION AND PROTOCOL

Somalia did not accede to the UN Convention and Protocol pertaining to child online protection.

2.3 INSTITUTIONAL SUPPORT

Somalia does not have any the officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Somalia does not have any the officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
SOUTH AFRICA

BACKGROUND

Total Population: 50 738 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 48.90%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Electronic communication and Transactions Act No 25 of 2002
- The National Cybersecurity Policy Framework 2012
- Regulation of Interception of Communications and Provision of communication-related Information Act of 2002
- Protection of Personal Information Act 2013.

1.1.2 REGULATION AND COMPLIANCE

South Africa does not have specific legislation and regulation related to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

South Africa has an officially recognized national CIRT (ECS-CSIRT).

1.2.2 STANDARDS

South Africa has officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards through the National Cybersecurity Policy Framework which aims to promote a cybersecurity culture by strengthening investigation, prosecution and judicial processes, to establish public-private partnerships for national and international action plans, ensure the protection of national critical information infrastructure and promote and ensure a comprehensive legal framework governing cyberspace.

1.2.3 CERTIFICATION

South Africa does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

South Africa has an officially recognized National Cybersecurity Policy Framework approved by the Cabinet in March 2012, to establish an environment that will ensure confidence and trust in the secure use of ICTs.

1.3.2 ROADMAP FOR GOVERNANCE

The approved National Cybersecurity Implementation Plan is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.3 RESPONSIBLE AGENCY

The State Security Agency is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

South Africa does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

South Africa does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

South Africa does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

South Africa does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

South Africa does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, South Africa has officially recognized partnerships with the 24/7 program.

1.5.2 INTRA-AGENCY COOPERATION

South Africa does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector. However South Africa is in the process of developing protocols for information and assets sharing between different stakeholders.

1.5.3 PUBLIC SECTOR PARTNERSHIP

South Africa does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector. However South Africa is in the process of developing protocols for information and assets sharing between different stakeholders.

1.5.4 INTERNATIONAL COOPERATION

South Africa is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. South Africa is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA).

ECS-CSIRT is a member of FIRST.

South Africa is on the finalization stage of the draft AUC Cybersecurity Convention workshop (African Countries). South Africa participated in international effort on cybercrime by taking part in EU GLACY project.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Sections 10 and 18-22 of the Amendment to the Sexual Offences and Related Matters Act.

-Section 27 of the Films and Publications Act, amended by the Bill number 75.

-Section 27A of the aforementioned Act, inserted by the Act number 18 of 2004. Sections 24C and 27A respectively inserted and amended by the Act number 3 of 2009.

2.2 UN CONVENTION AND PROTOCOL

South Africa has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. South Africa has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

South Africa does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

FPB PRO CHILD provides a phone number, 0800 148 148, and space in its website for the denouncement of child online pornography.

CYBERWELLNESS PROFILE
REPUBLIC OF SOUTH SUDAN

BACKGROUND

Total Population: unknown

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: unknown

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Penal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- None.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

South Sudan does not have any officially recognized national CIRT.

1.2.2 STANDARDS

South Sudan does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in South Sudan.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

South Sudan does not have an officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in South Sudan.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in South Sudan.

1.3.4 NATIONAL BENCHMARKING

South Sudan does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

South Sudan does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in South Sudan.

1.4.3 PROFESSIONAL CERTIFICATION

South Sudan does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

South Sudan does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

South Sudan does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

South Sudan does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in South Sudan.

1.5.4 INTERNATIONAL COOPERATION

South Sudan is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

- Article 260 of the Criminal Code – does not explicitly mention child pornography but obscene content.

2.2 UN CONVENTION AND PROTOCOL

South Sudan has not acceded to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. South Sudan has not acceded to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in South Sudan.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in South Sudan.

CYBERWELLNESS PROFILE

SPAIN

BACKGROUND

Total Population: 46 772 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 71.5719%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Penal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Law on Electronic Signature
- General Telecommunications Law
- Protection of Personal Data.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Spain has a national CIRT which is known as CNN-CERT.

1.2.2 STANDARDS

The OC/CCN is the officially recognized national agency responsible for cybersecurity frameworks and for implementing internationally recognized cybersecurity standards. It operates the Common Criteria (ISO-15408).

1.2.3 CERTIFICATION

The National Cryptology Centre (CNN) is the officially approved national (and sector specific) cybersecurity framework for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Spain has an officially recognized national cybersecurity strategy through The National Security Strategy.

1.3.2 ROADMAP FOR GOVERNANCE

The National Security Strategy provides a line of action for cybersecurity in its fourth chapter.

1.3.3 RESPONSIBLE AGENCY

The following are the officially recognized organizations responsible for implementing a national cybersecurity strategy, policy and roadmap:

- The National Cryptology Centre (CCN)
- National Centre of Intelligence
- The National Security Office (ONS).

1.3.4 NATIONAL BENCHMARKING

Spain does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Spain has officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines through the CCN-STIC series and SCADA guidelines.

1.4.2 MANPOWER DEVELOPMENT

Spain has officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals through the SICT Training and European Cyber Security Month.

1.4.3 PROFESSIONAL CERTIFICATION

CNN-CERT team members are certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

CNN-CERT is accredited by FIRST, TI and EGC Group government and public sector agencies under internationally recognized standards in cybersecurity. However there are no exact numbers of public agencies being certified.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

CCN-CERT maintains a direct contact with other CIRT teams from the rest of the world in order to, in the event of an attack, distinguish which information sources are reliable.

1.5.2 INTRA-AGENCY COOPERATION

There is no information about any platform or programs for sharing of cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no record of a framework for sharing cybersecurity assets between the public and private sectors in Spain.

1.5.4 INTERNATIONAL COOPERATION

Spain is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. CCN-CERT participates in the following international workshops:

- ENISA - APWG - TI - OTAN's NCIRC (NATO).

- TERENA - EGC -F IRST

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Articles 186 and 189 of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Spain has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Spain has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Internet User Security Office under the Ministry of Telecommunications and Information Society provides information on internet safety.

2.4 REPORTING MECHANISM

Child pornography can be denounced on the website of Alia2. Child pornography can also be denounced on the website of protegeles.com or by the phone number 91 74 00 019.

Computer incidents can be reported in a private area of the website of the Computer Security Response Capability CNN-CERT, the Spanish Government CERT.

CYBERWELLNESS PROFILE
SRI LANKA

BACKGROUND

Total Population: 21 224 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 21.90%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

-Computer Crime Act 2007.

1.1.2 REGULATION AND COMPLIANCE

Sri Lanka does not have specific legislation and regulation related to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Sri Lanka has an officially recognized national CIRT (Sri Lanka CERT).

1.2.2 STANDARDS

Sri Lanka does not have an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Sri Lanka does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Sri Lanka has an officially recognized national cybersecurity policy.

1.3.2 ROADMAP FOR GOVERNANCE

Sri Lanka does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Sri Lanka does not have an officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Sri Lanka does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

TechCERT along with Domain Registry conducts R&D programs and projects on cybersecurity. These programs will benefit both public and private sectors.

1.4.2 MANPOWER DEVELOPMENT

Sri Lanka CERT conducts various types of awareness programs on cybersecurity, for the general public as well as for public and private sector employees.

The annual Cyber Security Week (CSW) program was introduced from year 2008 which consists of a national cyber security conference, workshops, seminars, media campaigns, security quiz for the students of tertiary educational institutions, hacking challenge etc. Details of CSW 2014 can be seen at: http://www.cert.gov.lk/csw2014/index.html

(1) Tech Cert together with Domain Registry conduct awareness programs through mail across the country and especially for banking and office private sector organisations. In addition general public is also made aware through conducting workshops at schools.

(2) Internet Society Sri Lanka chapter supports and conducts similar programs.

Sri Lanka CERT|CC is also engaged in promoting the certification of cyber security professionals by hosting the Colombo Chapter of ISC2 that provides the CISSP certification

1.4.3 PROFESSIONAL CERTIFICATION

Sri Lanka does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Sri Lanka does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATIO

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Sri Lanka has officially recognized partnerships with the following organizations:

-ITU -APCERT -CYMRU

-FIRST -Shadowserver.

1.5.2 INTRA-AGENCY COOPERATION

Sri Lanka CERT has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Sri Lanka has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Sri Lanka is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Sri Lanka CERT|CC participates in regional and international cybersecurity drills, workshops, conferences and works closely with CERTs and other relevant organizations in those countries to resolve or mitigate cybersecurity incidents. Sri Lanka CERT|CC has been a full member of APCERT and FIRST for the past six years and continues to participate at their Annual General Meetings and Conferences. It is also a member of IMPACT and the Microsoft Security Corporation Program (SCP).

Sri Lanka participated in the International Cyber Shield Exercise 2014 in Turkey (ICSE 2014).

Sri Lanka CERT is a member of FIRST.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Section 3 of the Penal Code (Amendment) Act.

2.2 UN CONVENTION AND PROTOCOL

Sri Lanka has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Sri Lanka has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Sri Lanka does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Sri Lanka CERT is the officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
SAINT KITTS AND NEVIS

BACKGROUND

Total Population: 52 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 80.00%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

-Electronic Crime Act.

1.1.2 REGULATION AND COMPLIANCE

Specific regulation and compliance requirement pertaining to cybersecurity is as follows:

-Electronic Crimes (Investigation Procedures, Collection and Preservation of Electronic Crimes Evidence) Rules

1.2 TECHNICAL MEASURES

1.2.1 CIRT

St. Kitts and Nevis does not currently have an officially recognized national CIRT. ITU conducted a CIRT assessment for St.Kitts and Nevis in 2012.

1.2.2 STANDARDS

St. Kitts and Nevis does not have an officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

St. Kitts and Nevis does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

St. Kitts and Nevis does not have an officially recognized national cybersecurity strategy. However there is one cybersecurity policy that is currently developed at the CARICOM level for adoption by its Member States.

1.3.2 ROADMAP FOR GOVERNANCE

St. Kitts and Nevis does not have a national governance roadmap for cybersecurity. However there is one governance roadmap that is currently developed at the CARICOM level for adoption by its Member States.

1.3.3 RESPONSIBLE AGENCY

The Ministry of National Security is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

St. Kitts and Nevis does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development. However the Ministry of National Security is working with the Department of Technology for a new mandate.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

St. Kitts and Nevis does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

St Kitts and Nevis does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sector.

1.4.3 PROFESSIONAL CERTIFICATION

St. Kitts and Nevis does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

St. Kitts and Nevis does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

St. Kitts and Nevis does not have officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

St. Kitts and Nevis does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

St. Kitts and Nevis does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector. However BD CERT organizes events to share knowledge with the law enforcing agencies, industry and academia.

1.5.4 INTERNATIONAL COOPERATION

St. Kitts and Nevis is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. In addition, St. Kitts and Nevis also participated in OAS regional forums organized through CITCE.

St. Kitts and Nevis is among the beneficiary countries of the EU/ITU co-funded project “Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures” (HIPCAR).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

-Electronic Crime Act (Section 13).

2.2 UN CONVENTION AND PROTOCOL

St. Kitts and Nevis has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

St. Kitts and Nevis has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

St. Kitts and Nevis does not have an officially recognized agency that offers institutional support on child online protection. However the Department of Probation and Child Protection Services is the government's primary agency responsible for ensuring the rights of children.

2.4 REPORTING MECHANISM

St. Kitts and Nevis does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

SAINT VINCENT AND THE GRENADINES

BACKGROUND

Total Population: 109 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 52.00%

(data source: ITU Statistics, December 2012)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Saint Vincent and the Grenadines does not have any officially recognized criminal legislation pertaining to cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation to cybersecurity has been enacted through the following instruments:

- Electronic Transaction Act - Electronic Evidence Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

There is no available information regarding any officially recognized national CIRT in Saint Vincent and the Grenadines. A CIRT readiness assessment was conducted for Saint Vincent and the Grenadines by ITUin 2012.

1.2.2 STANDARDS

There is no available information concerning any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no available information concerning any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

There is no available information concerning any officially recognized national cybersecurity strategy in Saint Vincent and the Grenadines.

1.3.2 ROADMAP FOR GOVERNANCE

There is no available information concerning any officially recognized national governance roadmap for cybersecurity in in Saint Vincent and the Grenadines.

1.3.3 RESPONSIBLE AGENCY

The lead agency for cybersecurity in Saint Vincent and the Grenadines is the SVG Police Force, which has created an Information Technology Unit to oversee and support the investigation of all cybercrime and information security-related matters and thus is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

There is no available information regarding any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no available information regarding any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

There is no available information regarding any officially recognized sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

There is no available information regarding the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

There is no available information regarding any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

International cooperation has centered largely on solicitation of support when needed from the experts of the Cyber Forensic Laboratory in Antigua and Barbuda.

1.5.2 INTRA-AGENCY COOPERATION

There is no available information concerning any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no available information concerning any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Saint Vincent and the Grenadines is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

Personnel from the government's Technology Unit have also participated in cybersecurity and cybercrime related training offered by regional and international partners including the OAS, US Department of State (DS/ATA), CTU, and INTERPOL, among others.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION AND STRATEGY

Specific legislation on child protection has been enacted through the following instruments:

- Section 71 and 73 from the Electronic Transactions Act.

2.2 UN CONVENTION AND PROTOCOL

Saint Vincent and the Grenadines has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Saint Vincent and the Grenadines has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Saint Vincent and the Grenadines does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Saint Vincent and the Grenadines does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
SUDAN (REPUBLIC OF)

BACKGROUND

Total Population: 45 722 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 22.70%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-E-Crime Law -Informatic Offense (Combating) Act -Intellectual Property Law -Literary and Artistic Bill.

1.1.2 REGULATION AND COMPLIANCE

Sudan does not have specific regulation and compliance requirement pertaining cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Sudan has an officially recognized national CIRT (SUDAN CERT). ITU conducted a cirt assessment for Sudan in 2013.

1.2.2 STANDARDS

Sudan has officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards through the Information Security Law and the Regulation on measures for information security.

1.2.3 CERTIFICATION

Sudan does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Sudan has an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no available information concerning a national governance roadmap for cybersecurity in Sudan.

1.3.3 RESPONSIBLE AGENCY

The National Telecommunication Corporation is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

There is no available information concerning any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Sudan has officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines through the Sudan Cybersecurity Standards Committee.

1.4.2 MANPOWER DEVELOPMENT

Sudan has officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors. These include the National Awareness Project and the “Train the trainer” program.

1.4.3 PROFESSIONAL CERTIFICATION

There is no available information concerning any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

There is no available information concerning any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no available information concerning any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

There is no available information concerning any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no available information concerning any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Sudan is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Sudan has participated in many CIRT events. Precisely in the 2012 ITU-IMPACT Workshop on Cyber Drill in Jordan, in the ITU RCC Regional Cybersecurity Forum Cyber Drill 2013 in Oman and in the International Cyber Shield Exercise 2014 in Turkey.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-The Criminal Code (Section 235)

-Informatic Offense (Combating) Act (Section 14-16).

2.2 UN CONVENTION AND PROTOCOL

Sudan has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Sudan has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

SUDAN CERT is the officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

SUDAN CERT is the officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

SURINAME

BACKGROUND

Total Population: 534 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 37.40%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Criminal Code First Book

- Criminal Code Second Book.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- None.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Suriname has a now defunct national CIRT known as SurCIRT. It is in the process of being reactivated.

1.2.2 STANDARDS

Suriname does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Suriname.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Suriname does not have an officially recognized national or sector-specific cybersecurity strategy. Negotiations among stakeholders are ongoing regarding the creation of a national cybersecurity policy and strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Suriname.

1.3.3 RESPONSIBLE AGENCY

The Central Intelligence and Security Agency (CIVD) is the agency responsible for cybersecurity in Suriname. A Cyber Crime Unit is being created within the national police.

1.3.4 NATIONAL BENCHMARKING

Suriname does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Suriname does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

Personnel from the national defense force are currently participating in a course on cybersecurity.

1.4.3 PROFESSIONAL CERTIFICATION

Suriname does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Suriname does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Suriname does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Suriname does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Suriname.

1.5.4 INTERNATIONAL COOPERATION

Suriname is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Suriname also participates in the OAS-CICTE.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

- Article 292* of the Criminal Code – only for children under 16.

2.2 UN CONVENTION AND PROTOCOL

Suriname has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Suriname has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for the child online protection in Suriname.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Suriname.

CYBERWELLNESS PROFILE

SWAZILAND

BACKGROUND

Total Population: 1 220 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 24.70%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Swaziland does not have any officially recognized national legislation pertaining to cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Swaziland does not have any officially recognized regulation and compliance requirement pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU-IMPACT conducted a CIRT readiness assessment for Swaziland at Addis Ababa, Ethiopia in March 2014 (10-14th March 2014). Swaziland does not currently have an officially recognized national CIRT.

1.2.2 STANDARDS

Swaziland does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Swaziland does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Swaziland does not have any officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Swaziland does not have any national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The Ministry of ICT is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Swaziland does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Swaziland does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Swaziland does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Swaziland does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Swaziland does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Swaziland does not have any officially recognized partnerships to facilitate intra-state cooperation.

1.5.2 INTRA-AGENCY COOPERATION

Swaziland does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Swaziland does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Swaziland is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Swaziland is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA).

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Swaziland does not have any officially recognized legislation pertaining to child online protection.

2.2 UN CONVENTION AND PROTOCOL

Swaziland has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Swaziland has acceded, with no declarations or reservations to articles 2 and 3, the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Swaziland does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Swaziland does not have any officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

SWEDEN

BACKGROUND

Total Population: 9 495 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 94.7836%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Penal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Personal Data Act
- Electronic Communications Act
- Act on Qualified Electronic Signatures
- Act on Responsibility for Electronic Bulletin Boards
- Public Access to Information and Secrecy Act
- Act on Signals Intelligence in Defense Intelligence - FRA Law
- Act on Processing of Personal Records within the Scope of the Defence Intelligence and Development Activities of the National Defence Radio Establishment.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Sweden has an officially recognized national CIRT known as CERT-SE which is run by the Swedish Civil Contingencies Agency (MSB).

1.2.2 STANDARDS

There is no record indicating any internationally recognised cybersecurity standards in Sweden; however The National Defence Radio Establishment (FRA) is responsible for technical resources concerning information security.

1.2.3 CERTIFICATION

FMV/CSEC is the nationally recognized framework for certification and accreditation of national agencies and public sector professionals in IT security.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Strategy to improve Internet security in Sweden is the officially recognised national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Sweden's Information Security Action plan is the national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The following are the agencies responsible for implementing the cybersecurity policies, strategies and roadmaps:

- The Swedish Armed Forces (FM)
- Office of Information Assurance and Cybersecurity
- The Swedish Security Service (SÄPO)
- The Swedish National Bureau of Investigation (RPS)
- The Swedish Civil Contingencies Agency (MSB).

1.3.4 NATIONAL BENCHMARKING

The Swedish Data Inspection Board (DI) is responsible for auditing with regards to the protection of personal data and the privacy of individuals in the information society. DI also carries out inspections and issues guidelines on cybersecurity. This is the nationally recognized benchmarking and referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no information on any nationally recognized programs and/or exercises for research and development (R&D) of cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

Sweden has recognized various types of awareness programs on cybersecurity, for the general public as well as for public and private sector employees:

- European Cyber Security Month

- The Swedish Defense Research Agency (FOI) conducts research on many aspects of cybersecurity and maintains a Cyber Range and Training Environment (CRATE) for experiments, competitions and exercises.

- The Swedish National Defense College (FHS) conducts strategic cybersecurity and cyber defense studies and develops educational high-level courses on information assurance together with procedures and manuals on how to build technical cyber defense exercises (CDX).

-The Swedish International Development Cooperation Agency (Sida) has ICT development related activities as one of its prioritized focus areas and works through support to global, regional and local initiatives in the field of policy and rule of law, strengthening and protecting human rights, and both civic and cyber capacity building. Sida addresses cyber security related issues from a human rights based approach, focusing on bottom-up initiatives for democratization and economic growth. This is being made both through initiated policy related work in normative processes, International Training Programmes (ITP) and directed support to a large number of actors across the world.

1.4.3 PROFESSIONAL CERTIFICATION

CERT-SE team is certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

CERT-SE is the certified government agency in Sweden.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Sweden participates and contributes actively in various international cyberspace fora, while also seeking bilateral and regional dialogues on cyber-issues, including in the Nordic-Baltic region. Sweden contributes substantially to cyber capacity-building efforts in low- and middle income countries through its international development cooperation, with an explicit focus on improving access to and increasing the use of open and secure ICTs through by means of improved infrastructure, regulation and institutions.

1.5.2 INTRA-AGENCY COOPERATION

CERT-SE provides means for information sharing, collaboration and feedback between public administration bodies.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Sweden does not currently have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Sweden, through CERT-SE, actively engages international counterparts through platforms such as:

- FIRST - ENISA - OSCE - Nordic-Baltic (NB8) - UN GGE - IGF.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

-Chapter 16, §10(a) of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

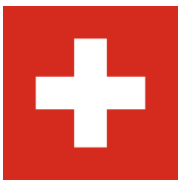
Sweden has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Sweden has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no information about the institution responsible for online protection for children.

2.4 REPORTING MECHANISM

BRIS website provides a helpline via a phone number but also email and chat services.



CYBERWELLNESS PROFILE SWITZERLAND

BACKGROUND

Total Population: 7 734 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 86.70%

(data source: ITU Statistics, December 2012)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Penal Code (art 143bis & art 144bis).

1.1.2 REGULATION AND COMPLIANCE

Switzerland has specific legislation related to cybersecurity and compliance. However disclosure of cyber incidents is not mandatory.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Switzerland has an officially recognized national GovCERT.ch which is part of MELANI a legally mandated institution aimed to protect information infrastructures in Switzerland.

1.2.2 STANDARDS

Switzerland does not have any officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Switzerland does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

A national cybersecurity strategy was approved by the Federal Council in 2012. At the moment Switzerland is working on the implementation of the 16 measures mentioned in the strategy. A few measures are already implemented. However Switzerland is still working on the bigger part of the strategy and all measures have to be implemented by the end of 2017, at the latest.

1.3.2 ROADMAP FOR GOVERNANCE

Switzerland does not currently have any national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The Federal Council is the officially recognized institution responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Switzerland does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

The national cybersecurity strategy will be the *officially* recognized national or sector-specific research and development (R&D) program/project for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector when it is fully implemented (by the of 2017).

1.4.2 MANPOWER DEVELOPMENT

The national cybersecurity strategy will provide various types of educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors, when it is fully implemented (by the of 2017).

1.4.3 PROFESSIONAL CERTIFICATION

Switzerland does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Switzerland does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no available information regarding any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

There is no available information regarding any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

MELANI provides officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Switzerland is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Articles 194 and 197* of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Switzerland has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Switzerland has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Reporting and Analysis Centre for Information Assurance (MELANI) provides information about risks on the internet and situation reports. The Cybercrime Coordination Unit (SCOCI (*)) provides information on internet safety. The Safer Surfing (*) website, under the Swiss Agency for Crime Prevention provides information on internet safety.

2.4 REPORTING MECHANISM

Incidents can be reported by completing the form provided by MELANI.

Suspicious online content can be reported by completing the form provided by (SCOCI (*)).

CYBERWELLNESS PROFILE

SYRIA

BACKGROUND

Total Population: 21 118 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 26.20%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation pertaining to cybercrime is mandated through the following legal instrument:

- Law on the network communication and computer crime control.

1.1.2 REGULATION AND COMPLIANCE

Syria does not have any officially recognised regulation pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Syria has an officially recognized National CIRT, which is part of the National Agency for Network Service (NANS).

1.2.2 STANDARDS

There is no available information concerning any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no available information concerning any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

There is no available information concerning any officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no available information concerning any national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The National Agency for Network Service (NANS) is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

There is no available information concerning any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no available information concerning any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

A center of excellence under management of NANS is dedicated to provide professional training in the field of cyber security.

1.4.3 PROFESSIONAL CERTIFICATION

There is no available information concerning any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

There is no available information concerning any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Syria has signed a Memorandum of Collaboration against Malicious Activities in Cyberspace with Japan Ministry of Information and Communication.

1.5.2 INTRA-AGENCY COOPERATION

There is no available information concerning any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no available information concerning any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Syria is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Syria is also a member of the OIC-CERT.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Syria does not have any officially recognized legislation pertaining to child online protection.

2.2 UN CONVENTION AND PROTOCOL

Syria has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Syria has acceded, with no declarations or reservations to articles 2 and 3, the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Syria does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Syria does not have any officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE REPUBLIC OF TAJIKISTAN

BACKGROUND

Total Population: 7 709 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 16.00%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Criminal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Law on Information
- Law on E-Signatures
- Law on Cryptography
- Law on Data Protection
- Law on Telecommunications
- Law on Electronic Document
- Law on the Right of Access to Information.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Tajikistan does not have any officially recognized national CIRT.

1.2.2 STANDARDS

Tajikistan does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Tajikistan.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Tajikistan does not have any officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Tajikistan.

1.3.3 RESPONSIBLE AGENCY

There is no information about any agency responsible for cybersecurity in Tajikistan.

1.3.4 NATIONAL BENCHMARKING

Tajikistan does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Tajikistan.

1.4.3 PROFESSIONAL CERTIFICATION

Tajikistan does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Tajikistan does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, a set of principles or action plan related to information security was adopted at the Shanghai Cooperation Organization's (SCO) seventh council meeting of heads of states. China and Tajikistan, in a joint declaration, agreed to further strengthen cooperation and exchanges between law enforcement, security and defense authorities of the two countries.

1.5.2 INTRA-AGENCY COOPERATION

Tajikistan does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Tajikistan.

1.5.4 INTERNATIONAL COOPERATION

Tajikistan is a member of the UN and SCO.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:
- None.

2.2 UN CONVENTION AND PROTOCOL

Tajikistan has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Tajikistan has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Tajikistan.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Tajikistan.

CYBERWELLNESS PROFILE

TANZANIA

BACKGROUND

Total Population: 47 656 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 4.40%

(data source: ITU Statistics,2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Electronic and Postal Communications Act

-Computer and Cybercrime Bills (currently being enacted).

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity is in the process of being enacted through the following instruments:

-Personal Data Protection Act

-Electronic Transaction Act

-The Electronic And Postal Communications (Computer Emergency Response Team) Regulations.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU conducted a CIRT readiness assessment for Tanzania at Kampala, Uganda, in April 2010. Tanzania CERT (TZ-CERT) is the naional CIRT established by the ITU- IMPACT.

1.2.2 STANDARDS

Tanzania has an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards through the Information Security Law and the Regulation on measures for information security.

1.2.3 CERTIFICATION

Tanzania does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Tanzania does not have an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Tanzania does not have an officially recognized national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Tanzania does not have any officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Tanzania does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Tanzania does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Tanzania does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Tanzania does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Tanzania does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Tanzania has officially recognized partnerships with the following organizations:

-ITU -African Union -GAC/ICANN

-FIRST.

1.5.2 INTRA-AGENCY COOPERATIO

Tanzania does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Tanzania does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Tanzania is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

There is officially recognized participation in East Africa region under the umbrella of East African Communications Organization (EACO). EACO has a dedicated platform referred as EACO Working Group 5 comprised of members from all 5 countries (Tanzania, Kenya, Uganda, Rwanda and Burundi) within the region that reports to Assembly of Regulators which is mandated to address IP Networks, Standards and Cybersecurity issues.

Tanzania is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

-The Criminal Code(Section 175).

2.2 UN CONVENTION AND PROTOCOL

Tanzania has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Tanzania has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Tanzania does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

The Tanzania Communications Regulatory Authority provides an online complaint form.

CYBERWELLNESS PROFILE

THAILAND

BACKGROUND

Total Population: 69 892 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 28.94%

(data source: ITU Statistics 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Thailand has a specific legislation pertaining to cybercrime. It is mandated through the following legal instrument:

- Act on Computer Crime B.E.2550 (2007).

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

- Ecommerce Act
- Law on Electronic Signatures
- Act on Processing of Personal Data
- Law on Electronic Communications Networks and Services
- Act on Processing of Personal Data by the Operation of the Government.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Thailand has an officially recognized and legally mandated government CSIRT (ThaiCERT).

1.2.2 STANDARDS

Through the Office of the National Security Council and the Ministry of Information and Communication Technology Thailand has an officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

The approved national certification and accreditation body in Thailand is the IT Crime Prevention and Suppression Bureau, Ministry of Information and Communication Technology, Thailand and ThaiCERT.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Thailand has an officially approved national and sector specific cybersecurity strategy and/or policy through the IT Crime Prevention and Suppression Bureau, Ministry of Information and Communication Technology, Thailand and ThaiCERT.

1.3.2 ROADMAP FOR GOVERNANCE

There is an officially recognized national or sector-specific governance roadmap for cybersecurity through the IT Crime Prevention and Suppression Bureau, Ministry of Information and Communication Technology, Thailand.

1.3.3 RESPONSIBLE AGENCY

The Ministry of Information and Communication Technology is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap in Thailand.

1.3.4 NATIONAL BENCHMARKING

The Ministry of Information and Communication Technology is responsible for national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Thailand's Ministry of Information and Communication Technology is officially answerable for national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

The officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors is the Ministry of Information and Communication Technology, Thailand.

1.4.3 PROFESSIONAL CERTIFICATION

Ministry of Information and Communication Technology, Thailand is responsible for educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sector.

1.4.4 AGENCY CERTIFICATION

There are government and public sector agencies certified under internationally recognized standards in cybersecurity in Thailand:

-Ministry of Information and Communication Technology

-Electronic Transaction Development Agency.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Thailand does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Thailand does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Thailand does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Thailand is a member of the ITU-IMPACT initiatives and has access to relevant cybersecurity services.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child protection has been enacted through the following instruments:

- Thailand Penal Code (Section 287)
-Computer Crime Act (Section 16).

2.2 UN CONVENTION AND PROTOCOL

Thailand has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Thailand has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Thailand has a Computer Emergency Response Team (ThaiCERT) but does not provide specific information on child online protection.

2.4 REPORTING MECHANISM

Thailand allows for computer incident report using the email: report@thaicert.or.th. ; the website provides keys to encrypt reports.

CYBERWELLNESS PROFILE

DEMOCRATIC REPUBLIC OF TIMOR-LESTE

BACKGROUND

Total Population: 1 187 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 1.10%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- None.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- None.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Timor-Leste does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Timor-Leste does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Timor-Leste.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Timor-Leste does not have an officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Timor-Leste.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Timor-Leste.

1.3.4 NATIONAL BENCHMARKING

Timor-Leste does not have an officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Timor-Leste does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Timor-Leste.

1.4.3 PROFESSIONAL CERTIFICATION

Timor-Leste does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Timor-Leste does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Timor-Leste does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Timor-Leste does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Timor-Leste.

1.5.4 INTERNATIONAL COOPERATION

Timor-Leste is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Article 176* of the Criminal Code – only for children under 17.

2.2 UN CONVENTION AND PROTOCOL

Timor-Leste has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Timor-Leste has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Timor-Leste.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Timor-Leste.

CYBERWELLNESS PROFILE
TOGO

BACKGROUND

Total Population: 6 283 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 4.50%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Togo does not have specific legislation on cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Togo does not have specific legislation and regulation related to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Togo does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Togo does not have officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Togo does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Togo does not have an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Togo does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The Electronic Communication Regulator is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Togo Electronic Communication Regulator has officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development. Two studies have been made but the results are not yet published.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Togo does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Togo does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors. However there are a lot of professional certification centers in the field of security and cybersecurity.

1.4.3 PROFESSIONAL CERTIFICATION

Togo does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Togo does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Togo does not have officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Togo does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Togo does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Togo is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Togo is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

Article 89* of the Criminal Code – does not mention explicitly child pornography

Article 392 of the Children’s Code of Togo.

2.2 UN CONVENTION AND PROTOCOL

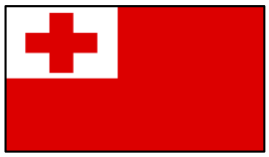
Togo has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Togo has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Togo does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Togo does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.



CYBERWELLNESS PROFILE

TONGA

BACKGROUND

Total Population: 105 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 35.00%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Computer Misuse Act 2003

-Evidence Act

-Criminal Offense Act

-Pornography Control Act 2002

-Copyright Act 2005

-Tongan Internet Corporation Registration Act 2000.

1.1.2 REGULATION AND COMPLIANCE

Tonga does not have specific legislation and regulation on cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Tonga does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Tonga does not have officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Tonga does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Tonga does not have an officially recognized national cybersecurity strategy. However on 13 December 2013, the cabinet approved the establishment of a Cyber Challenge Task Force. The Task Force, through its working groups, is currently drafting a three year implementation plan focusing on the three main areas of cybercrime, cybersecurity and cybersafety.

1.3.2 ROADMAP FOR GOVERNANCE

Tonga does not have a national governance roadmap for cybersecurity. However the working groups in the Cyber Challenge Task Force are working on a roadmap.

1.3.3 RESPONSIBLE AGENCY

The Cyber Challenge Task Force is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Tonga does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Tonga does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Tonga does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Tonga does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Tonga does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Tonga does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Tonga does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Tonga does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Tonga is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Tonga is among the beneficiary countries of the EU/ITU co-funded project “Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries” (ICB4PAC).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Section 115A of the Criminal Code

-Articles 4 and 5 of the Pornography Control Act

2.2 UN CONVENTION AND PROTOCOL

Tonga has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

2.3 INSTITUTIONAL SUPPORT

Tonga does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Tonga does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
TRINIDAD AND TOBAGO

BACKGROUND

Total Population: 1 351 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 63.80%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Trinidad and Tobago does not have specific legislation on cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:

-Law on Protection of Personal Information.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Trinidad and Tobago does not have an officially recognized national CIRT; however it is in the process of establishing the CIRT. ITUconducted a CIRT readiness assessment for Trinidad and Tobago in 2012.

1.2.2 STANDARDS

Trinidad and Tobago does not currently have an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Trinidad and Tobago does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Trinidad and Tobago has an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

The national cybersecurity strategy provides a national governance roadmap for cybersecurity in Trinidad and Tobago.

1.3.3 RESPONSIBLE AGENCY

Trinidad and Tobago does not currently have an officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap. Precisely this agency is mentioned in the national cybersecurity strategy but it has not yet been implemented.

1.3.4 NATIONAL BENCHMARKING

Trinidad and Tobago does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Trinidad and Tobago does not currently have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Trinidad and Tobago does not currently have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Trinidad and Tobago does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Trinidad and Tobago does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Trinidad and Tobago does not currently have officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Trinidad and Tobago does not currently have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Trinidad and Tobago does not currently have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Trinidad and Tobago is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Trinidad and Tobago also participated in the OAS/CICTE cybersecurity activities. Trinidad and Tobago is among the beneficiary countries of the EU/ITU co-funded project “Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures” (HIPCAR).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

Article 25 and part VIII of Act No. 12 of 2012.

2.2 UN CONVENTION AND PROTOCOL

Trinidad and Tobago has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Trinidad and Tobago has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Ministry of Education provides internet safety orientation under its program eConnect & Learn. Reference to child online protection can be found at the Policy and Guidelines on the use of laptops distributed by the government and on the National School Code of Conduct.

2.4 REPORTING MECHANISM

Trinidad and Tobago does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

TUNISIA

BACKGROUND

Total Population: 10 705 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 43.80%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:
-Art.199 bis and 199ter of Tunisia Penal Law.

1.1.2 REGULATION AND COMPLIANCE

Tunisia has officially recognized regulations regarding cybersecurity and compliance requirements through the following instruments:

- Law n° 2004-5, February 3, 2004, relative to computer security.
- Decree n° 1248 - 2004, May 25, 2004, setting the administrative, financial and operating procedures of the ANSI.
- Decree n° 1249 - 2004, May 25, 2004, on requirements and procedures for the certification of expert auditors in the field of computer security.
- Decree n° 1250 - 2004, May 25, 2004, on the institutional computer systems and networks subjected to the compulsory periodic Risk Assessment of computer security, and on the criteria relating to the nature and periodicity of the Risk Assessment and to procedures for monitoring the implementation of the recommendations made in the Risk Assessment report.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Tunisia has an officially recognized national CIRT (TunCERT).

1.2.2 STANDARDS

There is no available information regarding any officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

The National Institute for Standardization and Industrial Property (INNORPI) is the leading certification body for Tunisia. Its objective is to undertake every action concerning standardization, the quality of products and services, metrology, industrial property protection and the maintaining of a central commercial register.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Tunisia has an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

The national governance roadmap for cybersecurity in Tunisia is elaborated in the National Agency for Computer Security (ANSI).

1.3.3 RESPONSIBLE AGENCY

The National Agency for Computer Security (ANSI) is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap in Tunisia.

1.3.4 NATIONAL BENCHMARKING

The National Agency for Computer Security (ANSI) is responsible for the benchmarking and measuring cybersecurity development in Tunisia.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no available information concerning any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

The National Agency for Computer Security (ANSI) is responsible for providing educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Tunisia has numerous public sector professionals certified under internationally recognized certification programs in cybersecurity such as ISO270001, CEH, CISA, CISM and CISSP.

1.4.4 AGENCY CERTIFICATION

There is no available information concerning any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders with other nation states Tunisia has officially recognized partnerships with the following organizations:

- National Agency for Computer Security
- FIRST
- Honeypot Project
- OIC-CERT
- UNCTAD.

1.5.2 INTRA-AGENCY COOPERATION

The Tunisian honeypot project "Saher-HoneyNet" is an initiative launched by the Tunisian CERT, in order to mitigate threats related to malicious traffic and to improve the national cyberspace security by ensuring preventive and response measures to deal with malicious threats. It is the officially recognized program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

The Tunisian honeypot project "Saher-HoneyNet" is an initiative launched by the Tunisian CERT, in order to mitigate threats related to malicious traffic and to improve the national cyberspace security by ensuring preventive and response measures to deal with malicious threats. It is the officially recognized program for sharing cybersecurity assets within the private sector.

1.5.4 INTERNATIONAL COOPERATION

Tunisia is a member of the ITU-IMPACT initiatives and has access to relevant cybersecurity services. Tunisia participated in several cybersecurity activities with the following organizations/activities:

- National Agency for Computer Security
- Shadowserver
-Honeypot Project
- ArborNetworks

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child protection has been enacted through the following instrument:

- Articles 226, 226bis and 233-235 of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Tunisia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Tunisia has signed and ratified, with no declarations or reservations to articles 2 and 3, the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Tunisia Computer Emergency Response Team (TUN CERT (*)) provides information on tools for parental control.

2.4 REPORTING MECHANISM

TUN CERT makes available the number (+216) 71 843 200 or (+216)71 846 020 - ext. 119 and the email address incident@ansi.tn to report a computer incident.

CYBERWELLNESS PROFILE

TURKEY

BACKGROUND

Total Population: 74 509 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 46.25%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Law on Regulation of the publications on the Internet and Combating against committed crimes by these publications.

-Turkish Criminal Law

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Law on Security of Electronic Communications

-Regulation Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Turkey has an officially recognized national CIRT (TR-CERT).

1.2.2 STANDARDS

Turkey has officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards through the National Cyber Security Strategy and Action plan 2013-2014 and the Law on Security of Electronic Communications.

1.2.3 CERTIFICATION

Turkish Standards Institution provides system, personnel and product certification services according to many international standards including ISO IEC 27001, ISO IEC 15408, ISO IEC 12207.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Turkey has an officially recognized national cybersecurity strategy (National Cyber Security Strategy and Action plan 2013-2014). The strategy is based on the principal of securing the information systems used in critical infrastructures and taking necessary measures to provide national cybersecurity.

1.3.2 ROADMAP FOR GOVERNANCE

The National Cybersecurity Strategy and Action Plan allows for 29 main actions and 95 sub actions and assigns responsibilities about legislation, capacity building, development of technical infrastructure. This in turn provides a national governance roadmap for cybersecurity in Turkey.

1.3.3 RESPONSIBLE AGENCY

The Cybersecurity Board is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap. It was established, in order to determine the measures regarding cyber security, to approve the prepared plans, programs, reports, procedures, principles and standards and ensure the application and coordination of them.

1.3.4 NATIONAL BENCHMARKING

In last three years Turkey organized three cyber security exercises at the national level. Participants from both public and private sector have experienced real cyber-attacks and also worked on scenarios. These exercises played a big role in raising awareness of cybersecurity and also were a great tool for measuring the development of cybersecurity. Additionally the By-Law on Security of Electronic Communications obliges electronic communications service providers to comply with ISO IEC 27001. The audits performed by the NRA (ICTA) play a big role in measuring the cybersecurity development level of electronic communications sector.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Turkish Standards Institution is the institution that is responsible for standardization activities. Internationally recognized cybersecurity standards are adopted as Turkish standards as part of harmonization process. The institution provides also standardization services considering the country and sector specific needs.

1.4.2 MANPOWER DEVELOPMENT

Turkish Scientific and Technologic Research Agency and Turkish Standards Institution provide cyber security related training programs including CEH, ISO IEC 27001 lead auditor, internet governance, ICT law etc. There are also graduate programs like information security engineering, cybersecurity, ICT law in several universities like Bahçeşehir University and Şehir University. The graduate programs cover both technical and legal aspects of cybersecurity. Besides, several websites such as www.bilgiguvenligi.gov.tr, www.bilgimikoruyorum.org.tr, www.guvenliweb.org.tr have been established to raise awareness among the people.

1.4.3 PROFESSIONAL CERTIFICATION

Turkey has about 400 public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

There are 106 electronic communications service providers that have ISO IEC 27001 certification. The certification agencies include both accredited national (like Turkish Standards Institution, Kalitest etc) and international certification agencies (like BSI, Bureau Veritas, and DAS etc). There are nearly 15 governmental and public sector institutions that have certifications like ISO IEC 27001, ISO IEC 17025, ISO/IEC 18045. The certification agencies are generally accredited national certification agencies (like Turkish Standards Institution, Kalitest etc).

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Turkey has officially recognized partnerships with the following countries and organizations:

-Albania, Azerbaijan, Bosnia, Herzegovina, Bulgaria, Kosovo, Kyrgyzstan, Macedonia,

-Montenegro, Morocco, Niger, Republic of Sudan, Senegal, Serbia, Tunisia, Iran, Thailand, Egypt and Ukraine

-NATO.

1.5.2 INTRA-AGENCY COOPERATION

The National Cyber Security Strategy and Action Plan 2013-2014 encourages the efficient use and sharing of resources between governmental institutions in cybersecurity related activities.

1.5.3 PUBLIC SECTOR PARTNERSHIP

The National Cyber Security Strategy and Action Plan 2013-2014 encourages the efficient use and sharing of resources between public and private sector in cybersecurity related activities.

1.5.4 INTERNATIONAL COOPERATION

Turkey is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Turkey is also actively involved in the standardization work on cybersecurity within ITU-T. TR-CERT (USOM) is also candidate for FIRST and Trusted Introducer Membership. Turkey has co-organized with the collaboration of IMPACT and ITU, the International Cyber Shield Exercise 2014 (ICSE 2014), in May 2014 Istanbul, Turkey. Turkey participated in Applied Learning for Emergency Response Team (ALERT) 2012 during the ITU Regional Forum on Cybersecurity for Europe and CIS, in October 2012, in Bulgaria.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-The Criminal Code (Article 26)

-Law on Regulation of the publications on the Internet and Combating against committed crimes by these publications (Article 8).

2.2 UN CONVENTION AND PROTOCOL

Turkey has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Turkey has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Turkish Information and Communication Technologies Authority, Telecommunications Presidency (*), provides information and makes awareness raising activities about online safety and children online protection to the Turkish public.

2.4 REPORTING MECHANISM

Online illegal material (according to Law 5651) can be reported at the website of Turkish Internet Hotline which is a member of INHOPE.

CYBERWELLNESS PROFILE
TURKMENISTAN

BACKGROUND

Total Population: 5 170 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 9.60%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Criminal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Law on Communications
- Law on Electronic Document
- Law of Turkmenistan on the Legal Protection of Algorithms and Programs for Electronic Computers, Databases and Topographies of Integrated Circuits.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Turkmenistan does not have any officially recognized national CIRT.

1.2.2 STANDARDS

Turkmenistan does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Turkmenistan.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Turkmenistan does not have any officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Turkmenistan.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Turkmenistan.

1.3.4 NATIONAL BENCHMARKING

Turkmenistan does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Turkmenistan does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Turkmenistan.

1.4.3 PROFESSIONAL CERTIFICATION

Turkmenistan does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Turkmenistan does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Turkmenistan does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Turkmenistan does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Turkmenistan.

1.5.4 INTERNATIONAL COOPERATION

There is no information about any international cooperation initiative that Turkmenistan participates in.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:
- None.

2.2 UN CONVENTION AND PROTOCOL

Turkmenistan has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Turkmenistan has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Turkmenistan.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Turkmenistan.

CYBERWELLNESS PROFILE

TUVALU

BACKGROUND

Total Population: 11 200

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 37.00%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

There is draft legislation on cybercrime prepared and waiting Cabinet's approval and further progress.

1.1.2 REGULATION AND COMPLIANCE

Together with the draft legislation on cybercrime legislation, there is another draft awaiting further development, endorsement and implementation.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Tuvalu has not yet officially approved national or sector specific CIRT. However the Department of ICT is following PacCert developments, advice and recommendations.

1.2.2 STANDARDS

Tuvalu does not currently have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards. However, further development of the cybercrime policy and legislation are in process.

1.2.3 CERTIFICATION

Tuvalu does not currently have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Tuvalu does not have yet an officially recognized national cybersecurity strategy. However, further development of the cybercrime policy and legislation are in process.

1.3.2 ROADMAP FOR GOVERNANCE

Tuvalu does not have yet an officially recognized national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Tuvalu does not have yet any officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap. However further development from the Department of ICT are in process.

1.3.4 NATIONAL BENCHMARKING

Tuvalu does not have yet any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Tuvalu does not currently have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Tuvalu does not currently have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Tuvalu does not currently have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Tuvalu does not currently have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Tuvalu has officially recognized partnerships with the following organizations:

- ITU -PacCert -PiRRC.

1.5.2 INTRA-AGENCY COOPERATION

Tuvalu does not currently have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Tuvalu does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Tuvalu is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Tuvalu also participated in the following cybersecurity activities:

- ITU -PacCert -PiRRC -APT

Tuvalu also takes part in the Asia Pacific CIRT cybersecurity forums. Tuvalu is among the beneficiary countries of the EU/ITU co-funded project “Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries” (ICB4PAC).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Tuvalu does not have specific legislation on child online protection.

2.2 UN CONVENTION AND PROTOCOL

Tuvalu has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

2.3 INSTITUTIONAL SUPPORT

Tuvalu does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Tuvalu does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

UGANDA

BACKGROUND

Total Population: 36 621 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 16.20%

(data source: ITU Statistics, December 2012)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation pertaining to cybercrime is mandated through the following legal instrument:

- Electronic Transaction Act
- Electronic Transactions Regulations
- Computer Misuse Act
- Penal Code Act.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation to cybersecurity has been enacted through the following instruments:

- National Information Technology Authority of Uganda - NITA-U Act
- Access to Information Act
- Electronic Signatures Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Uganda has two national CIRTs CERT-UG operating under the National Information Technology Authority of Uganda (NITA-U) and ugCERT operating under the Uganda Communications Commission.

1.2.2 STANDARDS

There is no available information concerning any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no available information concerning any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Uganda has an officially recognized national cybersecurity strategy since 2011 (National Information Security Strategy 2011). The NITA-U has also developed a National Information Security Framework (NISF).

1.3.2 ROADMAP FOR GOVERNANCE

The Information Security Roadmap and the CERT-UG Roadmap provide national governance roadmaps for cybersecurity in Uganda.

1.3.3 RESPONSIBLE AGENCY

The Ministry of Information and Communication Technology and the National Information Technology Authority of Uganda are the officially recognized agencies responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

There is no available information regarding any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no available information regarding any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

The National Information Security Framework Validation Workshop provides sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Uganda does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity. However there are at least three within the CERT-UG.

1.4.4 AGENCY CERTIFICATION

The national CIRT (CERT-UG) is the only public sector agency certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Uganda does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Uganda does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Uganda does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Uganda is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION AND STRATEGY

Specific legislation on child protection has been enacted through the following instruments:

- Computer Misuse Act, 2011.

- Section 148 of the Criminal Code but does not mention explicitly pornography.

- The Draft of the Nation Information Security Strategy deals with emerging security risks, but has no specific provisions for child online protection.

2.2 UN CONVENTION AND PROTOCOL

Uganda has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Uganda has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Uganda does not have any officially recognized agency that offers institutional support to child online protection.

2.4 REPORTING MECHANISM

Uganda CERT (UgCERT) provides an online form to report incidents.

CYBERWELLNESS PROFILE
UKRAINE

BACKGROUND

Total Population: 44 940 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 41.80%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- The Penal Code Act
- The Computer Misuse Act.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- NITA-U Act
- Access to information Act
- Electronic Signatures Act
- Electronic Transactions Act
- The Electronic Transactions Regulations.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Ukraine has an officially recognized national CIRT known as CERT-UA.

1.2.2 STANDARDS

There is no officially approved national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards in Ukraine.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Ukraine.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Ukraine has an officially recognized National Security Strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national or sector-specific governance roadmap for cybersecurity in Ukraine.

1.3.3 RESPONSIBLE AGENCY

The function of overseeing cybersecurity is shared between: The Security Service of Ukraine (SBU), the State Special Communication Service, and the Ministry of Internal Affairs.

1.3.4 NATIONAL BENCHMARKING

Ukraine has no officially recognized national benchmarking and referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no nationally recognized program for research and development of cybersecurity standards, best practices and guidelines in Ukraine.

1.4.2 MANPOWER DEVELOPMENT

The OSCE project is responsible for the training of twenty Ukrainian police officers and experts, improving their knowledge and skills in investigating cyber-related crimes. The course was held at the request of the country's interior Ministry.

1.4.3 PROFESSIONAL CERTIFICATION

Ukraine does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Ukraine does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states Ukraine participates in regional cybersecurity activities especially through the OSCE.

1.5.2 INTRA-AGENCY COOPERATION

Ukraine has officially recognized national programs for sharing cybersecurity assets within the public sector through CERT-UA.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is a framework for sharing cybersecurity assets between the public and private sector in Ukraine through the CERT-UA.

1.5.4 INTERNATIONAL COOPERATION

Ukraine is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Ukraine participates in the:

- OSCE - ITU - NATO

CERT-UA is a member of FIRST.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Article 301 of the Criminal Code which does not explicitly mention child pornography but pornographic items in general.

- Law on the introduction of Amendments to several Legislative Acts of Ukraine regarding Counteraction to Distribution of Child Pornography.

2.2 UN CONVENTION AND PROTOCOL

Ukraine has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Ukraine has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no information about any institution responsible for the online protection of children in Ukraine.

2.4 REPORTING MECHANISM

The website of La strada Ukraine provides an online consultation form on child rights protection and a hotline. The CERT-UA also provides an online form to report incidents.

CYBERWELLNESS PROFILE
UNITED ARAB EMIRATES

BACKGROUND

Total Population:

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 88.00%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Federal Law by Decree No. 5 of 2012 regarding Cyber Crimes
- The Federal Law No. (2) Of 2006 on the Prevention of Information Technology Crimes.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Federal Law No. (1) of 2006 on Electronic Commerce and Transactions.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

The UAE has an officially recognized national CIRT known as aeCERT.

1.2.2 STANDARDS

There are no officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards in the UAE.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in the UAE.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

The UAE has officially recognised the General Policy for the Telecommunications Sector and the Cabinet Resolution No. 21 of 2013 regarding Information Security Regulation in Government Entities as the national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in the UAE.

1.3.3 RESPONSIBLE AGENCY

The Telecommunications Regulatory Authority (TRA) is the body responsible for the implementation of a national cybersecurity strategy and policy in the UAE.

1.3.4 NATIONAL BENCHMARKING

There is no national benching marking or referential to measure cybersecurity development in the UAE.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

aeCERT is the *officially* recognized national body responsible for research and analysis programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

TRA and the aeCERT launched its awareness campaign Towards a Safe Cyber Culture with Salim, a cyber-security advisor. The aeCERT is also responsible for Advisory, Education and Awareness.

1.4.3 PROFESSIONAL CERTIFICATION

There is a Certified Professional Statistics Database that holds this record of public sector professionals certified under the aeCERT.

1.4.4 AGENCY CERTIFICATION

There is no information on any certified government and public sector agencies certified under internationally recognized standards in cybersecurity in the UAE.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no information on any framework for sharing cybersecurity assets across borders with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

There is no information on any framework for sharing cybersecurity assets within the public sector in the UAE.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no information on any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector in the UAE.

1.5.4 INTERNATIONAL COOPERATION

The UAE is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

The UAE participates in the following cybersecurity activities:

- APWG - The Honeynet Project.

aeCERT is a member of FIRST.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

- Article 12 of the prevention of Information Technology Crimes.

2.2 UN CONVENTION AND PROTOCOL

The UAE has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. The UAE has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The aeCERT has no current project on child online protection. There is no information on any agency responsible for the online protection of children.

2.4 REPORTING MECHANISM

The website of TRA provides an online form for complaints and another one for contacting them. The aeCERT can be contacted by email: info@aecert.ae; the communication can be encrypted using the key available on the website.

CYBERWELLNESS PROFILE
UNITED KINGDOM

BACKGROUND

Total Population: 62 798 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 89.84%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Computer Misuse Act (1990) -Data Protection Act (1998) -Fraud Act.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-OFCOM Telecom Regulation -Info Commissioner Regulation.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

United Kingdom will be establishing a national CIRT by end of 2014. It has the 3 following governmental CIRTs:

-CSIRTUK (Critical Infrastructure) -GovCertUK (Govt Networks) -MODCERT (Military Network)

- csirtuk@cpni.gsi.gov.uk - enquiries@govcertuk.gov.uk -cert@cert.mod.uk.

1.2.2 STANDARDS

United Kingdom is the leading member of the Common Criteria standardization group, which mandates standardization of cyber security in information technology solutions.

1.2.3 CERTIFICATION

The Institute of Information Security Professionals *(*IISP*)* is the leading UK professional certification body for the United Kingdom. The government promotes Information Assurance Professionalism. In particular, there is a certification scheme run by the ISSP.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

United Kingdom has an officially recognized national cybersecurity strategy which was published in 2011.

1.3.2 ROADMAP FOR GOVERNANCE

The national governance roadmap for cybersecurity is elaborated in the national cybersecurity strategy.

1.3.3 RESPONSIBLE AGENCY

The Office of Cybersecurity and Information Assurance (OCSIA), part of the Cabinet Office, is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

OCSIA is responsible for the benchmarking and measuring the progress of the National Cyber Security Programme.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

United Kingdom does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Getsafeonline is a national program aimed at the general public and businesses to raise awareness about cybersecurity. In addition, the government published ten steps to cyber security for the private sector. Lastly, there is a certification scheme run by the ISSP.

1.4.3 PROFESSIONAL CERTIFICATION

United Kingdom has numerous public sector professionals certified under internationally recognized certification programs in cybersecurity. However it did not conduct a survey to gather the exact statistic.

1.4.4 AGENCY CERTIFICATION

United Kingdom's National Technical Authority for Information Assurance (CESG) is the only public agency certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, United Kingdom has officially recognized partnerships with the following organizations:

- ITU
- ENISA
- TRUSTED Introducer
- European CERT Group
- NATO.

1.5.2 INTRA-AGENCY COOPERATION

United Kingdom, through the OCSIA, has officially recognized a national program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

The OCSIA manage the cyber information security partnership (CISP) with private sector. In addition, the Centre for the Protection of National Infrastructure runs a series of sector-based information exchanges for private sector running critical information infrastructure.

1.5.4 INTERNATIONAL COOPERATION

The UK Government participates fully in the cybersecurity debates within the UN, ITU, ENISA, NATO, and OSCE. This work is spread among many government departments and is coordinated by Cabinet Office and the Foreign Office.

GovCertUK is a member of FIRST.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-§48-§50 of the Sexual Offences Act.

-§1 of the Protection of Children Act.

-§63 of the Criminal Justice and Immigration Act.

-§1 of the Malicious Communications Act.

2.2 UN CONVENTION AND PROTOCOL

United Kingdom has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

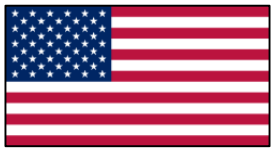
United Kingdom has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Child Exploitation and Online Protection (CEOP), under the UK Police, provides information on online safety for children and parents.

2.4 REPORTING MECHANISM

Inappropriate and offensive content can be reported in the website of CEOP. Online Criminal Content can be reported in the website of the Internet Watch Foundation. Computer Incidents can be reported by a filling a form found in the website of the UK Computer Emergency Response Team (GovCertUK) or by the phone number 01242 709311.



CYBERWELLNESS PROFILE
UNITED STATES

BACKGROUND

Total Population: 315 791 00

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 84.20%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- 15 USC Chapter 103 - Controlling the Assault of Non-solicited Pornography and Marketing
- 18 USC, Chapter 47, § 1029 - Fraud and related activity in connection with access devices
- 18 USC, Chapter 47, § 1030 - Fraud and related activity in connection with computers
- 18 USC, Chapter 47, § 1037 - Fraud and related activity in connection with electronic mail
- 18 USC Chapter 119 - Wire and Electronic Communications Interception and Interception of Oral Communications
- 18 USC Chapter 121 - Stored Wire and Electronic Communications and Transactional Record Access

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- 44 USC Chapter 35, Subchapter III
- Information Security (§3541)
- Uniform Electronic Transactions Act
- Electronic Signatures in Global and National Commerce Act
- Homeland Security Act
- Cyber Security Research and Development Act
- Protecting Children in the 21st Century Act
- Children's Internet Protection Act
- Adam Walsh Child Protection and Safety Act
- Keeping the Internet Devoid of Sexual Predators Act
- Freedom of Information Act (5 USC § 552)
- Privacy Act (5 U.S.C. § 552a)
- Federal Information Security Management Act of 2002.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

United States has an officially recognized national CIRT (US CERT) and an industrial control systems CERT (ICS-CERT).

1.2.2 STANDARDS

United States has officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards through the following instruments:

-National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.0

-Federal Information Security Management Act of 2002

-NIST SP 800-37 "Guide for the Security Certification and Accreditation of Federal Information Systems"
-The North American Electric Reliability Corporation (NERC) has created many standards. The most widely recognized is NERC 1300 which is a modification/update of NERC 1200.

-National Institute of Standards and Technology Special publication 800-12 provides a broad overview of computer security and control areas.

1.2.3 CERTIFICATION

The National Initiative for Cybersecurity Education (NICCS) offers a cybersecurity framework for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

United States has officially recognized International Strategy for Cyberspace. There is also an executive order in order to improve critical infrastructure cybersecurity. A Critical Infrastructure Protection Program has been in place since 1996.

1.3.2 ROADMAP FOR GOVERNANCE

The NIST Roadmap for Improving Critical Infrastructure Cybersecurity, the Cross-Sector Roadmap for Cybersecurity of Control Systems and the Roadmap to achieve energy delivery systems cybersecurity provide the national governance roadmap for cybersecurity in the United States.

1.3.3 RESPONSIBLE AGENCY

The White House has an appointed US Cybersecurity Coordinator at the level of Special Assistant to the President to guide Executive branch efforts. The Department of Homeland Security (DHS) and the Department of Defense (DoD) are the primary cybersecurity actors in order to monitor and coordinate the implementation of a national cybersecurity strategy, policy and roadmap by respective agencies.

1.3.4 NATIONAL BENCHMARKING

The National Checklist Program (NCP), defined by the NIST SP 800-70 Rev. 2, is the U.S. government repository of publicly available security checklists (or benchmarks) that provides detailed low level guidance on setting the security configuration of operating systems and applications. NCP is migrating its repository of checklists to conform to the Security Content Automation Protocol (SCAP). SCAP enables standards based security tools to automatically perform configuration checking using NCP checklists.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

The Department of Defense (DOD) established the Defense Industrial Base (DIB) Cybersecurity/Information Assurance (CS/IA) Program that aims to provide cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector. The National Institute of Standards and Technology (NIST) leads also in developing a Cybersecurity Framework of standards and best practices for protecting critical infrastructures.

The Cybersecurity Division (CSD) provides information resources—standards, frameworks, tools, and technologies to enable seamless and secure interactions among homeland security stakeholders and leads the government's charge in funding cybersecurity research and development (R&D).

Also the IT Security Essential Body of Knowledge (EBK) establishes a national baseline of the essential knowledge and skills that IT security practitioners in the public and private sector should have to perform specific roles and responsibilities.

1.4.2 MANPOWER DEVELOPMENT

United States has the following various types of awareness programs, industry talk, conferences, training programs and workshops on cybersecurity, for the general public as well as for public and private sector employees:

- National Cybersecurity Awareness Month
- Stop.Think.Connect. Campaign
- Cyber-Physical Systems Public Working Group Workshop
- National Initiative for Cybersecurity Education

- National Cybersecurity Education Council (NCEC)
- Cybersecurity Education and Training Assistance Program (CETAP)
- National Cybersecurity Workforce Framework - NICCS
- National Centers of Academic Excellence (CAEs) that provide students valuable technical skills in various disciplines of Information Assurance.
- The Federal Cybersecurity Training Events (FedCTE) that delivers training, labs, and competitions for Federal cybersecurity and IT professionals.

1.4.3 PROFESSIONAL CERTIFICATION

There is no available information regarding the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

There is no available information regarding any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, United States has officially recognized partnerships with the following organizations:

- DHS and Canada Public Safety Plan to Strengthen Cybersecurity Cooperation

- FIRST

- US CERT

- United States and Estonia: Partners in Cyber Security and Internet Freedom

1.5.2 INTRA-AGENCY COOPERATION

United States has officially recognized the following national or sector-specific programs for sharing cybersecurity assets within the public sector through the Department of Homeland Security (DHS) created by the Homeland Security Act of 2002.

- The National Infrastructure Protection Plan (NIPP)

- The Department of Homeland Security and the Department of Defense (DOD) signed a landmark memorandum of agreement in 2010 to protect against threats to critical civilian and military computer systems and networks.

- The Department of Homeland Security, the Department of Defense, and the Financial Services Information Sharing and Analysis Center launched a pilot initiative designed to help protect key critical networks and infrastructure within the financial services sector by sharing actionable, sensitive information.

- The Cybersecurity Partners Local Access Plan.

1.5.3 PUBLIC SECTOR PARTNERSHIP

The Administration provides officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector through a Cybersecurity Framework, a guide developed collaboratively with the private sector for private industry to enhance their cybersecurity, in 2014.

The National Cybersecurity Center of Excellence (NCCoE) provides businesses with real-world cybersecurity solutions—based on commercially available technologies. Finally the Department of Homeland Security's Critical Infrastructure Cyber Community C³ Voluntary Program helps align critical infrastructure owners and operators with existing resources that will assist their efforts to adopt the Cybersecurity Framework and manage their cyber risks.

1.5.4 INTERNATIONAL COOPERATION

United States is signatory to Council of Europe Convention on Cybercrime and there is an EU-US cooperation on cybersecurity and cyberspace.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION AND STRATEGY

Specific legislation on child online protection has been enacted through the following instruments:

- Section 15 of the US Code, Chapter 91, §§ 6501-6506, included in the US Code by the Children's Online Privacy Protection Act, 1998.

- Section 47 of the US Code, Chapter 5, §§ 254(h)(6).

- Section 18 of the US Code, Chapter 110, §§ 2251-2260A, amended by H.R. 1981, May 2011.

- Section 20 of the US Code, Chapter 72, §§ 9134 (f), included in the US Code by the Children's Internet Protection Act, 2000.

- Adam Walsh Child Protection and Safety Act, July 2006.

- Securing Adolescents from Exploitation Online Act, February 2007.

- Protect our Children Act, October 2008.

- Keeping the Internet Devoid of Sexual Predators, October 2008.

The International Strategy for Cyberspace does not outline child online protection.

2.2 UN CONVENTION AND PROTOCOL

United States has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. United States has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The following supports provide information on internet safety for parents, children and educators:

-Branch created within the Department of Justice: Internet Crime against Children Task Force.

-The Federal Trade Commission runs the OnGuardOnline website, the federal government website dedicated to bringing information on internet safety.

-Branch created within the US Department of Health and Public Service: Administration for Children and Families.

-Organization authorized to work in partnership with the US Department of Justice: National Center for Missing and Exploited Children.

-The United State Computer Emergency Response Team (US-CERT) does not provide specific information on child online protection but hosts a series of links redirecting to it.

2.4 REPORTING MECHANISM

Complaints can be filed through the OnGuardOnline website. Cyber Tipline of the National Centre for Missing and Exploited Children has a dedicated space to report incidents which include computer incidents related to child online protection.

CYBERWELLNESS PROFILE

URUGUAY

BACKGROUND

Total Population: 3 391 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 58.10%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Forgery of electronic documents. Article 4 of Act. 18. 600 (2009)

-Attack on the regularity of telecommunications. Act. 18.383 (2008)

-Child Pornography. Act 17.815 (2004)

-Intellectual Property Offenses and related rights. Act 17.616 (2003)

-Fraud. Article 160 and 347 of the Criminal Code

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Regulatory Framework on Cybersecurity. Decree 92/014

-Policy on Information Security in Public Sector. Decree 452/09

--Information Security Direction. Article 148 of Act 18.719 (2010)

-National Computer Incident Response Centre CERTuy. Article 73 of Act 18.362 (2008)

-National Computer Incident Response Centre CERTuy. Decree 451/009

- Personal data protection and habeas data action Act 18.331 (2008); regulatory Decree 414/009

-Authority: Unit for the Regulation and Control of Personal Data, www.datospersonales.gub.uy

- EU Commission decision on the adequate protection ofpersonal data by Uruguay (2012)

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Uruguay has an officially recognized national CIRT (CERTuy).

1.2.2 STANDARDS

Uruguay has an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards through Regulatory Framework on Cybersecurity. Decree 92/014.

1.2.3 CERTIFICATION

Uruguay does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Uruguay has an officially recognized national cybersecurity strategy through the Regulatory Framework on Cybersecurity. Decree 92/014 and the Policy on Information Security in Public Sector. Decree 452/09 .

1.3.2 ROADMAP FOR GOVERNANCE

The Regulatory Framework on Cybersecurity. Decree 92/014 and the Policy on Information Security in Public Sector. Decree 452/09 provide a national governance roadmap for cybersecurity in Uruguay.

1.3.3 RESPONSIBLE AGENCY

The Agency for e-Government and Information Society is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap and can be contacted at direccion@agesic.gub.uy.

1.3.4 NATIONAL BENCHMARKING

Uruguay does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Uruguay published public guides with recommendations and best practices on CERT's website. In addition, Uruguay also trained public servants about major security issues

1.4.2 MANPOWER DEVELOPMENT

Uruguay's national awareness campaign "safe-connected" includes recommendations related to cybersecurity issues and internet use in general. In addition, there are conferences on various topics such as secure web applications, management systems information security, security policies, electronic signatures and key challenges. Specialists are also trained, with the support of international partners such as the InterAmerican Committee against Terrorism (CICTE/OAS), ITU IMPACT-Alliance, ICANN and the U.S. Secret Service

1.4.3 PROFESSIONAL CERTIFICATION

Uruguay does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Uruguay does not currently have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity but it is part of its regulation's strategies.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Uruguay has officially recognized partnerships with the following organizations:

-ITU Impact -First -OAS/CICTE

-eLAC -LACNIC.

Uruguay has an active involvement in the Ibero-American Network of Data Protection and in the International Conference of Data Protection and Privacy Commissioners, hosted in Uruguay in 2012.

1.5.2 INTRA-AGENCY COOPERATION

Uruguay does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Uruguay does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Uruguay participated in cybersecurity activities by FIRST, OAS/CICTE, eLAC and LACNIC.

CERTuy is a member of FIRST. Uruguay hosted and participated in the ITU-IMPACT Applied Learning for Emergency Response Teams (ALERT 2013) in Montevideo, Uruguay.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Article 274* from the Criminal Code, modified by the Law n. 16.707* from July 1995;

-Law n. 17.815*, "Commercial or noncommercial sexual violence committed against children, teenagers or mental unable", August 2004.

2.2 UN CONVENTION AND PROTOCOL

Uruguay has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Uruguay has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Instituto del Niño y Adolescente del Uruguay is responsible for institutional support in child issues. The Dirección Nacional InFamilia is responsible for enforcing the National Strategy for Childhood and Adolescence.

2.4 REPORTING MECHANISM

The CERTuy provides an online form to report incident on its website. The child helpline Linea Azul Servicio Telefónico can be contacted at the number: **800 50 50**.

CYBERWELLNESS PROFILE
REPUBLIC OF UZBEKISTAN

BACKGROUND

Total Population: 28 077 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 38.20%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Criminal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Law on Electronic Signature
- Law on Informatization
- Law on Electronic Document
- Law on Communication
- Law on Electronic Commerce
- Law on Legal Protection of Software and Databases
- Law on Telecommunications
- Law on Principles and Guarantees of Freedom of Information
- Law on Protection of information in the Automated Banking System.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Uzbekistan has an officially recognized national CIRT known as UZ-CERT.

1.2.2 STANDARDS

Uzbekistan does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Uzbekistan.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Uzbekistan does not have any officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Uzbekistan.

1.3.3 RESPONSIBLE AGENCY

There is no information about any agency responsible for cybersecurity in Uzbekistan.

1.3.4 NATIONAL BENCHMARKING

Uzbekistan does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Uzbekistan does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Uzbekistan.

1.4.3 PROFESSIONAL CERTIFICATION

Uzbekistan does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Uzbekistan does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Uzbekistan does not have any officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Uzbekistan.

1.5.4 INTERNATIONAL COOPERATION

Uzbekistan is a member of the SCO.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

- Article 130* of the Criminal Code – does not mention explicitly child pornography but pornography in general.

2.2 UN CONVENTION AND PROTOCOL

Uzbekistan has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Uzbekistan has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Uzbekistan.

2.4 REPORTING MECHANISM

Incidents can be reported to the UZ-CERT using the email: cert@uzinfocom.uz.

CYBERWELLNESS PROFILE

VANUATU

BACKGROUND

Total Population: 252 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 11.30%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Electronic Transaction Act -E-Business Act

1.1.2 REGULATION AND COMPLIANCE

Vanuatu does not have specific regulation and compliance requirement pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Vanuatu is currently establishing a national CIRT and is also a member of the PacCERT. ITU conducted a CIRT assessment for Nepal in 2014.

1.2.2 STANDARDS

Vanuatu does not have officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Vanuatu does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

The Office of the Government Chief Information Officer (OGCIO) is currently formulating an officially recognized national cybersecurity policy.

1.3.2 ROADMAP FOR GOVERNANCE

Vanuatu will be developing a national governance roadmap for cybersecurity with the assistance of ITU once its national cybersecurity policy is formulated.

1.3.3 RESPONSIBLE AGENCY

The Office of the Regulator is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Vanuatu does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Vanuatu does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Vanuatu does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors. However the OGCIO and the Office of Regulator have conducted and continue to raise, on ad hoc basis, awareness in schools and general public using media such as radio and newspapers.

1.4.3 PROFESSIONAL CERTIFICATION

Vanuatu does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Vanuatu does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

The Financial Intelligence Unit, which is under the Prime Minister's Office and Police Force via the Transnational Crime Unit have official recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Vanuatu does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Vanuatu does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Vanuatu is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Vanuatu also participated in ITU related workshop in Pacific region and the APT Cybersecurity Forum in Asia region. Vanuatu is among the beneficiary countries of the EU/ITU co-funded project "Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries" (ICB4PAC).

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

-The Criminal Code(Sections 94, 101D, 147, 147A and 147B).

2.2 UN CONVENTION AND PROTOCOL

Vanuatu has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Vanuatu has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Vanuatu does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Vanuatu does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

VENEZUELA

BACKGROUND

Total Population: 29 891 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 54.90%

(data source: ITU Statistics, 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Penal Code

-Law on Electronic Signature

1.1.2 REGULATION AND COMPLIANCE

Venezuela has specific regulations and compliance requirements pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Venezuela has an officially recognized national CERT (VenCERT).

1.2.2 STANDARDS

Venezuela has an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Venezuela has an officially approved national (and sector specific) cybersecurity framework for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Venezuela has an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Venezuela has a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Venezuela has an officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Venezuela officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Venezuela has officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

The Superintendence of Electronic Certification Services SUSCERTE, the upper body of VenCERT, led a campaign to raise awareness about information security, the use of social media for children and adolescents and to publish the benefits of electronic certificates and electronic signatures.

This campaign led to visits of public institutions and communities in more than 10 states.

1.4.3 PROFESSIONAL CERTIFICATION

Venezuela does not know the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

VenCERT is officially the government and public sector agency certified under internationally recognized standards in cybersecurity, such as ISO 270001.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Venezuela has officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Venezuela has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Venezuela has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Venezuela is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Article 78* of the Federal Constitution.

-Articles 388 and 389* of the Criminal Code.

-Articles 23* and 24* of the Special Law against Computer Crimes, September 2001.

-Articles 73* and 74* of the Law of Information Technology, August 2005.

-Law for the Protection of Children and Adolescents Using Internet Facilities, Video and other Multimedia*, September 2006.

-Articles 33, 74, 75, 79(b), (c), (d), (e), 92(f), 235* and 265* of the Organic Law for the Protection of Children and Adolescents, December 2007.

-Articles 29.1, 41 and 46-49* of the Law against Organized Crime, January 2012.

2.2 UN CONVENTION AND PROTOCOL

Venezuela has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Venezuela has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Venezuelan Computer Emergency Response Team (VenCERT*) provides information* on child online protection. The Governmental organ responsible for implementing projects and writing general guidelines over children and youth issues is the "Consejo Nacional de Derechos del Niño, Niñas y Adolescentes" (IDENA).

2.4 REPORTING MECHANISM

Venezuela does not have any officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE
VIETNAM

BACKGROUND

Total Population: 89 730 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 43.90%

(data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Law on Information Technology.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Law on e-transactions
-Intellectual Property Law
-Law on Telecommunications
-Decree on Information Technology Application in State Agencies' Operations
-Decree No. 63/2007/ND-CP Providing for Sanctioning of Administrative Violations in the Domain of Information.
-Decree No. 90/2008/ND-CP against Spam
-Technology ended by Law No. 36/2009/QH12
-Circular. 12/2008/TT-BTTTT(12/2008) on Anti-Spam

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Vietnam has an officially recognized national CIRT known as VNCERT. In 2011 ITU conducted a CIRT assessment for Vietnam.

1.2.2 STANDARDS

Vietnam does not have an officially approved national cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Vietnam.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Vietnam does not have an officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Vietnam.

1.3.3 RESPONSIBLE AGENCY

The Vietnam Ministry of Posts and Telematics and Ministry of Information and Communication coordinate cybersecurity.

1.3.4 NATIONAL BENCHMARKING

There is no officially recognized national benchmarking or referential for measuring cybersecurity in Vietnam.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is a written guideline based on ISO 27001 followed by VNCERT staff on the appropriate usage of the CIRT's system.

1.4.2 MANPOWER DEVELOPMENT

VNCERT promotes its services to their constituency through website, events, workshops, seminars, publications (Law regulation relating to cyber security, guidelines), newspapers and also television. In addition, they also conduct an annual cyber security competition among universities as part of the awareness program. Ministry of Information and Communication has signed a memorandum of understanding (MoU) with Microsoft - both parties co-operate on bolstering cyber security, cloud infrastructure and application development, and infrastructure management skills in Vietnamese businesses.

1.4.3 PROFESSIONAL CERTIFICATION

Vietnam does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Vietnam does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no information on any framework for sharing cybersecurity assets across borders with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

VNCERT cooperates with other government agencies in the country such as Ministry of Public Security, Ministry of Defense and Ministry of Internal Affairs.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no information on any framework for sharing cybersecurity assets between the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Vietnam is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

Vietnam participates in the ITU.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

-Article 253 of the Criminal Code – only criminalizes the "dissemination" of decadent material.

2.2 UN CONVENTION AND PROTOCOL

Vietnam has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Vietnam has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no information on any agency responsible for child online protection.

2.4 REPORTING MECHANISM

A form can be filled at the website of VNCERT to report a computer incident.

CYBERWELLNESS PROFILE
REPUBLIC OF YEMEN

BACKGROUND

Total Population: 25 569 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 20.00%

(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- None.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Electronic Transactions Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Yemen does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Yemen does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Yemen.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Yemen does not have an officially recognized national or sector-specific cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Yemen.

1.3.3 RESPONSIBLE AGENCY

There is no agency responsible for cybersecurity in Yemen.

1.3.4 NATIONAL BENCHMARKING

Yemen does not have any officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Yemen does not have an officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

There are no educational and professional training programs for raising awareness, higher education and certification in Yemen.

1.4.3 PROFESSIONAL CERTIFICATION

Yemen does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Yemen does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Yemen does not have any framework to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Yemen does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Yemen.

1.5.4 INTERNATIONAL COOPERATION

Yemen is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- None.

2.2 UN CONVENTION AND PROTOCOL

Yemen has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Yemen has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no agency responsible for child online protection in Yemen.

2.4 REPORTING MECHANISM

There is no website or hotline dedicated to child online protection in Yemen.

CYBERWELLNESS PROFILE

ZAMBIA

BACKGROUND

Total Population: 13 884 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 15.40%

(data source: ITU Statistics,2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Computer Misuse and Crimes Act
- Information and Communications Technology Act

1.1.2 REGULATION AND COMPLIANCE

Specific regulation and compliance requirement pertaining to cybersecurity has been enacted through the following instrument:

- Electronic Communications and Transactions Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU conducted a CIRT readiness assessment and capacity building program for Zambia at Kampala, Uganda, in April 2010. A national CIRT Implementation was completed by ITUin September 2012.

1.2.2 STANDARDS

Zambia does not have officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Zambia does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Zambia is in the process of drafting an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Zambia does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Zambia does not have an officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Zambia does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Zambia does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Zambia does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Zambia does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Zambia does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Zambia does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Zambia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Zambia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Zambia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

Zambia is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA). Zambia will host and participates in the Applied Learning for Emergency Response Team (ALERT), cyberdrill for Africa in September 2014.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-The Penal Code (Section 177A)

-Electronic Communication and Transaction Act (Section 102)

2.2 UN CONVENTION AND PROTOCOL

Zambia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Zambia has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Zambia does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Zambia does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

CYBERWELLNESS PROFILE

ZIMBABWE

BACKGROUND

Total Population: 13 014 000

(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 18.50%

(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation pertaining to cybercrime is mandated through the following legal instruments:

-Criminal Law (Codification and Reform Act)

-Computer Crime and Cybercrime Bill (awaiting passing into law).

1.1.2 REGULATION AND COMPLIANCE

Specific regulation and compliance requirement pertaining to cybersecurity is mandated through the following legal instruments:

-Electronic Transaction and Electronic Commerce Bill (awaiting passing into law)

-Data Protection Bill (awaiting passing into law).

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU-IMPACT has conducted a CIRT readiness assessment for Zimbabwe in March 2014, at Addis Ababa, Ethiopia. Zimbabwe does not currently have an officially recognized national CIRT.

1.2.2 STANDARDS

Zimbabwe does not currently have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards. However it will be included in the upcoming National Cybersecurity Strategy.

1.2.3 CERTIFICATION

Zimbabwe does not currently have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals. However it will be included in the upcoming National Cybersecurity policy.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Zimbabwe is in the process of drafting the national cybersecurity policy.

1.3.2 ROADMAP FOR GOVERNANCE

Zimbabwe does not currently have any national governance roadmap for cybersecurity. However it will be included in the upcoming National Cybersecurity policy.

1.3.3 RESPONSIBLE AGENCY

The Government Telecommunication Agency of Zimbabwe is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap. However it is at a formative stage.

1.3.4 NATIONAL BENCHMARKING

Zimbabwe does not currently have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development. However it will be included in the upcoming National Cybersecurity policy.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Zimbabwe does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector. However it will be included in the upcoming National Cybersecurity policy.

1.4.2 MANPOWER DEVELOPMENT

Zimbabwe does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors. However it will be included in the upcoming National Cybersecurity policy.

1.4.3 PROFESSIONAL CERTIFICATION

Zimbabwe does not currently have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Zimbabwe does not currently have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Zimbabwe does not currently have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Zimbabwe does not currently have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Zimbabwe does not currently have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector. However it will be included in the upcoming National Cybersecurity policy.

1.5.4 INTERNATIONAL COOPERATION

Zimbabwe is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Zimbabwe is among the beneficiaries of the EU/ITU co-funded project “Support for Harmonization of the ICT Policies in Sub-Sahara Africa” (HIPSSA).

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Legislation on child protection has been enacted through the following instrument:

-Censorship and Entertainments Control Act (Section 26)

2.2 UN CONVENTION AND PROTOCOL

Zimbabwe has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.Zimbabwe has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Zimbabwe does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Childline Zimbabwe maintains a helpline on number: 116.

国际电信联盟（ITU）
电信发展局（BDT）
主任办公室
Place des Nations
CH-1211 Geneva 20 – Switzerland
电子邮件： bdtdirector@itu.int
电话： +41 22 730 5035/5435
传真： +41 22 730 5484

副主任
兼行政和运营协调部负责人（DDR）
电子邮件： bdtdeputydir@itu.int
电话： +41 22 730 5784
传真： +41 22 730 5484

基础设施、环境建设和
电子应用部（IEE）
电子邮件： bdtiee@itu.int
电话： +41 22 730 5421
传真： +41 22 730 5484

创新和
合作伙伴部（IP）
电子邮件： bdtip@itu.int
电话： +41 22 730 5900
传真： +41 22 730 5484

项目支持和
知识管理部（PKM）
电子邮件： bdtpkm@itu.int
电话： +41 22 730 5447
传真： +41 22 730 5484

非洲

埃塞俄比亚
国际电联
区域代表处
P.O. Box 60 005
Gambia Rd., Leghar ETC Building
3rd floor
Addis Ababa – Ethiopia

电子邮件： itu-addis@itu.int
电话： +251 11 551 4977
电话： +251 11 551 4855
电话： +251 11 551 8328
传真： +251 11 551 7299

喀麦隆
国际电联
地区办事处
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Cameroon

电子邮件： itu-yaounde@itu.int
电话： + 237 22 22 9292
电话： + 237 22 22 9291
传真： + 237 22 22 9297

塞内加尔
国际电联
地区办事处
19, Rue Parchappe x Amadou
Assane Ndoye
Immeuble Fayçal, 4e étage
B.P. 50202 Dakar RP
Dakar – Sénégal

电子邮件： itu-dakar@itu.int
电话： +221 33 849 7720
传真： +221 33 822 8013

津巴布韦
国际电联
地区办事处
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792 Belvedere
Harare – Zimbabwe

电子邮件： itu-harare@itu.int
电话： +263 4 77 5939
电话： +263 4 77 5941
传真： +263 4 77 1257

美洲

巴西
国际电联
区域代表处
SAUS Quadra 06, Bloco “E”
11º andar, Ala Sul
Ed. Luis Eduardo Magalhães (Anatel)
70070-940 Brasilia, DF – Brazil

电子邮件： itubrasilia@itu.int
电话： +55 61 2312 2730-1
电话： +55 61 2312 2733-5
传真： +55 61 2312 2738

巴巴多斯
国际电联
地区办事处
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown – Barbados

电子邮件： itubridgetown@itu.int
电话： +1 246 431 0343/4
传真： +1 246 437 7403

智利
国际电联
地区办事处
Merced 753, Piso 4
Casilla 50484, Plaza de Armas
Santiago de Chile – Chile

电子邮件： itusantiago@itu.int
电话： +56 2 632 6134/6147
传真： +56 2 632 6154

洪都拉斯
国际电联
地区办事处
Colonia Palmira, Avenida Brasil
Ed. COMTELCA/UIT, 4.º piso
P.O. Box 976
Tegucigalpa – Honduras

电子邮件： itutegucigalpa@itu.int
电话： +504 22 201 074
传真： +504 22 201 075

阿拉伯国家

埃及
国际电联
区域代表处
Smart Village, Building B 147, 3rd floor
Km 28 Cairo – Alexandria Desert Road
Giza Governorate
Cairo – Egypt

电子邮件： itucairo@itu.int
电话： +202 3537 1777
传真： +202 3537 1888

亚太

泰国
国际电联
区域代表处
Thailand Post Training Center, 5th floor,
111 Chaengwattana Road, Laksi
Bangkok 10210 – Thailand

邮寄地址：
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210 – Thailand

电子邮件： itubangkok@itu.int
电话： +66 2 575 0055
传真： +66 2 575 3507

印度尼西亚
国际电联
地区办事处
Sapta Pesona Building, 13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10001 – Indonesia

邮寄地址：
c/o UNDP – P.O. Box 2338
Jakarta 10001 – Indonesia

电子邮件： itujakarta@itu.int
电话： +62 21 381 3572
电话： +62 21 380 2322
电话： +62 21 380 2324
传真： +62 21 389 05521

独联体国家

俄罗斯联邦
国际电联
地区办事处
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

邮寄地址：
P.O. Box 25 – Moscow 105120
Russian Federation

电子邮件： itumoskow@itu.int
电话： +7 495 926 6070
传真： +7 495 926 6073

欧洲

瑞士
国际电联
电信发展局（BDT）欧洲处（EUR）
Place des Nations
CH-1211 Geneva 20 – Switzerland
Switzerland
电子邮件： eurregion@itu.int
电话： +41 22 730 5111

国际电信联盟
电信发展局
Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int

ISBN 978-92-61-15785-2
9 789261 157852

定价：258 CHF
瑞士印刷
2015年，日内瓦

04/2015