ITU出版物

国际电信联盟
发展部门

ITU-D第3/2号课题输出成果报告

保障信息和通信网络的安全：培育网络安全文化的最佳做法

2022-2025年研究期

ITU-D第3/2号课题输出成果报告

保障信息和通信网络的安全：培育网络安全文化的最佳做法

2022-2025年研究期

保障信息和通信网络的安全：培育网络安全文化的最佳做法：ITU-D第3/2号课题2022-2025年研究期输出成果报告

ISBN 978-92-61-41105-3（电子版）
ISBN 978-92-61-41115-2（EPUB版）

鸣谢

国际电信联盟电信发展部门（ITU-D）研究组提供了一个中立性平台，来自世界各地的政府、业界、电信组织和学术界的专家可在此汇聚一堂，开发解决发展问题的实用工具和资源。为此，ITU-D的两个研究组负责在成员所提出输入意见的基础上编写报告、导则和建议。研究课题每四年由世界电信发展大会（WTDC）确定。国际电联成员于2022年6月在基加利举行的WTDC-22上商定，在2022-2025年期间，第2研究组将在数字化转型的总体范围内处理七项课题。

本报告是针对第3/2号课题：**保障信息和通信网络的安全：培育网络安全文化的最佳做法**编写的，由ITU-D第2研究组的管理班子进行全面指导和协调。该研究组由主席Fadel Digham先生（阿拉伯埃及共和国）领导，并得到以下副主席的支持：Abdelaziz Alzarooni先生（阿拉伯联合酋长国）、Zainab Ardo女士（尼日利亚联邦共和国）、Javokhir Aripov先生（乌兹别克斯坦共和国）、Carmen-Mădălina Clapon女士（罗马尼亚）、Mushfig Guluyev先生（阿塞拜疆共和国）、Hideo Imanaka先生（日本）、Mina Seonmin Jun女士（大韩民国）、Mohamed Lamine Minthe先生（几内亚共和国）、Víctor Antonio Martínez Sánchez先生（巴拉圭共和国）、Alina Modan女士（罗马尼亚）、[1]Diyor Rajabov先生（乌兹别克斯坦共和国）、[1]巫彤宁先生（中华人民共和国）和Dominique Würges先生（法国）。

本报告是在第3/2号课题共同报告人Vanessa Copetti Cravo女士（巴西联邦共和国）、Nicole Darabian女士（大不列颠及北爱尔兰联合王国）和Jabin Vahora女士（美利坚合众国）[1]的领导下，与以下副报告人协作完成的：Damnam K. Bagolibe先生（多哥共和国）、Daniel Batty先生（Access Partnership有限公司)、[1]Maria Bolshakova女士（俄罗斯联邦）、[1]Tommaso De Zan先生（Access Partnership有限公司）、Idrissa Diallo先生（几内亚共和国）、Sidy Mouhamed Fall先生（塞内加尔共和国）、Álvaro García先生（Axon Partners集团）、Doğukan Ömer Gür先生（土耳其共和国)、Prachish Khanna先生（印度共和国）、马腾先生（中国通信建设集团有限公司）、Rodgers Mumelo先生（肯尼亚共和国）、Uliana Stoliarova女士（俄罗斯联邦）、Samuel Tew先生（Axon Partners集团)、[1]万欣欣女士（中华人民共和国）、Kacie Yearout女士（美利坚合众国）和Jaesuk Yun先生（大韩民国）。

特别感谢章节主要作者的奉献、支持和专业见解。

本报告是在ITU-D第3/2号课题联系人、编辑以及出版物制作团队和ITU-D第2研究组秘书处的支持下编写的。

[1] 在本研究期内卸任。

目录

图和框目录

图

框

内容提要

2022-2025年研究期ITU-D第3/2号课题输出成果报告体现了为从全球各国汲取网络安全经验和做法而做出的共同努力。本报告可作为协助各国制定发展强有力的网络安全文化的战略的一项资源。本报告考虑并体现了国际电联成员国的意见以及研究期内举行的讲习班的讨论成果，反映了旨在确保信息和通信网络安全的多元观点与经验。

在数字技术深度融入日常生活并构成全球经济支柱的时代，本报告承认，在日益复杂的网络威胁背景下，个人、组织和国家正面临更严峻的脆弱性。网络安全不再是小众议题，而成为数字化转型和发展的基本要素，需要政府、私营部门、个人和学术界等所有利益攸关方提供高优先级的输入意见。根据世界经济论坛《2024年全球风险报告》，网络安全问题被列为第四大短期全球重大风险。[2]

除本报告提及的国际电联及国际电联成员的举措和资源外，重要的是要认识到还有多项旨在共享网络安全信息和良好做法的全球举措。这些举措旨在支持各国和利益攸关各方推进网络安全建设，因为对发展中国家–特别是最不发达国家（LDC）而言，找到并获取网络安全信息可能存在困难。有鉴于此，应关注本研究期内提及的两个可使国际电联成员国受益的综合资源平台：联合国裁军研究所（UNIDIR）的网络政策门户网站[3]和全球网络专业知识论坛（GFCE）的网络能力建设知识门户网站。[4]

本报告中多次提及的另一个相关资源是国际电联全球网络安全指数（GCI），[5]该指数从法律、技术、组织、能力发展和合作措施这五个基本支柱方面衡量各国对网络安全的承诺。GCI由国际电联于2015年推出，并不断完善，以作为一种评估、提高认识和能力建设的工具，帮助各国发展和落实其网络安全能力。

本报告的定位是根据动态和不断变化的威胁态势提供最新思考和做法的一项资源，概要说明网络安全现状，并为未来发展奠定战略路径。

本报告的结构安排如下，每一章均侧重于网络安全的一个具体方面：

- 第1章探讨网络安全中至关重要的人的因素，强调亟需加大对提高用户认识和对网络安全员工队伍进行教育与培训的投入。本章着重强调了能够应对当代复杂数字威胁的熟练网络安全专业人员的迫切需求，敦促各国优先开展教育计划和人才招募方案，以培养具备能力且适应力强的网络安全员工队伍，同时优先考虑将提高认识作为促进网络安全文化的一个关键要素。
- 第2章转向网络安全保障做法，这些做法对于保护网络、系统和数据免受恶意活动侵害至关重要。本章评估了全球范围内为帮助预防和缓减网络攻击风险而采用的各种方法、控制措施、指导原则和标准。

---

2 https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

3 https://cyberpolicyportal.org/zh

4 https://cybilportal.org/

5 https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx

- 第3章突出了网络安全事件响应团队（CIRT）在保护关键基础设施中的核心作用。本章展示了成功的事件响应模式，并着重阐述了建立和发展CIRT的重要性，以及CIRT之间协调的重要意义。

- 第4章评估了国家网络安全战略的制定与实施和执行情况。本章详细阐述了将网络安全战略与整体数字化转型、国家安全和经济议程相协调以增强数字复原力的重要性。

- 第5章探讨了保护5G网络安全的努力。面对部署5G网络的全球性挑战，本章重点介绍了有助于应对5G网络安全威胁的政策、监管框架和积极的行业行动。

- 第6章研究了网络犯罪分子越来越多地使用复杂的短信钓鱼手段通过短消息业务（SMS）欺骗用户的行为，强调必须采取一种涵盖政府法规、行业举措和提高公众认识的综合方法，以保护消费者并维护通信网络的可靠性。

报告所附附件作为补充，提供了更多资源，包括本研究周期内国际电联成员国提交的详细文稿，以及ITU-D正在开展的网络安全项目与计划的概要。这些附件提供了宝贵的见解，并可作为利益攸关方加深对网络安全及其在数字时代关键作用理解的基础材料。

本质上，2022-2025年研究期ITU-D第3/2号课题输出成果报告是一份旨在帮助国际电联成员国提升网络安全水平的战略蓝图。本报告呼吁采取统一行动，确保我们的数字未来安全，强调了提高认识、开展教育、制定战略、CIRT能力建设、政策和战略制定以及国际合作对于管理和减轻数字化转型中网络安全挑战复杂性的重要性。

缩写词和首字母缩略语

缩写	术语
2G	第二代移动技术
3G	第三代移动技术
3GPP	第三代合作伙伴计划
4G	第四代移动技术
5G	第五代移动技术[6]
CI	关键基础设施
CIRT	网络安全事件响应团队
CISA	网络安全和基础设施安全局
COP	保护上网儿童
ENISA	欧盟网络安全局
ETSI	欧洲电信标准协会
EU	欧洲联盟
FIRST	事故响应和安全团队论坛
GCI	全球网络安全指数
GFCE	全球网络专业知识论坛
GSMA	GSM协会
ICT	信息通信技术
IoT	物联网
ITU	国际电信联盟
ITU-D	国际电联电信发展部门
ITU-R	国际电联无线电通信部门
ITU-T	国际电联电信标准化部门
LDC	最不发达国家
NESAS	网络设备安全保证方案

[6] 尽管本文件注意正确使用和指称各代IMT的官方定义（见ITU-R第56号决议“国际移动通信的命名”），但本文件的一些部分包含了成员提供的采用常用市场名称“xG”的材料。此材料不一定对应到特定的某一代IMT，因为成员的基本标准是未知的，但总的来说，IMT-2000、IMT-Advanced、IMT-2020和IMT-2030分别称为3G/4G/5G/6G。

（续）

缩写	术语
NIST	美国国家标准与技术研究院
OECD	经济合作与发展组织
RAN	无线接入网
SDN	软件定义网络
SDO	标准制定组织
SG17	ITU-T第17研究组
SMS	短消息业务
UNIDIR	联合国裁军研究所

第1章 – 提高用户在网络安全方面的认识并加强能力建设

实施强有力的网络安全技能和提高认识计划对于确保我们持续安全地享受数字化带来的惠益至关重要。网络安全举措不仅有助于降低网络钓鱼等网络威胁风险，还有助于建设具备应对数字时代复杂挑战能力的熟练员工队伍。本章探讨了关键要素和典型示例，为希望采取相同方法的国家指明前进的方向。

1.1 提高网络安全认识

人为失误仍然是网络安全漏洞的一个重要因素，研究表明，超过88%的网络安全事件都涉及某种形式的人为失误。[7]这突出表明需要制定超越技术解决方案并解决网络安全中人为因素的综合提高认识计划。

网络安全认识是指向个人、组织和社区普及网络风险和保护数字资产和信息的良好做法的战略方法。提高网络安全认识举措的主要目标是培养安全意识文化，使人们能够识别、预防和有效应对网络安全风险。提高认识计划包括多种方法和工具（即培训计划、模拟网络钓鱼演练、游戏化和微学习模块）。这些举措通常涵盖的关键主题包括社会工程学和网络钓鱼认识提高、密码管理、数据保护以及移动设备和社交媒体的安全使用。

实施得当的提高网络安全认识计划可产生显著成效。[8]优先考虑提高认识培训的组织通常能大幅降低钓鱼攻击成功率，并整体提升安全态势，研究显示攻击成功率最高可降70%。[9]投资于提高网络安全认识也会产生可观的投资回报率（ROI），研究表明，即便是最小规模的培训计划也能带来七倍的投资回报率。[10]此外，这些计划有助于建设超越工作场所的网络安全文化，帮助个人在其生活中成为负责任的“网络公民”。另外，提高网络安全认识对于遵守经修订的欧盟《网络和信息系统安全指令》（NIS2）等行业法规和数据保护法律也至关重要。许多行业要求组织实施安全培训计划，以满足监管标准并避免承担潜在的罚款或法律后果。[11]

全球网络安全指数（GCI）的数据表明，2021年至2024年，有152个国家针对普通公众开展了网络安全宣传活动。[12]国际电联成员国实施了若干举措，以提高对网络安全威胁的认识。这些举措包括针对不同群体制定的综合计划。一些项目特别关注网络犯罪和防止欺诈，还有一些项目则利用各种在线媒介向民众推广网络卫生做法。

---

7 https://blog.knowbe4.com/88-percent-of-data-breaches-are-caused-by-human-error

8 https://www.sciencedirect.com/science/article/pii/S0167404823004959

9 https://keepnetlabs.com/blog/2024-security-awareness-training-statistics；https://www.knowbe4.com/press/knowbe4-analysis-finds-security-awareness-training-and-simulated-phishing-effective-in-reducing-cybersecurity-risk

10 https://blog.usecure.io/does-security-awareness-training-work; https://ostermanresearch.com/wp-content/uploads/2021/01/ORWP_0313-The-ROI-of-Security-Awareness-Training-August-2019.pdf

11 https://www.cybsafe.com/blog/7-reasons-why-security-awareness-training-is-important/

12 https://www.itu.int/epublications/zh/publication/global-cybersecurity-index-2024

俄罗斯联邦推出的“全俄罗斯网络卫生计划”就是一项针对不同群体制定的全面计划的例子。这是一项为期三年的全面举措，于2022年8月启动，旨在提高俄罗斯联邦公民的网络安全认识。该计划将人群划分为三个年龄组来开展更有效的针对性宣传：儿童和青少年（12-18岁）、中青年人（18-45岁）和中老年人（45岁以上）。其中，12-18岁群体因易受网络威胁影响而受到特别关注，针对其实施了两个重点项目：

– “网络欺凌”项目为受害者、攻击者和观察者提供建议，强调用幽默和适度漠视的方式应对网络欺凌的重要性。

– “升级保护技能”项目的重点关注教育儿童识别网络游戏环境中的诈骗行为。

针对18-45岁的中青年人，该计划推出了以下项目：

– “网络健康生活方式”

– “复杂简单密码”和

– “了解您的职责”。

这些举措涉及移动设备保护、防止网络钓鱼、密码安全和电话欺诈认识等主题。该计划还能满足45岁以上中老年人的需求，重点关注防止其遭受电话欺诈。此外，还制定专门课程提升公务员的信息安全素养。2022年进行的一项全俄罗斯联邦研究显示，民众的网络素养指数为48.2分（满分100），涉及病毒防护、安全上网和个人数据安全等方面。网络卫生计划为年度更新机制，确保能持续应对新兴数字威胁和不断变化的民众需求。[13]

在**科特迪瓦共和国**，提高网络安全认识计划是该国通过主要网络安全机构实施的多项提高网络安全认识和培训举措之一，特别关注网络犯罪。打击网络犯罪平台（PLCC）在教育机构（包括中小学和高校）以及金融机构、宗教场所开展宣传活动，并在社交媒体发布教育内容和网络犯罪逮捕信息。科特迪瓦计算机应急响应团队（CI-CERT）是该国的国家网络安全协调中心，推出了名为“DIGISEC”的专项培训计划，旨在提高企业和机构的工作场所数字安全认识。近期值得关注的另一项举措是2024年非洲国家杯期间部署的CyberCAN23。该网络安全系统由CI-CERT管理，重点关注提高对数字平台诈骗，特别是网络钓鱼的认识。该活动通过社交媒体平台、电视和无线电等多渠道传播网络安全信息。该国还开展了名为“全民线上责任”（En ligne tous responsables）的全国性宣传活动，覆盖该国各个城镇[14]。

卢旺达共和国实施了多项加强网络安全教育、培训和提高认识的举措，包括“提高国家网络安全认识和培训计划”，该计划不仅促进提高互联网用户的网络安全认识，还培养网络安全专业人员，以协助公私机构保护关键系统免受网络威胁。[15]

中国以预防网络欺诈为重点，努力构建全社会、多维度的“反欺诈网络”，鼓励安装国家反欺诈中心软件，提高学生、老年人、农民等一系列目标人群对采取网络卫生措施的认识。[16]

---

13 俄罗斯联邦提交的ITU-D SG2 2/71号文件

14 国际数字技术女性专家网络（RIFEN）提交的ITU-D SG2 SG2RGQ/160号文件

15 卢旺达提交的ITU-D SG2 2/35号文件

16 中国提交的ITU-D SG2 2/370号文件

最后，在**巴西**，一项举措依托YouTube等在线传播工具，聚焦提升民众网络安全卫生做法。巴西通过国家电信管理局（Anatel）实施了这些网络安全卫生举措。Anatel在其2023-2027年战略规划中专门设立了数字诈骗防范与网络安全卫生门户网站，提供常见的数字威胁及防范策略信息。该机构定期与合作伙伴开展宣传活动，并在其YouTube频道上维护专门的网络安全内容播放列表。其他值得注意的举措包括2023年10月和2024年10月的#OctoberCyberSafe运动，以及2024年2月和2025年2月的“更安全的互联网日”活动。[17]

1.2 网络安全教育和培训方面的能力建设

世界经济论坛发布的《2025年全球网络安全展望》报告强调，网络安全技能短缺问题日益严峻。自上一份报告（《2024年全球网络安全展望》）发布以来，网络安全技能差距扩大了8%，三分之二的组织报告存在关键网络安全技能差距，这阻碍了其满足安全需求的能力。该报告还强调亟需通过培训、技能重塑以及招聘和留住人才等举措来弥合这一技能差距。[18]

网络安全教育和培训是一个综合过程，旨在使个人掌握保护数字资产、识别和缓解网络威胁以及确保信息系统安全所需的知识、技能与能力。网络安全教育和培训涵盖广泛的主题和方法，致力于培养能够应对网络安全领域不断变化的挑战的员工队伍。网络安全教育和培训可采取多种形式，包括正式的学术课程、专业认证、实训讲习班和持续学习计划。

在当今数字化背景下，网络安全教育和培训计划至关重要。这些计划通过使个人和专业人员掌握识别及应对潜在网络威胁的知识与技能，有助于防止数据泄露并降低网络风险。[19]美国网络安全和基础设施安全局（CISA）认为网络安全教育和培训“对保护国家关键基础设施至关重要”，[20]这凸显了训练有素的网络安全专业人员在保障国家安全和经济利益方面的关键作用。

不同国际电联成员国的网络安全教育和培训政策的规模和水平差异很大。一些成员国部署了全面政策工具以增加各级网络安全专业人才的数量，其他成员国则重点制定特定的网络安全培训计划。一些成员国通过在高校设立高等教育课程重点培养研究生，其他成员国则注重在职员工队伍的培训需求。此外，由国际组织开展的许多国际计划也已陆续出台。还注意到区域层面的差异，91%的欧洲国家提供大学水平的网络安全课程，而美洲地区国家为60%，非洲地区国家为61%。[21]

英国是实施多层次网络安全教育和技能政策的一个实例，该国通过推行各类政策与计划来缩小网络安全技能差距。其战略聚焦三大领域：成年人网络安全技能开发、年轻人网络安全技能开发以及网络安全职业体系建设。针对成年人，英国提供了12-16周的强化训练营课程，包括提升网络技能计划，以重新培训和提高个人网络安全技能。英国还推行学徒制，例如“网络优先学位学徒制”（CyberFirst Degree Apprenticeship），以提供

17 巴西提交的ITU-D SG2 SG2RGQ/165号文件 https://www.youtube.com/playlist?list=PLOmVJ5Ex3R10wEUM3edKTSErojXs_07xg（网络安全播放列表）

18 https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

19 https://www.forbes.com/councils/forbestechcouncil/2025/01/21/protecting-our-future-why-cybersecurity-training-is-essential-for-students/

20 https://niccs.cisa.gov/education-training

21 https://www.itu.int/epublications/zh/publication/global-cybersecurity-index-2024

实践性在职经验。针对年轻人，英国在“网络优先”（CyberFirst）旗下打造了一个产品生态系统。其中包括面向对网络安全职业感兴趣的女生的全国竞赛、学校假期期间开展的入门课程，以及网络安全教育优秀学校认证计划。针对英国年轻人的旗舰学习平台“网络探索者”（Cyber Explorers）面向11-14岁青少年免费开放，已实现接近平等的性别参与比例。英国还通过英国网络安全委员会（UKCSC）推进网络安全职业体系建设。该专业机构旨在为网络安全领域创建清晰的途径和标准，使之更加有组织性并使处于各个职业阶段的更加易于进入该领域。[22]

巴西提供了一个设计缜密、预期重点具体、成果明确的网络安全政策的典范。该国启动“白帽黑客”（Hackers do Bem）计划，培训了3万名网络安全专业人员填补空缺，以解决已发现的网络安全专业人员短缺23万个职位的问题。该计划由巴西国家教育和研究网络（RNP）、电力系统创新研究所（SENAI-SP）和巴西软件出口计划（Softex）联合实施，并获巴西科技创新部支持。该计划遵循结构化的五级网络安全教育方针，从涵盖IT基本概念的拉齐阶段开始，逐步到介绍基本和必要的网络安全概念，最后到进行专门培训。专业级别侧重于五个关键的专业概况：“红队”（安全评估）、“蓝队”（安全架构）、“DevSecOps”（应用程序安全）、“CSIRT”（事件响应）和“GRC”（治理、风险和合规）。最后一个级别包括为期六个月的网络安全驻留计划，在巴西各州提供专业指导。为确保可持续性，该计划建立了一个连接各利益攸关方的国家网络安全中心，这些利益攸关方包括教育机构、政府机构、企业和学生。该国家网络安全中心旨在使行业需求与教育成果保持一致，并扩大整个巴西的网络安全培训机会。[23]

一些国家一直在推动高校网络安全教育，以提升国民技能水平。例如，**卢旺达**政府已在高等教育机构的信息技术（IT）和计算机工程课程中引入了信息安全课程模块。位于基加利的卡耐基梅隆大学非洲分校（CMU-Africa）提供了涵盖网络安全、软件工程和其他信息通信技术（ICT）主题的课程。这些CMU-Africa的课程重点开展网络安全和隐私保护的教学与研究，内容涉及软件和网络系统安全防护，以及提升安全与隐私的适用性。[24]

另一些国家没有针对教育机构，而是将重点放在在职专业人员的培训上，特别是那些更易受网络威胁影响的行业。**阿根廷共和国**专门为公共部门雇员设计了培训计划，内容涵盖数据安全基础知识和信息管理良好做法。这些课程旨在使学员掌握保护信息隐私、保密性、完整性和可用性的必要知识和技能。该国还为被指定为网络安全联系人的公务员提供专门培训。这些专门培训课程涵盖新的网络安全挑战、数字证据、渗透测试和计算机系统的加固等主题。[25]

同样，**阿拉伯叙利亚共和国**也组织了针对政府部门员工、高校和银行业人员的培训活动。国家网络服务管理局设立的卓越中心提供过信息安全培训课程，尽管其活动在战争期间中断，后于2021年重新启动。[26]

埃及于2021年成立了埃及非洲电信监管培训中心（EG-ATRC），该中心通过提供学术和专业培训，提高非洲各国在信息和网络安全领域的人员能力，展现了区域合作的力量。[27]

---

22 英国提交的ITU-D SG2 2/77号文件
23 巴西提交的ITU-D SG2 SG2RGQ/184号文件
24 卢旺达提交的ITU-D SG2 2/35号文件
25 阿根廷提交的ITU-D SG2 2/150号文件
26 阿拉伯叙利亚共和国提交的ITU-D SG2 SG2RGQ/163号文件
27 埃及提交的ITU-D SG2 2/329号文件

另一个示例是拉丁美洲和加勒比网络能力中心（LAC4），这是由**欧洲联盟**、CyberNet和多米尼加共和国政府共同牵头开展的一项举措。LAC4通过广泛的网络安全与数字化转型知识交流、培训和良好做法开发来提升区域网络能力。该中心位于多米尼加共和国圣多明各，作为交流集体经验的中心枢纽，协助拉丁美洲和加勒比地区25个国家加强网络安全框架并促进区域合作。LAC4的广泛培训和网络演练活动包括提高认识、管理网络风险、保护关键基础设施以及制定网络安全政策和法律。它还提供众多技术培训课程，旨在提升整个区域网络安全专业人员的技能和知识。值得注意的是，LAC4高度重视网络安全领域的性别多样性，举办了旨在增强该领域女性权能的专门培训讲习班。这些努力对于建设一支多元、具有复原力的网络安全员工队伍至关重要，能够应对数字环境中不断变化的挑战。[28]

网络演练、模拟网络攻击、信息安全事件和其他类型的破坏活动是网络安全能力建设举措的重要组成部分，一直是**国际电联**电信发展局（BDT）工作的重点，作为提高各国网络安全就绪、保护和事件响应能力的一种手段。国际电联组织区域和全球网络演练以及国家演习，并开发支持这些活动的材料。[29]

随着网络安全在全球政治议程中的地位日益突出，国际组织也纷纷进入这一领域，制定旨在提升下一代网络安全技能的计划。值得关注的国际努力包括国际电联BDT实施的计划“妇女网络足迹”。该计划由三部分组成，包括网络安全政策和外交方面的线上线下技术培训、软技能培训课程、每月定期提供由导师引导的辅导、鼓舞人心的主题演讲介绍以及区域交流活动 – 所有这些都作为“政策与外交轨道”下的补充性一站式综合课程予以提供。该项目的目标是提高妇女的代表性和参与度，寻求改善妇女对国家和国际网络安全政策进程的贡献。[30]

1.3 保护上网儿童

根据儿童之光全球儿童安全研究所的数据，2024年，全球八分之一的儿童（约3.02亿青少年）曾遭受非自愿拍摄、分享和接触性图像和视频的侵害。[31]

保护上网儿童和安全指为保护儿童和青少年免受数字环境中的潜在风险和威胁而采取的措施、做法和策略。保护上网儿童包含一系列为未成年人创造更安全网络体验的努力，包括保护其免受各种形式的网络侵害（如性剥削和性诱骗）、[32]接触有害和不适龄的内容、网络欺凌、色情内容，以及防止利用网络平台从事非法活动等。[33]

---

28 多米尼加共和国提交的ITU-D SG2 SG2RGQ/117号文件

29 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx

30 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Skills-Development/Her-CyberTracks.aspx

31 https://www.ed.ac.uk/news/2024/scale-of-online-harm-to-children-revealed-in-globa

32 根据欧洲委员会《保护儿童免受性剥削与性虐待公约》第23条，诱骗的定义为通过信息通信技术，故意建议成年人与未达到法定性活动年龄的儿童见面，以实施性虐待行为或制作儿童性虐待材料 – https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=201

33 https://www.nspcc.org.uk/keeping-children-safe/online-safety/

在当今数字时代，儿童越来越多地接触互联网及其潜在风险，保护上网儿童和安全至关重要，因此，上网安全教育对培养儿童负责任地使用数字世界的能力显得尤为必要。通过教育儿童认识上网风险、培养批判性思维和负责任的上网行为，儿童可以发展必要的自我保护技能，并在网络环境中做出明智决策。[34]

成员国提交的文稿显示，近年来各国高度重视保护上网儿童，采用多种手段确保上网儿童安全。GCI数据显示，全球69%的政府已专门针对家长、教育工作者和儿童开展活动，作为保护上网儿童工作的一部分。[35]许多国家正在制定全面的法律政策框架和实操性计划及工具来保障儿童网络环境的安全。同时，各国还收集了关于儿童上网行为的实证数据，以更好地理解和应对最具挑战性的上网安全问题。各国已认识到利益攸关多方解决方案的重要性，这些解决方案能够将合适的利益攸关方聚集在一起，以解决这一多方面的问题。最后，各国实施了将提高网络安全认识与上网安全相结合的计划，显示了综合方法的重要性。

澳大利亚是选择通过健全法律框架应对保护上网儿童问题的国家示例。该国政府通过2021年颁布的《在线安全法》建立了强有力的框架，专门解决网络欺凌、成人网络暴力和基于图像的虐待等问题。2022年，澳大利亚还成立了由24名13-24岁成员组成的电子安全青年理事会，该机构就政策和计划提供直接意见，并与主要技术公司合作加强用户责任意识。[36]

中国是全面实施保护上网儿童政策的另一示例，该国实施了影响广泛的互联网安全教育计划。学校作为网络安全教育的主要渠道，覆盖了90.3%的未成年人，家庭以61.7%的覆盖率成为第二大重要教育渠道。总体来看，85.4%的未成年人接受过某种形式的网络安全教育。通过国家电信运营商实施的“护苗宽带”计划已助力守护1.6亿个有学龄儿童的家庭，处理能力超过10.2亿次呼叫。中国政府开展专项活动应对上网安全问题，还出台了儿童个人信息网络保护规定、未成年人网络保护条例等重要政策。统计数据表明了这些计划的有效性：超过70%的未成年人能识别网络诈骗，半数以上未成年人表现出健康用网的意识。[37]

其他国家也将提高网络安全认识与在线安全教育相结合。例如，**俄罗斯联邦**实施了“数字扫盲运动”，作为其2018年启动的更广泛的国家“数字经济”计划的一部分。该计划通过互动动画视频提供教学内容，涵盖钓鱼识别、个人信息保护、应对网络欺凌、安全使用社交媒体和信息验证等核心网络安全主题。课程还涉及版权意识、防范网络诈骗、计算机病毒防护、数字礼仪和电子货币安全等具体领域。为确保有效实施，该活动为教师提供教学方法材料，帮助将网络安全课程融入计算机科学课堂和家长会中。[38]

---

34 https://www.cois.org/about-cis/child-protection/resources；https://learning.nspcc.org.uk/online-safety

35 https://www.itu.int/epublications/zh/publication/global-cybersecurity-index-2024

36 澳大利亚提交的ITU-D SG2 2/167号文件

37 中国移动通信集团有限公司提交的ITU-D SG2 SG2RGQ/212号文件

38 俄罗斯联邦提交的ITU-D SG2 SG2RGQ/170号文件

一些政府主管部门已经开发了具体技术工具，以保护上网儿童。作为保护和赋能上网儿童及青少年国家战略的一部分，**科特迪瓦**推出了“在网上自我保护”（jemeprotegeenligne.ci）[39]网站，提供专为儿童设计的互动工具、搜索引擎和社交媒体网站。该网站还包含一个举报机制，允许用户匿名且隐蔽地举报侵犯行为。该举措由各利益攸关方合作开展，并得到了互联网观察基金会的支持。[40]

此外，各国和组织也已经认识到，有必要让更多利益攸关方参与保护上网儿童的进程。在**尼日利亚**，《保护上网儿童举措》作为主要框架，将相关政策纳入互联网服务提供商的条款和条件。作为该国的主要政策参与者之一，尼日利亚通信委员会（NCC）建立了针对虐待儿童内容的举报机制，并对此类内容实施了屏蔽措施。[41]**赞比亚共和国**于2020年启动了《国家保护上网儿童战略》，制定了五年实施计划（2020-2024年），侧重于组织结构、能力建设、法律措施、国际合作和技术程序。赞比亚总结了若干经验教训，包括扩大利益攸关方合作、可持续不间断的资金支持以及强有力的监测评估框架。[42]最后，**国际电联**保护上网儿童举措作为全球领导性平台，汇集了具有专业知识和十多年全球儿童在线保护活动成功技术援助经验的利益攸关多方群体。该举措由80多个知识伙伴组成，保护上网儿童活动包括制定儿童培训材料[43]、针对家长和教育工作者[44]、行业[45]和决策机构制定导则[46]、通过国际电联学院开展在线培训以及为教育工作者和青年提供线下培训。[47]上述导则为所有相关利益攸关方提供了一套全面建议，说明如何为儿童和青少年营造安全和赋权的在线环境。这些导则通过翻译、本地化和宣传活动得以开发和传播。

各国也关注能力建设活动以及实证数据的收集，以了解儿童如何在网上互动。**肯尼亚**通信管理局实施了“加入COP”和“别想忽悠我们，我们懂网络”（Huwezi Tucheza, Tuko Cyber Smart）宣传活动，面向家长、监护人、教师和青少年。肯尼亚还与非洲高级电信学院合作开发了教育资源并制定了能力建设举措，包括关于儿童上网保护和安全措施的培训计划。该计划已为各行各业的951名参与者提供了关于保护上网儿童和安全的培训。肯尼亚还在开展一项关于保护上网儿童和安全的全国调查，以收集关于儿童上网行为的实证数据。该全国调查本预计于2024年完成。[48]

---

39 https://www.jemeprotegeenligne.ci/

40 科特迪瓦提交的ITU-D SG2 2/34和2/137号文件

41 尼日利亚提交的ITU-D SG2 SG2RGQ/20号文件

42 赞比亚提交的ITU-D SG2 SG2RGQ/114号文件

43 https://www.itu-cop-guidelines.com/children

44 https://www.itu-cop-guidelines.com/parentsandeducators

45 https://www.itu-cop-guidelines.com/industry

46 https://www.itu-cop-guidelines.com/policymakers

47 https://www.itu-cop-guidelines.com/

48 肯尼亚提交的ITU-D SG2 2/119号文件

第2章 – 网络安全保障做法

网络安全保障做法已成为保护网络、系统和数据免受恶意活动干扰的关键因素。[49]网络安全保障做法泛指用于确保保护电子设备、系统、网络和数据机密性、完整性和可用性的相关控制程序。虽然网络安全保障做法不直接防止网络攻击，但如果实施得当，其目标是将此类攻击的风险降至最低。根据具体的安全控制、导则和标准，可以对网络安全保障做法进行检查，这些做法既可由监管实施，也可由业界自愿采用。但是，没有放之四海而皆准的方法，国家主管部门和行业监管机构经常采用不同的做法，从自我评估和自愿导则到贴标方案以及严格的合规检查。

虽然没有一种单一的方法可以推荐，但很明显，在最近几年里，随着若干国家和地区的不同发展，在全球范围内采用网络安全保障做法已取得了持续进展。例如，**经济合作与发展组织（OECD）**于2022年12月推出了理事会关于产品和服务数字安全的建议书，该建议书推荐通过相关政策，增强与风险相称的产品和服务的数字安全性，首先采用基于自愿政策措施的宽松方法，再探讨强制性措施的必要性。[50]本章阐述了面临的挑战，评估了影响，并介绍了迄今为止在确定和实施网络安全保障做法方面吸取的经验教训。

2.1 评估危急性、风险和成本的方法

在考虑实施网络安全保障做法时，至关重要的是首先确定一个实体正在试图保护什么以及确定的资产所面临的风险。希望防止网络攻击的国家和公司应优先确定哪些系统和资产需要保护，并评估其漏洞。在此方面，制定开展风险评估的框架或蓝图是一种有益的工具。用于实施风险评估的最知名的框架之一是**美国**国家标准技术局（NIST）的网络安全框架[51]该框架目前正在进行更新。[52]这是一种广泛使用的方法，用于帮助确定和尽量减少组织风险。它制定了非监管导则，使全球各组织能够确定其自身的风险状况，并实施适当的网络安全控制。2024年初发布的经修订的框架基于与使用这些导则的利益攸关方的广泛和长期接触，并继续与其他国际标准保持一致。[53]

NIST作为一个非监管机构的有利地位已使其与来自世界各地的行业利益攸关方进行更深入的接触，从而更加了解实际的挑战并收到反馈意见，这些已被纳入新导则。[54]这些导则具有适应性和灵活性，并适用于所有组织和部门。**BitSight**将NIST网络安全框架嵌入其平台，并已被负责网络安全的不同政府机构（如计算机应急响应团队、国家网络安全

---

49 操作安全与网络安全保障做法密切相关，因此操作安全可为保障做法提供良好基础。博通公司（Broadcom）介绍了良好条件的模型，强调该模型由四个关键要素组成：人员和流程、知识、安全产品（外源安全）和资产安全（内源安全）。见“降低风险和保护声誉”，博通公司提交的ITU-T SG17 SG17-C214号文件

50 https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0481

51 https://www.nist.gov/cyberframework

52 https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20

53 https://www.nist.gov/cyberframework

54 美国提交的ITU-D SG2 Q3/2_2023_07讲习班演示文稿

机构、电信监管机构）所使用。[55]通过该平台，各国可对其认为的关键基础设施和资产进行风险评估，并衡量其风险因素。

风险评估还有助于确定适当的保障水平，同时考虑到被保护数据和资产的敏感性、违规的后果以及威胁环境（即，实体是否易受网络攻击）。在某些情况下，保障水平取决于监管要求。保障级别越高，安全控制越严格。例如，较低的保障级别可能只需要一个系统密码或防火墙，而更高级别的保障需要增加更先进的控制，如先进的加密和多因素认证。

尽管网络安全保障做法增加了信息技术预算，但未能落实安全控制可能会付出更高的代价。遭受网络攻击的成本不仅体现在财务方面：额外声誉成本的危害要大得多。失去客户和公民的信任会造成长期影响，不仅仅是金钱问题，组织必须能够从战略上理解这一点。同样，对于公共部门而言，攻击如果成功，可能会影响公共服务和关键活动的供应，这种服务和活动的破坏力也不能仅从财务角度进行评估，因为其会对公民生活产生影响。

对各类组织而言，如何规划并为网络安全投入制定预算以确保符合国家法规可能颇具挑战。为支持组织做好法定网络安全控制措施的成本规划，**沙特阿拉伯王国**国家网络安全局（NCA）研发了《沙特阿拉伯基础网络安全控制措施》实施成本估算工具。[56]初期测试表明，NCA得出结论认为，该成本估算框架成效显著，它提供了良好的估算，特别是对于那些处于实施网络安全相关控制措施早期阶段的组织，这些组织往往缺乏实施此类网络安全控制措施所需的预算、时间或资源估算记录。

2.2 利益攸关多方方式

重要的是将举措与其他做法进行对比，了解良好做法，并在举措制定过程中从他人的成功和错误中吸取教训。同样重要的是与包括业界利益攸关方在内的利益攸关多方进行接触，从而获得重要见解以制定举措。

尽管在最不发达国家（LDC）实施网络安全保障做法越来越有必要，但可能仍然难以实施。**多哥**网络防御非洲（CDA）的案例可解释本地市场在向基本业务运营商（ESO）提供网络安全保障方面面临的一些挑战。[57]面对的挑战包括缺乏资金、对政府作为服务提供商缺乏信任，以及缺乏本地人力和设施等。为支持ESO遵守新公布的网络安全控制要求，多哥政府与大型知名网络安全提供商建立了公共私营伙伴关系，为公共和私营部门提供网络安全服务。通过这一合作伙伴模式，多哥创建了CDA，作为一个自给自足且高质量的本地网络安全提供商，在非强制性的基础上向ESO提供支持。自给自足的模式使多哥能够应对上述诸多挑战，并鼓励培养网络安全领域的本地人才，推动当地市场的发展。CDA作为竞争市场中的私营实体，对于确保适应性、高质量服务和竞争性定价十分重要。

同样重要的是，应加强那些可能确定监管环境的政策制定者与民间团体组织之间的合作。民间团体组织可以促进安全需求，同时根据现有的和确定的区域和国际做法，为政策和监管的发展提供信息。例如，**DiploFoundation**是一个国际组织，就与网络安全相关的主题向政府、监管机构、企业、民间团体提供培训项目和能力建设专业知识，并参

[55] BitSight提交的ITU-D SG2 Q3/2_2023_02讲习班演示文稿
[56] 沙特阿拉伯提交的ITU-D SG2 SG2RGQ/201号文件
[57] 网络防御非洲提交的ITU-D SG2 Q3/2_2023_09讲习班演示文稿

与“有关网络空间负责任行为的日内瓦对话”。[58]2020年，日内瓦对话促成了一系列良好做法，[59]其中包括建议对安全设计和漏洞管理、威胁建模、第三方和供应链安全、安全开发、漏洞管理和披露以及组织文化做出的定义。

全球网络专业知识论坛（GFCE）是一个国际平台，支持项目的协调，促进知识和专业技术的共享，将提供能力建设支持的请求与开发研究项目相互匹配。[60]GFCE在太平洋岛屿、非洲、美洲和加勒比以及东南亚建立了四个区域中心。鉴于其全球足迹和在发展中国家得到的各种支持，GFCE完全有能力就网络能力建设的需要和需求提出区域性的多元观点。GFCE拥有一个在线门户网站，作为已落实的、当前网络能力建设项目以及资源和工具的存储库。GFCE在线门户网站还有助于减少重复工作并确定一些项目或能力建设方面的差距和模式。[61]

2.3 不断演进的监管方式

在许多情况下，网络安全保障做法在成为强制性之前是自愿引入的。向强制性的转变通常发生在政府认为行业在确保产品安全方面做得不够，消费者不一定掌握评估产品是否安全的知识。这可导致政府和国家主管部门采取行动并规定他们期望行业满足的保障做法。无论是否出于法律要求，面对不断变化的威胁形势和日益演进的网络安全风险，定期审查并调整网络安全保障做法都是良好做法。

巴西电信管理局（Anatel）就有这样一个不断演进的示例，其在国内建立了认证机构和测试实验室系统，用于客户驻地设备（CPE）或家庭网关的认证。Anatel最初的做法是为电信行业提供非强制性的网络安全导则。然而，通过进行风险评估，Anatel发现，考虑到此类设备的脆弱性和威胁，当前建议不足以保护CPE的安全，因此有必要为此类产品制定强制性的最低安全要求。巴西通信服务提供商的强制性要求于2023年初公布，重点解决密码不安全和不必要启用的服务部件等漏洞。[62]这些要求已于2024年初生效，作为产品获批的强制性实验室测试的一部分。[63]Anatel解释说，只有与该部门进行全面讨论之后，才能从非强制性方法向对特定设备的网络安全强制认证要求演进。

同样，在**沙特阿拉伯王国**，国家网络安全局（NCA）强调了创建独立验证和检验（IV&V）生态系统[64]的一项举措，以便在国家层面从网络安全保障的角度测试和认证产品。该举措亦旨在确定对网络风险和威胁高度敏感的硬件和软件并对其进行分类。此外，该举措还寻求为IV&V中的人力发展做出贡献。该举措路线图考虑从自愿计划开始，然后再将网络安全保障作为强制性义务。NCA还提到，这一生态系统最终实现“自我持续”十分重要，这为NCA鼓励市场利益攸关方进行此类IV&V评估的方法提供了信息。

---

58 DiploFoundation提交的ITU-D SG2 Q3/2_2023_11讲习班演示文稿

59 https://genevadialogue.ch/goodpractices/

60 全球网络专业知识论坛提交的ITU-D SG2 Q3/2_2023_12讲习班演示文稿

61 https://cybilportal.org/

62 巴西提交的ITU-D SG2 SG2RGQ/58号文件

63 巴西提交的ITU-D SG2 Q3/2_2023_12讲习班演示文稿；https://informacoes.anatel.gov.br/legislacao/index.php/component/content/article?id=1505；和https://informacoes.anatel.gov.br/legislacao/atos-de-certificacao-de-produtos/2023/1850-ato-2436

64 https://nca.gov.sa/en/news?item=535

在物联网（IoT）安全领域，英国和澳大利亚还提供了从自愿方式向强制性网络安全保障方式演进的案例研究。近年来，两国决定通过立法，根据欧洲电信标准协会（ETSI）EN 303 645号标准[65]（全球首个适用于消费者物联网设备的网络安全标准）为物联网消费品制定基本安全要求。

在**英国**，制造商、进口商和分销商必须遵守13条ETSI安全导则中的3条，法律授权政府在必要时根据定期的威胁评估采用附加要求。在自愿通过一段时间后，决定强制规定一个安全要求基准。2018年，英国制定了消费者物联网安全的自愿行为准则[66]，但行业合规性并未达到预期。通过磋商活动收集的证据表明，消费者重视安全，并愿意为安全产品支付溢价。然而，网络安全威胁不受与产品安全同等程度的强健监管，导致制造商缺乏透明度并延缓采用安全政策。证据还发现，消费者可连接的产品市场抑制了基本安全功能的采用，因为绝大多数消费者认为产品已经是安全的。产品安全和电信基础设施（PSTI）旨在通过强制规定行为准则中的要素来弥补这一差距，以确保制造商了解漏洞并采取措施减轻这些漏洞的影响。PSTI制度已于2024年4月生效，适用于可连接到互联网的任何消费产品。[67]

澳大利亚政府同样发现其2020年发布的《保护消费者物联网安全》自愿行为守则采用率较低。2024年，澳大利亚政府提出一项强制推行该行为守则的法律提案，经公众咨询后获得一致认可。该法律与英国的做法高度一致，旨在通过二级立法（规则）授权部长对物联网设备强制执行特定安全标准。通过将标准纳入规则而非主要立法，澳大利亚政府意在快速更新这些标准，确保本国消费者能基于国际和行业良好做法获得保护。[68]

在**英国**，已确定的挑战之一是对小微企业可能产生的影响，这些企业在遵守新PSTI制度方面面临困难。英国PSTI执法机构正在制定导则，以减轻任何不相称的影响。除了与业界合作外，英国还指出，计划中必须满足的三大要求已经确定并透明地传达了数年。在此期间，英国对该制度的实施过程进行了多次演练，包括密码要求、产品基本架构、漏洞暴露和安全透明度要求。影响评估表明，减少针对消费者和企业的网络攻击量的总体益处有望超过与实施PSTI制度相关的成本。由于《2022年PSTI法案》是世界上第一项强制性网络安全产品立法，执行这一制度的成本尚不确定，但初步估计，划拨的资金将足够。

在某些情况下，用户或客户的类别决定了网络安全保障做法是强制性的还是自愿的。例如，**大韩民国**推出了云安全保障计划（CSAP），这是一项云计算服务的安全认证。[69]通常情况下，CSAP认证是自愿的。但是，公共部门的客户（公共机构）需要使用已根据相关规定获得CSAP认证的云服务，因此，云服务提供商在向公共机构提供云服务时需要获得CSAP认证。

开展定期内部审计有助于确定控制和风险暴露方面的差距并了解威胁情报，这被认为是一种良好做法。即使产品获得认证，也可能在其生命周期内受到安全缺陷的困扰。接受认证方案的过程要求在特定的时间提交信息，而这并未考虑未来威胁的动态变化。**BitSight**最近进行的一项研究表明，漏洞“打补丁节奏”不佳与发生网络安全事

---

65 https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

66 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf

67 英国提交的ITU-D SG2 Q3/2_2023_03讲习班演示文稿

68 澳大利亚提交的ITU-D SG2 2/320号文件

69 https://isms.kisa.or.kr/main/csap/intro/index.jsp和大韩民国提交的ITU-D SG2 SG2RGQ/34号文件

件的可能性[70]之间存在强相关性，这表明了一旦有安全补丁可用就必须立即更新系统的重要性，同时要铭记已报告的补丁在全球各地的不同分布情况。

渗透测试或“笔测试”是一种安全保障活动，有助于评估IT系统的安全性，并确定可能被用来利用的系统漏洞。**英国**通信监管机构Ofcom自愿与电信提供商共同实施TBEST计划，这是一项笔测试，旨在刺激网络攻击，以发现安全漏洞，然后通过补救程序加以解决，以改善运营商的网络安全态势。[71,72]从更广泛的意义上讲，这一计划是Ofcom采用的监督体制方法的一个范例，它强调了与监管机构监管的行业建立协作关系的重要性。迄今为止，英国所有通信提供商都已经或正在自愿接受TBEST计划，并因此实施了变革。TBEST既不是一项“标准”，也不是一个认证程序。其目标是使通信提供商能够认识到网络威胁并及时实施适当的变革，以提高其网络防御能力。通过认识到和解决这些漏洞和薄弱环节，运营商在保护其网络方面将处于更加有利的地位。

2.4 教育消费者和制造商

为使公众了解网络安全的重要性以及选择更安全产品的好处，已开展了工作。

为此采取的一种方法是制定网络安全标签方案，以**新加坡共和国**为例，经认证的产品可以附有标签。标签方案主要是为消费者提供信息工具。在新加坡，网络安全局（CSA）负责网络安全标签方案，旨在帮助消费者区分安全程度较高和较低的物联网设备。[73]该方案是自愿性的（Wi-Fi路由器除外，因为它是强制性的），分为四个级别，第1级是安全基线。第1级和第2级基于制造商的自我评估，第3级和第4级涉及由经认可的实验室进行的第三方评估。该方案分为多个级别，以激励制造商在基本要求之外采取额外的安全措施。

CSA还考虑了强制执行网络安全标准所涉及的权衡问题，包括制造商因合规成本增加而绕过市场的风险。相反，我们的目标是改变制造商的心态，将网络安全视为一种促进因素和市场差异化因素，而不是一种额外成本。关于网络安全标签方案在新加坡的影响，目前仍处于初期阶段，鼓励制造商参与该方案并改善其网络安全的工作仍在进行中。今后将开展公众调查，以评估消费者的认识和行为。第1级和第2级制造商的合规成本已降至最低，消费者的产品成本也没有显著增加。随着自愿计划的实施，市场力量有望推动制造商提高网络安全水平。

在**美国**，新设立的美国网络信任标志计划是物联网产品自愿网络安全标签计划的一个示例。[74]在制定该计划时，美国联邦通信委员会（FCC）强调，征求所有相关利益攸关方（包括行业、政府和民间团体）的公众意见和评论，对于满足已确定需求的计划设计和执行至关重要。该计划由FCC牵头，但网络信任标志的实施需要联合多个跨机构合作伙伴，并与所有相关政府部门保持紧密协作。

---

70 https://www.bitsight.com/press-releases/study-finds-significant-correlation-between-bitsight-analytics-and-cybersecurity

71 与科学、创新与技术部（DSIT）和国家网络安全中心（NCSC）密切合作运营

72 英国提交的ITU-D SG2 SG2RGQ/74号文件

73 新加坡提交的ITU-D SG2 Q3/2_2023_05讲习班演示文稿

74 美国提交的ITU-D SG2 2/196号文件

除标签外，投资于技术控制与提高民众认识并教育他们了解各组织和国家所面临的网络安全风险同样重要。目前，勒索软件攻击是最令人担忧的趋势。对于这些类型的攻击，攻击的主要载体，即犯罪分子进入网络或系统的方式，是网络钓鱼电子邮件。[75]在这种情况下，网络犯罪分子往往只需受害者点击网络钓鱼电子邮件，就能绕过安全控制。因此，让普通公民和员工了解此类问题对网络安全保障至关重要。本报告第1章探讨了提高用户网络安全意识的问题。

2.5 寻求国际协同/统一和互惠协议的方式

网络安全保障模式（如认证和标签方案）之间是否存在互惠协议，可成为这些做法能否推广的决定因素。正如利益攸关方所强调的那样，互惠协议可以帮助在多个市场上运营的行业参与者更容易地遵守规定。然而，考虑到互惠协议是一种正式机制，可能有许多国家条件，而且批准和签署需要时间，网络安全保障做法需要与符合国家需求和优先事项的现有国际方法找到协同效应。这将减轻产品和服务提供商的监管负担，以避免相互矛盾的要求。

网络安全局（CSA）强调了在制定和实施网络安全标签方案方面开展国际合作的重要性。**新加坡**已与芬兰和德意志联邦共和国签署了互认安排，并正在努力扩大在此领域的伙伴关系。新加坡回顾了其经验，指出政府需要积极主动地建立认可，尽管制造商也有兴趣支持认可进程，因为互认安排可以减轻重复测试和认证的负担，并有助于进入不同管辖区的市场。这一进程涉及将相关各方汇聚一堂，统一要求并制定现实且不过于繁琐的共同标准。

在欧洲层面，**欧盟网络安全局（ENISA）**负责开发三种认证方案，这些方案将在内部市场得到认可，从而在整个欧盟实现自动“互认”。这些方案是：*欧盟ICT产品的通用标准方案*，其实施条例于2024年初通过；*云服务方案*，正在进行广泛讨论；以及*5G方案*，正在制定中。[76]

除互惠外，考虑到国际市场行业的运作，统一基本安全要求也是一项重要考虑。有关物联网消费产品的ETSI标准是努力统一基本安全要求的一个示例。主要问题是不同监管框架在多大程度上是同步的，以及它们将在多大程度上通过相同的国际标准相互连接。在此方面，加强对话，甚至找到适当的对话场所提出了一项挑战。为了协调统一，ENISA在网络安全标准化和5G方面的活动需要欧洲标准化委员会（CEN）、欧洲电工标准化委员会（CENELEC）、ETSI、国际标准化组织（ISO）、国际电工委员会（IEC）、GSM协会（GSMA）、第三代合作伙伴计划（3GPP）和全球平台（GlobalPlatform）之间的协作。ENISA的主要输出成果之一是将不同标准制定组织（SDO）的5G安全控制整合到一个存储库中。[77]

---

[75] 网络犯罪分子的常见策略，用来诱骗人们泄露敏感信息或下载感染目标系统/网络的恶意软件。

[76] 欧盟网络安全局提交的ITU-D SG2 Q3/2_2023_10讲习班演示文稿

[77] https://www.enisa.europa.eu/publications/5g-security-controls-matrix

第3章 – CIRT国家协调促进关键基础设施复原力和网络安全事件响应

在当今快速演变的数字环境中，各组织面临着日益增长的网络安全事件威胁，这些事件可能导致敏感数据泄露、业务中断并损害利益攸关方的信任。网络安全事件响应团队（CIRT）的国家协调可强化关键基础设施（CI）的复原力。通过促进协作、信息共享和标准化协议，此类举措旨在提升检测、缓解网络事件并从中高效恢复的集体能力。为实现这一目标，成员国应加大力度建立和发展CIRT，这通常是构建网络安全文化的首要关键步骤。应当指出，CIRTS也称为网络安全事件响应团队（CSIRT）和计算机应急响应团队（CERT），本报告中视作同义词。[78]

国家CIRT的核心职责之一是应对针对关键基础设施（CI）的威胁。关键基础设施是指对公共安全至关重要的系统、网络和资产集合。虽然各国根据自身需求和优先事项对“关键基础设施”的定义不尽相同，但其定义通常涵盖交通运输、能源系统、通信系统、供水系统、金融系统和卫生保健等领域。针对国家关键基础设施的恶意网络活动仍是各国政府面临的重大挑战，可能对公民构成风险。KnowBe4 2024年报告显示，自2022年以来，针对关键基础设施的恶意网络活动增加了30%，2023年1月至2024年期间累计发生超4.2亿次攻击，相当于每秒13次攻击。[79]

关键基础设施攻击对民众的日常生活造成的威胁最大。常见的攻击目标包括医疗急救服务，影响手术实施和处方开具等医疗服务能力。能源基础设施（如电网）也屡遭攻击。鉴于此类事件可能危及生命安全，建立协调响应机制就成为CIRT的关键职能所在。

在CIRT发展和成熟的过程中，各国通常会制定全面的网络安全事件响应计划，以有效检测、遏制、缓解安全漏洞并从中恢复。积极主动且定义明确的网络安全事件响应计划对组织有效减轻安全事件的影响至关重要。各国采用了多种网络安全事件响应计划模式来优化风险管理并减少恶意网络活动。这些模式通常采用整体方法，整合良好做法，并培养持续改进的文化，以增强对网络威胁的复原力并保护数字资产。随着威胁形势的演变，事件响应策略应领先于网络对手，保护组织的完整性和信任度。

事件响应管理的一个新趋势是建立国家网络协调中心，以加强政府的整体协调。在严重的网络事件中，往往涉及多个政府组织；能否协调快速响应可能决定事件影响的轻重。设立集中协调中心或协调单位可以实现快速响应以及整体管理和控制。需要指出的是，关键基础设施不一定是公共部门拥有和管理的基础设施，因此确保与私营部门的协调也是面对和应对网络事件时极其重要的因素。

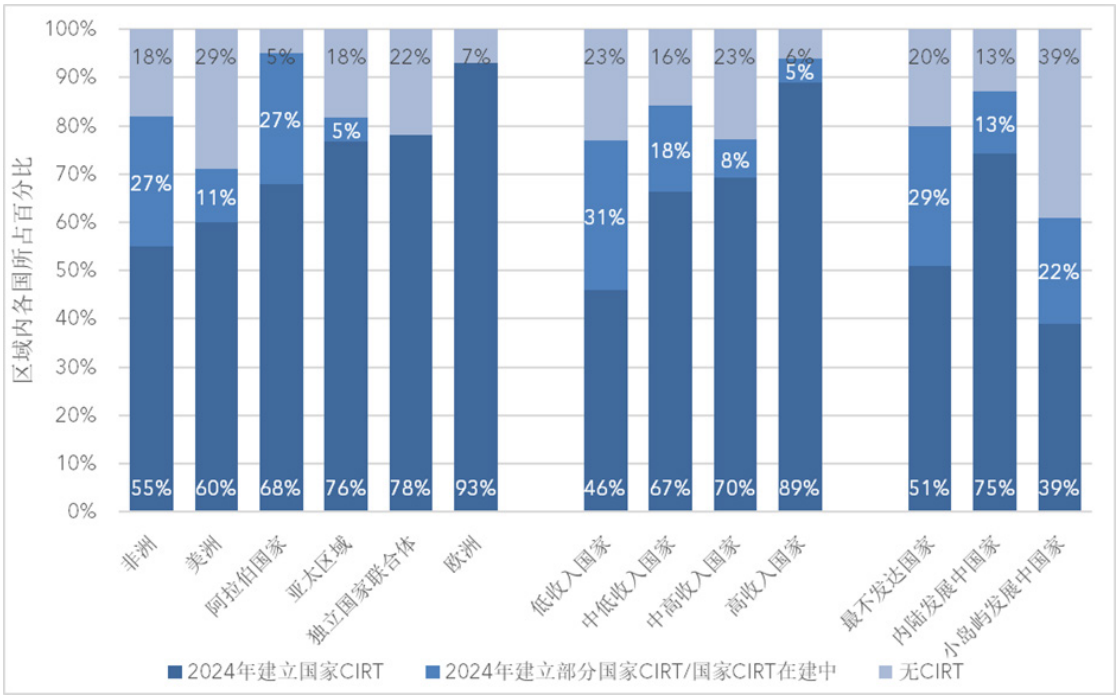
[78] 有关术语的更多信息，见ENISA出版物《如何建立CSIRT和SOC》 – https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

[79] https://www.knowbe4.com/hubfs/Global-Infrastructure-Report-2024_EN_US.pdf?hsLang=en-us

3.1 CIRT的建立

根据2024年全球网络安全指数（GCI），[80]“139个国家已经建立了国家CIRT，55个国家尚无CIRT或正在建设中”。

图1：按区域/收入组别/发展状况分列的建立CIRT的国家百分比



来源：国际电联

CIRT的职责各有不同，其主要职能之一是检测和分析网络与系统中的潜在威胁，并采取响应措施减轻事件影响。建立CIRT通常是培养提高网络安全认识和复原力文化的重要一步。CIRT的建立工作包括保护关键基础设施所需的能力和机制建设。

肯尼亚政府成立了肯尼亚国家计算机事件响应团队协调中心（国家KE-CERT/CC），负责协调国家网络安全工作，并作为网络安全事务的国家联络点。该中心由具备多元技能的利益攸关多方团队组成，能够有效响应和管理计算机安全事件。认识到网络安全对发展数字经济的重要性，肯尼亚通信管理局（CA）推出了“通信管理局网络安全训练营和黑客马拉松系列”活动，以提升本地网络安全能力。[81]

在国际电联的协助下，**吉尔吉斯共和国**一直致力于建立国家CIRT。该CIRT的职责包括识别、管理和应对网络威胁，具备监测预警和事件响应能力，同时进行国家能力建设并转让知识技能，促进关键信息基础设施保护水平的进一步提升。[82]

国际电联与成员国和全球各组织合作，通过建立和加强国家和区域CIRT强化网络安全。国际电联通过电信发展局（BDT）开展CIRT成熟度评估，帮助84个国家评估其网络安全准备情况，建立或完善了国家CIRT。国际电联实施了21个与CIRT相关的项目，目前

[80] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf
[81] 肯尼亚提交的ITU-D SG2 2/112号文件
[82] 国际电联BDT提交的ITU-D SG2 2/170号文件和ITU-D SG2 SG2_2023_05情况通报会议演示文稿

正在开展另外三个项目。已在阿塞拜疆、塞拉利昂和坦桑尼亚联合共和国进行了CIRT成熟度评估，津巴布韦共和国、不丹王国和莱索托王国的评估正在进行中。[83]这些评估为国家CIRT起草改进运营计划提供了依据。国际电联还与事故响应与安全团队论坛（FIRST）社区合作，强化CIRT服务框架，并修改培训材料加强能力建设，管理国家CIRT的运作。[84]

3.2 CIRT和关键基础设施的作用和职责

CIRT通过实时监控、事件管理、威胁分析和脆弱性评估，在保护各领域关键基础设施方面发挥着关键作用。通常情况下，CIRT负责确保信息通信技术（ICT）系统的复原力，快速检测和解决网络安全威胁，并协调各方努力以尽量减少事件对国家安全、公共安全和经济的影响。根据国家需求、发展水平和关键基础设施领域的不同，CIRT在确保网络安全方面发挥不同的作用和关系。

在**立陶宛共和国**，国家CIRT隶属于更广泛的国家网络安全中心（NCSC），专门负责关键基础设施领域的网络事件响应和复原力协调工作。该国政府努力确保CIRT承担积极保护关键基础设施的必要职责并具备相应的技术能力，这一工作为希望建设CIRT能力的其他国家提供了示例。该CIRT为公共和私营部门的利益攸关方提供事件管理服务，确保在网络攻击期间和之后做出适当的响应。CIRT在事件管理中的关键作用之一是其能够与受影响的网络或系统管理员协调，推进运行的快速恢复。

在重大事件期间，立陶宛CIRT专家会现场部署，协助关键基础设施运营商恢复正常运营。例如，在立陶宛电信部门遭受分布式拒绝服务（DDoS）攻击期间，国家CIRT发挥了关键作用，协调受影响运营商之间的通信并提供技术建议，帮助其迅速恢复服务。

关键基础设施保护的关键不仅在于应对恶意网络事件，还在于通过CIRT更高级的功能，预防恶意网络事件发生。立陶宛还赋予其CIRT通过从公开来源、封闭论坛和漏洞报告机制收集信息来进行漏洞管理的职责。该团队主动扫描立陶宛的数字资产，识别可能被恶意行为者利用的漏洞。通过传播有关漏洞和威胁的信息，国家CIRT帮助强化关键基础设施系统以防范潜在的网络攻击，确保关键领域获得主动防护。[85]

巴西已经建立了若干核心组织，确保关键基础设施具备响应能力、受到保护，并采取必要的网络安全措施。在巴西，有两个CIRT承担国家责任：巴西国家计算机应急响应团队（CERT.br）和政府网络事件预防、处置和响应中心（CTIR Gov）。此外，还有多个行业CIRT，以及2021年成立的由CTIR Gov中心协调的联邦网络事件管理网络（ReGIC）。[86]

行业CIRT的一个示例是国家教育和研究网络（RNP）下属的安全事件响应中心（CAIS）。自1997年成立以来，CAIS一直是巴西学术网络的主要CIRT。在第2350号征求意见稿（RFC）的指导下，CAIS负责检测、解决和预防巴西学术网络内发生安全事件。虽然CAIS对学术机构没有直接管辖权，但在事件处理中发挥着关键的协调作用。CAIS的

---

83 国际电联BDT提交的ITU-D SG2 2/201号文件

84 有关国际电联CIRT项目的更多详细信息，见https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx

85 NRD网络安全提交的ITU-D SG2 2/322号文件

86 巴西提交的ITU-D SG2 SG2RGQ/182号文件

工作体现了特定行业内部加强协作以有效管理网络安全风险的重要性。CAIS的案例提供了一个特定行业CIRT确保关键基础设施得到保护的示例。[87]

作为巴西近期加强国家网络安全的另一项举措，联邦网络事件响应框架ReGIC加强了联邦政府机构之间在关键基础设施保护方面的协调。

ReGIC为联邦机构设定了任务和期望。根据ReGIC，联邦机构必须参与该网络，其中包括在活动事件期间共享威胁情报、发布网络攻击警报以及在事件发生时进行协调等。ReGIC的另一个具体作用是行业协调，要求巴西国家电信管理局（Anatel）等监管机构建立行业网络安全事件响应团队（CSIRT）并提交行业报告。

除了建立国家CERT之外，**坦桑尼亚**[88]还采取了建立针对行业的计算机应急响应团队（CERT）的方式，针对金融和银行机构建立了TZ-Fincert，针对学术机构建立了学术CERT，针对政府部委、部门、机构和主管部门建立了eGSoC。这些进展提升了应对威胁响应的有效性，加强了保护，还改善了整体事件响应能力，并进一步提升了在特定行业相关事务中的协调水平。

CIRT在防范网络威胁、保护关键基础设施方面发挥着不可替代的作用。通过协调事件管理、共享威胁情报、开展漏洞评估和提供针对性的指导，CIRT增强了关键系统的网络复原力，确保快速恢复并降低网络攻击的影响。本章中提到的示例突出了针对特定部门的响应、公共和私营实体之间协作的重要性，以及持续提升复原力以保护国家基础设施免受复杂网络威胁的必要性。为确保国家CIRT应用良好做法应对网络安全事件，并促进国家CIRT之间的技术合作，**国际电联**在区域层面和区域内组织网络演练[89]。通过网络安全演习，国际电联成员国培养了提高就绪水平、加强保护和事件响应的能力。

3.3 进阶工作：跨境协作确保成功

随着各国CIRT的不断发展完善和网络安全文化的深化，在基础工作之外还有更多促进关键基础设施保护的协调模式和推进步骤。国家一旦建立起完善的CIRT及国内事件处理项目和政策后，必须将目光投向国界之外，通过国际协作来预防、响应和缓解网络事件。在当今互联互通的世界中，网络威胁往往跨越国界，需要协同策略来增强全球网络安全复原力。美国和欧盟都建立了成功的国际合作模式，展现了此等工作的重要性，包括在国内外建立合作关系。

在**美国**，网络安全和基础设施安全局（CISA）实施了“勒索软件事前预警计划”，这是一项前瞻性举措，旨在识别并应对勒索软件威胁，防患于未然。该计划通过早期预警体现了主动防御的网络安全理念，帮助机构避免因勒索软件攻击导致的关键数据丢失、业务中断和财务损失。该计划依靠两大支柱：强有力的合作伙伴关系和系统性收集可采取行动的情报。[90]

---

87 巴西提交的ITU-D SG2 SG2RGQ/183号文件

88 坦桑尼亚提交的ITU-D SG2 2/346号文件

89 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx

90 美国提交的ITU-D SG2 SG2RGQ/164号文件

CISA的联合网络防御协作小组（JCDC）在其中发挥核心作用，负责筛选来自网络安全研究机构、基础设施提供商和威胁情报组织的线索。与私营实体和研究人员的紧密合作进一步确保了高质量情报的及时提交。一旦收到可靠线索，JCDC就会调动其国家和现场人员通知潜在受害机构并提供缓解指导。

该计划的重要特点是通过与外国CIRT的紧密协调实现国际覆盖。当威胁线索涉及美国境外的机构时，JCDC会与国际同行合作，确保及时向受影响实体发出警报。这种CIRT之间的协作关系至关重要，在需要快速行动阻止勒索软件攻击的情况下尤为如此。对于已经遭受勒索软件攻击的机构，JCDC会提供关于威胁行为体战术、技术和程序的深入分析，并协助调查和补救工作。这类援助通常包括识别外泄数据，以及提供减轻攻击长期影响的指导。

欧盟同样将国际协调作为提升网络复原力的重点任务。一个典型的示例是PESCO网络快速响应小组和网络安全互助（CRRT）项目。[91]该计划帮助欧盟成员国快速部署网络安全专家对大规模事件进行响应，特别是针对关键基础设施的事件。通过整合专门知识和资源，欧盟增强了其在国家和区域层面应对网络危机的集体能力。该举措也体现了欧盟对协作网络安全的承诺，因为它确保了成员国能够在紧急情况下相互支持。

除上述举措外，美国和欧盟都强调共享威胁情报、建立互信关系以及制定跨境协调标准化协议的重要性。

随着网络威胁日益复杂化和规模化，跨境协调已成为取得成功的关键要素。上述模式展示了国际合作如何提升事件响应能力、强化全球网络防护。通过优先开展合作并善用国际伙伴的专门知识，各国能更好地应对互连程度日益增强的数字环境带来的挑战。

3.4 协调中心的建立

澳大利亚和俄罗斯联邦都建立了国家协调中心，并在各自模式中获益。对两国政府而言，国家协调中心都是政府全面应对网络事件的重要组成部分。这些协调中心并非CIRT，而是与CIRT协同运作。

在2022年发生Optus和Medibank数据泄露事件后，**澳大利亚**政府在内政部下设立了网络安全响应协调处（CSRCU）。其目的是建立国家重大网络事件的中央协调。[92]**俄罗斯联邦**根据国家法律建立了国家计算机事件响应和协调中心（NCIRCC），旨在加强关键信息基础设施。这些中心职能相似：协调事件响应和关键信息通报。NCIRCC侧重于网络事件的响应措施协调，以及与关键基础设施沟通此类事件的数据收集、存储与分析方式和方法。[93]澳大利亚的CSRCU和俄罗斯的NCIRCC均有权组建工作组、召集相关机构和专家、发布信息和参考资料。

---

91 NRD网络安全提交的ITU-D SG2 2/322号文件
https://www.pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/

92 澳大利亚提交的ITU-D SG2 SG2RGQ/218号文件

93 俄罗斯联邦提交的ITU-D SG2 SG2RGQ/79号文件

第4章 – 实施国家网络安全战略和政策的方式、良好做法以及经验收集

随着全球对数字技术依赖程度的不断加深，制定强有力的国家网络安全战略和政策显得尤为重要。网络威胁正在快速演变，发达国家和发展中国家同样面临风险。为保护关键基础设施、数字经济及公民隐私，各国必须采取全面且适应性强的网络安全战略。本章探讨了各国构建具有复原力的网络安全框架的不同路径和良好做法。通过分析不同国家的经验，本章旨在为国家网络安全政策和战略的设计和实施提供路线图。

国家网络安全政策和战略涵盖广泛的做法，每种做法都针对不同国家独特的政治、社会、经济、法律和技术背景量身定制。实施这些政策和战略面临独特的挑战与机遇，深受各国具体国情的影响。本节深入探讨了各国的实践经验，重点介绍在威胁不断演变的背景下，加强数字保护和复原力过程中遇到的挑战和取得的成功。

讨论涉及战略协调、利益攸关方参与、能力建设和对不断演变的网络威胁形势的持续适应等关键领域。这一全面探讨不仅旨在阐明在日益复杂的网络领域中有效维护国家利益所涉及的复杂性，更希望为政策制定者和网络安全专业人士提供战略见解，以指导其完善自身战略。

4.1 战略和领导的统一及政策框架

国家网络安全战略的成功实施关键在于与数字化转型、国家安全和经济政策保持整体统一。这种统一确保网络安全举措不仅能支持国家总体目标与治理框架，更能与之深度融合。以因数字社会建设领先而受到广泛认可的**爱沙尼亚共和国**为例，该国将网络安全战略与电子政务和数字经济目标有机统一，构建起支撑公私部门举措的具有复原力的数字基础设施。[94]爱沙尼亚通过定期更新网络安全战略实现这种统一，确保战略始终与技术和地缘环境的变化保持同步。

此外，有效的网络安全政策和战略还需与国家整体政策和经济目标保持一致。这种统一既确保网络安全措施能应对当前威胁，还能支持国家的长期利益，营造有利于增长和创新的安全且具有复原力的数字环境。此类战略统一对提升网络安全措施效能和支持更广泛的国家目标至关重要，既能增强国家预防、处置和应对网络事件的能力，又能促进国内网络安全行业的发展。

东帝汶民主共和国[95]的案例有力证明了在数字化转型政策、战略、规划和路线图中突出网络安全的重要性。东帝汶认识到，数字化转型必须同步管控网络安全风险，防范网络攻击和数据泄露。从这个意义上说，最不发达国家（LDC）需要将网络安全作为基本支柱放在首位，反映出对网络安全在国家发展和数字化转型所发挥关键作用的理解。

---

94 https://www.weforum.org/stories/2020/07/estonia-advanced-digital-society-here-s-how-that-helped-it-during-covid-19/

95 东帝汶提交的ITU-D SG2 2/120号文件

作为更广泛的政府网络安全社区的重要组成部分，确保国家网络协调机构内部领导力的强效统一对于促进网络安全同样至关重要。指定协调员可以促进和推动政府的整体响应工作。**澳大利亚**模式即包含国家网络安全协调员一职，主要负责领导国家网络事件处置工作。该协调员职位设立于2023年2月，指定协调员直接向网络安全部长汇报。[96]**俄罗斯联邦**总统于2022年5月颁布法令，严格规定信息安全负责人的任职标准，强调需具备相关专业教育背景和经验等资质要求。该国还鼓励对缺乏信息安全专门背景的个人进行职业再培训。[97]

4.2 法律框架和治理

中非共和国[98]和**刚果民主共和国**[99]的实践表明，针对性强的立法行动与治理框架能显著提升网络安全能力。在中非民主共和国，政府通过启动法律改革并设立专门网络安全机构来推行政策，展现出为强化数字防御所采取的主动方法。同样的，刚果民主共和国采用基于国际良好实践的综合章程，涵盖政策立法、多层级协作和广泛的公众宣传活动。这些措施对于各国，特别是发展中区域尤其重要，可帮助其应对日益猖獗的网络安全威胁。

阿尔巴尼亚共和国[100]近期实施的全面网络安全改革为此增添了新维度。国家CSIRT的建立和网络安全主管部门的重组，体现了该国推动网络安全框架与国际规范和良好做法对标的承诺。这些战略举措通过确保协同网络事件响应、优化网络安全治理，旨在强化国家网络安全基础设施。此外，阿尔巴尼亚的法律改革还着力更新完善现有立法框架，确保其能应对当前网络安全的挑战和威胁。阿尔巴尼亚网络安全战略中法律、制度和运行要素的协调统一，为其他国家通过整体性治理改革强化网络安全防御树立了典范。

作为其到2025年建立数字信任的政策目标的一部分，**科特迪瓦**也在进行一系列立法更新。[101]值得注意的举措包括完善法律体系以建设可信的信息社会，并与西非国家经济共同体区域标准、《非洲联盟网络安全和个人数据保护公约》等对标。科特迪瓦电信/ICT管理局（ARTCI）发挥核心作用，重点聚焦数字信任与网络安全、个人数据保护及电子交易管理。数字信任咨询委员会和个人数据保护咨询委员会等咨询委员会的成立，彰显了该国构建安全网络环境的坚定承诺。这些结构化工作旨在打造可信数字空间，既增强了数字基础设施的安全性，又提升了公众对数字经济的信心。

这些示例揭示了网络安全战略与国家治理框架统一的重要性 – 不仅能提升战略有效性，更能确保其在面对不断变化的网络威胁时的可持续性和适应性。

96 澳大利亚提交的ITU-D SG2 SG2RGQ/218号文件
97 俄罗斯联邦提交的ITU-D SG2 SG2RGQ/79号文件
98 中非共和国提交的ITU-D SG2 2/141号文件
99 刚果民主共和国提交的ITU-D SG2 2/115号文件
100 阿尔巴尼亚提交的ITU-D SG2 2/309号文件
101 科特迪瓦提交的ITU-D SG2 SG2RGQ/29号文件

4.3 国际协作和支持

国际组织在支持各国网络安全建设方面发挥着关键作用，**世界银行**的多项举措就是明证。[102]世界银行为其客户国（特别是最不发达国家）提供资金和技术支持，帮助后者夯实数字基础并加速各领域的数字化应用。这类支持对这些国家至关重要，使其网络安全政策与战略能与全球发展动态保持一致，在应对当前及新兴网络威胁过程中保持复原力。

世界银行的工作彰显了全球伙伴关系和专门知识共享对增强国家网络安全框架的重大意义。通过促进前沿技术和良好做法的整合，世界银行不仅帮助各国抵御网络威胁，更推动其借助数字化转型实现经济社会发展。

在**海地共和国**，[103]与世界银行和美洲开发银行等国际伙伴的合作提供了关键的资金和技术支持。这些支持对建设强健的数字基础设施、强化全国网络安全措施具有重要意义。

一项重要举措是由海地国家电信委员会（CONATEL）和海地统计和信息学研究所（IHSI）组成的联合工作组。这一联合工作组负责制定协调统一的国家网络安全战略，重点保护关键基础设施和打击网络犯罪。CONATEL通过监管职能确保安全协议落实，而IHSI则负责管理网络安全威胁与风险，全面提升海地数字系统的安全水平。

这些工作得到“海地数字加速项目”等国际项目的支持，该项目旨在改善宽带连接并构建数字复原力。这种综合举措不仅可以保护海地抵御新兴网络威胁，还可以支持其在数字时代实现社会经济增长。为进一步加强建设，海地还与全球网络安全能力中心和世界银行合作开展了全面的网络安全成熟度评估。该评估涉及多个利益攸关方，采用“国家网络安全能力成熟度模型”来确定需要战略投入的关键领域。评估结果为针对性改进工作提供了指导，有力强化了海地网络安全基础设施。

4.4 协作框架和利益攸关方的参与

巴西[104]通过积极包容的利益攸关方参与机制，实施了一系列强化国家网络安全基础设施的战略性措施。巴西的做法特别强调政府部门、私营机构和学术组织之间的协作。通过多项举措和伙伴关系，这种利益攸关多方的参与是通过各种举措和伙伴关系推动的，利用各领域的独特优势和观点提升整体网络安全水平。最新的一项进展是成立了国家网络安全委员会，负责监督《国家网络安全政策》的实施和更新。委员会有25名成员，其中15名成员代表联邦公共行政部门的实体和机构，包括Anatel，10名成员代表其他组织，如巴西互联网指导委员会（CGI.br），民间团体、学术界和网络安全相关的私营部门各有3个席位。

除CIRT之外，**澳大利亚**还采取了更多措施来确保关键基础设施得到保护且具有复原力，这是网络安全发展迈出的一大步。不同于单纯的响应和防护，关键基础设施提升计划（CI-UP）旨在帮助澳大利亚关键基础设施组织提升应对复杂网络攻击的复原力。这

---

102 世界银行提交的ITU-D SG2 2/74号文件

103 海地提交的ITU-D SG2 SG2RGQ/121号文件

104 巴西提交的ITU-D SG2 SG2RGQ/57和SG2RGQ/181号文件

项由政府主导的计划与私营领域关键基础设施运营商协同合作，强化对关键基础设施资产和运行技术环境攻击的防护。CI-UP作为全国性自愿计划，以威胁为导向开展行动。[105]

CI-UP的主要重点是在以下关键领域帮助关键基础设施组织改善网络安全态势：

- 提高可见性和认识：CI-UP帮助实体更好地了解网络事件，并提高对其系统中潜在漏洞的认识。
- 事件遏制和响应：该计划加强了关键基础设施组织有效遏制和响应网络事件的能力。
- 促进网络安全文化：CI-UP进一步鼓励在澳大利亚的关键基础设施领域发展提高网络安全认识的文化。

该计划体现了政府和私营部门之间利益攸关多方协作对安全保障的重要性。CI-UP通过专题报告、讲习班、信息交流及详细缓解指南等多种形式提供服务。该计划还与澳大利亚最重要的关键基础设施实体的工作人员进行现场合作，根据每个组织的特定需求提供专门的深入建议。

广泛吸纳利益攸关方参与对于有效实施国家网络安全政策与战略至关重要。这种参与包括政府机构、私营部门实体、学术界和民间团体，各方都能提供独特的视角、需求、优先事项和专门知识。通过协作共建、审议完善国家政策，可确保所实施战略切实可行，并真实反映各领域的需求与实际状况。

4.5 基础设施发展促进网络安全

刚果民主共和国[106]已着手实施一项全面革新数字基础设施的宏伟计划。推动这一举措的原因是该国认识到，强大、安全的数字系统是有效网络安全的支柱，对国家发展至关重要。该国政府已将关键网络基础设施的升级作为优先事项，不仅能抵御日益增多的网络威胁，还能支持经济不断增长带来的数字化需求。刚果民主共和国的战略包括部署先进的网络安全技术，如最先进的防火墙、入侵检测系统和全面的数据加密方法。这些技术对于防止未经授权的访问和保护敏感信息至关重要。此外，刚果民主共和国正着力扩大宽带覆盖，确保网络安全措施能惠及包括偏远落后地区在内的全国范围。

布隆迪共和国[107]正在推进其网络安全基础设施建设，将其作为未来国家网络安全战略的核心组成部分。该国政府认识到ICT对发展的关键作用，致力于服务的数字化转型和数字化。为应对日益严重的网络威胁，布隆迪信息通信技术部成立了一个专门委员会，负责制定综合性国家网络安全战略，包括加强网络安全治理的法律框架、促进网络安全文化、建立技术知识能力、参与区域和国际工作，以及提高各行业对网络安全威胁的认识。该基础设施开发通过数据保护与安全机制的实施，确保了用户与服务提供商间的数据完整与信任。

105 澳大利亚提交的ITU-D SG2 SG2RGQ/214号文件
106 刚果民主共和国提交的ITU-D SG2 SG2RGQ/104号文件
107 布隆迪提交的ITU-D SG2 SG2RGQ/134号文件

4.6 能力建设

实施国家网络安全战略需要必要的能力建设，包括提升网络安全专业人员的技能水平、建设技术基础设施以及建立法律监管框架。持续投入培训和能力建设对维护国家网络安全至关重要。如第1章所述，通过不断提升网络安全专业人员技能和公众教育水平，各国不仅能更有效地管理和相应网络事件，还能通过提高ICT熟练程度来支持经济社会发展的更广泛目标。

4.7 持续适应网络威胁形势

网络威胁形势的动态性要求国家网络安全政策和战略必须具备内在适应性，其他网络安全法律或法规亦需如此。网络安全适应性有三个关键要素：持续监测不断变化的威胁形势（包括新的和新兴技术带来的挑战）、定期评估和政策战略的实施效果，以及及时更新网络安全做法。第2章探讨网络安全保障做法时讨论了具有适应性的网络安全的必要性。

第5章 – 5G网络安全的挑战和途径

5G技术的引入标志着电信业的重大发展，它提供了更快的速度和更好的连接，有可能改善行业，扩展物联网应用，并为数字通信带来新的方法。然而，促成这些进步的复杂架构也带来了复杂的网络安全挑战，需要全面的了解和强有力的保护措施。

随着5G网络在全球部署，建立一个安全的生态系统对于确保信息的完整性、可用性和机密性以及保护已成为数字经济支柱的基础设施至关重要。

本章介绍了关于5G网络安全的复杂性的讨论，旨在分享有关现有做法的信息，并探索应对新出现的威胁的创新解决方案，分享公共电子网络的5G网络安全的思考和良好做法，供国际电联成员国在其国家背景下考虑和实施。

5.1 5G网络安全概述

5G的特点是其先进的软件系统，能够实现更灵活的配置以及用户和设备的大规模连接。5G技术支持增强现实、远程手术和综合互联网服务等低时延应用，这些均依赖于稳健可靠的网络。5G的主要用例之一是物联网，它利用了5G连接大量端点的能力。5G技术即将彻底改变连通性，但这也带来了动态网络安全的新风险和挑战。

与前几代无线技术不同，5G引入了向基于云的架构、软件定义网络（SDN）和网络功能虚拟化（NFV）的重大转变。这一转变创造了一个更加复杂和动态的网络安全格局。

随着5G的日益普及，电信基础设施有望成为恶意网络活动更具吸引力的目标，因此需要采取先进的安全措施来适应不断变化的威胁。5G的网络安全应侧重于提高整个生态系统的复原力，包括基础设施和应用。这包括保护相互连接设备、数据和网络免受网络威胁的影响。

认识到不同的组织使用不同的网络安全定义，[108]应记住本报告中的“5G网络安全”一词是指5G背景下的网络安全，需要对其新参数、标准和技术功能进行适当管理，以保护整个数字生态系统并确保网络复原力。

[108] https://www.enisa.europa.eu/publications/definition-of-cybersecurity

框1：网络安全的定义

在国际电联，电信标准化部门（ITU-T）X.1205建议书将网络安全定义为“用以保护网络环境和机构及用户资产的各种工具、政策、安全理念、安全保障、指导原则、风险管理方式、行动、培训、最佳做法、保证和技术。机构和用户的资产包括相互连接的计算装置、人员、基础设施、应用、服务、电信系统以及在网络环境中全部传送和/或存储的信息。网络安全工作旨在确保防范网络环境中的各种安全风险，实现并维护机构和用户资产的安全特性。网络安全的总体目标包括以下内容：

- 可用性
- 完整性（其中可能包括真实性和不可否认性）
- 机密性。”

5.2 传统网络部署

电信服务提供商最初倾向于在非独立（NSA）基础上部署5G网络，在部署独立（SA）端到端网络之前利用现有的4G基础设施。[109]5G NSA网络继承了4G网络、甚至是2G/3G网络的传统漏洞，需要对其进行相应的管理。对一些运营商而言，这相当于一种“技术债务”：管理老旧系统意味着需要开发一套标准化的安全控制措施来衡量不同世代成熟度的基础设施组件的安全状况。[110]

需要强调的是，与过去几代移动技术相比，5G SA提供了提高网络安全性的机会，因为它被设计为比4G更安全。在用户安全和隐私、无线接入网（RAN）、网络核心和漫游安全等领域都取得了进展。[111],[112]

5.3 5G安全方面的标准活动

5.3.1 活跃在5G网络安全领域的SDO

由于5G技术的复杂性和涉及到的问题，没有一家标准制定组织（SDO）能独自负责5G的网络安全工作。为避免重复工作，已经建立了SDO之间共享信息和协调提案与工作项目的机制。

---

109 当设备需要加大带宽和降低时延（例如，智能汽车之间的通信）时，其将连接到5G频率进行数据传输，或者减少物联网设备的功耗，但仍将依赖4G甚至2G/3G网络进行语音通话和短信发送。来源：https://www.gsma.com/get-involved/gsma-membership/wp-content/uploads/2019/11/5G-Research_A4.pdf

110 https://www.itu.int/md/D22-SG02.RGQ-ADM-0019和https://www.itu.int/md/D22-SG02.RGQ-ADM-0043

111 https://www.cisa.gov/sites/default/files/publications/5G_Security_Evaluation_Process_Investigation_508c.pdf

112 https://www.gsma.com/solutions-and-impact/technologies/security/securing-the-5g-era

为帮助描述这些不同的活动并告知**国际电联**电信标准化部门（ITU-T）中5G相关的安全标准化工作的方向，第17研究组（SG17）编制了一份技术报告，将现有标准和正在制定的标准与SDO及其在5G网络中的应用进行了对照说明。[113]该报告确定了ITU-T、第三代合作伙伴计划（3GPP）、欧洲电信标准协会（ETSI）以及电气和电子工程师学会标准协会（IEEE SA）的标准以及与5G网络安全相关的非标准资源。

该研究组已经根据运营商、供应商、智能手机制造商、内容提供商等起草的文稿发布了11份关于5G安全的建议书。这些建议书重点关注五个领域的安全问题：软件定义网络 – 网络功能虚拟化（SDN-NFV）、网络切片、移动边缘、5G网络管理和5G业务。第17研究组已与其他SDO（如3GPP和互联网工程任务组（IETF））以及从事5G网络安全标准化相关规范制定工作的行业组织建立了联络关系。

GSM协会（GSMA）就是这样一个行业组织。虽然GSMA自身并不是一个标准机构，但它编写规范，召集其成员与SDO合作，使这些规范得到改进和/或被采纳为标准。GSMA发布了一份基线安全控制清单，移动运营商可在部署5G网络时，在自愿基础上加以考虑。[114]

鉴于与5G安全相关的信息来源众多，**欧盟网络安全局**（ENISA）发布了一个统一的5G网络技术安全控制资料库 – 5G安全控制矩阵。[115]该资料库目前作为电子表格发布，但该机构也在开发一个网络工具来提高可用性。

随着网络的日益复杂以及电信与IP网络的融合，越来越难以让某个SDO承担标准化工作的具体领域。这增加了工作重叠和重复的风险，使得标准制定组织之间的沟通和信息共享变得更加重要。

5.3.2 将标准纳入强制性监管要求中

标准有助于确保技术之间的互操作性，并减少创新进入全球市场所需的时间。网络安全标准可定义公认的共同安全基线，反映普世的最佳做法。标准产生于基于共识的过程。它们可以是强制性的，但在绝大多数情况下是可选的，使得供应商和运营商在做部署决定时有更大的灵活性。在某些情况下，如果国家技术法规在其安全要求中包括了特定的标准，那么这些标准可以是强制性的。

国家5G网络安全战略应反映全球良好做法与本地运作现实之间的平衡。一般而言，国家监管要求应借鉴国际公认的标准，使其适应当地环境和本地要求，以便确保5G的部署和网络的安全。

---

113 https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTS-2022-2-PDF-E.pdf

114 https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/fs-31-gsma-baseline-security-controls/

115 https://www.enisa.europa.eu/publications/5g-security-controls-matrix

5.4 用积极主动的网络安全措施补充标准和规范

5.4.1 供应商层面的安全考虑

标准和规范只是5G网络安全的一个组成部分。供应商和运营商如何实施这些标准并对其进行配置，决定了5G网络的安全状况。爱立信对5G安全采取了一种整体方法，涉及四个层面：标准、供应商产品开发、网络部署和网络运营。[116]该公司认为，这种综合方法可以确保缓解措施的实施方式既可顾及各层之间的相互依存关系，又可满足各层的具体需求。

作为5G安全措施的一个具体示例，由**GSMA**和**3GPP**开发的网络设备安全保障方案（NESAS）[117]旨在通过提供可在全球范围内适用的保障方案来提高移动网络设备的安全水平。该保障方案以内部和独立专家审计为基础，即供应商流程评估和产品评估的混合体，并提供认证。该方案的目的是减轻往往在全球范围运营的网络设备提供商的安全测试负担。主要供应商已获得NESAS认证。NESAS也是欧盟5G网络安全认证方案[118]的一个候选者。该方案是欧盟级别的认证，将使欧盟各成员国符合要求。该认证不会取代当前的NESAS方案，而是与之协同存在。鉴于威胁形势在不断变化，以一种既保持灵活性又可快速更新的方式制定方案/认证计划至关重要。

在**英国**，国家网络安全中心（NCSC）建议使用供应商评估框架，[119]该指南帮助运营商评估与使用供应商设备相关的网络风险。

5.4.2 运营商层面的安全考虑

NESAS可以提供一定程度的保证，确保部署前的网络设备是安全的。随着运营商部署和运营其网络，需要纳入其他安全考虑，例如攻击检测和自动响应。此时运营商应考虑利用人工智能（AI）、威胁情报和分析来帮助支持网络安全。5G网络安全提供了实时安全性和零信任策略等优势，可以提高系统可见性。然而，5G网络安全自身面临着一些挑战，例如：以不同的安全级别维护不同网络的连接；使用传统组件和不同的网络类型；以及将人工智能集成到安全措施中的复杂性。根据“最小特权”原则实施严格的访问控制，可确保将网络中的各种权限（如网络功能间的访问权限、网络管理员权限、虚拟化配置）最小化。有很多关于5G具体网络安全策略的文献供运营商考虑。[120]

对真实的电信网络进行测试对于确定电信网络真正的网络风险也至关重要。运营商可利用内部资源或雇用独立的外部承包商，针对自己的网络和系统进行某种形式的安全测试。在**英国**，TBEST是一种基于结果的渗透测试方案，它模拟资源雄厚的网络攻击者可能使用的技术和战术。TBEST评估通信提供商如何能够检测、遏制和应对这种攻击。其总体目标是在提供商的功能、流程、政策、系统或网络中发现并解决安全漏洞或其他弱点，如果不被发现，这些漏洞或弱点可一起危害企业的关键系统。通过实施自愿性TBEST

116 https://www.ericsson.com/en/public-policy-and-government-affairs/cyber-network-security

117 https://www.gsma.com/solutions-and-impact/industry-services/certification-services/network-equipment-security-assurance-scheme-nesas/

118 https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification

119 https://www.ncsc.gov.uk/report/vendor-security-assessment

120 例如见：https://www.5gamericas.org/wp-content/uploads/2020/07/Security-Considerations-for-the-5G-Era-2020-WP-Lossless.pdf和https://www.5gamericas.org/security-for-5g/

计划，通信提供商可以确定其安全方面可以提高的特定领域。监管机构Ofcom也与提供商合作，协助他们及时做出适当的改变。[121]

5G网络安全强有力的商业案例至关重要。虽然运营商需要看到他们在5G业务方面的投资得到回报，但应认识到遵守基线安全措施是必不可少的，并应相应地做出预算。

框2：开放RAN

开放RAN是对无线接入网（RAN）进行分解，并对连接这些分解元素的接口进行标准化，从而能够使用来自不同供应商的部件来构建网络。

一方面，开放RAN可进一步增加电信网络供应链的复杂性。这种架构鼓励RAN中供应商的多样化，需要在整个网络供应链中进一步开展集成工作，这可能会增加攻击向量。另一方面，开放RAN提高了供应链的透明度，提高了运营商的可见性并允许他们监测和检测安全风险。简而言之，开放RAN使运营商们更好地了解网络架构和设备，并可更全面地扫描和管理漏洞。O-RAN联盟（制定开放RAN规范的主要场所）正在为开放RAN架构制定安全规范，并旨在使这些规范在ETSI中实现标准化。

在日本，NTT Docomo因其设备选择的灵活性而成为采用开放RAN架构的运营商之一。这一决定从安全角度提出了质疑，因为通常认为开放性意味着有更多的攻击机会。然而，该运营商已经比较了传统RAN和开放RAN，并得出结论，两者之间的安全差异很小。[1]

[1] 有关开放RAN安全性的更多信息，例如见：https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/09/enhancing-the-security-of-communication-infrastructure_79b78b4d/bb608fe5-en.pdf

5.5 保护5G网络安全的国家政策和法规示例

除了供应商和运营商的标准和做法之外，可在国家层面提出保护5G网络的政策和法规。这可能采取供应商评估、测试、认证、制定导则或要求等各种形式。虽然方法因国情而异，但这些举措都旨在减轻5G带来的安全风险，包括具体针对网络的风险。实施和遵守机制也应被视为总体框架的组成部分。

以下示例提供了不同国家和地区为实现5G网络安全所采取的行动及其当前状态的简要介绍：

– **巴西**对5G网络安全的整体方法侧重于运营商的风险管理。根据5G频谱拍卖的条款和《电信行业网络安全条例》[122]的要求，5G运营商需遵守监管框架，其中包括确保整个行业网络安全的原则、导则和事前控制。这些控制措施结合了网络安全治理、强

[121] 英国提交的ITU-D SG2 SG2RGQ/74号文件

[122] https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740；https://informacoes.anatel.gov.br/legislacao/resolucoes/2024（均为葡萄牙文）。

制性事件通知、信息共享、漏洞评估周期、关键基础设施报告和其他规定。巴西国家电信管理局（Anatel）也与学术界合作，在此方面开展研究。[123]

– **英国**政府通过《2003年通信法》为公共电子通信网络或服务提供商制定了安全框架，该法案后由《2021年电信（安全）法》（TSA）予以修订。该框架适用于5G和所有其他网络：虽然英国正在向5G和全光纤未来全网络过渡，但许多网络提供商将旧技术纳入其基础设施。TSA规定了所有公共电信提供商[124]的新安全义务，并赋予了国务大臣制定法规和发布行为守则的新权力。这些守则已得到制定，并通过公众咨询进行了通报。[125]TSA还包括加强Ofcom监管权力的条款，以监督和强制提供商履行其新职责。

– **大韩民国**的5G网络安全法规和政策被公认为是全球最严格的法规和政策之一，反映了该国在采用5G技术方面的领先地位。韩国政府通过科学和信息通信技术部（MSIT）和韩国互联网与安全局（KISA）实施了保护5G网络的综合框架。该框架包括对电信运营商实施严格的网络安全要求，以确保网络基础设施的安全、保护用户数据并降低网络安全风险。这些法规强调需要安全的供应链、先进的加密标准以及在网络架构中部署安全设计原则。此外，韩国还与国际合作伙伴和标准组织合作，以确保其5G安全措施符合全球良好做法。

– **印度**为加强5G网络安全而建立的法律和技术框架包括：

  - 关于电信行业的国家安全指令，确保解决电信供应链和来源中的问题和漏洞；
  - 电信设备的强制性测试和认证，确保符合每个5G网络功能的基本安全要求；和
  - 电信服务提供商的许可条件，包括对电信基础设施安全的定期公共审计。

  为支持上述目标，印度建立了各种体制机制：成立了国家通信安全中心（NCCS），负责制定电信安全要求/标准（印度电信安全保证要求（ITSAR））及其相关的安全测试和认证实验室；为国家电信部门成立了电信CSIRT；以及，制定多项以公民为中心的欺诈管理和消费者保护措施等。关于安全协议和3GPP等标准，印度审议了行业标准提出的合规性监测和进一步的电信许可条件（包括对服务提供商网络的定期安全审计）的规范。

– 在**阿拉伯联合酋长国**，通过多管齐下的战略确保5G网络安全，其中包括严格的国家网络演习和培训、建立国家安全运营中心（SOC）以实时了解和应对威胁，以及网络脉冲举措，以提高关键防御战略方面的认识并培训人员。该国强调与国际合作伙伴、供应商、学术界和其他利益攸关方的合作和信息共享，以加强网络安全措施。此外，该国建立了符合国际标准（如ISO和NIST发布的标准）的具有复原力的网络安全框架，以确保整个电信部门的合规性。为了树立消费者和企业对5G安全的信心，该国制定了治理政策、程序和法律，以促进供应商之间的安全设计原则和负责任的安全实践。最后，该国采取了以人为本的网络安全方针，侧重于培训、提高认识和

123 部分结果见：https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica/estudos-e-pesquisas（葡萄牙文）。

124 微实体除外。

125 https://www.legislation.gov.uk/uksi/2022/933/contents/made；https://assets.publishing.service.gov.uk/media/6384d09ed3bf7f7eba1f286c/E02781980_Telecommunications_Security_CoP_Accessible.pdf

支持，以增强个人和组织对抗网络威胁的能力，从而巩固对5G网络潜在威胁的强大防御。

– **津巴布韦**正在解决5G网络安全问题，重点关注边缘计算日益增长的重要性，并探索采用开放RAN技术以提高供应商的灵活性。虽然津巴布韦没有制定具体的5G安全法，但现有的数据保护立法和正在制定的AI治理文件支撑着该国的做法。津巴布韦将使其安全做法与ISO/IEC 27001和NIST标准等国际标准保持一致，确保新的5G无线接口符合既定的安全协议。津巴布韦邮电管理局负责执行安全准则，并提高业界对维护国家电信基础设施完整性的认识。

– **肯尼亚**于2022年4月通过了其5G移动通信路线图和战略。该战略认识到安全是5G网络架构的一个重要方面。互联服务不断发展的性质以及预期互联设备数量和类型的显著增加提高了数据隐私、数据保护和网络安全对肯尼亚的重要性；其中包括检测威胁、用户认证和优秀实践做法。5G通过设计提供更好的安全性，在网络演进和根据早期技术已取得经验加以调整的基础上纳入了更高的安全要求。肯尼亚通信管理局通过了国际电联和3GPP制定的已批准国际标准，以确保移动系统的互操作性和安全性。管理局计划利用各利益攸关方的专业知识和网络安全方面的国际良好做法来制定技术规范并实施标准化的最低安全评估清单，以确保5G网络符合最新的技术标准，并符合与5G安全相关的全球规范。

– 在对5G网络的网络安全风险进行广泛审查后，**欧盟**开发了“风险缓解措施工具箱”，[126]旨在确定一套缓解主要5G网络安全风险的通用措施，并协助确定欧盟和国家层面响应计划中相关措施的优先级。《数字十年网络安全战略》强调了保护下一代宽带移动网络的重要性，并就5G网络安全的下一步制定了具体附录。[127]《欧盟认证框架》包括正在制定的5G网络安全认证计划。[128]

5.6 实施和合规挑战

政策的制定与注重有效实施同等重要。报告机制、对相关标准的遵守以及切实可行的政策和监管执行措施对于确保强有力的5G网络安全至关重要。新框架对电信网络安全带来的变化将要求电信服务提供商持续合规，因此需要与行业密切接触。在**英国**，Ofcom在其电信安全政策下采用了一种监督模式，并与电信提供商的监管和技术团队合作。监管机构认为，实施不仅涉及技术措施，还需要从文化上转变电信提供商对网络安全的思维方式，要求他们确定其外包的部分网络和服务并对其负责。与高层接触并获得政府、监管机构和业界高层的承诺和支持是取得成功的先决条件。[129]

在**马来西亚**，政府批准了一项新的网络安全法案，该法案规定将由单一机构管理所有关键基础设施。包括5G网络在内的电信网络在这项新的网络安全法案的规定范围之内。监管机构[130]正在制定一套让运营商报告安全合规情况的要求。[131]该国一家运营商强调，作为第3/2号课题关于5G网络安全中期交付成果的一部分，新政策的实施可能具有挑

126 https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures
127 https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
128 https://certification.enisa.europa.eu/index_en
129 英国提交的ITU-D SG2 SG2RGQ/191号文件
130 https://www.nacsa.gov.my/act854.php
131 https://www.itu.int/hub/publication/d-stg-sg02.03.2-2024/#/zh

战性，因为它涉及传达风险和阐明最低安全要求，这需要时间、成本和开展大量工作，通常还涉及股东方的考虑。对于有股东的运营商而言，安全方面的结构、政策和法规有时并不一致，这可能给安全团队带来挑战。因此，在考虑新的安全框架时，有必要让所有团队，包括高管参与。

5.7 优先投资于教育和培训劳动力队伍的必要性

根据Allied Market Research的数据，[132]到2031年，全球5G安全市场预计将达到378亿美元，对网络安全专业人员的需求也将大幅飙升，尤其是那些拥有保护5G网络专业技能的专业人员。各国、组织和机构应优先考虑劳动力培训和招聘，确保5G网络安全的推进。目前，劳动力队伍中很难找到所需的专业技能；此外，实现招聘的性别平衡也是一项挑战。如果劳动力队伍未做好准备，将会减缓向5G的过渡步伐并使其复杂化。虽然各国应通过国家计划优先考虑培训和教育，但私营部门也可以探索培训和技能提升计划，因为需要更广泛行业的参与才能确保需求得到满足。

土耳其是正在寻找应对劳动力挑战解决方案的国家的一个例子，该国加大了对教育和培训劳动力的投资，使之能够应对5G安全的复杂性。作为这一承诺的一部分，土耳其信息通信技术管理局、中东技术大学、İhsan Doğramacı Bilkent大学、Hacettepe大学和电信运营商土耳其电信（Türk Telekomünikasyon A.Ş.）、Turkcell İletişim Hizmetleri A.Ş.和沃达丰电信（Vodafone Telekomünikasyon A.Ş.）等主要机构建立了一个5G谷开放测试场。该测试场作为5G及之后技术的研究、开发和测试的重要平台，为学术界和业界提供了合作的机会。由上述机构代表组成的5G谷执行委员会确保了该举措的有效实施。通过为学者、研究人员、博士生和初创企业提供一个可以参与5G及之后相关工作的平台，5G谷开放测试场不仅促进了创新，而且有助于培养高技能的劳动力。这一举措是土耳其战略不可或缺的组成部分，旨在通过持续投资于教育、培训和研究来优先考虑和增强5G网络的安全性。[133]

5.8 超越5G：设定6G网络安全的方向

尽管在许多国家和地区，5G仍处于规划和部署阶段，但研发和标准化进程的注意力已开始转向5G之后的网络。因此，到2023年底，**国际电联**无线电通信部门（ITU-R）批准了2030年及之后IMT的未来发展的框架和总体目标，[134]即商业上所说的6G。

---

132 https://www.alliedmarketresearch.com/5g-security-market-A12820

133 https://5gtrforum.org.tr/en

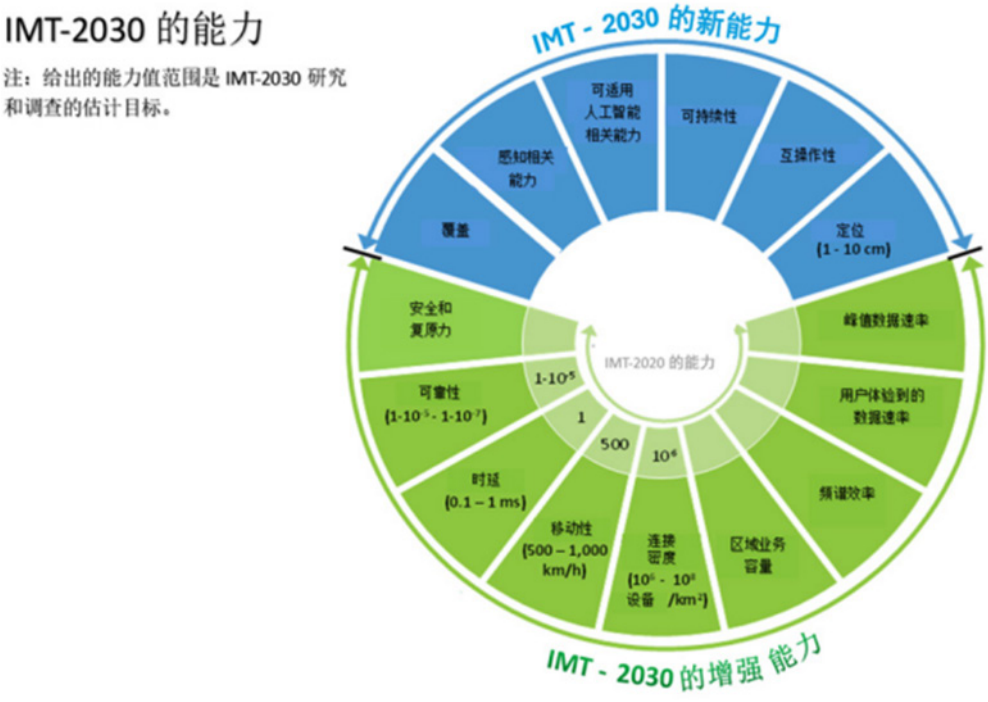
134 ITU-R M.2160建议书，见https://www.itu.int/rec/R-REC-M.2160-0-202311-I/en

框3：IMT-2030

该框架强调，IMT-2030有望成为实现增强的安全性和复原力的重要推动因素。预计设备在设计上是安全的，并有能力在破坏性事件（无论是自然事件还是人为事件）期间继续运行并从中迅速恢复。该文件还重申，IMT-2030系统的安全性和复原力是实现更广泛社会和经济目标的基础。

在IMT-2030的背景下，该框架将安全定义为“保护信息（如用户数据和信号）的机密性、完整性和可用性，保护网络、设备和系统免受黑客攻击、分布式拒绝服务、中间人攻击等网络攻击”。复原力定义为“网络和系统在自然或人为干扰（如主电源丢失等）期间和之后继续正常运行的能力”。

图2：IMT-2030的能力



来源：国际电联

很明显，人们正在设想6G，并开始其标准化过程，对安全性和复原力有着强烈的关注，这与5G技术的早期设计阶段（包括从标准化的角度来看）不同。与2015年批准的IMT-2020（商业上称为5G）愿景[135]相比，这令人信服地说明了思维的转变，同时亦认识到需要适当解决网络安全和网络复原力问题，将其作为数字化转型和数字经济的有利支柱。

[135] ITU-R M.2083建议书，见https://www.itu.int/rec/R-REC-M.2083-0-201509-I

第6章 – 处理短信钓鱼的挑战和方式

短消息业务（SMS）一直被恶意行为者用作攻击媒介。全球范围内，利用短信进行垃圾信息[136]推送和短信诈骗的行为显著增加。后者通过欺骗手段诱导用户提供个人数据（包括财务数据），并在用户的设备中下载恶意软件。短信诈骗不仅会降低用户对电信短信服务的信任度和满意度，还会造成网络资源浪费。

美国联邦贸易委员会的数据显示，2022年短信诈骗造成的损失达3.3亿美元，较2021年增长逾一倍。[137]同期，澳大利亚国家反诈骗中心的Scamwatch平台收到近8万起短信诈骗举报案件，涉及金额超过2 800万澳元。[138]

尽管各国短信服务使用情况存在差异，且电信/ICT领域的创新催生了包括全球普及的移动通讯应用在内的新型通信方式，但由于短信服务操作简便且适用于所有移动电话，其仍具有重要价值。

在此背景下，本章介绍了最常见的短信安全事件类型“短信钓鱼”、关于打击短信钓鱼的标准建议，以及各国应对此类挑战的经验与做法。[139]

6.1 短信钓鱼

“网络钓鱼”（phishing）是指通过电子邮件、短信、语音电话或社交媒体消息等看似合法的通信方式实施欺骗的行为。攻击者通常伪装成银行、政府机构、雇主或家庭成员等可信的个人或实体。用户通常被引导访问某个网站，输入个人详细信息，导致身份盗用，或被诱导提供个人信息（如银行账户或信用卡资料）或向诈骗账户转账。

在网络安全领域，短信钓鱼（smishing）是最猖獗的诈骗手段之一，该术语由“phishing”和“SMS”组合而成，特指通过手机短信实施的钓鱼攻击。根据ITU-T X.1242建议书增补29，[140]短信钓鱼是“诱骗用户在手机等移动设备下载木马、病毒或其他恶意软件的攻击”；网络钓鱼是“在电子通信中伪装成一个可信的实体，恶意获取用户名、密码和信用卡信息等敏感数据的攻击”。

近年来短信钓鱼攻击的威胁持续升级，人工智能（AI）工具的使用更助长其蔓延态势，反映出这类新型网络攻击的规模化和高复杂度的特征。2022年，超过半数的个人移动设备和四分之一企业移动设备每季度都会遭遇至少一次网络钓鱼攻击，作为非邮件类钓鱼攻击一类的短信钓鱼在2022年第二季度激增逾七倍。[141]

---

136 垃圾信息的定义是“通过终端如计算机、移动电话、电话等由发送方向接收方发送的电子信息，该信息对接收方来说通常是未经请求、不需要和有害的。”见ITU-T X.1242建议书 – https://www.itu.int/rec/T-REC-X.1242-200902-I

137 https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/06/iykyk-top-text-scams-2022

138 https://www.scamwatch.gov.au/research-and-resources/scam-statistics

139 该议题与广泛的电信业务和在线反欺诈活动有重要的交集。第6/1号课题（消费者信息、保护和权利）的最后报告有包含关于网络诈骗的专项内容。

140 https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13409

141 https://www.lookout.com/documents/reports/Global-State-of-Mobile-Phishing-Report.pdf

通信服务用户往往难以识别此类攻击。恶意行为者利用社会工程技术，向移动设备发送虚假信息，诱骗收件人点击短信中的URL链接。网络罪犯可能使用网址缩短业务来隐藏虚假登录链接，增加辨别信息真伪的难度。诈骗短信通常具有以下特征：内容与收件人无关；常营造紧迫感；来自陌生号码；存在拼写和语法错误；包含可疑链接。

用户需提高风险意识，并了解可采取哪些措施以避免成为短信钓鱼攻击的受害者。服务提供商和公共部门也肩负重要责任 – 既要与电信行业协作，确保标准及良好做法的落实，也要加强关于短信钓鱼的公众宣传教育。

6.2 打击短信钓鱼的举措

6.2.1 各国打击短信钓鱼的举措

研究周期内，国际电联成员国重点推进制定法规、提高认识、私营部门协作和国际合作以打击短信钓鱼。尽管为应对短信钓鱼带来的挑战已付出了诸多努力，但显然不存在放之四海皆准的解决方案，需要采取多管齐下策略，包括将此类攻击列为刑事犯罪。

俄罗斯联邦采取了后一种做法，[142]将电话诈骗（含短信钓鱼诈骗）定性为刑事犯罪，根据《俄罗斯联邦刑法典》第159条予以惩处。此外，俄罗斯联邦的主管部门自2024年9月起实施虚拟移动号码租用禁令。租用虚拟移动号码被认为是一种安全威胁，因为恶意行为者会使用临时号码在社交网络中注册账户，并使用消息应用程序来传播威胁。俄罗斯联邦的主管部门采取的另一项措施是推出反欺诈平台，提供电话呼叫验证。通过该平台，联网电信服务提供商在信息到达接收方之前验证号码并核实其真实性，拦截可疑呼叫或短信。所有获准提供语音通信服务的电信服务运营商必须接入该系统且免费使用，违者将面临60万至100万卢布的罚款。除这些举措外，还辅之以增强用户能力的宣传活动。

澳大利亚政府采取涵盖行业举措、政府行动与提高认识活动的综合方针。澳大利亚通信和媒体管理局（ACMA）近年将打击短信诈骗列为合规重点，并出台系列新规。这些规定包括：要求电信提供商识别、追踪和拦截诈骗电话和诈骗短信；移动号码在提供商之间转网时，必须加强身份验证程序；对高风险交易（包括SIM卡更换和账户变更要求等）加强身份验证程序。管理局对发送大量短信的电信服务提供商进行审计，这些执法行动表明，恶意行为者利用违规操作形成的漏洞来向澳大利亚国民实施重大短信诈骗。[143]

ACMA还开展了以下打击电信诈骗的执法行动：发布关于政府机构仿冒和远程接入诈骗的消费者警示；与电信服务提供商、政府机构和知名品牌合作，暗中阻断电话诈骗；与其他国家及国际监管机构合作，加强全球范围内打击诈骗、未经请求的电话营销和垃圾信息的战略协作。

此外，澳大利亚政府于2023年开始分阶段推出专项反诈措施，包括设立国家反诈骗中心（NASC）、开发可下架投资诈骗网页的网页，以及实施短信发送者ID注册制度。

---

142 俄罗斯联邦提交的ITU-D SG2 2/158号文件

143 澳大利亚提交的ITU-D SG2 2/154号文件

多方协作机制是许多国家的一致做法，也是**大韩民国**实施相关举措的基石。该国建立了短信钓鱼威胁情报共享机制，支持快速识别和减缓新型攻击载体，并开发自动举报系统供用户使用，相关数据与电信服务提供商共享用于拦截。

AI工具也可助力打击短信钓鱼。例如，韩国科学和信息通信技术部（MSIT）与韩国互联网与安全局（KISA）联合实施了一系列旨在解决特定短信钓鱼问题的项目，包括：

- 通过分析短信模式的AI检测过滤系统实时监控拦截短信钓鱼信息；
- 标记可被拦截的可疑信息，检测短信内容中的恶意链接；
- 建立由电信服务提供商维护并与其共享的恶意号码数据库；
- 采用AI过滤系统；以及
- 搭建国家举报热线（118）和KISA运营的在线举报网站。[144]

这些活动体现了解决若干方面现象的重要性，以及电信服务提供商参与进来的必要性；运用新的和新兴技术协助分析、过滤和屏蔽；实施必要的程序和流程；开发和维护举报系统；充分利用举报数据；以及持续提高民众认识。提高用户认识的重要性不容小觑。随着恶意行为者不断变化、完善，甚至不断涌现新手段，具备充分认知和防范能力的用户更能避免受害。

6.2.2 业界打击短信钓鱼的举措

电信行业已采取积极措施打击一般性诈骗和短信钓鱼活动并减小其影响。在技术方法方面，提供商引入了举报机制、短信防火墙、封禁已知钓鱼网站URL和短信发件人ID保护注册机制等措施。短信防火墙可拦截大量垃圾信息，短信发送者ID注册系统则允许组织注册并保护其客户短信的信息标题，从而限制短信钓鱼和伪装攻击的影响。多个移动运营商协调开展诈骗举报行动是识别和消除诈骗的有效方式。**英国**和**加拿大**开通了7726举报服务，方便用户上报可疑信息以供调查。[145]2014年，英国四家主要移动运营商与英国信息专员办公室合作，自发提供7726举报服务，人们可将可疑短信和垃圾信息免费转发至7726。截至2025年3月，2.6万个诈骗号码已被删除。[146]

授权推送支付（APP）诈骗是导致消费者遭受重大财务损失的另一大问题，因为犯罪分子通过短信或电话联系受害者，冒充银行等合法机构实施作案，然后提取转账。为此，**GSMA**和**英国金融业**联合英国移动运营商和银行推出“诈骗信号”（Scam Signal）方案，利用应用程序可编程接口（API）帮助银行更有效识别和拦截欺诈交易。[147]

144 大韩民国提交的ITU-D SG2 2/312号文件

145 https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/7726-reporting-scam-texts-and-calls/；https://www.getcybersafe.gc.ca/en/blogs/reporting-spam-text-messages-7726

146 英国提交的ITU-D SG2 2/393号文件

147 https://www.gsma.com/newsroom/press-release/mobile-and-banking-industries-join-forces-to-fight-fraud/

在移动货币服务十分普及的撒哈拉以南非洲地区，提升这些平台的安全性是重中之重。**肯尼亚**M-Pesa及其他国家的类似服务已集成生物识别认证、改进的加密技术和高级反欺诈系统，防范假冒和钓鱼攻击。[148]全球范围内，运营商正广泛部署“号码验证”（Number Verify）等API接口，通过验证用户设备是否绑定预注册/配对手机号来替代传统的一次性口令（OTP）和密码验证。“了解您的客户”（KYC）流程也日益普及，通过核实用户联系信息来提供更安全的注册服务（包括移动货币业务），有效防范身份盗用。

澳大利亚最大的电信运营商**澳大利亚电信**（Telstra）部署了短信诈骗过滤系统，扫描信息内容，识别可疑模式和特征，识别并拦截含恶意链接或电话号码的短信。[149]电信提供商还与银行业协作打击电话诈骗。例如，澳大利亚第二大电信提供商**Optus**与澳大利亚金融犯罪交易所（Australian Financial Crimes Exchange）和包括主要银行在内的银行成员联合发起了“呼叫拦截”举措。[150]针对回拨诈骗，该计划可防止Optus用户拨打已标记的诈骗号码，系统将自动转接至风险提示语音，而非接通诈骗方。银行与电信运营商还通过宣传教育普及防范知识，形成打击短信钓鱼和电信欺诈的合力。

GSMA通过反欺诈安全小组（FASG）[151]以及电信信息共享和分析中心（T-ISAC）促进协作和情报共享。[152]两者都是有助于促进全球范围内实时信息共享的安全平台。

有效打击短信钓鱼和电信诈骗需要所有利益攸关方的紧密合作。单靠政府无法根除诈骗活动。继ACMA于2020年12月注册并实施诈骗电话识别拦截规则，并于2022年7月扩展至诈骗短信以来，电信提供商报告称，截至2023年6月底，已阻止了超过14亿次诈骗电话和超过2.57亿条诈骗短信。[153]

此外，应考虑开展有关举报诈骗的公众宣传活动，以增加举报数量。在**英国**，国家网络安全中心和一些地方警察部队等组织宣传了7726举报服务，通信监管机构Ofcom通过步骤介绍视频提供了简单的指引，解释了在大部分主要型号的智能手机上向7726举报短信和电话的方法。最近，英国市场上绝大多数智能手机都配有垃圾信息举报按钮，大幅增加了欺诈消息的举报率。这一新功能与7726服务有相同的举报作用，通过共享的第三方数据库与移动运营商分享信息。这一变化导致举报数量在一年内增加了约800%。[154]

由于迄今为止采取的措施产生了积极结果，应考虑采用涵盖政府机构、银行和电信运营商以及用户等不同利益攸关方的整体方法。

---

148 https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/social-engineering-and-impersonation-fraud/; https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2024/05/Mobile-Money-Fraud-Typologies-and-Mitigation-Strategies-20.05.24.pdf

149 澳大利亚提交的ITU-D SG2 2/154号文件

150 同上

151 https://www.gsma.com/get-involved/working-groups/fraud-security-group/

152 https://www.gsma.com/solutions-and-impact/technologies/security/t-isac/

153 澳大利亚提交的ITU-D SG2 2/154号文件

154 英国提交的ITU-D SG2 2/393号文件

结论

电信/ICT的应用对推动全球发展和社会经济增长具有不可估量的价值。在当前电信/ICT应用持续扩大的背景下，确保信息通信网络的安全并形成网络安全文化至关重要。在本研究期内，第3/2号课题审议了网络安全的多个维度，审议了国际电联成员的文稿，并举办了两次讲习班，为该报告及其结论提供了依据。

第1章表明，提高网络安全认识举措既包含面向不同群体的综合性计划，也有针对网络安全卫生和提高诈骗认识等主题的具体干预措施。同样，各成员国的网络安全教育与培训政策成熟度各异。一些国家已经实施了旨在缓解网络安全专业人才短缺问题的成熟战略，另一些国家则选择针对特定从业群体的专项培训方案。成员国均高度重视保护上网儿童举措，实施健全的法律框架并开发务实的工具和计划，为儿童构建更安全的网络环境。

第2章探讨了各类网络安全保障做法，这些做法已成为保护网络、系统和数据免受恶意活动影响的关键因素。虽然它们不能直接防止网络攻击，但若实施得当，可显著将此类攻击的风险降至最低。尽管没有特别推荐的方案，但举措样本显示，全球范围内正朝着采用这些做法的方向发生可持续转变。各国主管部门通常采取不同和混合的方法，各国当局通常采取多种不同的方法，这些方法包括自我评估、自愿导则、标签方案以及严格的合规性检查。

第3章强调了CIRT如何在提升国家网络复原力方面发挥重要作用。指出发展中国家应进一步优先建立和运作CIRT。国际电联可为旨在提升关键基础设施复原力而提高CIRT能力的国家提供CIRT成熟度评估与发展支持。

第4章讨论了国家路线图中可指导强化国家网络安全框架的方法和经验。强调在威胁态势持续演变的背景下，全面规划、利益攸关方包容性参与和主动适应性等基本原则仍是成功实施网络安全战略的核心。展望未来，正是这些原则将继续塑造互联世界中保障国家利益所需的具有复原力的网络安全防御体系。

第5章侧重于保护5G网络安全的措施。各标准制定组织和行业团体已制定相关标准和规范，其实施需要供应商和运营商采取主动的网络安全措施，并辅以国家政策法规的支撑。根据各国实际情况，这些措施可采取多种形式，包括供应商评估、测试、认证，以及制定相关导则或要求。

最后，第6章讨论了打击电信诈骗（特别是短信钓鱼）的努力，并强调了公共和私营部门建立强有力的合作伙伴关系的必要性。本章重点介绍了政府和行业应对短信钓鱼风险问题的成功示例。随着此类攻击手段日益复杂且难以识别，提高用户认识和教育也显得尤为关键。

关于第3/2号课题的未来发展方向，只要全球网络安全形势持续演变，共享网络安全信息和方法的必要性就始终存在。在下一个研究期保留这一课题具有重要价值，但需重新审视其职责范围，使其更加聚焦于反映ITU-D研究组职责范围和目标受众的具体网络安全问题。

Annexes

Annex 1: List of contributions and liaison statements received on Question 3/2

Contributions for Question 3/2

Web	Received	Source	Title
2/408	2025-04-29	RIFEN	Securing contractualization and deed production during the real estate sales process via blockchain technology and machine learning: practices and use cases
Describes the integration of blockchain technology and machine learning solutions for securing real estate transactions. Together, these technologies strengthen stakeholder confidence, while improving the efficiency of real estate transactions. This contribution takes into account existing work and provides an overview of the system we have implemented in Cameroon for the sale of real estate.			
2/405	2025-04-28	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
This contribution provides an update on the activities currently being undertaken by BDT to enhance cybersecurity in ITU Member States. It also highlights future actions envisaged and new initiatives being formulated.			
2/393	2025-04-23	United Kingdom	Scam reporting within the UK
Summarises how the largest mobile operators in the United Kingdom voluntarily provide the 7726 reporting service, as a way of identifying, removing, and preventing scams calls and messages.			
2/392	2025-04-2025	RIFEN	Developing countries: strengthening cybersecurity
Describes how developing countries face multiple and complex cybersecurity challenges, but with limited means to address the question of how they can ensure that disparities in technical capabilities and funding do not hamper their efforts to enhance cybersecurity.			
2/370	2025-04-14	China	Jointly building cybersecurity: typical practices of safeguarding cyberspace security
Provides an overview of the laws and regulations enacted by China to safeguard cyberspace security, the national campaigns launched to raise people's awareness of cybersecurity, as well as the international initiatives proposed by China on cybersecurity, with the aim of providing reference practices and paths for the world to build secure cyberspaces together.			
2/350	2025-02-27	RIFEN	Artificial intelligence for the detection and reporting of online cyberbullying
Presents the challenge to combat online harassment and the opportunity to integrating artificial intelligence, particularly deep learning techniques, as a promising avenue for improving the protection of sensitive data. The contribution highlights the advantages of designing an intelligent system capable of proactively and automatically identifying threats by combining advanced analysis techniques with proactive cybersecurity strategies.			

(continued)

Web	Received	Source	Title
2/346	2025-02-04	Tanzania	Best practices for coordinating efforts and developing cybersecurity culture
Highlights good practices for coordinating efforts to promote a culture of cybersecurity in Tanzania. It outlines how various legal, technical, organizational, and capacity development measures, along with cooperation, have been vital in enabling Tanzania to achieve a "Tier 1" ranking and be recognized as a "role model" in the Global Cybersecurity Index (GCI) published by the International Telecommunication Union (ITU). It also identifies areas for continuous improvement, especially in technical and capacity development measures.			
2/TD/10 +Ann.1	2024-11-12	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
Reports on the recently conducted CIRT Maturity Assessments in Azerbaijan, Bhutan, Sierra Leone, and Tanzania, the cyberdrills carried out in 2024 to enhance incident response readiness across different regions, the launch of the 5th edition of the Global Cybersecurity Index, BDT assistance in countries and territories in the assessment of their cybersecurity strategies, the Women in Cyber Mentorship Programme and the Her CyberTracks programme, the launch of new online safety tools for children and ongoing capacity building efforts, and other initiatives.			
2/339	2024-11-07	Republic of the Congo	Online communication and transactions via new and emerging telecommunications/ICTs, such as the Internet of Things (IoT)
Outlines challenges in consumer protection with the rise of IoT technology. It highlights issues with data protection, privacy, fair business practices, and device security. Various international responses include legislation, certification, monitoring, and technical standards to safeguard consumer rights and ensure device security.			
2/329	2024-10-29	Egypt	Egypt capacity building centre for African countries (EG-ATRC)
Details Egypt's dedication to enhancing African nations' communication and information technology skills via the Egyptian African Telecom Regulatory Training Centre (EG-ATRC), providing ITU-accredited training and hosting 381 participants from 30+ countries.			
2/322	2024-10-29	NRD Cyber Security	Strengthening cyber resilience: the role of Lithuania's national CIRT in critical infrastructure protection
Presents a case study on Lithuania's National Computer Incident Response Team within the National Cyber Security Centre, highlighting its functions in critical infrastructure protection through monitoring, incident handling, threat analysis, and collaboration efforts, including European Union initiatives.			
2/320	2024-10-29	Australia	Mandating a minimum standard for consumer-grade smart devices
Describes Australia's transition to mandatory smart device security standards from voluntary security standards, prompted by poor guideline adoption. A Bill proposes enforceable Internet of Things standards, requiring compliance statements from manufacturers and suppliers, and introduces a regulatory model with update flexibility.			
2/312	2024-10-28	Republic of Korea	Challenges and approaches to addressing smishing and SMS incidents in South Korea

(continued)

Web	Received	Source	Title
Examines smishing threats in the Republic of Korea, detailing the Ministry of Science and ICT and Korea Internet & Security Agency countermeasures, challenges, and government strategies such as AI detection, awareness campaigns, and international cooperation, with recommendations for improvement.			
2/309	2024-10-25	Albania	Creation of a safer cyber ecosystem in a country: the case of Albania
Summarizes Albania's post-cyberattack cybersecurity reforms, including legal and strategic updates, new operations centres, human capital investment, and enhanced international cooperation with entities like the UN and NATO, leading to stronger legal frameworks and preparedness.			
2/301	2024-10-22	China	Mobile anonymous subscription service based on data security protection
Proposes a service for user privacy protection by using temporary numbers and anonymous IDs, with a focus on balancing privacy and digital economy growth, detailing a system architecture that ensures availability, scalability, reliability, usability, observability, and audit logs.			
2/300	2024-10-22	China	Based on anonymous data exchange network, release the value of telecommunications data
Examines the importance of telecommunications data in the digital economy and the challenges of using it, such as privacy issues and integration with Internet data. It details the China Academy of Information and Communications Technology creation of an anonymous data network, enhancing financial risk management and advertising, and supporting sustainable growth and employment in line with the United Nations Sustainable Development Goals.			
2/299	2024-10-22	China Telecommunications Corporation	Building security capabilities to alert phishing websites
Outlines the difficulties the elderly encounter with digital threats such as phishing, and details the China Telecom security tool, which shields them through gateway plug-ins, cloud engines, and a security database, serving over 10 million users in 31 provinces.			
2/276	2024-09-30	Côte d'Ivoire	Cybersecurity in action: strategies and challenges in a connected world - experience of Cote d'Ivoire
Presents the "O'KOHI" web series by a Platform for the Fight against Cybersecurity (PLCC), designed to educate on cybersecurity via videos. Funded by ARTCI and the Ministère de l'Economie Numérique, des Télécommunications et de l'Innovation, it addresses hacking, data protection, and cyberattacks, ensuring content accuracy through expert collaboration.			
2/273	2024-09-29	RIFEN	Machine learning-based CVE and CWE analysis
Highlights the need for machine learning to automate Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) analysis, improve identification and prioritization of software vulnerabilities, and overcome challenges such as data quality and model complexity through solutions including data validation and continuous learning. It advocates for collaboration to enhance cybersecurity.			
2/271	2024-09-29	RIFEN	Cybersecurity and cyberspace protection in developing countries

(continued)

Web	Received	Source	Title
Examines the Internet and information and communication technology impact on Africa's socio-economic progress, addressing cyberattack risks and the necessity for collaborative security efforts. It discusses Africa-specific challenges, infrastructure vulnerabilities, and advocates for a multi-stakeholder strategy to safeguard essential Internet resources.			
2/268	2024-09-24	RIFEN	Cybersecurity awareness for rural youth through online training organized by RIFEN-SADA
Outlines the RIFEN-SADA (Smart Africa Digital Academy) cybersecurity training, which enhanced awareness and skills in cybersecurity among young Africans through fourteen modules. It fostered a security-conscious culture, practical protection knowledge, and guided talent development, leading to certifications and improved job prospects.			
2/254	2024-09-19	Co-Rapporteur for Question 6/1; Co-Rapporteur for Question 3/2	Report of the workshop on Increasing Consumer Awareness Mechanisms to Promote Informed Consumer Decision: A joint workshop for Question 6/1 and Question 3/2 held in Brasilia from 18-20 June 2024
Presents the workshop on consumer protection in the digital age, discussing infrastructure in underserved regions, security, digital literacy, and data privacy. It stressed digital inclusion, consumer behaviour, and skill gaps, concluding with good practices for ITU deliverables.			
2/246	2024-09-16	RIFEN	Securing the contracting procedure and the production of deeds of purchase in the real estate sale process using blockchain technology and machine learning
Discusses how blockchain technology and machine learning are revolutionizing the real estate industry by enhancing security, efficiency, and decision-making in the sales process. It highlights the benefits of smart contracts and improved market analysis, while acknowledging the challenges of adoption and regulation.			
2/242	2024-09-12	Central African Republic	Operationalization of CSIRT/SOC/PKI platforms and training
Outlines the Central African Republic's cybersecurity measures post-broadband expansion, including the deployment of a Security Operations Centre - Computer Security Incident Response Team (SOC-CSIRT) and public key infrastructure (PKI) systems, and requests Union support for network security.			
RGQ2/218	2024-04-29	Australia	National Office of Cyber Security and the Cyber Security Response Coordination Unit
Presents the Cyber Security Response Coordination Unit, the National Office of Cyber Security and the National Cyber Security Coordinator, entities established by the Government of Australia within the Department of Home Affairs for central coordination, following the Optus and Medibank data breaches of 2022.			
RGQ2/214	2024-04-19	Australia	Critical Infrastructure Uplift Program (CI-UP)
Outlines the Critical Infrastructure Uplift Programme (CI-UP) in Australia, designed to enhance cyber security and resilience of critical infrastructure against cyber-attacks. It details CI-UP activities and emphasizes the voluntary and collaborative nature with industry partners.			
RGQ2/212	2024-04-18	China Mobile Communications Co. Ltd.	China's initiatives to protect the cyber-security rights and interests of minors

(continued)

Web	Received	Source	Title
Presents the critical nature of cybersecurity for Chinese minors, addressing their high online presence, urban-rural digital divide, and exposure to risks such as addiction and privacy violations. It underscores China's advancements in safeguarding minors' Internet use and the collective role of government, industry, and society in bolstering cyber-security education and safety.			
RGQ2/201	2024-04-16	Saudi Arabia	Cost estimation tool for cybersecurity controls
Outlines the National Cybersecurity Authority (NCA) development of the "ECC Cost Estimation Tool" to aid Saudi organizations in budgeting for cybersecurity compliance. It details the creation process, including research, implementation and testing phases.			
RGQ2/191	2024-04-16	United Kingdom	Considerations in implementing a new and significant regulatory security framework for the telecoms sector: an example from the UK's Telecoms Security Act (TSA)
Outlines the United Kingdom new telecoms security framework under the Telecommunications Security Act 2021, detailing enhanced security duties for providers, a tiered approach based on turnover, and the Ofcom role in ensuring compliance and fostering a collaborative security culture.			
RGQ2/184	2024-04-15	Brazil	Creating cybersecurity capabilities: Hackers do Bem
Describes Brazil's "Hackers do Bem" ("White Hat Hackers") initiative, aiming to train 30 000 students in cybersecurity through a five-level curriculum, with government support, to build a national hub, boost employability, and strengthen the cybersecurity ecosystem.			
RGQ2/183	2024-04-15	Brazil	Cybersecurity in Brazilian National Research and Education Network: CAIS
Outlines the work of the Brazilian National Research and Education Network (RNP), which created the first network security centre in Brazil in 1995 (CAIS). CAIS serves as CSIRT for the Brazilian academic network, being the focal point for security incident notifications and providing coordination and support for the incident handling.			
RGQ2/182	2024-04-15	Brazil	Brazilian Federal Cyber Incident Management Network
Presents the Brazilian Federal Cyber Incident Management Network (ReGIC), presenting the two CSIRTs with national responsibilities, such as the Brazilian National Computer Emergency Response Team (CERT.br) and the Centre for Prevention, Treatment and Response to Government Cyber Incidents (CTIR Gov), as well the CSIRT ecosystem in Brazil.			
RGQ2/181	2024-04-15	Brazil	Brazilian National Cybersecurity Policy
Summarizes Brazil's National Cybersecurity Policy and the formation of the National Cybersecurity Committee, detailing its principles, goals, and tasks like promoting cybersecurity, resilience, education, and global collaboration, with diverse members overseeing policy execution.			
RGQ2/170	2024-04-04	Russian Federation	Implementation of the educational project "Digital Literacy Campaign" in the Russian Federation
Outlines the Russian Federation's "Digital Economy" programme for human capital and economic growth by 2024, including "Digital Literacy Campaign" with partners like Kaspersky Lab to educate children on digital safety through animated videos.			

(continued)

Web	Received	Source	Title
RGQ2/165	2024-04-02	Brazil	Meaningful connectivity
Summarizes the Anatel 2023 Strategic Planning, highlighting digital transformation and meaningful connectivity, which encompasses a cyber safety perspective. It details cyber hygiene initiatives, including the launch of a dedicated page to combat digital scams and frauds.			
RGQ2/164	2024-03-29	United States	U.S. Pre-Ransomware Notification capability
Details the CISA Pre-Ransomware Notification programme to pre-empt ransomware attacks. It emphasizes early warnings, international cooperation, and the success of the #StopRansomware campaign in averting threats in 2023.			
RGQ2/163	2024-03-26	Syrian Arab Republic	A paper on digital development in Syria and the current reality
Summarizes the Syrian Arab Republic digital transformation strategy for government services, detailing a phased approach from 2021 to 2030, encompassing e-government services, citizen centres, and cybersecurity. It includes strategic axes, programmes, and annexes on Internet capacity and security.			
RGQ2/160	2024-03-26	RIFEN	Initiatives to strengthen digital trust in Côte d'Ivoire
Highlights Côte d'Ivoire's National Digital Development Strategy 2021-2025, aiming to transform the nation into West Africa's digital hub by improving digital skills, cybersecurity, and women's tech inclusion, and by creating a national data centre.			
RGQ2/155	2024-03-26	RIFEN	Building a resilient security culture: a comprehensive approach to cybersecurity enhancement
Highlights the need for a robust cybersecurity culture in organizations, advocating for comprehensive strategies such as employee training, simulations, incident response teams, access control, encryption, and continuous monitoring to combat cyber threats.			
RGQ2/149	2024-03-15	Democratic Republic of the Congo	Development of cybersecurity in the Democratic Republic of Congo: issues and strategies for the protection of ICT infrastructures and digital actors
Outlines the Democratic Republic of the Congo's cybersecurity challenges, including its vulnerability to cyberattacks and the lack of a national strategy, legal framework, and incident reporting. It mentions a workshop for creating a national CIRT and ITU strategy support.			
RGQ2/140	2024-03-11	RIFEN	Internet and ICT: development levers and cybersecurity challenges in developing countries
Highlights the importance of Internet and ICTs for development, stressing security against cyberthreats. It combines research with expert opinions, identifies vulnerabilities, and addresses Africa's connectivity issues, advocating for information sharing, legislation, and collaboration to protect digital infrastructure.			
RGQ2/134	2024-03-05	Burundi	Implementation of a national cybersecurity strategy

(continued)

Web	Received	Source	Title
Outlines the significance of information management and ICTs for a country's progress, emphasizing the necessity of cybersecurity measures in light of rising cybercrime. It details Burundi's efforts, supported by ITU, to create a national cybersecurity strategy by 2040, concentrating on legal structures, infrastructure security, and skill development.			
RGQ2/130	2024-02-29	RIFEN	Côte d'Ivoire's cybersecurity initiatives
Outlines Côte d'Ivoire's cybersecurity strategies, including the Platform for Combating Cybercrime and CI-CERT, stressing public awareness and education to foster a cybersecurity culture and safeguard the online space, particularly during events like the African Cup of Nations.			
RGQ2/128 +Ann.1	2024-02-29	Syrian Arab Republic	Cybersecurity strategy in Syria
Summarizes the Syrian Arab Republic cybersecurity strategy, focusing on creating a strong infrastructure, handling threats, legal development, capability enhancement, research, governance, and international collaboration via six programs, while stressing the importance of multi-layered protection.			
RGQ2/121	2024-02-29	Haiti	Taking control of cybersecurity in Haiti
Outlines Haiti's Haitian Institute for Statistics and Information and the CONATEL partnership to create a national cybersecurity strategy, aided by the World Bank and Inter-American Development Bank, including forming a working group, evaluating cybersecurity maturity, and establishing a CERT to enhance digital security.			
RGQ2/117 +Ann.1	2024-02-28	Dominican Republic	Cyberskills Center for Latin America and the Caribbean LAC4: Knowledge exchange, training and training in best practices at LAC4
Describes how the Latin America and Caribbean Cyber Competence Centre has enhanced cybersecurity in over 25 Latin American and Caribbean countries through workshops, legal framework support, and promoting regional cooperation, including empowering women and raising cyber awareness.			
RGQ2/114 +Ann.1	2024-02-27	Zambia	The role of the Authority in Child Online Protection in Zambia: A Zambia case study on the implementation of the National COP Strategy - Lessons learnt
Summarizes Zambia's dedication to child online safety by adopting ITU Resolution 179 and executing a national child online protection strategy, focusing on legal frameworks, education, combating exploitation, stakeholder cooperation, and ensuring effective oversight.			
RGQ2/104	2024-01-24	Democratic Republic of the Congo	Making Congolese cybersecurity a lever for integration and socio-economic growth
Describes the Democratic Republic of the Congo's strategy for using cybersecurity to enhance integration, governance, and growth, focusing on infrastructure, cybercrime, and digital services. It advocates for expert capacity building and ITU partnership for a secure digital transformation.			
2/212	2023-10-31	Republic of Korea	Misuse of Personally Identifiable Information

(continued)

Web	Received	Source	Title
Presents the Republic of Korea’s data protection mechanism that has been updated to address concerns related to the misuse and abuse of personal identifiable information (PII). The Personal Information Protection Act (PIPA) amended the existing PII Anonymization Guidelines on 28 April 2022, which aim to offer six step-by-step guidelines for the treatment (de-identification) of personal information. The Republic of Korea highlighted the challenge of crafting guidelines that guard against the abuse and misuse of PII without jeopardizing the benefits of new technologies.			
2/201	2023-10-17	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
Discusses ongoing efforts to improve cybersecurity in ITU Member States, including future plans and new initiatives as well as how the Global Cybersecurity Agenda, launched in 2007, promotes international cooperation, and how BDT works with Member States and global organizations to establish national and regional CIRTs, measures cybersecurity commitments, supports strategy development, encourages diversity, and works to protect children online through the child online protection initiative.			
2/199	2023-10-17	United Kingdom	Building local capacity to adopt secure connected place technology: the UK's Secure Connected Places Playbook
Recognizes the benefits that connected places ("smart cities") technology can bring societies and local areas. However, it also recognizes that this interconnectivity creates cyber vulnerabilities and the potential for cyberattacks. Through its National Cyber Strategy 2022, the United Kingdom has been developing a 'Secure Connected Places Playbook'. This product, currently in alpha phase, has been developed in partnership with a diverse set of local government authorities and an industry consortium. The Playbook provides guidance on: i) governance; ii) procurement and supply chain management; and iii) risk and threat analysis. The United Kingdom has identified several good practices, including: i) working hand-in-hand with intended beneficiaries; ii) using a “test and iterate” approach; and iii) co-developing and testing with local government authorities. The United Kingdom has now begun beta testing, working with 13 local authorities.			
2/196	2023-10-17	United States	U.S. proposed Cyber Trust Mark Program: certifying that IoT products meet U.S. cyber standards
Presents the proposed Cyber Trust Mark program, by the United States Federal Communications Commission (FCC), a voluntary cybersecurity labelling initiative for IoT products. The programme aims to help consumers make informed decisions, differentiate trustworthy products, and encourage manufacturers to meet higher cybersecurity standards. The FCC seeks input on various aspects of the programme, including eligible devices, oversight, security standards, and consumer education. Certified products could be available for purchase by the end of 2024.			
2/187	2023-10-16	Republic of Korea	Privacy by Design certification in South Korea
Shares its contribution on Privacy by Design (PbD), a proactive approach to embedding privacy into the design and operation of information technologies and systems. The Personal Information Protection Committee (PIPC) of the Republic of Korea is piloting a PbD certification system to strengthen the safety of personal information collection devices. The certification helps organizations demonstrate their commitment to user privacy, increasing consumer trust and reducing the risk of privacy breaches.			
2/167	2023-10-11	Australia	eSafety Youth Council

(continued)

Web	Received	Source	Title
Presents the eSafety Youth Council, established in April 2022, that consists of 24 members aged 13-24 from diverse backgrounds in Australia. It aims to involve young people in decision-making processes for policies and programmes impacting them. The Council is informed by the Western Sydney University Youth Engagement Report and follows six good practice principles. Members engage in various activities, including conferences, resource launches, and discussions with technology companies. The Council priorities include collaboration, improved reporting processes, age-appropriate content access, and increased engagement on online safety.			
2/158	2023-10-09	Russian Federation	Challenges and approaches to addressing smishing and SMS incidents. Combating illegal use of virtual mobile numbers
Contextualize smishing as a type of phishing attack that uses SMS messages to trick users into downloading malware or revealing personal information. The rise of mobile services and the pandemic have increased its popularity. To combat smishing, users should be cautious of unexpected messages, use anti-spam settings, and report suspicious messages. Governments, banks, and telecommunication operators are also working together to fight smishing through regulations, public awareness campaigns, and technological solutions.			
2/154	2023-10-05	Australia	Combating telecommunications scams
Presents the Australian Communications and Media Authority (ACMA) work to combats scams through regulatory powers, new rules, and international cooperation. Initiatives include varying the telecommunications numbering plan, registering the Reducing Scam Calls and Scam SMS Code, and mandating stronger identity verification processes. ACMA also collaborates with other nations and industries to fight scams. Despite progress, SMS scams remain a significant issue. A holistic approach involving industry, government, and consumer awareness is needed.			
2/150 +Ann.1	2023-09-29	Argentina	Promoting cybersecurity in Argentina: challenges, strategies and advances in the digital era
Presents the growing reliance on ICT for essential services highlighting the need for governments to prioritize cybersecurity. Challenges include fostering a cybersecurity culture and promoting safe cyberspace usage. Efforts include a National Cybersecurity Awareness Campaign, a joint publication on cybersecurity issues, training programmes for civil servants, strengthening legal frameworks, and addressing the gender gap in ICT access and use through national and international initiatives.			
2/141	2023-09-28	Central African Republic	Criminal aspects of physical protection of information and communication network infrastructures
Central African Republic shares the implementation of legislative reforms and creation of agencies to control and secure information systems. However, the country faces vandalism and theft on its new fibre optic network. Proposed solutions include adopting laws against theft, fraud, and vandalism in public information networks and establishing a national CIRT team to coordinate incident management.			
2/137	2023-09-14	Côte d'Ivoire	Cybercrime: Continuing campaign on child online protection

(continued)

Web	Received	Source	Title
Discusses the digital knowledge challenge facing Côte d'Ivoire, that is hindering its development in the digital world. To address this, public and private sectors, along with international organizations, have launched an awareness campaign for middle and high school students. The campaign aims to educate and raise awareness about online risks, promote responsible digital behaviour, and provide support for reporting abuse. Over 1 000 students participated in the campaign, which emphasizes the importance of a safer digital environment for all citizens.			
2/120	2023-09-07	Timor-Leste	Advancing cybersecurity for Timor-Leste's digital transformation
Presents Timor-Leste digital transformation journey, focusing on improving government services, inclusivity, and crucial sectors such as healthcare, education, and agriculture. However, as a least developed country (LDC), it faces significant cybersecurity challenges, including weak frameworks, limited awareness, and inadequate resources. To enhance digital resilience, Timor-Leste must invest in infrastructure, capacity building, legal frameworks, public-private partnerships, awareness, incident response, and international cooperation. Addressing these challenges is crucial for sustainable development and economic growth in the digital era.			
2/119	2023-09-06	Kenya	The Authority's Child Online Protection and Safety Programme in Kenya: A case study on the implementation of the ITU's Guidelines on Child Online Protection
Shares the implementation of child online protection initiatives since 2011, by the Communications Authority of Kenya (CA), focusing on raising awareness and promoting responsible Internet usage. The CA has launched two campaigns, "Be The COP" and "Huwezi Tucheza, Tuko Cyber Smart," targeting parents, guardians, teachers, and children. The authority collaborates with various stakeholders, including government agencies, industry players, and NGOs, to implement the ITU Guidelines on Child Online Protection. Initiatives include legal and regulatory frameworks, reporting mechanisms, research and surveys, national strategies, industry initiatives, educational resources, capacity building, and national awareness campaigns.			
2/115	2023-09-04	Democratic Republic of the Congo	Digitalization of public services in the Democratic Republic of the Congo: key challenges and requirements for information security and cyberdefence
Presents the implementation of cybersecurity measures, including the enactment of Law No. 20/017 in 2020, and the adoption of a digital code in 2023. The country is working on creating a computer incident response team (CIRT) and improving its broadband infrastructure with a planned 50 000 km of optical fibre network. Cooperation and public awareness-raising are also essential components of their cybersecurity strategy.			
2/112	2023-08-21	Kenya	CSIRT/CIRT approaches and experiences towards the resilience of critical infrastructure in Kenya
Introduces the establishment of the National Computer Incidents Response Team (KE-CIRT) by the Communications Authority of Kenya to mitigate cyber threats and ensure a safer cyberspace. The country has a legal framework defining critical infrastructure and has adopted a cybersecurity framework supported by policy and operational frameworks. Challenges faced include a rapidly evolving threat landscape, lack of international cooperation, insufficient expertise, limited resources, balancing privacy and security, coordination and information sharing, technological advancements, insider threats, public-private collaboration, and public awareness and education.			

(continued)

Web	Received	Source	Title
2/98	2023-07-25	Australia	Australia's national online safety awareness campaign
Introduces the Online Safety Act 2021, to keep pace with new technology and emerging online threats. The Online Safety campaign aimed to raise public awareness of the Online Safety Act and the strengthened laws for online safety. The campaign targeted various audience groups and successfully drove traffic to the eSafety Commissioner website.			
RGQ2/85	2023-05-18	Beihang University	Development of policies and legislation to protect consumer rights and interests in China in the digital era
China attaches great importance to the protection of consumer rights and interests. Firstly, in terms of policy guidance, the goal is to improve the consumer environment, strengthen consumer rights protection, and achieve social fairness and justice, adhering to the equal emphasis on development and regulation; Secondly, in terms of the legal system, China has steadily promoted the formulation and implementation of laws, regulations, and standards related to consumer rights protection. It has continuously strengthened the protection of consumers' digital rights and focused on the special protection of vulnerable consumers, gradually forming a comprehensive and three-dimensional legal system for consumer rights protection to adapt to the new development and needs of consumer rights protection. The content of this paper is based on the policy and legislative protection of consumer rights in China's new development pattern, so as to provide assistance for the international consumer rights protection cause.			
RGQ2/80	2023-05-10	Russian Federation	Information sharing practices to protect children from disruptive online content - Award "For a Safe Digital Childhood"
Presents its contribution which contained information on some practices on the exchange of information between two Russian Federation federal executive bodies to protect children from destructive online content, as well as information about the award "For a Safe Digital Childhood" by Alliance for the Protection of Children in the Digital Environment, aimed at supporting projects to develop a safe digital environment throughout the Russian Federation.			
RGQ2/79	2023-05-10	Russian Federation	National computer incident response and coordination centre - information security leaders
Presents a contribution on the operation of its National Computer Incident Response & Coordination Centre (NCIRCC) to ensure a stable critical infrastructure, as well as approaches regarding the appointment of leaders in the field of information security. In response to questions received during the meeting, the Russian Federation clarified that NCIRCC is not the only such centre, and the main criteria for leaders in the field of information security is not only their professional degree, but also wide-ranging experience and relevant professional skills.			
RGQ2/74	2023-05-09	United Kingdom	TBEST: an example of outcome-based pen-testing for communications providers to help improve their network security posture

(continued)

Web	Received	Source	Title
Contribution on the TBEST scheme, an example of cybersecurity assurance practice that Ofcom, the United Kingdom regulator, runs voluntarily with communications providers. TBEST is a penetration testing that aims to stimulate a cyber-attack in telecommunications networks in order to identify security vulnerabilities which can then be, through a process of remediation, addressed to improve the operators' network security posture. The contribution provides an overview of the process, and the various stakeholders involved. More broadly, this scheme is an example of supervisory policy approach that Ofcom is taking, which stresses the importance of building collaborative relationships with the industry that Ofcom regulates. To date, all communications providers in the United Kingdom have already or are undergoing the TBEST scheme voluntarily and have implemented changes as a result. TBEST is not a "standard" nor a certification process. The goal is to enable communications providers to gain awareness of cyber threats and implement appropriate changes in a timely manner to improve their cyber defence capabilities. By being aware of, and addressing such vulnerabilities and weaknesses, the operator is in a much stronger position to protect their networks.			
RGQ2/66	2023-05-10	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
Provides an update on the activities currently being undertaken to enhance cybersecurity in ITU Member States. It also highlights future actions envisaged and new initiatives being formulated. The presentation addressed the ITU cybersecurity mandate, and through BDT, work on the national CIRT programme, regional and national cyberDrills, the Global Cybersecurity Index (GCI), national cybersecurity strategy (NCS) assistance, Women in Cyber, Her CyberTracks, child online protection, partnerships and collaboration, and Cyber for Good. The document emphasizes the importance of collaboration, partnerships, and resource mobilization to allow ITU to fulfil its mandate, considering the extensive list of tasks that membership have requested BDT to undertake. BDT also presented information about the 5th edition of the Global Cybersecurity Index.			
RGQ2/58	2023-04-27	Brazil	Cybersecurity assurance practices - Brazil experience
Introduces the contribution referring to the efforts of the Brazilian National Telecommunications Agency (ANATEL) regarding the establishment of cybersecurity minimum requirements for telecommunication equipment. ANATEL initially adopted a non-mandatory approach (Act 77/2021), which evolved into a cybersecurity compulsory certification requirement for a specific set of equipment (Act 2436/2023). This evolution was only possible with a comprehensive debate within the sector.			
RGQ2/57	2023-07-27	Brazil	Brazilian cybersecurity-related policies and regulations
Presents an overview on the cybersecurity-related policies and regulations that have been developed in Brazil in recent years, including the National Information Security Policy, the National Cybersecurity Strategy, the Cybersecurity Regulation for the Telecommunication Sector, the Federal Cyber Incident Management Network, and the 5G Spectrum Auction Notice. There were questions about the modular approach adopted by the National Information Security Policy, and the Brazilian delegation explained that in Brazil cybersecurity is one of the elements of Information Security.			
RGQ2/53	2023-04-25	Mexico	Privacy reports on user information in the use of digital platforms

(continued)

Web	Received	Source	Title
Presents the Privacy Reports, which purpose is to make available in a clear, simple and transparent manner the privacy policies of operating systems, terminal equipment, social networks, and digital platforms that enable the provision of services such as: online commerce, transport and entertainment. These reports published by the Federal Telecommunications Institute help users to learn about the information that is collected by the platforms, and how this information is treated, and helps users make responsible use of such platforms. The Reports also empower users by providing transparent information about privacy policies.			
RGQ2/51	2023-04-25	Mexico	Internet of Things Devices Catalog
The Internet of Things Devices Catalogue is an electronic tool that allows users of telecommunication services to know the main characteristics of IoT devices, as well as the privacy policies defined by the manufacturers. The IoT devices published are those that are marketed in Mexico and have been certified by the Federal Telecommunications Institute. The tool allows users to be empowered with transparent information about privacy policies and the characteristics of terminal equipment that comply with technical regulations, for informed decision-making and for the proper use of IoT equipment.			
RGQ2/48	2023-04-25	Access Partnership Limited	Cybersecurity assurance practices - international standards and satellite communications
Contains information related to developing cybersecurity assurance practices for commercial satellite operators, as well as highlighting some of the existing general cybersecurity assurance practices which may be adopted by any commercial satellite operator, including ISO 27001. The contribution noted some of the unique cybersecurity threats which need to be overcome in satellite operations, including the cross-jurisdictional nature of satellite operations, and the vulnerabilities of ground stations. The contribution explained specific technical standards including the ETSI technical standard 103 732 and its measures to protect consumer mobile devices, as an example of standards towards specific technology which could inform the further development of standards for commercial satellite operators.			
RGQ2/44	2023-04-24	South Africa	The domain name cybersecurity culture
Provides a contribution concerning the security of the country code top-level domain name (.za). The South African Domain Name Authority (ZADNA) manages the .za domain namespace under the mandate of the Electronic Communications and Transactions Act (ECTA). Its policy framework was designed to ensure a secure, resilient, and efficiently managed domain namespace, promoting stakeholder engagement, growth of the namespace, policy compliance, and entrance of new Internet service providers. ZADNA also addresses cybersecurity threats through education and awareness programmes, alternative dispute resolution (ADR) workshops and regulations, and DNS training courses. Additionally, it adheres to international standards for dispute resolution, working in line with the World Intellectual Property Organization (WIPO) and organizations such as the South African Institute of Intellectual Property Law (SAIIPL) and the Arbitration Foundation of Southern Africa.			
RGQ2/38	2023-04-13	Australia	Sharing advice from Australia on securing smart places
Shares information on the lessons learned by the Australian Cyber Security Centre in response to risks identified for smart places. The contribution defined smart places as those designed to provide enhanced services through the use of smart information and ICT enabled systems and devices. The contribution noted that the highly connected nature of smart places makes them vulnerable to intrusions. This is exacerbated when the system scales. The contribution gave examples of Australian policies used to protect the various aspects of smart cities including IoT, supply chains, operational technology and cloud computing. The contribution also raised several examples of strategies which may be employed to mitigate security risks as well as ensuring operational redundancy.			

(continued)

Web	Received	Source	Title
RGQ2/34	2023-04-06	Republic of Korea	Cloud Security Assurance Program (CSAP) in South Korea
Introduces the Cloud Security Assurance Programme (CSAP), a security certification for cloud computing services that meet security certification standards to improve and guarantee information protection levels. The purpose of the CSAP is to provide private cloud services with proven safety and reliability to national and public institutions. Also, it aims to implement an objective and fair security certification system for cloud services to address user security concerns and secure competitiveness of cloud services. The CSAP provides a number of benefits. By certifying the security level of a cloud system, CSAP helps to improve the cyber resilience of national and public institutions. This can also help to ensure that sensitive information is protected and that cloud services are reliable.			
RGQ2/29	2023-03-30	Côte d'Ivoire	Policy and strategy of Côte d'Ivoire for building a trusted digital space
Shares the initiatives taken by Côte d’ Ivoire in its efforts to build digital trust, which concerns all economic sectors that use ICTs, such as media and communication, transport, health, industry, telecommunications and computing, distribution of goods and consumption, construction, finance and insurance, tourism, agriculture and e-commerce. To consolidate the freedom of online public communication and ensure interactions are secure, Côte d’ Ivoire has enhanced the means for combating cybercrime and protecting personal data in order to build trust in cyberspace. Cybersecurity has become an issue of privacy, competitiveness and national sovereignty. A capacity to anticipate, build trust and protect personal data is essential. In this sense, the country has updated its legal and institutional framework, setting a visionary policy to enhance digital trust by 2025. The country has established a Consultative Committee for Digital Trust (CCCN) and a Consultative Committee for the Protection of Personal Data (CCDCP).			
RGQ2/20	2023-03-22	Nigeria	Child Online Protection practices in Nigeria
Presents its efforts in regard to child online protection through the Nigerian Communications Commission (NCC), the independent national regulatory authority for the telecommunication industry, in collaboration with the Office of the National Security Adviser in Nigeria who works with other stakeholders to ensure child protection in Nigeria’ s cyber space. It was decided by the meeting to liaise with the Council Working Group on Child Online Protection (CWG-COP) to share the relevant experiences shared by Nigeria.			
2/80	2022-11-24	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
Provides an update on the activities currently being undertaken by BDT and new initiatives to enhance cybersecurity in ITU Member States: CIRT programme, regional and national cyberdrills, national cybersecurity strategy (NCS) , work related to Bridge the Cybersecurity Divide: Cyber for Good project, work on promoting a diverse and inclusive cybersecurity community through the Women in Cyber Mentorship Programme and Youth4Cyber initiative, child online protection, and partnerships and collaboration initiatives.			
2/77	2022-11-22	United Kingdom	Sharing experience from the UK on promoting and developing cybersecurity skills
Outlines the country's policy approach to address the cyber skills gap which, in addition to the final report of the study cycle, can also be included in a future repository of good practices as agreed through Resolution 130 (Rev. Bucharest, 2022) of the Plenipotentiary Conference. The United Kingdom's initiatives are focused in three areas: (1) cyber skills for young people, (2) cyber skills for adults, and (3) developing the cyber profession.			

(continued)

Web	Received	Source	Title
2/74	2022-11-18	World Bank	World Bank Study Group 2 Submission: Digital transformation
Highlights their readiness to support the least developed client countries with a special emphasis on fragility, conflict and violence (FCV) and small island developing states (SIDS). Through the analytical work programme and strategic partnerships, the World Bank is working closely with client countries on issues related to the SG2 Questions' scopes. Relevant examples from the World Bank around using ICT services and applications for the promotion of transformative and sustainable development are provided in the contribution. For instance, one relating to cybersecurity is the Cybersecurity Multi-Donor Trust Fund, being a part of the broader Digital Development Partnership umbrella programme, aims at systematically incorporating cybersecurity in the development agenda as well as in World Bank operational programmes. Work includes building global knowledge to better define the cybersecurity development agenda, and country-specific technical assistance.			
2/71 (Rev.1)	2022-11-18	Russian Federation	New practices of the Russian Federation in the field of creating a culture of cybersecurity
Presents the Russian Federation Cyber Hygiene Program, launched in August 2022. The programme is planned for a three year period and includes various activities aimed at attracting the attention of citizens of the Russian Federation to the issues of cybersecurity and the training in skills on safe behaviour on the Internet. Large-scale information campaigns are one part of the programme. Citizens were segmented into age groups, and their online behaviour and the type of digital content consumed were taken into account. Based on this segmenting approach, more specifically targeted means of information dissemination could be applied for the 3 segmented groups of population (12-18 / 18-45 / 45+ years old). The contribution also covers the means of improving the information security literacy of civil servants, as well as the results of an all-Russian Federation study of the citizens' information security literacy.			
2/35	2022-10-12	Rwanda	National cybersecurity initiatives: current status
Highlights the programmes and initiatives put in place to guarantee the security and resilience of Rwanda's cyberspace. To support national economic growth and social mobility, the Government of Rwanda (GoR) is actively deploying various information technologies and has made major investments in ICT infrastructure and applications. GoR established the National Cybersecurity Authority (NCSA) as the authority to spearhead the implementation of National Cyber Security policies and strategies. Additionally, GoR established a law relating to protecting personal data and privacy and passed the prevention and punishment of cybercrimes law. NCSA roles include: coordinating national cybersecurity functions across the private and public sectors; promoting national education programmes and fostering awareness of cybersecurity good practices amongst the Rwandan population; operating the Rwanda Computer Security Incident Response Team (Rw-CSIRT); and overseeing the implementation of the Protection of Personal Data and Privacy Law. Furthermore, the Rwanda Utilities Regulatory Authority (RURA), Regulation No. 010/R/CR-CSI/RURA/020 OF 29/05/2020), Rwanda Information Society Authority (RISA), and capacity building collaborations and initiatives have been put in place to ensure preparation in preventing and responding to evolving cyber threats.			
2/34	2022-10-12	Côte d'Ivoire	Initiatives to support children and young people, national strategy for the protection and empowerment of children and young people online: the experience of Côte d'Ivoire

(continued)

Web	Received	Source	Title
Presents an initiative undertaken by Côte d'Ivoire to protect children against the dangers and threats of using ICTs. The initiative, www.jemeprotegeenligne.ci is a website targeted at children between 5 and 19 years old as well as teachers and parents with the goal of educating children and young people and raising awareness.			
2/30	2022-10-11	Côte d'Ivoire	Proposal for State actions and initiatives to foster a culture of cybersecurity and ensure that information and communication networks are secure: the case of Côte d'Ivoire
Contextualizes cyberattacks and threats as a major concern for governments in this increasingly connected world, particularly in developing countries. Cybersecurity is now the priority issue for many States. This contribution gives an overview of the cybersecurity situation in developing countries, notably Côte d’ Ivoire, and highlights strategies for raising user awareness and experience-sharing among Member States.			

Incoming liaison statements for Question 3/2

Web	Received	Source	Title
2/410 +Ann.1	2025-04-30	ITU-T Study Group 17	Liaison statement form ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 LS on update on the work of the Correspondence Group on Child online protection (CG-COP)
2/409	2025-04-30	ITU-T Study Group 17	Liaison statement form ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 on request to update security contacts and to provide information on security-related Recommendations or other texts under development
2/241	2024-09-11	ITU-T Study Group 17	Liaison statement from ITU-T Study Group 17 to ITU-D Study Groups 1 and 2 on SG17 update on the work of the Correspondence Group on Child online protection (CG-COP)
RGQ2/151	2024-03-18	ITU-T Study Group 17	Liaison statement from ITU-T Study Group 17 to ITU-D Study Group 1 Question 6/1 and ITU-D Study Group 2 Question 3/2 on Establishment of the Correspondence Group on Child online protection (CG-COP)
RGQ2/107	2024-02-12	Chairman, ITU Council Working Group on COP	Liaison statement from ITU Council Working Group on COP to ITU-D Study Group 2 Question 3/2 on child online protection
RGQ2/83	2023-03-08	ITU-T Study Group 17	Liaison statement from ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 on status of security studies in ITU-T SG17
2/20	2022-06-16	ITU-T Study Group 17	Liaison statement from ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 on request to update security contacts and to provide information on security-related Recommendations or other texts under development

Annex 2: List and summary of BDT on-going cybersecurity activities

Activity type	Activity	Targeted / invited countries	Partners	Outputs
Data	Global Cybersecurity Index v5	ITU Member States	GCI Expert Group	Global Cybersecurity Index report and country reports. Link
Governance	Capacity-building sessions for the cybersecurity ecosystem in Guinea-Bissau	Guinea-Bissau	Government of Guinea-Bissau	Capacity-building sessions for the cybersecurity ecosystem in Guinea-Bissau with the aim to empower Guinea-Bissau's cybersecurity ecosystem by guiding key national stakeholders in developing strategic approaches to CIRT implementation and enhancing cybersecurity in Guinea-Bissau
Governance	Mauritania's Cybersecurity Governance Development	Mauritania	Government of Mauritania	Sessions to enhance of a national cybersecurity governance framework to enable Mauritania to strengthen the protection of the critical information systems of official institutions and vital operators, the fight against cybercrime, awareness raising, training, confidence-building in digital, more effective regional and international integration through cooperation.
Governance	National cyber risk assessment	Lesotho	Ministry of Communications Science and Technology	Workshop to enhance strategic thinking on cybersecurity governance among key national stakeholders, thereby advancing the objectives of Lesotho's National Cybersecurity Strategy.
Governance	Strengthening Critical Information Infrastructure Resilience	Cambodia	Ministry of Post and Telecommunications Cambodia (MPTC, Japan International Cooperation Agency (JICA)	Workshops on technical incident response, national cybersecurity strategy, and crisis management for critical information infrastructure stakeholders
Governance	Tabletop Exercise and a Cybersecurity Incident Simulation Exercise	ITU Arab States region Member States	CSC UAE	Tabletop exercise centred around cyber-attack directed at a financial institution.
Incident Response	13th Event of Cyber Capacity Building in America - Andino	ITU Americas region Member States	Ministry of Popular Power for Science and Technology of Venezuela, National Commission of Information Technologies (CONATI), Superintendency of Electronic Certification Services (SUSCERTE)	Incident response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	Americas Regional CyberDrill	ITU Americas region Member States	INICTEL-UNI, Peruvian Ministry of Transportation and Communications, General Secretariat of the Andean Community	Incident response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	CIRT Establishment in Bahamas	Bahamas	Government of Bahamas	Building and deploying the technical capabilities and related training necessary to develop Bahamas national cybersecurity strategy and to establish its National Cybersecurity Incident Response Team (CIRT). Link

(continued)

Activity type	Activity	Targeted / invited countries	Partners	Outputs
Incident Response	CIRT Maturity Assessment	Timor-Leste	ANC	Conducted Maturity Assessment of country CIRT through series of workshops, discussions, and inventories, providing recommendations for the Timor-Leste computer security incident response team (TLCSIRT) in collaboration with the Autoridade Nacional de Comunicações (ANC) to ensure TLCSIRT can enhance its cybersecurity maturity level. Link
Incident Response	Cyber 100x Global CyberDrill 2024	ITU Member States	Cyber Security Council United Arab Emirates	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	CyberQ	ITU Member States	United Arab Emirates Cybersecurity Council	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Included specific trainings for women. Link
Incident Response	Cybersecurity Forum and CyberDrill for Europe and the Mediterranean	ITU Europe region and Arab States region Member States	Ministry of Transport and Communications of Bulgaria, Ministry of Electronic Governance of Bulgaria	Cybersecurity forum featuring trends and challenges, CSIRTs capacity-building training, and two days of cyberdrill exercises with emerging attack scenarios and collaborative learning sessions. Link
Incident Response	ITU National CyberDrill for Armenia	Armenia	Ministry of High-Tech Industry of Armenia	Incident response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	ITU Regional Asia-Pacific CyberDrill	ITU Asia and the Pacific region Members States	Cyber Security Brunei (CSB)	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	ITU Regional Cybersecurity Readiness Exercise	ITU Arab States region Member States	Directorate General for Information Systems Security (DGSSI) Morocco	Incident response trainings, discussions, and information sharing. Link
Incident Response	National CIRT Establishment in Gambia	Gambia	Ministry of Information and Communication Infrastructure (MOICI)	Assist MOICI in building and deploying the technical capabilities and related trainings necessary to establish its national CIRT. Link
Incident Response	National Computer Incident Response Team (CIRT) Implementation – Suriname	Suriname	e-Government Directorate, Cabinet of the President of Suriname	Support for operationalization of Computer Incident Response Team. Link
Incident Response	Regional Cybersecurity Week	ITU Arab States region Member States	ARCC Oman	Regional Cybersecurity Conference focusing on "Cybersecurity as an enabler for the Digital Economy", the FIRST Organization Seminar, and the Regional and OIC-CERT Cyber Drill. Link
Incident Response	Rwanda National CyberDrill	Rwanda	Rwanda National Cyber Security Authority, Ministry of Foreign Affairs of the Czech Republic	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	Twelfth Edition of the Regional Cyberdrill for Africa Region (ITU-INTERPOL CyberDrill)	ITU Africa region Member States	Ghana’s Cyber Security Authority (CSA), INTERPOL	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Link

(continued)

Activity type	Activity	Targeted / invited countries	Partners	Outputs
Partnerships	Cyber for Good	Least developed countries (LDCs)	Axon Consulting, BitSight Technologies, CTM360, DreamLab Technologies, ImmuniWeb, WelchmanKeen	Tools, trainings, and services offered for free to Least Developed Countries. Link
Skills Develop-ment	Child Online Protection National Assessment - Andorra	Andorra	SWGfL/UK Safer Internet Centre	Child Online Protection National Assessment with the national stakeholder consultation event
Skills Develop-ment	Child Online Protection Train the Trainers and Cybersecurity briefings - Maldives	Maldives	National Centre for Information Technology (NCIT)	Trainings on Child Online Protection as well as briefings on key topics. Link
Skills Develop-ment	Creating a Safe and Prosperous Cyberspace for Children	ITU Member States	CTO, CNIL, Council of Europe, European Commission, EC-Council, EBU, Europol, ILO, Interpol, MICITT, NCA KSA, OECD, United Nations Human Rights Special Procedures, UNICRI, UNESCO, UNICEF, UNODC, WIPO, World Bank, UC Berkley, LSE, Middlesex University London, Western Sydney University, Youth and Media, BBC, Disney, Ericsson, worldwide Group, Facebook, IBM, IEEE, Microsoft, Sony, TIM, Privately, Tencent, TrendMicro, Twitter, ASCSA, ACOPEA, 5Rights Foundation, ASDRA, Child Helpline International, Child Rights Connect, Family Online Safety Institute, Childhood, ChildOnline Africa, DeafKidz International, DISC Foundation, Families Europe, Halley Movement, End Violence Against Children, DOInstitute, ecpat, Fard Digital, HABLATAM, Cuber Coluntarios.org, Global Kids Online, GSMA, iKeepSafe, Inclusion international, InHope, Ins@fe, International Centre for Missing & Exploited Children, International Disability Alliance, Internet Matters, Internet Watch Foundation (IWF), Human Trafficking Front, ParentZone, Plan International, RNW media, Save the Children, Paniamor, Stiftung digitale chancen, SWGfL, Tech Coalition, terre des hommes suisse, United Kingdom Safer Internet Centre, WeProtect Global Alliance, Wise Kids, World Economic Forum, YouthIGF, Together Against Cybercrime	Advocacy, research, and in-country programmes related to Child Online Protection. Link

(continued)

Activity type	Activity	Targeted / invited countries	Partners	Outputs
Skills Develop-ment	Her CyberTracks 2024	Algeria, Angola, Bahrain, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cabo Verde, Central African Republic, Comoros, Chad, Côte d'Ivoire, Democratic Republic of the Congo, Djibouti, Egypt, Equatorial Guinea, Eritrea, Eswatini, Ethiopia, Gabon, Gambia, Ghana, Guinea, Guinea-Bissau, Iraq, Jordan, Kenya, Kuwait, Lebanon, Lesotho, Liberia, Libya, Madagascar, Malawi, Mali, Mauritania, Mauritius, Morocco, Mozambique, Namibia, Niger, Nigeria, Oman, Qatar, Republic of the Congo, Rwanda, São Tomé and Príncipe, Saudi Arabia, Senegal, Seychelles, Sierra Leone, Somalia, South Africa, South Sudan, State of Palestine*, Sudan, Syrian Arab Republic, Tanzania, Togo, Tunisia, Uganda, United Arab Emirates, Yemen, Zambia, Zimbabwe	GIZ, Microsoft	Her CyberTracks provides specialized, targeted training, maintaining the essential mentorship and role modelling aspects. The programme is poised to propel the next generation of women in cybersecurity into roles of leadership, ensuring that their voices and expertise shape the future of this critical field through training, mentorship, and inspiration across three tracks: Policy & Diplomacy, Incident Response, and Criminal Justice (implemented by UNODC). Link
Skills Develop-ment	Translation of Child online protection guidelines and capacity building activities - Albania	Albania	National Authority on Electronic Certification and Cyber Security	Child online protection guidelines translated into Albanian and the roll out of capacity-building activities
Skills Develop-ment	Translation of Child online protection guidelines and capacity building activities - Malta	Malta	SWGfL/UK Safer Internet Centre	Child online protection guidelines translated into Maltese and the roll out of capacity-building activities

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）
Place des Nations
CH-1211 Geneva 20
Switzerland

电子邮件： bdtdeputydir@itu.int
电话： +41 22 730 5131
传真： +41 22 730 5484

数字网络和社会部（DNS）
电子邮件： bdt-dns@itu.int
电话： +41 22 730 5421
传真： +41 22 730 5484

数字知识中心部（DKH）
电子邮件： bdt-dkh@itu.int
电话： +41 22 730 5900
传真： +41 22 730 5484

数字化发展合作伙伴部（PDD）
电子邮件： bdt-pdd@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
Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Addis Ababa
Ethiopia

电子邮件： itu-ro-africa@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
8, Route du Méridien Président
Immeuble Rokhaya, 3e étage
Boîte postale 29471
Dakar - Yoff
Senegal

电子邮件： itu-dakar@itu.int
电话： +221 33 859 7010
电话： +221 33 859 7021
传真： +221 33 868 6386

津巴布韦
国际电联
地区办事处
USAF POTRAZ Building
877 Endeavour Crescent
Mount Pleasant Business Park
Harare
Zimbabwe

电子邮件： itu-harare@itu.int
电话： +263 242 369015
电话： +263 242 369016

美洲

巴西
国际电联
区域代表处
SAUS Quadra 6 Ed. Luis Eduardo Magalhães,
Bloco “E”, 10º andar, Ala Sul (Anatel)
CEP 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
传真： +1 246 437 7403

智利
国际电联
地区办事处
Merced 753, Piso 4
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 Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa
Honduras

电子邮件： ituteguci galpa@itu.int
电话： +504 2235 5470
传真： +504 2235 5471

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： itu-ro-arabstates@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
4th floor NBTC Region 1 Building
101 Chaengwattana Road
Laksi,
Bangkok 10210,
Thailand

电子邮件： itu-ro-asiapacific@itu.int
电话： +66 2 574 9326 – 8
+66 2 575 0055

印度尼西亚
国际电联
地区办事处
Gedung Sapta Pesona
13th floor
Jl. Merdeka Barat No. 17
Jakarta 10110
Indonesia

电子邮件： bdt-ao-jakarta@itu.int
电话： +62 21 380 2322

印度
国际电联
地区办事处和
创新中心
C-DOT Campus
Mandi Road
Chhatarpur, Mehrauli
New Delhi 110030
India

电子邮件：
地区办事处： itu-ao-southasia@itu.int
创新中心： itu-ic-southasia@itu.int
网址： ITU Innovation Centre in New Delhi, India

独联体国家

俄罗斯联邦
国际电联
区域代表处
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

电子邮件： itu-ro-cis@itu.int
电话： +7 495 926 6070

欧洲

瑞士
国际电联
欧洲处
Place des Nations
CH-1211 Geneva 20
Switzerland

电子邮件： eurregion@itu.int
电话： +41 22 730 5467
传真： +41 22 730 5484

国际电信联盟
电信发展局
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN 978-92-61-41105-3

瑞士出版
日内瓦，2025

图片鸣谢: Adobe Stock