ITU出版物
2018-2021年研究期

国际电信联盟
发展部门

第2研究组 第3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

ITU-D第3/2号课题的输出成果报告

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

2018-2021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 2018-2021年研究期第3/2号课题的输出成果报告

ISBN 978-92-61-34105-3（PDF版）
ISBN 978-92-61-34115-2（EPUB版）
ISBN 978-92-61-34125-1（Mobi版）

封面图片鸣谢： Shutterstock

鸣谢

国际电联电信发展部门（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汇聚一起，制定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基础上制定报告、导则和建议。研究课题每四年在世界电信发展大会（WTDC）上决定。国际电联成员于2017年10月在布宜诺斯艾利斯举行的WTDC-17上商定，在2018-2021年期间，第2研究组将在“信息通信技术服务和应用促进可持续发展”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Ahmad Reza Sharafat先生（伊朗伊斯兰共和国）领导，并得到以下副主席的支持：Nasser Al Marzouqi先生（阿拉伯联合酋长国）（2018年辞职）；Abdelaziz Alzarooni先生（阿拉伯联合酋长国）；Filipe Miguel Antunes Batista先生（葡萄牙）（2019年辞职）；Nora Abdalla Hassan Basher女士（苏丹）；Maria Bolshakova女士（俄罗斯联邦）；Celina Delgado Castellón女士（尼加拉瓜）；Yakov Gass先生（俄罗斯联邦）（2020年辞职）；Ananda Raj Khanal先生（尼泊尔共和国）；Roland Yaw Kudozia先生（加纳）；Tolibjon Oltinovich Mirzakulov先生 （乌兹别克斯坦）；Alina Modan女士（罗马尼亚）；Henry Chukwudumeme Nkemadu先生（尼日利亚）；王珂女士（中国）；和Dominique Würges先生（法国）。

该报告由第3/2号课题共同报告人Michael Beirne（美国）（2020年辞职）；Kwadwo Burgee先生（美国）（2020年辞职）；Aimee K. Meacham女士（美国）和Dominique Würges先生（法国）与以下副报告人协作撰写：Damnam Kanlanfei Bagolibe先生（多哥）；Amine Adoum Bakhit先生（乍得）；Maria Bolshakova女士（俄罗斯联邦）；Sonam Choki女士（不丹）；Yakov Gass先生（俄罗斯联邦）（2020年辞职）；Karim Hasnaou先生（阿尔及利亚）；Cissé Kane先生（非洲信息社会民间团体）；Miho Naganuma先生（日本）；Jean-David Rodney先生（海地）；Jabin Vahora女士（美国）；万欣欣女士（中国）；Jaesuk Yun先生（韩国）和Mohamadou Zarou先生（马里）。

特别感谢该章协调人的奉献、支持和专业知识。

本报告是在电信发展局研究组联系人、编辑以及出版物制作团队和ITU-D研究组秘书处的支持下编写的。

目录

鸣谢 iii

表和图列表 vi

内容提要 vii

第1章 – 垃圾邮件和恶意软件的最新情况，包括缓解对策 1

1.1 垃圾邮件和恶意软件的现状 1

1.2 垃圾邮件和恶意软件：统计、趋势、演变和对电子通信网络的影响 2

1.3 打击垃圾邮件和恶意软件，减轻其影响的方法 2

1.3.1 打击垃圾邮件和恶意软件，减轻其影响的技术方法 2

1.3.2 打击和减轻垃圾邮件和恶意软件影响的监管方法示例 3

1.3.3 与第3/2号课题下打击和减轻垃圾邮件和恶意软件影响工作相关的文稿 3

第2章 – 改善国家网络安全态势：认识提高和能力建设机会 6

2.1 组建国家相关网络安全机构 6

2.2 计算机应急响应团队（CERTs）/计算机安全事件响应团队（CSIRTs）/计算机事件响应团队（CIRTs） 8

2.3 宣传活动 8

2.4 网络安保风险框架 10

2.5 公私伙伴关系 12

2.6 其他能力建设措施/举措 13

2.6.1 建立网络安全教育机构 13

2.6.2 其他能力建设举措 13

第3章 – 保护上网儿童 14

3.1 概述 14

3.2 国际电联成员国的最佳做法和共同趋势 15

3.3 经验教训、未来步骤、行动和结论 20

第4章 – 残疾人面临的网络安全挑战 23

4.1 引言 23

4.2 使用案例 23

4.2.1 以残疾人为对象的垃圾邮件人和网络钓鱼者 23

4.2.2 与物联网辅助技术相关联的网络风险 26

4.2.3 考虑信息通信技术无障碍服务的安全问题 28

4.3 实用信息 29

第5章 – 网络安全挑战的现状，包括面对物联网（IoT）和云计算等新兴技术的挑战....30
5.1 引言 30
5.2 网络安全威胁、实施者和动机....31
5.2.1 从技术角度看的风险....32
5.2.2 从行业4.0的角度看风险....35
5.3 现有和新出现的解决方案....37

第6章 – 网络安全如何支持个人数据保护 42
6.1 引言 42
6.2 成员国的法律环境和最佳做法....42
6.3 汲取的经验和前进方向....45

第7章 – 课题的未来....46

Annexes 47
Annex 1: List of contributions and liaison statements received on Question 3/2 47
Annex 2: List of lessons learned received on Question 3/2 53

表和图列表

表目录

表1：保护云基础设施、应用程序、数据和隐私的安全架构 38
表2：保护物联网基础设施、应用、数据和隐私的安全架构 39
表3：隐私设计应用的八个关键策略 44
表4：隐私目标和隐私设计策略之间的联系 45

图目录

图1：威胁模型 32

内容提要

国际电信联盟发展部门（ITU-D）第3/2号课题（“保障信息和通信网络安全：培育网络安全文化的最佳做法”）的目的是就网络安全的各个方面编写最佳做法报告。

本文件是第3/2号课题最近四年研究期（2018-2021年）各项活动的最后报告，2017年布宜诺斯艾利斯世界电信发展大会（WTDC-17）制定了第3/2号课题的工作计划。

以往各研究期开展的活动侧重于已有的课程（2010-2014年）和将广泛的参与者和内容带到发展中国家而举办的讲习班（2014-2017年）。

在2018-2021年研究期间，ITU-D第2研究组已经解决了工作计划中所列的大部分问题。在本研究期间还举办了一次讲习班。

这份关于第3/2号课题的报告借鉴了研究期国际电联成员文稿中提交的材料。本报告概述了垃圾邮件和恶意软件问题及其解决方法。报告还包含可供国家网络安全应对规划和提高认识运动借鉴的一些经验。报告还指出了针对残疾人和儿童在内的弱势群体开展的具体行动。此外，本报告还包含智慧城市、新兴技术和数据保护方面的思路。

在当今的数字化世界中，人们的日常生活和经济越来越依赖数字技术，但是也变得更加脆弱，暴露于网络攻击的风险也越来越大。网络安全已被认定为全世界行业、政府和互联网用户的一个优先事项和最关切的问题，对于保障安全的进步使社会得以发展至关重要。

本报告旨在根据国际电联成员的经验提供最新的思路和做法。在认识到总体环境和威胁格局不断变化的情况下，提供了网络安全这一非常敏感领域的最新写照。本报告也是在一个特定的未知背景下发表的：虽然未提及当前的疫情大流行，但在第3/2号课题活动期间，参与者和讨论中并未忽略新冠疫情的影响。

除了国际电联采取的其他行动之外，本报告中汇编的对策和建议旨在帮助国际电联成员实现高水平的网络安全，也可以作为应对未来潜在危机的实用工具。

第1章，恶意软件和垃圾邮件现状以及缓解对策的更新情况。注意，研究组没有收到针对该问题的文稿。

第2章，如何利用提高认识和能力建设机会来改善国家网络安全态势。

第3章，有关保护上网儿童活动的信息。

第4章，残疾人面临的网络安全挑战。

第5章，新兴技术的网络安全挑战，如物联网（IoT）和云计算。

第6章，网络安全如何支持个人数据保护的观点。

第7章，未来的探索领域。

除本报告外，还应该指出，第3/2号课题审查了作为全球网络安全指数（GCI）基础的问卷，并提供了意见和建议，使电信发展局（BDT）能够在国际电联成员国中开展年度调查。特别是，通过巴西的倡议，第3/2号课题制定了这项调查，并作为附件纳入了全球网络安全指数。拟议的修订被纳入2020年全球网络安全指数第四版。

本报告没有广泛地介绍全球网络安全指数。然而，第3/2号课题强调了集体努力和与BDT丰富协作的积极成果，因为对附件的答复将提供有关监管政策的信息，BDT将向成员提供这些信息，从而实现第3/2号课题职责范围中的研究项目“n”。

第1章 – 垃圾邮件和恶意软件的最新情况，包括缓解对策

本章审查了垃圾邮件和恶意软件的演变，并根据关于加强网络安全合作机制的世界电信发展大会（WTDC）第45号决议（2014年，迪拜，修订版）[1]，提出了将在国家、区域和国际各层面实施的若干对策，包括抵制和打击垃圾邮件。因此，本章对WTDC-17最后报告中提出的第3/2号课题的职权范围项目2(b)和(m)作出回应：

b) 探讨评估一网络内垃圾信息和恶意软件所产生影响的方法和最佳做法以及不断变化的和新兴的威胁，并且在考虑到现有标准和可用工具的前提下，提出可供发展中国家使用的必要措施和导则方面的输入意见，包括缓解技术、立法和监管方面。

m) 制定导则，促进在各国、区域和国际层面采取措施，打击垃圾信息和恶意软件[2]。

1.1 垃圾邮件和恶意软件的现状

虽然垃圾邮件没有一个普遍接受的定义，但它通常是指未通过电子邮件和短信擅自发出的、经计算机或移动电话传递的批量电子通信[3]。消费者通常会看到广告形式的垃圾邮件，包括垃圾或无用商业电子邮件、文本和社交媒体联系人。

虽然垃圾邮件通常意味着商业潜在机会，但它也可以将用户生成的类似数据用于犯罪目的，包括网络钓鱼。通过伪装成可信的第三方，攻击者使用网络钓鱼电子邮件诱使收件人泄露个人数据（访问账户、密码等）和/或银行数据。

垃圾邮件给联网用户和组织的安全带来风险，不仅因为它容易通过互联网和电子通信服务（电子邮件、网站、社交媒体、短信和彩信）传播，还因为它会携带恶意软件。各国正在实施各种技术和监管机制来打击垃圾邮件，并取得了一些成效。

由于互联网的发展，尤其是移动互联网的发展，恶意软件近年来十分猖獗。恶意软件是专为危害计算机或计算机系统而设计的软件的总称[4]。

此外，连接的增加、新技术和用户数量的增长为恶意软件的创建和使用提供了新可乘之机。由于漏洞的出现和恶意软件威胁攻击面的扩大，网络安全问题更加复杂性。除了传统的恶意软件（病毒、蠕虫、特洛伊木马、间谍软件、广告软件、垃圾邮件、rootkits等），还出现了新的、更复杂的恶意软件类型，如僵尸网络、勒索软件和移动恶意软件。

简而言之，抵制垃圾邮件和恶意软件对于用户的安全和企业的发展至关重要。

---

1 国际电联。世界电信发展大会（2017年，布宜诺斯艾利斯）最后报告，第409页。

2 同上，第727-728页。

3 见关于打击垃圾邮件的ITU-T X.1230 to X.1240建议书。

4 见 ITU-T X.1205建议书增补9 (09/2011)。减少信息和通信技术网络中的恶意软件指南的增补。

1.2 垃圾邮件和恶意软件：统计、趋势、演变和对电子通信网络的影响

截至2020年3月，垃圾邮件在全球电子邮件流量中的比例为53.95%[5]。近年来，这一比例大幅下降，从2012年的69%降至2018年的55%，这可能是网络安全意识和技术进步的结果。用户收到的大多数垃圾邮件本质上都是促销性的，包括营销信息。据估计，垃圾邮件每年给企业造成近205亿美元的生产力损失和技术费用。有人认为，如果垃圾邮件继续以目前的速度增长，这一成本可能会上升到每年2570亿美元[6]。

据估计，诈骗和欺诈约占所有垃圾邮件的2.5%，其中很大一部分（92%）可能是恶意的，即与恶意软件有关，意图是伤害用户或出于各种目的损害其信息技术系统[7]。根据另一项估计，2018年发现了约8.1267亿起与恶意软件相关的各种感染[8]。移动恶意软件增加了54%，勒索软件增加了350%，而软件感染造成的经济损失估计每年高达60亿美元（截至2021年）。

由于垃圾邮件和恶意软件会产生大量流量，它们会对网络基础设施和运营商产生重大负面影响，进而影响消费者的用户体验。与垃圾邮件相关的问题，包括由此产生的网络问题，也会损害运营商的声誉。

为了解决这些问题，包括潜在的大量无用流量，并确保网络质量，运营商可能需要开发新的工具，包括投资保护和扩展扩容基础设施。例如，服务提供商可以投资开发反垃圾邮件过滤器，提高他们提供的服务质量。这些都会给运营商和电子通信服务提供商增加必要的额外成本。

1.3 打击垃圾邮件和恶意软件，减轻其影响的方法

1.3.1 打击垃圾邮件和恶意软件，减轻其影响的技术方法

未经请求的电子邮件是恶意软件传播的主要渠道之一。为了有效打击垃圾邮件和恶意软件，必须打破传播链。随着技术的进步，垃圾邮件过滤器和防病毒软件等工具仍然是对抗垃圾邮件和恶意软件的有效机制。通过将这些工具与人工智能（AI）等新技术结合使用，可以提高这些工具的有效性。因此，定期更新垃圾邮件过滤器和防病毒软件对用户来说是一个很好的做法。

在服务提供商中，可以使用诸如发送者策略框架[9]、域名密钥识别邮件[10]、基于域的消息认证、报告和一致性[11]以及实时阻止列表注册等策略来减少这些传输链。

---

5 Statista。2014年1月至2020年9月每月全球垃圾邮件量占电子邮件总量的百分比

6 垃圾邮件的法律。垃圾邮件的统计数据和事实

7 DataProt。你收件箱的另一边是什么 – 2021年20个关于垃圾邮件的统计数据

8 PurpleSec。2021年网络安全统计数据 – 统计、数据和趋势的最终清单

9 Mimecast。关于SPF你需要知道的一切

10 DKIM.org。域名密钥识别邮件（DKIM）

11 DMARC。基于域的消息认证、报告和一致性

电子通信网络运营商和互联网服务提供商还可以采取某些措施来解决与封锁知识产权地址有关的问题。例如，使用资源公钥基础设施的边界网关协议安全性[12]。其他措施还包括：

– 双方认可路由安全规范，旨在共同防止最先进的路由被劫持、IP地址欺骗和其他可能导致分布式拒绝服务（DDoS）攻击、窃听、收入损失、声誉损害等的恶意活动[13]。

– 消息、恶意软件和移动反滥用工作组，定期发布打击滥用信息、所有类型的恶意软件（包括僵尸网络）、垃圾邮件、病毒、拒绝服务（DoS）攻击和任何类型的在线滥用的最佳做法[14]。

打击垃圾邮件和恶意软件的其他举措包括互联网协会[15]、全球移动通信系统协会[16]、垃圾邮件项目[17]、反网络钓鱼工作组[18]和反间谍软件联盟[19]。

1.3.2 打击和减轻垃圾邮件和恶意软件影响的监管方法示例

鉴于打击垃圾邮件和恶意软件所涉及的问题和成本，近年来一些地区和国家通过或加强了现有立法，以便提供工具来加强打击此类攻击。各国一直在根据本国需求制定立法和政策，例如《欧盟通用数据保护条例》（GDPR），该条例要求用户同意收集数据。

另一个示例是《非洲联盟网络安全和个人数据保护公约》（《马拉博公约》），该公约制定了一套标准，鼓励非洲区域的缔约国将其纳入国内立法。《公约》第4条第3款规定，“缔约国应禁止通过任何形式的间接通信，利用未事先同意通过这种手段接受所述直接营销的个人的资料进行直接营销”。然而，该公约在某些条件下授权直接销售；例如，“在下列情况下，允许通过电子邮件进行直接营销：(a) 收件人的详细资料是直接从他/她那里获得的；(b) 收件人同意营销合作伙伴与其联系；(c) 直接营销涉及同一个人或法人团体提供的类似产品或服务”（第4.4节）。

随着《欧盟通用数据保护条例》和《马拉博公约》的实施，我们将能够评估和了解它们在减少垃圾邮件和恶意软件方面的全部效果。

1.3.3 与第3/2号课题下打击和减轻垃圾邮件和恶意软件影响工作相关的文稿

在研究期内，一些国家和国际电联部门成员提供了打击垃圾邮件和恶意软件的其他方法示例：

– 一些撰稿人投稿人描述了他们如何收集关于实时网络安全威胁信息，以便提供信息和建立弹性网络安全战略。在复杂的信息技术世界中，实时数据对于保护信息至关重要。态势感知和网络威胁情报相结合，有助于各国以及公共和私营组织在威胁出

---

12 RFC编辑器。RFC 6480 – 支持安全互联网路由的基础设施。2012年2月。
13 MANRS。相互商定的路由安全规范
14 消息、恶意软件和手机反滥用工作组（M³AAWG）。M³AAWG为什么重要？
15 互联网协会。互联网协会的反垃圾邮件工具包
16 GSMA。GSMA安全
17 Spamhaus。Spamhaus ZEN + DBL + RPZ
18 APWG。通过开展数据交换研究和提高公众意识，统一全球对网络犯罪的应对
19 反间谍软件联盟。互联网，Marketing y Actualidad

现时识别威胁，从而更有效地保护其资源。为了更好地保护组织免受有针对性的攻击和持续的威胁，有必要开发基于安全情报的网络弹性策略[20]。

- 一些撰稿人正在绘制网络犯罪威胁图，以了解垃圾邮件和恶意软件对互联网用户（如网络钓鱼和彩票欺诈）和企业（如未经授权的系统访问和拒绝服务攻击）的各种影响。例如，2017年，科特迪瓦监测到与网络犯罪有关的威胁和违法行为，并由打击网络犯罪平台（PLCC）记录下来，从而提供了有用的定性信息，指导改善消费者和企业教育的业务活动。确定移动货币服务欺诈模式，记录了453起案件，损失近80万美元。移动货币服务欺诈是一种精心设计的骗局，其中，在使用非结构化补充服务数据（USSD）语法将资金转移到移动货币账户或从移动货币账户转移资金后，受害者会接到欺诈者的电话，声称转移存在问题；如果受害者中了骗局，欺诈者能够使用相同的USSD语法从受害者的移动货币账户远程取款[21]。

- 一些撰稿人描述了他们如何创建开放和透明的流程，以确定和促进相关利益攸关方采取行动，从而显著减少自动和分布式攻击（如僵尸网络）构成的威胁。随着新僵尸网络的出现，它可以对网络造成巨大的压力，每秒使用超过1TB的数据，传统的基于网络访问提供商预留资源的DDoS缓解技术不再有效。减轻来自自动化和分布式网络攻击的威胁需要公共和私营部门之间的持续合作[22]。

- 采取一些简单的步骤可以帮助公司有效地保护自己免受软件攻击的威胁。在最近的一份勒索软件咨询中，英国国家网络安全中心（NCSC）推荐了一些简单的风险缓解技术，例如：

  - （通过快速更新、补丁和定期扫描）保持设备和网络处于最新状态；
  - 防止和检测公司网络中的横向移动；
  - 使用病毒扫描器；
  - 备份所有文档[23]。

  关于完整而详细的建议清单，可查阅NCSC网站[24]。

- 一些撰稿人描述了他们如何创建一个适应不断变化的需求的灵活的国家网络安全框架。例如，英国启动了主动网络防御方案，注重采取积极的技术步骤，为所有人改善在线环境。该方案为政府网络带来了显著的、可衡量的好处。该项目已在英国的公共服务网络中实施，以展示实际效果和可能的后续步骤[25]。为持续应对这些挑战，英国在该方案启动一年后对其进行了完善[26]。

---

20 来自（美国）赛门铁克公司的ITU-D第2研究组第2/167号文件
21 来自科特迪瓦的ITU-D第2研究组第2/174号文件
22 来自美国的ITU-D第2研究组第SG2RGQ/153号文件和附件
23 来自英国的ITU-D第2研究组第SG2RGQ/155号文件
24 英国国家网络安全中心（NCSC）。指南：缓解恶意软件和勒索软件的攻击。
25 来自英国的ITU-D第2研究组第SG2RGQ/55号文件
26 来自英国的ITU-D第2研究组第SG2RGQ/175号文件

– 一些撰稿人正在采取措施，教育弱势群体(如残疾人)他们的风险水平增加。垃圾邮件发送者和黑客正在使用越来越复杂的技术来确定潜在的劫持对象是否有残疾。在某些情况下，劫持者利用一个人的残疾作为手段从劫持的电子邮件账户冒充该人[27]。

– 一些撰稿人正在启用针对网络钓鱼邮件的报告服务。众包收集恶意电子邮件，并对其包含的域和其他实体采取行动，是减少网络犯罪和欺诈的有效工具。例如，在可疑电子邮件报告服务运行的头四个月，英国国家网络安全中心和伦敦市警察局清除了公众报告的16 000多项在线威胁[28]。

[27] 来自包容性信息和通信技术全球倡议（G3ict）的ITU-D第2研究组第2/71号文件

[28] 来自英国的ITU-D第2研究组第SG2RGQ/234号文件

第2章 – 改善国家网络安全态势：认识提高和能力建设机会

近年来，信息通信技术经历了快速增长和创新。世界范围内，信息通信技术在帮助各国扩大数字经济和支持社会繁荣方面发挥着重要作用。此外，新冠疫情大流行表明，人们在日常生活中越来越依赖信息通信技术。有鉴于此，各国继续采取重要步骤，改善和加强其国家网络安全态势，防范网络安全风险和挑战至关重要。

本章审查了改善国家网络安全态势的关键重点领域，包括：

- 建立国家相关的网络安全机构
- 计算机应急响应团队（CERT）/计算机安全事件响应团队（CSIRT）/计算机事件响应团队（CIRT）
- 网络安全宣传活动
- 网络安全风险管理框架
- 公私伙伴关系
- 其他能力建设举措。

在本研究期内，有些实体就这些问题提供了意见。关于各成员国、各组织、私营部门和民间团体在国家、区域和国际层面正在开展的相关网络安全活动的概要，请参阅**附件1**。关于其中实体提交的相关最佳做法和经验教训清单，请参见**附件2**。

2.1 组建国家相关网络安全机构

随着信息通信技术的新进步和创新，网络安全风险和挑战也在增加。各国政府需要不断评估和改进其国家网络安全态势和战略，包括组建国家相关网络安全机构以应对这些挑战。在本研究期内，成员国介绍了它们组建这种机构的方式。各国家根据其国内治理结构、规则、条例和政策采取不同的方法。

这些网络安全机构的专业知识和工作重点不尽相同，但通常其关键职能大体相同，包括制定和协调监管政策；制定和实施网络安全宣传活动；向用户（从大型组织到个人和小型企业）提供最新信息；发布关于网络安全事件的声明和指南。鉴于网络安全涉及面十分广泛，各国政府必须促进不同机构和实体之间以及公共和私营部门之间的协调与合作。

例如，在英国，国家网络安全中心会同政府他相关部门开展工作，大幅减少勒索软件攻击的影响[29]。在发生攻击时，建议有关组织与国家犯罪署、网络事件响应认证公司或网络安全信息共享合作伙伴取得联系。国家网络安全中心与国家犯罪署合作，领导英国

[29] 来自英国的ITU-D第2研究组第SG2RGQ/155号文件

应对WannaCry勒索软件攻击。在每次事件过程中，该中心为大型组织以及家庭用户和小企业发布声明和指南。最新信息也通过该中心的推特账户（@NCSC）公布。

巴西概述了其国家网络安全战略，该战略由巴西总统批准，并于2020年2月公布[30]。这一前瞻性战略构成了联邦政府2020-2023年的网络安全愿景，为此，巴西采取了一种详尽和全面的方法，包括政府、私营部门和学术界等众多利益攸关方的参与。随着E-Ciber的批准，巴西补齐了以前缺位的法律框架。根据E-Ciber，巴西制定了10项战略行动，其中每一项都列出了措施和倡议。这些战略行动包括：

- 加强网络安全治理；
- 建立国家网络安全集中治理模式；
- 完善国家网络安全法律框架；
- 扩大巴西在网络安全领域的国际合作。

在贝宁，不同的政府部门参与了该国信息通信技术的管理[31]。信息系统和服务局（ASSI），其前身是贝宁信息技术和通信局（ABETIC），是该国负责落实发展安全数字信息系统和服务方案和项目运作和制定战略的国家机构。其负责的主要活动包括：

- 落实智慧政府、电子商务旗舰项目；
- 起草、更新和实际落实国家信息系统总计划；
- 确保国家信息系统和服务在技术、应用和财政上的一致性；
- 确保国家和重要基础设施运营方关键信息和数据的托管、控制和安全访问。

在乍得，2015年2月成立的国家信息安全和电子认证机构直接向总统办公室报告[32]。该机构自2018年1月开始运作，拥有广泛的权力和职能，包括全国各地信息系统和网络的安全。

英国还分享了其为消费者物联网（IoT）设备实施良好安全做法的最新案例研究，特别是通过：

- 颁布了《消费者物联网安全业务守则》，其中列出了13项宏观原则（也有德语、西班牙语、法语、日语、韩语、普通话和葡萄牙语版本）；
- 就拟议的法律法规开展公开协商；
- 支持由欧洲电信标准协会（ETSI）发布的第一个全球适用的物联网安全标准ETSI·EN 303 645[33]。许多组织已经围绕标准及其前身ETSI TS 103 645制定了各自的产品和认证方案；

30 来自巴西的ITU-D第2研究组第SG2RGQ/216号文件
31 来自贝宁的ITU-D第2研究组第2/152号文件
32 来自乍得的ITU-D第2研究组第2/136号文件
33 欧洲电信标准协会（ETSI）。ETSI EN 303 645标准。面向消费者物联网的网络安全：基准要求。

– 就英国监管提案征求意见，收集利益攸关方对拟议范围、义务、安全要求和执法方法的反馈意见；

– 委托数字、文化、媒体和体育部以及英国国家网络安全中心为物联网制造商联合编制指导材料和组织在线网络研讨会，这些活动在全球各时区举办多次；

– 维护现行标准的格局地图，并支持各组织在物联网中实施好的做法[34]。

2.2 计算机应急响应团队（CERTs）/计算机安全事件响应团队（CSIRTs）/计算机事件响应团队（CIRTs）

国家事件应对能力（以应急反应小组/综合反应小组/综合反应小组的形式）是应对网络安全业务挑战的重要手段。这种能力有助于协调网络安全信息和应对安全事件。在本研究期内，研究组收到了国际电联成员国和部门成员关于这一专题提交的关键文稿，其中许多成员都认为，国家应急反应小组/通信和信息技术中心/通信和信息技术中心应成为网络安全问题的主要联络点和事故应对的协调机构。

例如，不丹计算机事件应对小组（BtCIRT）成立于2016年4月，旨在通过促进网络安全信息的协调和建立国家处理计算机安全事件的能力来加强该国的网络安全[35]。BtCIRT是信息和通信部信息技术和电信司下属的一个单位。该中心按其授权承担网络安全问题的国家联络点工作，在国际论坛上代表国家。由一个组织来协调所有网络安全举措，可确保工作或发展不会重复。由于大多数以网络安全为重点的国际论坛和团体都与拥有国家授权的中心联系，因此各国政府必须指定一个CIRT或单一指定组织来领导国家网络安全倡议和计划。

虽然不丹网络安全研究中心是作为网络安全相关问题的联络点建立的，但该小组一直难以获得利益攸关方的信任，主要是因为其技术能力有限，而且是一个相对较新的小组。此外，电信运营商和银行等大型企业已经拥有强大的信息通信技术基础设施和技术能力，这使得政府与此类大型组织之间的合作具有挑战性。利益攸关方之间的协作与合作，特别是互联网服务提供商和中心，对于为互联网用户提供统一的安全解决方案至关重要。不丹向国际组织求助，帮助建设BtCIRT的关键技术能力。

最后，立陶宛公司NRD网络安全公司提议，除了作为网络安全事件的主要联络点和反应协调部门之外，国家和行业CSIRT还应作为促进者或催化剂，提高本国独立和分布式网络威胁的应对能力[36]。

2.3 宣传活动

世界各地的各种利益攸关方 – 从政府和商业实体到社区组织和普通个人 – 广泛使用信息通信技术。然而，许多用户并没有完全意识到他们在使用中所涉及的网络安全风险。对一些发展中国家来说，最大的挑战是缺乏用户意识。在本研究期期间收到的文稿

[34] 来自英国的ITU-D第2研究组第SG2RGQ/241号文件
[35] 来自不丹的ITU-D第2研究组第SG2RGQ/79号文件
[36] 来自（立陶宛）NRD网络安全（CS）的ITU-D第2研究组第2/172号文件

中，人们普遍认为，网络安全意识宣传活动在应对这些挑战方面发挥着重要作用。这些活动的主要目的是鼓励人们在网上采取安全行为。

国家和企业正在寻找创造性的方法来开展有效的活动，包括如何接触到广泛的用户。

例如，墨西哥分享了其开发和进行互联网用户调查的经验，该调查可用于指导提高网络安全意识宣传活动的各种方法[37]。

一些国家利用调查来确定人们的主要关切，并根据调查结果开展有针对性的宣传活动。根据其经验，墨西哥还确定了以下经验教训：

- 安装和更新防病毒保护；
- 定期更改密码，并确保密码是强密码（即使用数字、字母和特殊字符的组合）；
- 定期备份数据；
- 只连接到安全的公共网络。

在另一个示例中，不丹的BtCIRT制定了专门的宣传方案，以满足全国普通最终用户对日常职业和个人交往中的网络安全需求[38]。向参与者展示了网络攻击是如何通过社交工程和网络钓鱼诈骗实施的，如何使用电子邮件和社交媒体服务进行安全通信，以及常见的威胁和补救措施。不丹的宣传方案成功的让用户意识到安全风险，并收到了积极的反馈。虽然目前的工作重点是政府官员，但BtCIRT团队正计划将儿童和其他弱势用户群体纳入进来。

不丹提供的另一个有创意的示例是由信息和通信部信息技术和电信司组织的年度国家网站竞赛[39]。所有政府网站都提交给竞赛，根据以下核心标准选出国内最佳网站：

- 可用性和可靠性；
- 内容和实时性；
- 安全和正常运行时间；
- 外观；
- 互动设计。

同样，2019年11月，巴西通过巴西国家电信局（Anatel）发起了#ConexãoSegura（“安全连接”）网络安全宣传活动[40]。该活动为消费者提供了保护个人数据和创建安全密码的建议。促使这场活动诱因是消费者对欺诈企图的投诉以及对如何保护个人数据的疑虑。随着新冠疫情的到来和新骗局的激增，发布有关新冠疫情欺诈和骗局的新帖子来帮助用户。这些帖子还通过Anatel的社交媒体网络分享以及Facebook、Twitter、Instagram和LinkedIn进行转发。从这场活动中得出的主要最佳做法是：

---

37 来自墨西哥的ITU-D第2研究组第2/165号文件
38 来自不丹的ITU-D第2研究组第SG2RGQ/79号文件
39 来自不丹的ITU-D第2研究组第SG2RGQ/135号文件
40 来自巴西的ITU-D第2研究组第SG2RGQ/215号文件

– 使用移动应用提供的所有安全选项，如双元素认证；

– 通过组合大小写字母、数字和特殊字符来创建强而安全的密码；

– 警惕附有发票的电子邮件和信息，并经常联系公司的客户服务部以核实文件是否真实；

– 在接听莫名电话时不提供个人信息或密码[41]。

英国提供了一份关于中小企业网络安全复原力最佳做法的案例研究，概述了为提高全国各组织的网络复原力所做的努力[42]。这种努力的一个示例是网络意识宣传活动，该活动不仅仅是提高认识，还要努力推广基本的网络安全行为。该活动针对公众和小企业，于2020年4月启动，为应对新冠疫情造成的不断变化的网络威胁进行了快速调整。该活动推广可行的缓解措施，并对于如何安全地居家办公、将业务移至网上和使用视频会议提出新指南。其他工具包括：

– 小企业指南：网络安全；

– 《小企业指南：应对和恢复》，该指南提供了一个连续性计划，以帮助中小企业为网络事故做好准备并降低潜在影响；

– 练习题，这是一个免费的在线工具，帮助中小企业测试其网络应变能力，完成微型课程，而不需要大量的技术知识；

– 新冠疫情指南，帮助企业在适应疫情保持安全，涵盖居家工作和将业务迁移上网等主题。

英国还提供了其政府支持的认证计划“网络基础”的详情，该计划旨在保护企业免受商品网络攻击，而不要求它们遵守多种复杂标准。网络安全要素是所有组织都可以做到的，即使是那些没有网络安全知识或专门网络团队的组织也可以做到。

2.4 网络安保风险框架

网络安全风险框架对政府和非政府组织都至关重要。这些通常是自愿的框架，为管理数字风险提供指导方针和最佳做法。在本研究期期间，研究组收到了各实体提供的关于网络安全风险框架的不同实例和方法意见。

例如，美国国家标准与技术研究院（NIST）改善关键基础设施网络安全的框架[43]。该框架是为在不同经济部门中运行的各种规模的企业设计的自愿网络风险管理一种业务驱动的主动框架。框架为评价网络风险提供共同起点和语言，并且适应性强，无论规模、网络安全风险程度或网络安全复杂度，都能使组织机构实施风险管理原则和最优方法，从而改善关键基础设施的安全性和恢复力。

---

41 更多关于Anatel安全连接活动的信息，请访问以下网站：https://www.anatel.gov.br/consumidor/component/content/article/109-manchetes/960-conexaoseguro-confira-dicas-para-proteger-dados-pessoais .

42 来自英国的ITU-D第2研究组第SG2RGQ/272号文件

43 来自美国的ITU-D第2研究组第SG2RGQ/151号文件

框架的建立是网络安全风险管理公私合作的一个成功案例。框架历经一年，有来自产业、学术界、政府及国际伙伴的超过3 000名成员的自愿参与了开发过程。

框架借鉴了现有的在网络威胁中被证明能有效保护IT系统和商业机密和保护个人隐私及公民权利的国际标准、指导方针和产业最优方法，通过风险管理促进关键基础设施的保护。另外，框架提供了组织方法的结构和支持使用标准和实践的工具。因为它参照全球认可的网络安全标准，框架也具有一定的灵活性，可用作管理网络风险的国际模式。

根据利益相关方的反馈，NIST对1.1版的框架进行了以下更新：

- 宣布该框架适用于“技术”，至少包括信息技术、操作技术、网络物理系统和物联网；
- 强化了该框架应用于供应链风险管理的指导；
- 总结了组织自我评估框架中提供的衡量标准的相关性和实用性；
- 提供了关于网络安全风险自我评估的补充信息；
- 更加重视授权、认证、身份验证和漏洞披露要求；
- 对参考资料进行了行政更新，以反映私营和公共组织在标准和准则方面的进步。

此外，在不丹，皇家货币管理局（中央银行）发布了一项指令，推动落实金融机构网络安全框架，以提高银行系统应对未知和先进网络风险的能力[44]。该指令涵盖以下方面：

- 所有成员银行必须努力遵守支付卡行业数据安全标准，保护持卡人数据环境。此外，银行应实施关于信息安全管理系统的ISO/IEC 27001:2013标准，作为其自身的网络安全措施的补充。
- 指令概述了建立金融机构网络反应小组促进银行和皇家货币管理局之间积极合作和有效共享网络安全相关信息的必要性。该小组将积极监测网络威胁，规划和协调反威胁措施，防范网络安全风险，并随时向相关主管或当局报告网络安全事件。最近，由皇家货币管理局牵头成立了一个银行网络团队。
- 成员银行还必须落实相关的网络安全控制框架和应对措施，并立即采取措施确保基本信息安全。

在另一个示例中，中国利用三级递进复杂指标制定了一个评估指数，衡量规划、发展和实施网络安全方面的国家目标[45]。第一级评估五个指标：

- 政策：国家战略、立法、政府机构、国际合作
- 产业：市场化条件下的网络安全产业发展水平，包括发展环境、规模、企业竞争力、自主化能力等

44 来自不丹的ITU-D第2研究组第SG2RGQ/135号文件

45 来自中国的ITU-D第2研究组第2/155号文件

- 技术：网络安全技术研发与应用水平，包括科研项目、投入、技术标准、人才培养
- 能力：网络安全保护和威胁防御水平，包括风险感知、安全防护、应急处置、主动防御等
- 资源：支撑能力建设所必要的资源掌握情况，包括网络基础资源、安全意识、国际影响力等

该指数还包括19个二级指标和53个三级指标。在该指数的评分系统下，每个指标值0到1分，最高分为53分。每项指标的计算依据国家和国际网站以及研究机构发布的官方公开信息。

2.5 公私伙伴关系

仅靠政府部门无法改善国家网络安全态势。网络安全的努力和项目的成功需要公共和私营部门实体之间建立强有力的伙伴关系。

在美国，国家标准和技术研究院通过公私伙伴的合作，制定了《改善关键基础设施网络安全框架》[46]。正如第2.4节更详细指出的那样，研究所注意确保所有利益攸关方参与更新工作，鼓励最大限度地遵守该框架。通过利益攸关方的参与将他们的反馈纳入框架的1.1版，利益攸关方更有可能遵守和实施框架所包含的最佳做法、准则和标准。

在韩国，科学和信息通信技术部与包括学术界、工业界和公共组织在内的相关利益攸关方协商，为私营部门制定了2019年国家网络安全基本计划[47]。该计划设定了两个目标：确保安全的网络空间和发展信息安全产业。为此，主要战略项目的宗旨是扩大网络安全网，促进信息安全产业，加强信息安全基础设施。

鉴于信息通信技术环境快速变化，该部打算每年对该计划进行更新。韩国公私协商理事会每年举行两次会议，监测计划的进展并确定需要改进的领域。

如第2.1节所述，巴西的国家网络安全战略，E-Ciber，再次证明了公私伙伴关系（PPP）在制定全面的国家网络安全战略方面的重要性。E-Ciber所载的关键战略行动突出了公私伙伴关系，其中包括促进在公共、私营部门和民间团体之间建立合作、参与、安全和值得信赖的环境，拓展公共和私营部门、学术界和民间团体之间的网络安全伙伴关系。

为进一步说明公私伙伴关系，巴西概述了其在2018年举行全国网络演习的经验，该演习被称为网络卫士演习，重点是国家关键基础设施[48]。2019年，巴西进行了一次后续演习，大大扩大了参与者的范围，纳入了国防部、司法部和外交部、机构安全办公室、军队、联邦政府机构，如Anatel、国家CSIRT、巴西中央银行、公共和私营银行、核、电气和电信公司、学术研究人员的代表，并邀请了区域和国际观察员。

---

[46] 来自美国的ITU-D第2研究组第SG2RGQ/151号文件
[47] 来自韩国的ITU-D第2研究组第2/168号文件
[48] 来自巴西的ITU-D第2研究组第SG2RGQ/214号文件

公私伙伴关系的其他示例还有CERT/CSIRT/CIRT。通过这些团队，公共机构和私营部门能够共同努力解决网络安全事件。然而，协作和信任对于确保这些团队有效性的关键。

2.6 其他能力建设措施/举措

2.6.1 建立网络安全教育机构

认识到网络安全培训和教育的投资对应对日益增长的网络安全挑战的必要性，许多国家政府建立了教育机构培训下一代网络安全专家。在本研究期内，国际电联成员国提出意见认为，需要在这一领域做出努力，包括加强公共利益攸关方、大学和研究中心之间的关系。

例如，2015年，乍得建立了国家信息通信技术高等学院，清楚地表明该国最高当局具有建立高等信息通信技术教育体系的政治意愿（包括设立网络安全、网络、电信等学位）[49]。

同样，塞内加尔建立了以区域为重点的国家网络安全学校（ENC），培养该区域数字生态系统的决策者、高级别防务人员等的能力和认识[50]。

学校的主要任务是提供：

– 对国家官员、塞内加尔和外国工作人员、学生以及公共和私营网络安全部门人员进行培训和提高认识，提高对风险和威胁的认识；

– 定期培训，帮助专业的CERT/CSIRT员工处置最复杂的网络攻击；

– 定期培训国家和次区域机构的工作人员，传授预防、防范、应对和事故恢复的能力和知识。

2.6.2 其他能力建设举措

在本研究期内，电信发展局（BDT）网络安全协调中心定期更新电信发展局的工作计划，包括其各种能力建设举措。该局一直与各组织和实体合作，为发展中国家提供能力建设培训，包括开展网络演习演练、协助建立CSIRT和举办培训班。成员国和部门成员的文稿也强调了这些努力。更多信息见**附件1**。

[49] 来自乍得的ITU-D第2研究组第2/136号文件

[50] 来自塞内加尔的ITU-D第2研究组第SG2RGQ/146号文件

第3章 – 保护上网儿童

3.1 概述

现代互联网不再仅仅是一个知识库 – 如网络1.0时代的一个“庞杂的图书馆”。它已经成为包括孩子在内的所有人使用的交流平台。事实上，根据联合国儿童基金会（UNICEF）的数据，儿童占全球互联网人口的三分之一[51]。

儿童面临的网络威胁发生了本质的变化。早期的威胁完全是基于信息的，例如，获取有关毒品、色情或极端主义运动的信息，而目前的威胁本质上是行为性的，如社交冷淡、赌博成瘾、无节制的消费、虚拟欺凌、泄露个人数据和危险的熟人。

在过去的10年里，技术界一直在积极探索保护儿童免受包含不适当信息的网站攻击的方法，但开发者和家长现在面临着一个新的挑战，即如何以适当的方式将年轻用户引入数字空间，以及如何快速控制和纠正虚拟行为。全球已形成共识，随着互联网技术的迅速发展，儿童保护问题自然延伸到网络空间。儿童在使用数字设备和互联网时，网络空间的安全至关重要。

WTDC-17成员国通过《布宜诺斯艾利斯宣言》指出，“电信/ICT提供的机遇应该得到充分利用，以确保电信/ICT和创新的公平获取，这些创新可促进可持续社会经济发展、脱贫、创造就业机会、性别平等、保护上网儿童、创业精神并促进数字包容性和全民赋能的实现”[52]。

国际电联全权代表会议第179号决议（2018年，迪拜，修订版）和WTDC第67号决议（2017年，布宜诺斯艾利斯，修订版）规定了国际电联和国际电联发展部在保护上网儿童方面将发挥的作用。

正如新冠疫情所显示的那样，攻击者和犯罪网络的行为方式不断演进，犯罪分子正在利用许多儿童比平时花更多时间上网这一事实。在这种情况下，发布2020版《保护上网儿童指南》，保护孩子们的福祉、品格和安全，可谓及是时雨[53]。

该《指南》由国际电联和一个工作组共同撰写，该工作组由来自活跃在信息通信技术和儿童（上网）保护问题领域的主要机构的撰稿人组成。该《指南》针对如何为儿童和青少年营造安全的上网环境并增强他们的能力，为所有相关利益攸关方提供了一套全方位建议。该《指南》的目的是提高对保护上网儿童范围的认识，提供资源和工具，帮助儿童及其家庭学习数字技能，并帮助行业和政府利益攸关方制定企业和国家保护上网儿童政策和战略。该《指南》的对象是儿童、家长、教育工作者、企业和决策者，意在提供一个蓝图，可根据本国或当地习俗和法律进行调整。

---

51 联合国儿童基金会。2017年世界儿童状况。2017年12月。

52 国际电联。世界电信发展会议（2017年，布宜诺斯艾利斯）。《布宜诺斯艾利斯宣言》。2017年10月。

53 国际电联。《保护上网儿童指南》

根据国际电联全权代表大会第71号决议（2018年，迪拜修，订版）中规定的国际电联战略计划，国际电联发展部门的目标之一是“促进电信/ICT和应用的发展和使用，使人们和社会能够支持可持续发展”（§ D.4）。尤其是，ITU-D必须提供“针对年轻女性和女性以及有具体需求人群（老年人、青年、儿童和原住民）的数字包容性产品及服务，例如提高人们对数字包容性战略、政策和做法的认识，开发数字技能、工具包和导则，并通过论坛讨论共享做法与战略。”其目的首先是支持保护上网儿童（§ D.4-3）。

第3/2号课题的职责范围第2(d)项规定了ITU-D及其成员的保护上网儿童活动：

d) 继续从成员国收集网络安全和保护上网儿童方面的经验，并在这些经验中确定并研究其共同主题，同时利用这些信息编写导则，帮助成员国制定有效的数字环境安全机制。

3.2 国际电联成员国的最佳做法和共同趋势

在本研究期内，成员国开展的主要保护上网儿童活动侧重于提高认识、制定法规和开展专题调研。

提高认识

网络空间保护儿童涉及许多方面，不仅需要工具和平台，还需要适当的数据。应利用文化项目在全社会传播这些资源。

例如，伊朗信息技术组织开发了儿童与互联网（KOVA）项目，以保护网络空间的儿童，该项目被2018年信息社会世界高峰会议奖竞赛选为冠军项目。

鉴于近年来互联网基础设施的快速发展以及包括儿童在内的年轻互联网用户数量增多，伊朗政府于2016年启动了一项保护互联网儿童的国家方案。作为该方案的一部分，信息通信技术部启动了KOVA项目，以提高儿童及其父母对互联网风险以及如何保护儿童免受其害的认识。该项目的主要目标是：

- 确定网络空间中对儿童的最大威胁，并提供解决方案和法律保护服务；
- 使小学生、中学生、教师和家长意识到不同年龄的儿童面临的各种威胁；
- 帮助儿童和青少年安全可靠地使用社交媒体和互联网；
- 回答了儿童、青少年、教育工作者和家长提出的关于网络空间安全和安保挑战的问题。

为了实现该项目的目标，使用了各种各样的工具和方法（如戏剧、电影和动画）对儿童进行在线安全教育。在项目的第一阶段，900所学校的20多万名学生接受了培训，第二阶段的目标是达到4000所学校[54]。

在不丹，自2016年以来，由于接入更加方便、连接更加便宜、智能手机更加普及，互联网用户数量增加了28%以上。大多数学生都可以使用智能手机，因而增加了安全事

[54] 来自（伊朗伊斯兰共和国）伊朗科技大学的ITU-D第2研究组第2/82号文件

故的风险。不丹还没有关于网络安全的学校课程，因为互联网和移动设备使用的增加是最近的趋势。然而，重要的是，各国政府应通过将网络安全纳入学校课程来迎接不断变化的时代。不丹的私立大学已经开始探索如何提供相关的学位课程，特别是网络安全方面的课程。学龄儿童需要意识到网络风险，因为他们更容易受到网络钓鱼和在线游戏形式的攻击[55]。

针对这些考虑，在研究了儿童的上网习惯和行为后，不丹正在制作动画视频，内容包括贩卖儿童、网络欺凌、隐私和网络游戏安全等主题，并将在国家电视台播出。它还在制作海报和小册子，其中包括针对学生的网络安全最佳做法，这些海报和小册子将被分发给该国的各个学校。不丹还在组建一个由各相关机构代表组成的国家任务组，以制定该国的相关保护上网儿童准则[56]。

中国每年举办全国网络安全宣传周，通过展览、论坛、竞赛、讲座、专题宣传日等活动，提高网络安全意识，提高全民网络保护技能。例如，根据不同群体的信息技术技能水平，如中小学生、老年人和特殊群体（如残疾人），举办网络安全讲座，分享知识和技能[57]。

美国为父母和老师们提供有关儿童和青少年实践的信息，包括：您发布的内容可以持续一生！请留意正在共享的内容！小心透露过多的个人信息！发布他人信息时，注意己所欲者，亦施于人！通过限制可以查看和共享信息的人来掌握您的在线生活！了解正在收集哪些数据！[58]

监管

鉴于信息技术的广泛普及，各国政府正在采取认真的监管措施，以确保所有能够上网的公民的安全，特别是未成年人。尽管全球网络安全立法略有不同，但问题的根源是相同的。

制定此类法规的主要原因之一是学龄前和小学年龄的儿童在互联网上特别容易受到伤害，他们很容易成为网络掠夺者（通过互联网对未成年人进行性骚扰的人）、羞辱和在线诱导（陌生人为一己私利获取儿童的信任）以及滥用个人数据的受害者。

儿童逐渐成为隐私泄露和身份盗窃风险最高危的群体。因此，保护儿童的个人信息迫在眉睫。

例如，中国最近颁布了儿童个人信息网络保护特别规定，该规定明确了对收集、存储、使用、转移和披露儿童个人信息的全周期管理[59]。规定提出专门保护、明确的原则及合作治理，从而为儿童健康成长创造有利且有益的网络环境。出其他外，特别保护涵盖童个人信息删除权和非披露，而原则涉及合法正当必要、知情同意、目的明确、安全保障、依法利用。该规定主要适用于保护14岁以下儿童的个人信息。

---

55 来自不丹的ITU-D第2研究组第SG2RGQ/79号文件
56 来自不丹的ITU-D第2研究组第2/385号文件
57 来自中国的ITU-D第2研究组第2/286号文件
58 来自美国的ITU-D第2研究组第2/400号文件
59 来自中国的ITU-D第2研究组第SG2RGQ/179号文件

俄罗斯联邦2010年12月颁布了关于保护儿童免受对其健康和发展有害的信息的法律，确保未成年人的信息安全，并且确立向儿童传播信息内容的条件和程序[60]。

俄罗斯联邦《媒体法》禁止在媒体或任何信息通信网络（即互联网）上传播有关任何非法行为（或不作为）的未成年受害者信息，包括：

- 未成年人或其父母或其他法定代表人的姓氏、名字或教名
- 以及照片或视频图像；
- 未成年人的生日；
- 未成年人声音的音频记录；
- 未成年人的住所或临时地址；
- 未成年人学习或工作的地点；
- 可用于直接或间接确定未成年人身份的任何其它信息[61]。

专题调查

国际电联已为不丹起草国家网络安全战略提供了技术援助[62]。在此过程中，对126名学生（平均年龄为16岁）进行了调查，其中使用了多项选择题来评估互联网使用情况、网络欺凌等安全事件以及计算机病毒泛滥或学生犯罪情况。

调查显示，学生们正在大量使用互联网。几乎所有参与调查的学生都使用互联网，超过40%的学生每天使用互联网超过两小时。网络安全对学生来说是一个紧迫的话题：尽管近40%的学生经历过恶意软件感染，但只有约10%的学生报告说他们使用了防病毒软件。

关于网络安全教育，学校仍然是学生的重要知识来源。近40%的学生表示，他们在学校学到了网络安全知识。

学生们还接触到网络犯罪和其他有害活动。除了计算机病毒之外，超过10%的被调查学生曾遭受网络欺凌，25%的学生曾在网上被陌生人联系过。问卷还包含一个关于非法或不适当行为的部分，显示约35%的学生发送过可被视为网络欺凌的恶意或有害信息。大约相同数量的学生尝试或成功闯入受保护的无线网络。

由于本次初步调查范围有限，不丹在国家层面进行了另一项关于上网儿童安全和保护的调查。该项调查是联合国教科文组织曼谷办事处（UNESCO Bangkok）在韩国信托基金（KFIT）的支持下发起的亚太区域数字儿童（DKAP）项目的一部分。调查对来自全国45所学校的2381名12至17岁的学生，提出了112个问题，以确定网络安全意识、威胁和预防措施的水平。研究发现，大多数学生（81%）可以在家中使用智能手机。大多数学

60 来自俄罗斯联邦的ITU-D第2研究组第2/264号文件

61 见联邦法案第2124号第4条，https://digital.gov.ru/ru/documents/6406/ [仅俄文]；来自俄罗斯联邦的ITU-D第2研究组第2/264号文件

62 来自不丹的ITU-D第2研究组第SG2RGQ/135号文件

生每天平均花一到两个小时上网。此外，54% 的学生缺乏区分可靠信息与不可靠信息的知识。大约 49% 的学生担心有人滥用他们的个人信息。

一小部分学生（10%）通过提供虚假信息、欺凌他人和登录他人账户来规避年龄限制应用。此外，85%的学生愿意在网上结交新朋友，68%的学生不介意与来自不同地方或背景的人交谈。该调查引发了安全方面的担忧，因为51%的学生曾与他们最初在网上认识的陌生人见面，另有22.8%的学生对认识陌生人持开放态度，女性比男性更愿意与陌生人见面[63]。

在科特迪瓦，PLCC对阿比让三所高中的200名年轻人进行了调查，以分析儿童的网上行为，确定风险，并提出打击网络污秽的有效安全战略[64]。

总体而言，83%的调查受访者报告说他们使用互联网。其余受访者不使用互联网的主要原因是智能手机和终端的费用高。对于15-18岁的儿童来说，电视已被降至次要地位，86.3%的儿童拥有社交媒体账户。这个年龄段的人更喜欢通过智能手机上网。据报道，暴力图像和电影是网上负面体验的主要来源，其次是盗版，最后是侮辱和威胁。为数不多的受访者报告了具有性内涵的负面经历。有些受访者报告称，他们因露骨的性视频而被勒索。

根据调查，对儿童最有害的潜在体验是：

- 病毒、蠕虫、垃圾邮件或黑客（24%）
- 性视频（7.5%）
- 暴力图像或视频（28.6%）
- 未经事先同意使用照片（7.5%）
- 侮辱、恶意或威胁（19.5%）
- 身份盗窃案（6.7%）
- 与陌生人接触（4.51%）
- 骗局（0.75%）
- 性勒索（0.75%）

国际电联为成员国提供保护上网儿童的支持

2018年4月4日至6日，国际电联与A. S.波波夫敖德萨国家电信研究院合作，在乌克兰敖德萨举行欧洲和独立国家联合体（独联体）网络安全和保护上网儿童区域讲习班[65]。所有文件的最终版本（包括议程、报告、结论和建议、与会者名单、专题介绍和照片）都

63 来自不丹的ITU-D第2研究组第2/385号文件
64 来自科特迪瓦的ITU-D第2研究组第2/201号文件
65 来自（乌克兰）A.S. Popov敖德萨国家电信学院的ITU-D第2研究组第2/75号文件

公布在研究院网站[66]和国际电联网站上[67]。参与讲习班的14个成员国代表得出结论认为，欧洲和独联体区域需要加强合作，以便优化利用现有资源并取得实际成果，包括通过翻译关于网络安全和保护上网儿童的培训材料。研讨会与会者提出的结论和建议载于成果文件[68]。

保护上网儿童是国际电联欧洲区域性举措的重点领域之一，该倡议旨在建立使用电信/信息通信技术的信心和安全。为响应成员国对保护上网儿童倡议路线图的要求，国际电联在区域性举措覆盖的各国政府中开展了一项调查，解决了与数字空间中儿童和青年使用的所有技术平台的当前政策和做法有关的广泛问题。该调查于2009年首次在所有成员国中进行，修改后2016年在中欧、波罗的海和巴尔干成员国中进行。

根据调查结果，BDT于2017年发布了欧洲保护上网儿童国家活动的区域回顾，说明参与国在保护上网儿童领域的政策制定、通过、实施和监测方面的现状[69]。介绍了阿尔巴尼亚、波斯尼亚和黑塞哥维那、保加利亚、塞浦路斯、克罗地亚、爱沙尼亚、芬兰、希腊、匈牙利、拉脱维亚、列支敦士登、立陶宛、北马其顿、摩纳哥、黑山、波兰、斯洛伐克、捷克共和国、罗马尼亚、塞尔维亚、斯洛文尼亚和土耳其当现行做法。

国际电联理事会保护上网儿童工作组（CWG-COP）根据国际电联理事会第1306号决议（2009年）以及第179号决议（迪拜，2018年，修订版）开展工作，全权代表会议在该决议中决定，国际电联应继续将保护上网儿童倡议作为提高对上网儿童安全问题认识的平台；继续向成员国，特别是发展中国家提供援助和支持，以制定和实施该倡议的路线图；并与相关利益攸关方合作，继续协调该倡议[70]。

为审议第3/2号课题，提供了分别于2019年9月26日、2020年2月4日和2021年1月26日在日内瓦和远程举行的CWG-COP会议第15、16和17次会议的信息[71, 72]。

会议上介绍了一下文件：

- 国际电联《保护上网儿童指南》[73]
- 介绍青年在线咨询结果[74]
- 介绍国际电联保护上网儿童工作和活动[75]

---

66 A.S. Popov敖德萨国家电信学院。国际电联欧洲和独联体区域讲习班 – 网络安全和保护上网儿童，乌克兰敖德萨，2018年4月4-6日。

67 国际电联。国际电联关于网络安全和保护上网儿童的欧洲和独联体区域讲习班，乌克兰敖德萨，2018年4月4-6日。

68 国际电联。“结论和建议”。国际电联关于网络安全和保护上网儿童的欧洲和独联体区域讲习班，乌克兰敖德萨，2018年4月4-6日。

69 国际电联电信发展部门。“欧洲保护上网儿童国家活动区域审查”，2017年。

70 国际电联。全权代表大会。关于“国际电联在保护上网儿童方面的作用”的第179号决议（2018年，迪拜，修订版）。

71 来自理事会保护上网儿童工作组（CWG-COP）的ITU-D第2研究组第SG2RGQ/242号文件

72 来自成员和外部专家的文件可在以下链接找到：第15次会议、第16次会议、第17次会议

73 国际电联。理事会保护上网儿童工作组（CWG-COP）。第CWG-COP-14/2号文件：国际电联保护上网儿童倡议的最新情况。

74 国际电联。理事会保护上网儿童工作组（CWG-COP）。第CWG-COP-15/INF/3号文件：青年在线协商

75 国际电联。理事会保护上网儿童工作组（CWG-COP）。第CWG-COP-16/5号文件：国际电联在保护上网儿童方面的工作和活动

– 介绍2019-2020年《保护上网儿童指南》的审议流程[76]

– 介绍国际电联保护上网儿童倡议和2020年《保护上网儿童指南》的执行情况[77]

鉴于评估方案有效性的重要性，会议的主要成果之一是承认有必要就如何增加青年人的回应数量和增加利害关系方对CWG-COP的参与提供指导。

2020年，国际电联举办了一系列专题论坛[78]，在各利益攸关方之间分享保护上网儿童的经验，宣传《保护上网儿童指南》，并促进其在国家和区域层面的推广、调整和本地化：

– 非洲：2020年10月30日[79]

– 美洲：2020年10月19日[80]

– 阿拉伯国家：2020年11月23日[81]

– 亚洲及太平洋：2020年11月3日[82]

– 独立国家联合体：2020年10月27日[83]

– 欧洲：2020年11月26-27日[84]

3.3 经验教训、未来步骤、行动和结论

在新冠疫情期间，保护上网儿童变得尤为迫切。

可以从成员国在保护上网儿童相关问题上的活动中吸取一些经验教训，例如：

– 每个国家都应该承认自己有责任确保互联网及其相关技术对儿童和年轻人是安全的；

– 国家逐渐将在线风险意识更广泛的纳入儿童保护和育儿议程；

– 虽然互联网也可以成为促进民众意识和学习的积极因素，但在许多情况下，缺少资源和当地现有专业知识成了发展障碍；

---

76 国际电联。理事会保护上网儿童工作组（CWG-COP）。第CWG-COP-16/4号文件：国际电联保护上网儿童：2019-2020年《保护上网儿童指南》审查进程

77 国际电联。理事会保护上网儿童工作组（CWG-COP）。第CWG-COP-17/2号文件：国际电联《2020年保护上网儿童指南》：保护上网儿童和赋权

78 国际电联。区域性发布：《2020年保护上网儿童指南》

79 ITU-D。经修订的《非洲保护上网儿童指南》区域性发布。2020年10月30日。

80 ITU-D。《美洲保护上网儿童指南》2020年10月19日。

81 ITU-D。关于国际电联《2020年保护上网儿童指南》以及在阿拉伯地区实施机会的在线区域对话。2020年11月23日。

82 ITU-D。国际电联亚太区域发展论坛（RDF ASP）。论坛后关于网络安全的会议 – 发布《2020年亚太保护上网儿童指南》。2020年11月3日。

83 ITU-D。国际电联-联合国教科文组织教育信息技术研究所（UNESCO IITE）关于保护上网儿童的独联体区域论坛。2020年10月27日。

84 ITU-D。国际电联保护上网儿童欧洲论坛。2020年11月26-27日。

– 虽然许多国家的立法体系与国际和区域法律文书大体一致，但每个国家都必须确保其法律措施和立法体系与技术发展和行为变化保持同步，这一点极其重要；

– 国家联络点是有效在线保护的关键要素，所有国家都应该有一个资源充足的国家联络点，参与区域和国际举措[85]。

成员国还可以在多个领域进一步促进保护上网儿童活动，例如：

– 提高认识，为专业网络安全专家以及儿童、家长和教师提供数字扫盲培训；

– 制定法律法规保护网上儿童；

– 开展了有代表性的调查，以更好地调整保护上网儿童相关的现行政策、举措和行动。

公益协会和社区组织不妨采取措施，帮助儿童提高认识和培养技能，让他们在安全的环境中更好地使用互联网，例如：

– 减少对预防的恐惧，否则可能会助长父母对孩子使用互联网的恐惧文化，从而避免采用可能会增加父母的焦虑的方法，因为他们已经对不太了解的技术感到担忧，从而影响互联网这一杰出的学习工具的作用；

– 鼓励教育计划开发内容管理的最佳做法，提高儿童对如何负责任地使用互联网的认识；

– 创建互联网门户网站，为儿童、青少年、家长和教师提供教育基础；

– 让所有利益攸关方参与社区宣传活动，包括政府机构、私营互联网企业、非政府组织、社区团体和公众[86]。

总体而言，可以得出以下结论：

– 国际合作和国家支持在确保网络安全和保护上网儿童方面发挥的关键作用；

– 发展中国家应利用国家政策工具制定网络安全战略；

– 公私伙伴关系对于提高网络安全的组织和技术工具的效力十分重要；

– 为保护上网儿童制定新的战略和监管机制，对现有机制的评估，已达到一个高潮；

– 教育机构和私营公司应参与包括在国际电联区域性举措的框架内的项目实施，为保护上网儿童创建组织和技术工具；

– 必须开发适合残疾儿童需求的保护上网儿童教育方案和工具；

– 成员国应审查其全球网络安全指数承诺，并开展进一步行动；

– 教育机构、私营部门实体和非政府组织应参与ITU-D的活动，包括国际电联研究组和提供网络安全培训课程的英才中心的工作。

---

[85] 来自BDT第3/2号课题联系人的ITU-D第2研究组第SG2RGQ/47号文件

[86] 来自科特迪瓦的ITU-D第2研究组第2/201号文件

要制定更有效的解决方案，关键是所有利益攸关方应分享关于网络安全和保护上网儿童领域现有工具的信息，因为全球保护上网儿童日益重要，在这一领域，尤其是在ITU-D的活动中，需要开展合作[87]。

[87] 来自（乌克兰）A.S. Popov敖德萨国家电信学院的ITU-D第2研究组第2/75号文件

第4章 – 残疾人面临的网络安全挑战

4.1 引言

对于网络攻击者来说，没有人被认为是禁区。不应仅仅因为缺乏信息或认识，就让残疾人面临更高的网络风险。

在2014-2017年研究期内，ITU-D第2研究组做了一次网络安全意识调查，调查结果公布在最终报告中。[88]调查结果表明，老年人和残疾人是网络安全意识活动中最不受关注的两个群体。此外，参加调查的69%的成员国没有将残疾人纳入其提高网络安全意识的目标群体中。

调查结果证明，这方面还需进一步工作。为了提高残疾人和包括政府和私营组织在内的其他利益攸关方对具体网络安全需求的认识，第3/2号课题继续根据使用案例审查具体的安全考虑和网络漏洞。本章报告了使用案例、经验教训和其他有用的信息。

4.2 使用案例

4.2.1 以残疾人为对象的垃圾邮件人和网络钓鱼者

概述

垃圾邮件发送者和电子邮件劫持者变得越来越老练，他们已经发展出识别潜在目标是否有残疾并利用这种残疾作为目标的能力。残疾人在获得电子邮件提供商的安全和反欺诈部门的帮助方面也面临挑战。

垃圾邮件发送者和劫持者以残疾人为目标，他们利用残疾人的残疾作为识别标志，假扮残疾人。在一个案例中，有一名使用手语的听障人士，他的电子邮件账户被劫持。此时，受害者有一个Gmail账户，但该账户可能属于任何电子邮件账户提供商的。遗憾的是，Gmail客服提供的支持很少。一旦受害者点击了网络钓鱼链接，并且他的账户被劫持，垃圾邮件发送者就能够访问受害者的地址簿，还可能进入受害者计算机上的其他文件。

客服告诉受害者，唯一的解决办法是更改他的电子邮件提供商和电子邮件地址。虽然这个示例中的残疾是听力障碍，但不难想象，任何残疾都可能遭受此类身份盗窃。

重要的是，电子邮件用户，包括残疾用户，应该认识到，在点击链接之前要验证发送给他们的所有链接，即使是来自朋友的链接。电子邮件提供商的客服也需要积极关注这种形式的滥用，特别是当弱势群体成为目标时。在这种情况下，受害者通过朋友或聋人电话转接服务联系客服电话号码；服务提供者应该更认真地对待这种电话，或者应该

[88] 国际电联。ITU-D第2研究组第3/2号课题2014-2017年研究期最后报告。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。国际电联，2017年。

提供一个有人值守的特殊电话号码，聋人用户可以使用电传打字机直接联系。如果服务提供商应该雇佣谙熟手语的服务台工作人员就更好了。例如，在美国，亚马逊已经采取措施提供这样的服务。

电子邮件示例

下面介绍两个上述示例中垃圾邮件发送者发送给受害者联系人列表的电子邮件类型的示例。作为对策，受害者通知其联系人他被黑客攻击后变更了电子邮件提供商。

例1：垃圾邮件发送者冒充残疾人。

发件人：残疾人personwithdisability@gmail.com

发送时间：2018年3月23日13:00

主题：哇！！X国每月增加70%的聋哑人津贴

哇！X国领导人为所有聋哑人和听障人士考虑，决定将SSA、SSI和SSDI提高70%。这对于X国所有的聋人和听障人士来说是个好消息。

阅读了解你的SSA、SSI和SSDI增加了多少。

点击这里：http://noisecancel.net/js/gggg/G/G/us/index.php

[注意：原钓鱼链接已被更改。]

用你的电子邮件登录，确保准确填写

聋人新闻（DeafNews）

例2：从受害者发出通知他的联系人他被黑。

大家好！

就像我之前说的，三周前我被引诱用看了一个美国手语视频，我的老邮箱Gmail被黑了！

[注：ASL代表美国手语。]

黑客继续用我的Gmail账户发送假冒邮件。可怕的是内容看似是真的，都与我的聋哑活动有关。

我花了几个小时在谷歌机器人网络找到了一个电话号码，(855) 836-3987，可以联系到真人。

你猜怎么着？他们没想办法帮助我，而是说“太糟糕了”。

你的Gmail安全吗？

同时，删除所有来自<personwithdisability@gmail.com>的电子邮件。

道歉

残疾人

吸取的经验教训和建议的最佳做法

- 应对残疾人社区进行宣传，让他们了解已发现的垃圾邮件和恶意软件问题。
- 服务提供者安排训练有素的工作人员处理残疾人社区的客户咨询。
- 电子邮件用户不应该点击任何来源未核实的网址。
- 电子邮件劫持的受害者应该：
  - 通知他们的电子邮件服务提供商；
  - 将可疑电子邮件转发给电子邮件提供商的反欺诈部门；
  - 请求截断被劫持的电子邮件地址；
  - 更改电子邮件地址；
  - 通知所有联系人电子邮件地址已被黑客攻击，并向他们提供新地址。

4.2.2 与物联网辅助技术相关联的网络风险

背景

根据世界卫生组织统计，超过20亿人患有残疾，占全球人口的37.5%[89]。正如联合国经济和社会事务部指出的那样，各国对“残疾人”没有统一的定义，因此采用了不同的分类和门槛[90]。根据国际公认的世卫组织定义，残疾人是指身体功能或结构有问题、活动受限或执行任务或行动有困难的所有人[91]。

根据这一定义，残疾有多种类型。每种残疾都是影响人们生活的障碍。然而，技术在打破这些障碍和帮助残疾人享受更好的生活条件方面发挥着重要作用。

如今，技术是普遍的，影响着个人的日常生活和整个社会。在过去十年中，物联网展示了改善残疾人生活的潜力[92]。因此，物联网辅助技术越来越多地被用来克服残疾带来的限制[93]。

《残疾人权利公约》将信息通信技术确定为帮助残疾人的一个基本要素。具体而言，关于无障碍的第九条强调了信息通信技术在促进残疾人在不同领域的独立性和充分参与方面的作用，并授权缔约国有意识地共同努力推进信息通信技术的获取[94]。

信息通信技术和物联网都提高了安全性、移动性和独立性；从连接互联网的假肢到可以振动来引导穿着者的智能鞋，许多物联网设备和服务的设计都是为了改善生活条件，减少残疾人对他人的依赖[95]。例如，盲人或有视觉障碍的人可以利用技术帮助他们导航和获取书面信息。此外，智能家居技术使人们能控制家中可能难以触及的电器和其他物品，如灯、门锁和安全系统。

技术：一把双刃剑

物联网辅助技术在提供诸多好处的同时，也成倍增加了用户面临的网络风险。鉴于对辅助技术的依赖日益增加，对这种技术的任何破坏或改变都可能导致脆弱性增加。

通常，物联网设备和服务是安全级别不够理想。例如，他们可能没有使用适当的加密来传输数据，这可能会导致数据的不当披露和数据泄漏。特别是对残疾人而言，个人数据可能具有敏感性，因为它们可能会泄露个人医疗状况的细节。

鉴于辅助技术对残疾人的重要性，网络风险带来的负面影响可能是灾难性的。例如，一些身体残疾的人依靠生物力学假体来恢复完全或部分运动。这种假肢使用特定的传感器来读取和分析肌肉收缩参数，以便通过该装置再现运动（例如，移动假肢的手指）。假体通常会将数据发送到云中，以通知他们的计算分析并提高他们的效率。这种连接性使得此类设备容易受到攻击，这些攻击旨在获取、操纵或删除云中保存的数据或

---

89 世界卫生组织。《2011年世界残疾报告》。世界卫生组织，2011年。

90 联合国经济和社会事务部（UNDESA）。《残疾与发展报告：由残疾人、为残疾人和与残疾人一起实现可持续发展目标》。联合国，纽约，2018年。

91 世界卫生组织。同上引，第1章。

92 隐私未来论坛。“物联网和残疾人：探索益处、挑战和隐私紧张”。2019年1月。

93 世界卫生组织。卫生主题。“辅助技术”。

94 联合国经济和社会事务部（UNDESA）。《残疾人权力公约》（CPRD）。第九条 – 无障碍。

95 隐私未来论坛。同上引。

获取用户的个人数据。此外，攻击者可以远程控制假肢。如果假体与大脑植入物相连，后果可能会更糟[96]。

另一个示例，一些有听障人士依赖耳蜗植入，这比标准助听器更具侵入性。这项技术依赖于三个基本组件，即麦克风、语音处理器和植入式接收器刺激器。一些现代人工耳蜗配有遥控设备，允许用户通过移动应用程序控制人工耳蜗的设置。在最基本的层面上，攻击者可能会试图关闭植入物，使受害者失聪。更复杂的攻击可能会阻止语音处理器从麦克风接收输入信号，或者修改接收器以传输攻击者产生的声音。这些更复杂的攻击可能更难探测，尤其是当人工耳蜗使用者没有其他方法来验证他们听到的内容时。

除了针对辅助技术的攻击之外，攻击者还可以针对残疾人常用的技术。例如，如果视力障碍者使用的全球定位系统工具出现故障或被攻击者故意破坏，他们将失去所有可靠的导航手段。在GPS欺骗攻击中，位于目标附近的无线电发射机被用来干扰合法的GPS信号[97]。然后，攻击者可以传输不准确的坐标或中断数据传输，这可能会导致物理伤害和其他重大后果。

虽然这些只是针对数字辅助技术的可能网络攻击的几个示例，但它们突出了网络安全在保障依赖此类技术的残疾人的安全方面的相关性。

供考虑的后续步骤

互联网和物联网可以促进残疾人的社会、经济和公民参与。虽然这些技术的潜力显而易见，但需要不断努力，以物联网设备安全性为重点，协调物联网生态系统中的社会、立法、个人和基础设施因素。政府可以采取具体行动来提高辅助技术的安全性和可靠性。

各国政府可以采取措施，完善物联网无障碍和安全的立法和政策，建立机制促进和执行这些立法和政策。这些法规需要从评估残疾人的需求出发，规定明确的作用和责任。由于这一主题可能涉及政府各方面（例如技术和电信、福利和医疗）代表，合作是关键，应在每一项举措中加以推进。

可以提出具体的倡议。例如，政府可建立辅助技术网络安全认证制度，包括定期安全检查和测试，以及定期更新系统以适应技术发展。政府还可以出台激励措施，促进公私伙伴关系以及提供启动资金和研发拨款支持制造商。

同样，需要促进安全文化建设，应对这些技术带来的风险。各国政府应与私营部门合作，在民众中开展网络宣传运动。

总之，虽然物联网辅助技术是支持残疾人的一个关键要素，但它也可能带来一些风险，如果处理不当，可能会产生严重后果。因此，辅助技术应符合最高安全标准，并应适应技术发展。

吸取的经验教训和建议的最佳做法

如上所述，应为残疾人，特别是听力有困难的人实施网络安全措施，如电信中继服务和远程字幕，以提高信息和通信服务的无障碍性。

---

96 Vladimir Dashchenko。“如何攻击和保护假肢”。Securelist（卡巴斯基），2019年2月26日。

97 Maria Korolov。“什么是GPS欺骗？如何抵御”。CSO网站，国际数据集团（IDG），2019年5月7日。

4.2.3 考虑信息通信技术无障碍服务的安全问题

引言

信息通信技术无障碍服务，如电信中继服务和远程字幕，使残疾人能够交流和获取信息。这种服务自然需要采取安全措施来保护残疾人的安全和隐私，并减轻这些群体以及儿童和老年人等有特殊需求的其他群体的网络脆弱性。

远程字幕的安全问题

远程字幕是一种将会议上的讲话在会议举办地点以外的另一地点进行文字转录的服务[98]。信息通信技术服务，如电话、手机或电脑麦克风，用于将说话者的声音发送给字幕人员，字幕人员将声音转录成文本。然后，转录的文本被实时传输回会议地点，在那里可以阅读文本。远程字幕文本通常显示在会议室的公共屏幕或监视器上，或者显示在个人显示器上。远程字幕服务不仅对聋哑人或听障人士人参加会议必不可少，而且对第一语言不同于会议使用的语言的人或不同声音和口音的人参加各种团体（如在工作场所、教室或社区会堂）也很有用。为远程字幕服务提供转录的人，称为“字幕员”，必须具备逐字记录员的资格。字幕员通常也被称为“语音转文本记者”。

根据各种国家或地方行为习惯，需要远程字幕服务。提供商必须采取一切合理的预防措施来保护会议的隐私，因为会议可能包含机密信息。

机密信息的类型

以下是潜在机密信息的不完全列表：

- 会议中讨论的敏感信息
- 患者病例信息
- 关于个人的法律信息
- 咨询会议
- 关于遵守数据保护法规的信息。

远程字幕服务提供商必须遵守适用的隐私和数据保护法律法规，如欧盟规定的法律法规[99]。

字幕文本加密

发送到显示器或个人终端的文本应该有密码保护。远程字幕服务提供商负责脚本的安全性，并应遵守相关的数据保护要求。建议使用安全套接层（SSL）协议或其他相关技术对文本和文本源的网址（如果适用）进行加密。

音频加密

---

[98] 国际电联电信标准化部门（ITU-T）。FSTP-ACC-RCS号技术文件 – 远程字幕服务概述，2019年10月17日

[99] 欧盟。欧洲议会和欧盟理事会2016年4月27日关于涉及个人数据处理的自然人保护以及此类数据自由流动的条例并废除第95/46/EC号指令的（欧盟）第2016/679号条例（《通用数据保护条例》）。

活动的原始音频数据必须得到安全保护。

电信中继服务的安全考虑

功能等同性

功能等同性被定义为“具有不同能力的人（特别是残疾人和有特殊需求的人）能够使用通信服务或系统的能力，其提供的功能和使用便利程度与向人口中更广泛的用户群体提供的服务或系统相似[...]这就包括技术和经济方面的考虑，不得对中继服务用户实行任何经济上的歧视。”[100]

功能等同性包括适用于任何给定管辖区内通信服务提供商的安全义务。功能等同性意味着中继服务的用户必须与社区中的其他用户处于平等的基础上，特别是在中继服务允许的话务类型方面，这可能会影响安全性。

功能等同性的安全要求

为了实现功能等同，必须确保电话中继服务、此类服务使用的技术以及为其工作的人员通信助理的保密性、隐私性和安全性。

电话中继服务对保密性和通话安全性（包括加密）的要求应与相关国家或地区一般电信服务的要求一致。

有特殊需求者的网络脆弱性考虑

确保互联网的安全使用对残疾人和有特殊需求的群体，如老年人和儿童尤为重要。降低这些群体的网络脆弱性是一个紧迫而重要的问题，需要制定和遵守准则。

4.3 实用信息

ITU-D第1研究组第7/1号课题涉及“残疾人和有具体需求的其他群体的电信/信息通信技术服务无障碍获取”并讨论了这一领域的各种主题[101]。

隐私未来论坛发布一份报告，题为“物联网与残疾人：探索益处、挑战和隐私紧张”[102]。

可以从那些来源获得更多信息。

---

100 ITU-T。ITU-T第F.930号建议书。“多媒体电信中继服务”。

101 ITU-D第1研究组。第7/1号课题。

102 隐私未来论坛。同上引。

第5章 – 网络安全挑战的现状，包括面对物联网（IoT）和云计算等新兴技术的挑战

5.1 引言

技术能力的指数性增长开启了一个日益数字化、互联互通的世界。根据世界经济论坛，一个被称为“全球化4.0”的时代已经到来，数字资产和服务构成了经济和出口的支柱[103]。

创新正在改变技术格局，满足新的业务和实际需求。物联网设备和5G技术日益普及，到2025年，全球预计将有416亿台联网设备[104]。云解决方案对运营至关重要，全球94%的企业都依赖云解决方案[105]。鉴于数据的可用性和准确性不断提高，人工智能将继续得到更广泛应用。

然而，新技术的出现对网络安全提出了更高的需求。数字创新带来了更多更复杂的产品，从而增加了漏洞和弱点被利用的可能性。

网络威胁不断增加。2018年，每天有80 000次网络攻击，相当于每年3 000多万次攻击[106]。2019年，每天都有超过900亿次试图破坏敏感信息的记录[107]。网络威胁也越来越复杂，威胁着整个数字化世界和经济，包括家庭、智能城市、车辆、生产系统和关键基础设施中的网络物理系统。专家表示，黑客攻击植入人体的医疗设备，如起搏器和胰岛素泵都是可能的[108]。

这种攻击的增加源于黑客作为服务通过暗网的扩散，价格比较低廉。网络犯罪正日益商业化，并已发展成为一个很大的行业，黑客在其中销售各种各样的恶意工具和服务，从低级密码盗窃到高度复杂的套件和攻击技术的利用，如DDoS、恶意软件、勒索软件和间谍软件[109]。此外，经常用于改进网络防御解决方案的新兴技术可能被恶意用来提高黑客工具的效率和影响力[110]。人工智能、自动僵尸网络、物联网和云解决方案越来越多地被用于大规模网络攻击，新的黑客技术（如自动网络钓鱼工具）与新兴技术的结合增加了潜在网络风险。

---

103 Klaus Schwab。“全球化4.0 – 它意味着什么？”。世界经济论坛，2018年11月5日。

104 商业连线。“根据IDC最新预测，物联物联网设备的增长预计将在2025年产生79.4ZB的数据”，2019年6月18日。

105 Kim Weins。“云计算趋势：2019年云现状报告”。Flexera博客，2020年5月21日。

106 PurpleSec。“2019年网络安全统计趋势和数据：网络安全统计最终列表”，PurpleSec（博客），2020年4月27日访问。

107 Check Point。“为2020年新网络冷战做准备，Check Point发出警告”。新闻稿，2019年10月24日。

108 Lily Hay Newman。“这些黑客开发一款杀戮应用程序来自证明自己的观点”。Wired，2019年7月16日；Dan Goodin。“胰岛素注射泵黑客通过无线方式释放致命剂量”，The Register，2011年10月27日。

109 Armor。“黑暗市场报告：新经济”。2020年9月28日。

110 德勤。防范不断变化的网络安全风险。“数字时代风险的未来”。德勤有限公司（Deloitte & Touche LLC），2019年。

网络安全的主要挑战是普遍缺乏专业技能和员工意识不足。随着网络威胁日趋复杂，各机构正在努力招募能够保护其系统的熟练网络安全专家[111]。2017年，82%的雇主报告称其员工网络安全技能不足。2021年，专业网络安全职位缺口将达到400万个[112]。此外，一般人员对网络威胁知之甚少。人是网络安全的关键因素，并已被证明其责任重大。2018年，一项研究发现，99%的数字事件是由员工遭人暗算引发的，而只有1%完全是由技术故障或被利用引起的[113]。

网络安全是一个动态的领域，各组织必须不断重新审视其网络安全态势，以抵御新出现的威胁。为了创造一个更加安全的环境，利益攸关方参与网络安全和隐私风险管理的对话十分重要；验证、补充和完善现有的网络安全和隐私风险管理流程；针对特定技术解决方案和环境确定网络安全和隐私关键问题。本章讨论了许多与新兴技术相关的网络安全威胁，包括物联网、云、5G、人工智能和第四次工业革命（被称为“工业4.0”）。还概述了当前的趋势、挑战和应对威胁的可能解决方案，这些威胁可能会逆转数字创新成果。

5.2 网络安全威胁、实施者和动机

网络威胁的目的是破坏网络安全的三个传统目标，即保密性、完整性和可用性。机密性保护信息不被授权访问以外的其他任何人获取。完整性是指确保信息的准确性和可靠性，防止未经授权对数据进行篡改。可用性是指在需要时访问数据和信息的能力。

网络威胁格局纷繁复杂，充斥着各类目的不同、能力各异的人。大体上，恶意分子可分为以下几类：

- **内部人士：**根据最近的报告，大约40%的事件是内部人员所为，他们通常是心怀不满的员工，寻求报复他们的雇主[114]。内部人员尤为危险，因为他们可以直接访问数据、信息和数字资产。
- **黑客分子：**他们是受政治和社会原因驱使的个人。他们通常窃取和传播敏感信息，目的是让政治领导人或名人尴尬，他们以言论自由为名披露特有和机密数据。他们还经常破坏网站，并对特定的服务或网站进行分布式拒绝服务攻击[115]。
- **网络罪犯：**他们是受经济利益驱使的罪犯。他们瞄准与个人、公司和组织相关的信息，目的是获取经济利益。他们通常勒索目标，盗取并在黑市上出售数据和知识产权，利用勒索软件实施攻击。如上所述，网络犯罪已经演变成一种服务，其中各种团体出售用于攻击的商品和服务，从系统操纵到攻击全过程。
- **高级持续威胁（APTs）：**根据美国国家标准和技术研究院（NIST）的定义，这些是十分老练诡计多端的对手，能够在目标网络中立足，以达到诸如盗取信息、破坏或

111 William Crumpler and James A. Lewis。“网络安全劳动力缺口”。战略和国际研究中心，2019年1月29日。

112 Rob Saunders。“2021年134项网络安全统计和趋势数据”。Varonis。2021年3月16日更新。

113 Proofpoint。“Proofpoint年度人为因素报告详细说明了网络犯罪的主要趋势：超过99%的网络攻击需要人类点击”。2019年9月9日。

114 威瑞森（Verizon）。“2019年数据泄露调查报告”。Verizon，2019年。

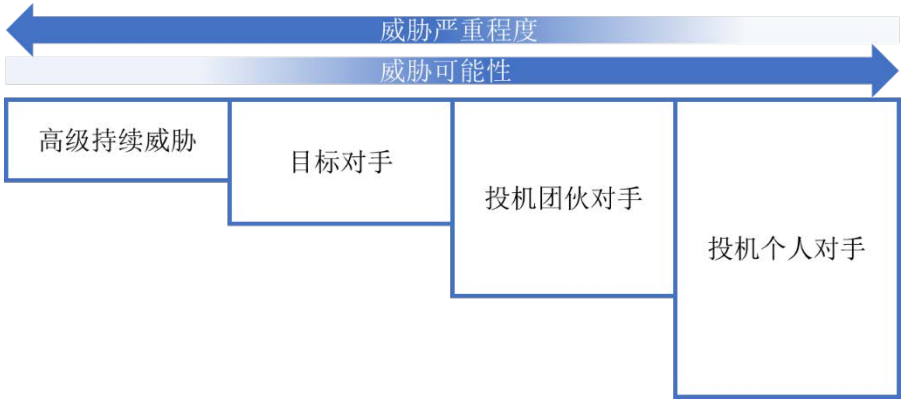
115 Lillian Ablon。“数据窃贼：网络威胁参与者的动机及其对被盗数据的使用和货币化”。兰德公司，2018年。

阻碍被攻击对象完成任务的关键环节或削减其数字资产的目的。高级持续威胁通过使用多种攻击媒介来适应受害者的防御系统，他们能够长时间隐秘地追求他们的目标[116]。就技术技能、资金和组织资源而言，这些对手非常老道，并且往往得到寻求其地缘政治利益的国家的资助。

尽管所有恶意分子都以信息和资产的机密性、完整性和可用性为目标，但网络入侵后果可能是多种多样的。“网络攻击”是统称，涵盖各种各样的行动，从诸删除网站页面或DoS攻击等滋扰，到通过武器化攻击对数据和系统进行严重破坏。

恶意行为者及其攻击在复杂程度、持续时间和危害性方面有所不同。虽然不可能防御所有威胁，但各组织可以根据其特征、风险和背景使用威胁模型来识别相关威胁。**图1**是一个通用的网络威胁模型，它表明大多数组织面对的通常是随机的不太复杂的威胁，因此所需防御态势不是很清晰。

图1：威胁模型



相反，大型企业、关键战略性行业的组织和管理高价值信息和资产的主体更有可能成为有针对性的威胁或高级持续威胁攻击的对象。

本节概述了网络空间威胁。本章的其余部分将提供关于这种威胁如何被用于新兴技术以及有哪些可行的战略、框架和解决方案来抵御攻击的信息。

5.2.1 从技术角度看的风险

新兴技术收集、共享、存储和分析海量数据的速度前所未有。但是，各种设备互联增加，环境日渐复杂，这些特点从技术和组织层面给安全带来大量挑战。

虚拟化

虚拟化是现代技术环境的一个关键支柱，因为它能够让开发者建立专用基础架构来满足网络应用程序的需求，并支持在理想环境中开发新的架构和协议[117]。但是，在多租户技术情况下共享通信通道和路由器设备会带来众多安全风险[118]：

---

[116] 美国国家标准和技术研究院（NIST）。联合任务组转型倡议。“NIST特别出版物800-39：管理信息安全风险：组织、任务和信息系统观点”，2011年3月。

[117] Leonardo Richter Bays等人。“虚拟网络安全：威胁、对策和挑战”。《互联网服务和应用杂志》第6期，第1篇（2015年）。

[118] 欧洲网络和信息安全局（ENISA），“虚拟化的安全问题”，2017年2月10日。

- 在虚拟环境中，物理资源在多个客户端或用户之间共享，这加剧了有意和无意的数据未经授权泄露的风险。如果系统允许对各种用户进行交叉检查，将会为拦截和搜集(在网络中搜索数据残余以获取信息)等恶意活动打开方便之门。
- 多租户技术可能会增加来自供应链的风险，并使抵御入侵变得更加困难。对手可通过使用保护等级较低的共用同一物理层作为载体的资源获得特权并入侵目标的网络。
- 在虚拟化环境中，由于权限管理系统层级严格，身份处理结果特别复杂。这种环境为图谋不轨者实施身份欺诈和提升权限提供了空间。
- 资源共享也会加大恶意或非主动系统中断的风险，从而影响服务供应。例如，物理资源过载会降低虚拟网络的性能，结果造成通信中断。

云安全

在云解决方案中，信息技术服务和资源的供应，包括相关的安全职能和责任，被外包给云提供商。一方面，这可以使新技术快速扩展并增强安全性，因为提供商可以在规模经济的基础上提供先进的保护措施和控制。然而，云漏洞可能会吸引网络攻击者，因为一次成功的黑客攻击可能会危及许多客户。云解决方案包含若干抽象层（即应用程序、操作系统、体系结构和网络），这意味着对手可以通过多种途径介质对其进行攻击：

- 通过结构化查询语言注入和其他攻击模式对软件漏洞加以利用。在这种情况下，云客户必须知道谁负责修补（即软件即服务解决方案的云解决方案提供商，以及基础架构即服务和平台即服务解决方案的客户）。
- 云解决方案提供商提供广泛的服务和互联网连接的应用编程接口，让客户管理和监控其资产。这种连接使云解决方案成为网络攻击的潜在目标，例如嗅探/窃听网络流量、DoS攻击和中间人攻击。
- 如果攻击者能够非法获取用户的凭证，就可能访问管理员用来管理大量资产的管理界面。因此，必须建立强有力的认证和授权机制，对高特权员工尤其如此。
- 如果分离控制失败或被黑客攻击（隔离失败），多租户会增加数据盗取或数据泄露的风险。
- 当过渡到云解决方案时，客户通常对其数据和资产的可见性和控制较少。这就加大了安全删除存储在云解决方案提供商基础架构内多个设备上的数据相关的风险。验证数据已被安全彻底地删除非常重要。多云解决方案致使这一问题更加严重。
- 供应商锁定增加了客户向另一云解决方案提供商迁移的困难，可能会带来严重的安全风险。用户应在其业务连续性战略中应制定变更提供商的计划，以标准、易于传输的格式存储所有数据。
- 据纳米比亚通信管理局称，将客户数据存储在位于境外的云服务数据中心是一个紧迫的问题。在托管数据服务器的国家，当发生网络攻击，导致个人身份被盗、个人信息泄露以及在某些情况下潜在的收入损失时，监管机构没有管辖权和监督权，无

法处理客户保护和网络安全问题。此外，托管国在在获取信息、数据保护和合法拦截方面的立法有所不同，这可能使客户面临未经授权获取个人数据的风险[119]。

物联网

通过设计确保安全的文化仍处于萌芽阶段，增加连接性是最令人担忧的风险趋势之一，它带来了重大的安全挑战[120]：

- 智能设备 – 从照相机、门和制冷设备到空调系统和可穿戴设备 – 收集了大量信息（数据和元数据）。攻击者可以通过窃听目标智能对象传感的数据了解目标的生活。
- 物联网面临的一个新威胁是勒索软件。智能设备为攻击者提供了一个诱人的勒索环境，不仅因为大量目标易于攻击，还因为这种形式的攻击会破坏设备的功能，从而给目标带来不便，迫使他们支付赎金[121]。
- 物联网设备特别容易受到DoS和DDoS攻击，因为大多数设备的技术能力有限（内存、存储、中央处理器等）。攻击者很容易消耗掉其有限的资源，导致服务中断。
- 在设置安全措施时，物联网设备中的资源限制成了一大挑战，因为需要大量计算[122]。
- 物联网安全的关键在于其复杂程度。设备融合各种不同的技术，如虚拟化、云计算、传感器和网络，这些技术都有自己的弱点。保护物联网意味着保护这类组件的完整链条。同样，物联网在几个领域都有应用（家庭自动化、医疗保健、可穿戴设备等）。安全要求不同，受到的威胁也不一样。
- 虽然通过互联网进行攻击最常见，但物联网设备也可能成为物理攻击的目标。在监控缺失或根本没有监控的领域，攻击者可以轻松进入和篡改物联网设备。
- 物联网设备可以用作发起DDoS攻击的介质。例如，2016年，一家著名的域名系统提供商受到来自数千万IP地址的DDoS攻击，多数恶意流量来自打印机、路由器和摄像头等物联网设备[123]。

5G

第五代通信技术，即5G，由于其高速快和延迟低，将提供更可靠和高质量的连接，这将最大限度地提高能源、健康和制造等领域新兴技术应用的输出。这些资产对攻击者来说是一个有诱人的目标，由于其固有的弱点，网络安全十分严峻。此外，由于5G解决方案仍处于试验阶段，网络攻击事件的资料和数据很少，这使得认识潜在威胁变得更加困难[124]：

---

119 来自纳米比亚的ITU-D第2研究组第SG2RGQ/75号文件。

120 Amit Ashbel。“物联网的兴起及相关安全风险”。2016年7月7日。

121 Syed Rameem Zahra and Mohammad Ahsan Chishti。“勒索软件和物联网：新的安全噩梦”。第九届云计算、数据科学工程国际大会（Confluence）论文集，印度北方邦，2019 年1月10-11日。

122 Ammar Rayes and Samer Salam。“物联网从炒作到现实：数字化之路”。Springer国际出版公司，2019年。

123 Nicole Perlroth。“黑客使用新武器破坏美国主要网站”。《纽约时报》，2016年10月21日。

124 欧洲网络和信息安全局（ENISA）。“ENISA如何看待5G网络面临的威胁”。2019年11月。

- 5G威胁涉及面广而复杂；由于结合各种不同技术，它也承袭原有的缺点和威胁。特别是，5G网络和资产沿袭了第二、第三和第四代技术的遗留不安全性、传统的基于IP的弱点以及虚拟化技术带来的流量而成为攻击的目标。攻击者还可以针对5G核心、接入点和边缘元素等特定资产实施攻击。

- 对5G技术的攻击可能包括试图窃取、操纵或破坏数据、拦截或干扰通信、损坏实物资产或中断服务供应。5G连接的行业广泛而深入，极有可能会改变网络安全格局，导致新的漏洞的出现。

- 一个关键威胁因素来自供应链，尤其是受到损害的供应商和服务提供商。风险在于，供应商可能会恶意在其产品中嵌入隐藏的后门、软件或关键漏洞。自动(和不受控制的)更新和功能操控也带来了安全问题。5G与国家安全的关系是显而易见的，应根据风险导向仔细选择供应商。

人工智能

人工智能解决方案在社会各领域的广泛应用将在几个方面影响网络安全局面。此类资产可能成为不法之徒的目标，或攻防双方所利用：

- 通过更改自动决策和行为可以操控人工智能资产，主要是通过毒化数据、篡改分类模型和后门[125]。所有这些方法利用系统的学习能力，通过向系统提供错误数据和信息从而改变输出[126]。

- 黑客正在转而使用人工智能解决方案提高其攻击范围和能力。人工智能可以用来提供能够自主规避防御措施的恶意软件，根据成功率调整策略，改进其运行。

- 人工智能还是一个重要的防御资源。它可以通过增强典型的防御活动，如检测威胁和异常、事件处置和威胁分析，大幅提高系统的恢复能力。

5.2.2 从行业4.0的角度看风险

行业4.0要求将自动化、物联网、虚拟化解决方案、分析和人工智能应用于不同的垂直行业。这些技术允许收集、存储、共享和解释大量数据，并可在速度、效率、成本效益和服务供应方面带来显著改善。行业4.0可以应用于各个行业，每个行业都容易受到特定威胁和安全风险的影响。

智能家居

智能家居是可以应用工业4.0的众多垂直领域之一，尤其是在智能能耗、照明和供暖领域。智能家居包含各种各样使用传感器和执行器的智能设备，通过互联网进行远程管理[127]。将设备连接到互联网会带来许多安全风险：

---

[125] Battista Biggio和Fabio Roli。《野生模式：对抗性机器学习兴起十年后》。《模式识别》（Pattern Recognition）第84卷，2018年12月，第317-31页。

[126] Matthew Jagielski等人。“操纵机器学习：回归学习的中毒攻击与对策”。IEEE安全与隐私研讨会（SP），2018年。

[127] Ado Adamou Abba Ari等人。“在物联网中实现隐私和安全：架构、应用、安全和隐私挑战”。应用计算和信息学，2020年7月31日。

- 智能家居产生大量易受攻击的数据。正如乍得邮政和新信息通信技术部所指出，联网设备（包括智能电视）都暴露于信息系统安全威胁。例如，使用联网电视可以允许未经授权人员通过互联网访问私人数据，为基于互联网的身份盗窃提供方便。连接设备的缺点类似于与连接到计算机网络的个人计算机，同样会受到恶意软件威胁[128]。

- 智能设备安全性差，容易被劫持。获得设备控制权的攻击者可以在国内网络中横向移动，以控制其他节点。

- 智能设备通常计算资源贫乏，因而使其特别容易受到DoS和DDoS攻击，这使这些设备或网络时不时出现故障，原本用户无法使用。

智慧城市

智能城市将新兴技术与数据集成和任务自动化相结合，优化城市组织并提供更好的服务。智能城市的基础是日益紧密互联的交通、能源供应和医疗保健等的关键服务之间共享的大量数据流。产生的数据规模以及数据在智慧城市运作中发挥的作用对网络安全提出了迫切需求，以防止信息隐私和数字资产的完整性受到各种安全威胁：

- **电子卫生：**随着对技术的依赖和健康数据量的增长，医疗保健提供商必须保护敏感信息并确保服务的提供。尽管还没有相关事件的报道，但模拟表明，无线关闭植入式心脏除颤器[129]，侵入胰岛素注射泵以释放致命剂量[130]，甚至渗透到患者监护系统以实时修改患者的生命体征都是可能的[131]。

- **智能电网：**这是智能城市的关键组成部分。它使用双向设备，如传感器、执行器和仪表，对从生产者到消费者的电力进行持续平衡和监控[132]。由于智能电网依赖信息通信技术协议和互联网连接，因而很容易受到网络攻击[133]。智能电网成为诱人的攻击目标；然而，智能电网具有复杂的体系结构，造成大规模危害需要高水平的技术和组织资源。迄今为止，只有两起已知的由网络攻击造成的大停电事件，即BlackEnergy3（黑暗力量3）和Crashoverride攻击，这两起事件都被认为是由国家行为者实施的[134]。

- **智能交通：**数字资产、物理系统、通信网络和自动化可应用于交通基础设施，以优化质量和效率。攻击者可以通过改变数据和信息阻碍交通，甚至引发事故。此外，智能交通系统涉及大量需要保护的个人和敏感信息。

---

128 来自乍得的ITU-D第2研究组第2/140号文件

129 Daniel Halperin等人，“起搏器和植入式心脏除颤器：软件无线电攻击和零功率防御”。IEEE安全和隐私研讨会（SP），2008年。

130 Arundhati Parmar。“黑客展示无线胰岛素注射泵的漏洞”。MedCityNews，2012年3月1日；David C. Klonoff。“联网糖尿病设备的网络安全”。《糖尿病科学与技术杂志》第9卷第5期，2015年4月16日。

131 Douglas McKee。“5秒内80到0：伪造患者的生命体征”。迈克菲，2018年8月11日。

132 Lindah Kotut和Luay A. Wahsheh。“智能电网中的网络安全挑战和解决方案调查”。2016年网络安全研讨会（CYBERSEC）。

133 Muhammed Zekeriya Gunduz和Resul Das。“智能电网的网络安全:威胁和潜在解决方案”。《计算机网络》，第169卷，2020年3月14日。

134 Dragos公司。CRASHOVERRIDE：分析攻击电网的恶意软件。2017年6月12日。

工业物联网

工业物联网使物联网适应工业环境。当与机器人和自动化结合时，它可以为工业企业带来宝贵的利益，包括通过提高质量、相抵成本和改善生产流程的维护。这些网络物理系统具有特殊性和具体要求，因此对采用传统网络安全措施特别成问题。

网络物理系统是具有高度确定性的硬实时环境，其中数据可用性比完整性和保密性更重要[135]。在这类系统中，数字元件与物理过程对接，例如物体的运动、化学反应、物质的释放和冷却过程，数据流作为执行任务的输入。在这种情况下，采用普通的安全控制措施，如防病毒软件、加密或防火墙，可以减慢数据流并干扰活动管理，导致延迟，尽管数量不大，但对运行的影响不可小觑[136]。

此外，网络物理系统中的大多数设备无法处理复杂的安全措施或更新，这导致连接互联网的资产可能容易受到攻击。对工业网络物理系统的网络攻击会打乱工厂的运行并造成停产，因而造成严重的经济损失。

然而，人们主要担心的是，网络攻击者通过操纵数据流，改变系统运行，直到它达到机械断点，引起动能冲击，对公共安全产生严重后果。例如，如果攻击者给系统输入改动的数字，告诉控制器温度骤降，控制器将通过增加热量自动补偿，导致过热而没有被察觉[137]。例如，在2014年，一家德国钢铁厂被成功入侵，攻击者通过阻止熔炉正常关闭，给关键器件造成巨大的物理损坏[138]。

能造成实质影响的进攻性网络操作极其复杂，不仅需要对在用数字资产了如指掌，还需要对目标物理过程有广泛的认知，对各种变量有详细的了解。因此，高级持续威胁和国家资助的代理最有可能拥有执行此类操作所需的技术和组织资源。

5.3 现有和新出现的解决方案

很大一部分物联网设备没有内置基本的网络安全功能。经过与行业代表和国家网络安全中心专家长达18个月的合作，英国数字、文化、媒体和体育部于2018年10月发布了《消费者物联网安全行业规范》[139]。该准则中有13条自愿准则，为物联网设备提供了一个基准，制造商应将其嵌入产品中，以使其“通过设计实现安全性”。该规范为全球适用的第一部物联网安全标准，即ETSI TS 103 645，的制定做出了贡献[140]。

---

135 Roberto Setola等人。“作战技术的网络威胁”。《国际系统工程学报》，第10卷，第2期，2020年。

136 Roberto Setola等人。“工业控制系统的网络攻击概述”。《化学工程学报》，第77卷，2019年。

137 Stephen McLaughlin等人。“工业控制系统中的网络安全前景”。《电气和电子工程师协会学报》，第104卷，第5期，2016年5月。

138 Robert M. Lee等人。“德国钢厂网络攻击”。工业控制系统防御使用案例，2014年12月30日。

139 英国数字、文化、媒体和体育部。“消费者物联网安全行业规范”。2018年10月。

140 欧洲电信标准协会（ETSI）。ETSI TS 103 645 V1.1.1（2019-02）。网络；面向消费者物联网的网络安全。

阿尔及利亚电信还强调了制定保障新兴技术（如云和物联网）安全的指南和建议的重要性，这些技术将成为信息系统和数字经济发展的重要引擎[141]。

表1和**表2**提供了ITU-T建议书的列表，这些建议分别涉及云和物联网的基础设施、应用程序、数据和隐私的保护。

表1：保护云基础设施、应用程序、数据和隐私的安全架构

标题	主题	机构	链接
云计算安全概述			
ITU-T X.1601	云计算的安全框架	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12613
云计算安全设计			
ITU-T X.1602	软件即服务应用环境的安全要求	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12615
ITU-T X.1603	云计算监测业务的数据安全性要求	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13406
ITU-T X.1604	云计算中网络即服务（NaaS）的安全要求	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14093
ITU-T X.1605	云计算中公共基础设施即服务（IaaS）的安全要求	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14094
ITU-T X.1631	信息技术 – 安全设置 – 基于ISO/IEC 27002云服务标准的信息安全控制行业规范	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12490
云计算安全最佳做法和指导原则			
ITU-T X.1641	云业务客户数据安全导则	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12853
ITU-T X.1642	云计算的操作安全导则	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12616

[141] 来自阿尔及利亚电信协会（阿尔及利亚）的ITU-D第 2 研究组第2/66号文件

表2：保护物联网基础设施、应用、数据和隐私的安全架构

标题	主题	机构	链接
物联网（IoT）安全			
ITU-T X.1361	基于网关模型的物联网安全框架	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13607
ITU-T X.1362	物联网（IoT）环境的简单加密程序	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13196
ITU-T X.1364	窄带物联网的安全要求和框架	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14088
ITU-T X.1365	在电信网络上使用基于身份的密码来支持物联网（IoT）服务的安全方法	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14089
ITU-T X Suppl. 31	ITU-T X.660 – 物联网使用对象标识符指南补充	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13411

其他新兴的安全技术和框架

– 人工智能应用，包括机器学习和深度学习，有利于大幅提高网络安全战略的效率和成本效益。这些解决方案使用回归、分类和聚类方法检测异常，识别不同类型的攻击，并开发潜在的补救对策。人工智能系统能够针对特定事件建议具体应对措施，增强事件处置活动。这些应用还能够根据描述自动为新漏洞和错误配置分配风险值，从而改进风险管理活动，并通过显著加快提取、细化和应用有关威胁、参与者、攻击、恶意软件、漏洞和危害指标的数据来主动防止攻击[142]。

– 分布式台账技术（DLT）的具体功能为安全应用带来了希望[143]。首先，基于DLT的存储是分散的，这大大降低了大规模数据泄露的风险，因为攻击者不再能够通过单个接入点访问所有保存的数据。同样，分散化为物联网网络带来了重要的安全优势，传统上，物联网网络是根据客户端-服务器模型逻辑组织的，其中中央机构管理网络内的数据和设备。物联网设备可以借助DLT应用识别异常，并隔离异常行为的节点。此外，DLT可以确保交换数据的可用性、可审计性、可问责性、完整性和保密性保持稳定，从而在物联网网络中建立信任[144]。

– 安全协调、自动化和响应（SOAR）方法需要连接安全工具和系统的解决方案，以便以一体化和有机的方式执行漏洞管理、事件响应和安全操作自动化等活动。安全流程的自动化允许系统在没有人工干预的情况下实施补救和维护活动（漏洞扫描、访问和日志监控）。

---

142 Padmavathi Ganapathi和D. Shanmugapriya。“计算机和深度学习应用于网络安全的研究手册”。IGI全球，2019年；和Dave Shackleford。“谁在使用网络威胁情报以及如何使用？”。SANS，2015年2月12日。

143 Nir Kshetri。“区块链在加强网络安全和保护隐私方面的作用”。《电信政策》，第41卷，第10期，2017年11月。

144 Ben Cole。“物联网数据安全固有的‘信任供应链’”，《物联网议程》，2016年11月28日。

- 另一种选择是零信任模型，在这种模型中，网络环境是内部分段的，访问是根据最小特权原则进行管理的。这意味着每个模块，包括用户、设备、应用编程接口和物联网设备，只能访问其合法功能所需的资源、数据和资产。零信任模型极大地提高了内部安全性，因为它使攻击者更难以进行横向移动和权限升级，因为要而获得对整个网络的访问权限，攻击者需要对付多个目标设备。

- 云接入安全代理是在用户和云提供商之间运行的策略执行点。例如，强制实施的安全策略可以包含身份验证、单点登录、授权、凭证映射、设备配置、加密、令牌化、日志记录、警报和恶意软件探测/预防[145]。

- 特权访问管理是指一套用于监控和保护特权账户的工具和解决方案，例如用于访问关键资产、数据和资源的管理员账户。此类解决方案将关键账户隔离在一个安全且受监控的存储库中，从而降低了凭证被盗的风险。

- 各组织应该从开发和运营（DevOps）方法转向开发、安全和运营（DevSecOps）方法，将安全作为开发和运营的一个固有部分。在DevSecOps框架和工具中，安全性从开发的最初阶段就被认为是一个不可或缺的重要特性，而不是固定在最终产品上（比如软件和应用程序）。这种方法使安全性更加可靠，降低了风险并降低了合规成本。

- 高德纳的持续适应性风险和信任评估（CARTA）框架提出了一种适应性安全方法，根据风险和效率进行决策[146]。CARTA需要三个阶段：“运行”，侧重于重大威胁的分析；“构建”，指在产品开发和运营过程中发现的威胁和漏洞；和“计划”,通过分析确定安全风险并评估降低风险是否会对生产效率产生负面影响[147]。

经济高效的解决方案

- 根据英国数字、文化、媒体和体育部的数据，通过重点关注影响最常见复杂程度相对较低攻击的投资回报，开始应对大规模网络攻击的影响，已取得显著的全球效益是可能。主动网络防御（ACD）计划的目的是提高针对英国发起商品网络攻击的成本和风险，从而降低犯罪分子的投资回报[148]。2018年，该计划通过其取缔服务产生了最大影响，该服务可识别恶意网站（攻击或支持攻击的基础设施），并通知托管或所有者必须将其从互联网上删除：以这种方式共取缔了192 256个欺诈网站，其中64%在24小时内被取缔。此外，在授权给英国的知识产权空间中托管的22 133个网络钓鱼活动（总共142 203次个人攻击）被删除，14 124个与政府相关的网络钓鱼网站被删除[149]。

- 据立陶宛NRD网络安全公司称，为了大幅改善国家数字环境的安全，国家和行业部门的计算机安全专家小组不仅要成为联络点、事件应对协调员和分析员，还应成为有感染力的促进者，在行业、专业团体、教育中心、研究、活动、会议、大会以及私人和内部计算机安全专家小组内发展更多的独立网络安全能力[150]。

---

145 Gartner。Gartner词汇。“云接入安全代理（CASB）”

146 Gartner。“Gartner数字时代的信息技术安全方法”。2017年6月12日。

147 Gartner。“Gartner主题演讲：利用自动化实现现代安全”。2019年6月17日。

148 Ian Levy and Maddy S。“积极的网络防御 – 第二年”。英国国家网络安全中心。2019年7月15日。

149 来自英国的ITU-D第2研究组第SG2RGQ/175号文件

150 来自（立陶宛）NRD网络安全部门的ITU-D第2研究组第2/172号文件

– 据爱沙尼亚Guardtime公司称，网络演习对建立可持续的网络恢复能力至关重要，因为这有助于团队了解缓解网络危机所需的流程。爱沙尼亚建议制定一个网络复原力治理方案，涵盖教育、培训和网络演习，从地方活动到定期的全国规模的针对性演习。此类方案应全面考虑到国家组织结构和社会经济状况、各利益攸关方的作用和责任、国家监管环境、国家的区域和国际伙伴关系以及国家在变化的网络威胁环境中面临的各种风险[151]。

[151] 来自（爱沙尼亚）Guardtime AS的ITU-D第2研究组第SG2RGQ/32号文件

第6章 – 网络安全如何支持个人数据保护

6.1 引言

随着新信息技术的出现，各种日用的新型便利服务喷涌而出。但是，新信息技术的出现也双向改变了个人面临的隐私和数据保护风险。尽管个人数据面临的新危险不断出现，但可以使用各种技术来减小或避免此类风险。为此，必须更加重视网络安全和增强隐私的技术，这些技术通过虚名化和隐私设计达到支持保护个人数据的目的。

虚名化是一种数据管理和去识别过程，通过这一过程，数据记录中的个人可识别信息字段被一个或多个人工标识符或“虚名”所取代。每个替换字段或替换字段集合的单个虚名使得数据记录不太容易识别，同时仍可用于数据分析和处理[152]。虚名化有助于保护个人身份信息，并可能减轻收集和保存此类数据的实体的负担。

在隐私设计上，人们不会等到出现漏洞后才采取安全措施。相反，开发人员预测或预判隐私威胁，或者通过预防措施（如服务规划或设计）防患未然[153]。

二者的区别在于，虽然虚名化需要某些技术措施，但隐私设计能够使数据控制器灵活地确定哪些额外的技术措施最能确保数据安全和隐私。

6.2 成员国的法律环境和最佳做法

巴西新近通过的《一般数据保护法》包括各种类型的个人和处理数据的定义，并规定了国内和国际处理的法律许可、数据主体的基本权利和建立国家数据保护机构[154]。该法案确立了数据最小化、防止数据泄露和数据安全的原则，并对这些领域的管理做了具体规定。该法案还包括设计安全，规定保护个人数据的安全措施应从产品或服务概念到执行全程落实。

2017年，中国正式发布了一套关于信息安全技术中个人信息安全规范的国家标准，对其《网络安全法》中规定的个人信息安全要求进行了补充。这些标准提供指南和操作说明。中国正在继续研究和制定个人信息保护标准[155]。

中国地方数据安全企业正在积极研发安全产品和服务，包括数据防泄漏（DLP）、数据库安全审计、数据库漏洞扫描、数据库加密、数据屏蔽等安全产品，为个人信息保护防护提供技术支撑。

---

[152] 维基百科。https://en.wikipedia.org/wiki/Pseudonymization

[153] 从设计着手保护隐私原则在现有的建筑领域应用，但是这个概念是次要的。它在20世纪90年代中期被加拿大安大略省信息和隐私专员Ann Cavoukian博士引用后开始受到关注。

[154] 来自巴西的ITU-D第2研究组第SG2RGQ/143号文件

[155] 来自中国的ITU-D第2研究组第2/156号文件

韩国对其《个人信息保护法》进行了重大修订，对个人数据保护的技术措施做出规定[156]。修正案简化了监管监督和提出了“虚名化数据”概念，使数据控制器和处理器能够更安全地处理数据，通过数据保护和默认设计等其他技术和组织措施最大限度地降低数据误用和泄露的风险。

此外，韩国政府公布了关于个人数据自动处理的保护准则。虽然人工智能大数据分析和物联网设备中用于收集数据的传感器等新技术有利于服务创新，但在理解个人数据处理流程和后续处置的限制方面存在困难。在物联网设备个人数据自动处理中，该指南鼓励通过应用隐私设计，从规划步骤之处到整个数据生命周期，要全面考虑了个人数据泄露的可能性。

准则包含自动处理个人数据保护的10条规定：

- 规划阶段
  - 规定1：确认服务所需的个人数据
  - 规定2：收集个人数据时确认是否合规
- 设计阶段
  - 规定3：数据最小化和仅处理必要的个人数据
  - 规定4：在每个个人数据处理步骤中采取适当的安全措施
  - 规定5：透明发布个人数据处理程序和方法
  - 规定6：保证数据主体能够方便地行使其权利
  - 规定7：向第三方提供和委托个人数据是要对数据主体给出明确说明
  - 规定8：在数据主体终止服务时，销毁个人数据并防止进一步收集
  - 规定9：业务终止时保障数据主体权利的计划
- 审查阶段
  - 规定10：服务启动前检查个人数据泄露风险因素。

鉴于最近需要跟踪世界各地的新冠确诊病例，韩国采取了各种制度和技术措施来保护个人数据。除了修订相关法规确保追踪确诊患者的法律基础之外，还采取了技术措施来分离和管理身份信息，以防止个人信息泄露。发现确诊病例时，单独使用信息另外用于流行病学调查，对个人用户和访问者信息进行安全管理，例如在生成后四周自动销毁[157]。

意大利某公司开发了一种专有方法，各组织可以轻松使用该方法来开展一系列技术活动，以使云基础架构（私有、公共或混合）符合隐私法规[158]。该方法包括一项建议，

156 来自韩国的ITU-D第2研究组第2/342号文件
157 来自韩国的ITU-D第2研究组第SG2RGQ/268号文件
158 来自（意大利）Proge-Software的ITU-D第2研究组第SG2RGQ/25号文件

即界定成员国可以用来建立自己的国家配置器的一般准则，以便更高效、更廉价地实现多国合规标准化，利用云作为一个强大的平台，促进数字经济的爆炸式发展。

在另一个最佳做法案例中，《欧盟通用数据保护条例》（GDPR）关于设计和默认数据保护的第25条认可隐私设计是防止物联网设备、大数据、人工智能和其他新技术带来的个人数据保护风险的最佳方法。根据隐私设计的概念，确保个人数据安全和隐私的适当组织和技术措施被嵌入到该组织的产品、服务、应用程序以及业务和技术程序的整个生命周期中。技术措施可以包括但不限于虚名化和数据最小化[159]。

欧洲网络和信息安全局（ENISA）提出了八项关键策略，目的是在帮助企业通过运用隐私设计，检查保护个人数据中的各种可接近性方法、策略和技术因素[160]。

表3：隐私设计应用的八个关键策略

	原则	内容
1	最小化	个人数据量处理目的明确，尽量减少已处理的数据量，降低侵犯隐私的可能性
2	隐藏	处理个人数据时隐藏纯文本传输，以防止外部访问
3	分离	分离和存储各种个人数据，防止数据库中对单体的歧视
4	汇总	汇总大量的个人数据处理，以最大限度地减少对个体的歧视，对处理结果进行分类，杜绝歧视
5	告知	告知数据主体个人数据处理的整个过程，保证数据用途的透明和理解
6	控制	控制个人数据的使用。数据主体必须了解个人数据处理的整个过程，并能够根据第五项策略“告知”行使其关于错误使用其个人数据或安全级别的权利
7	执行	内部个人数据保护政策必须体现法律和系统责任，并且必须强化执行
8	证明	证明遵守法律义务，例如有效执行个人数据保护政策并针对涉及数据外流的事件立即采取措施

欧洲网络和信息安全局（ENISA）还就各利益攸关方开展的隐私和数据保护活动提出了建议。建议决策者促进和支持制定新的奖励措施，推动个人数据保护服务，建议研究和开发组织通过跨学科方法研究保护个人数据的工程方法，并通过决策者和媒体宣传研究成果。最后，该机构建议软件开发者提供可以直观地实现隐私属性的技术，支持在公开和相互建立的基础设施项目中保护个人数据。

美国联邦贸易委员会（FTC）强调隐私保护的实际和程序原则，如隐私设计、简化消费者选择以及保证透明度等实质性和程序性原则。委员会还强调在商业机构、产品和服务开发的各个阶段要全程保护消费者隐私[161]。

---

159 欧盟。欧洲议会和欧盟理事会2016年4月27日关于涉及个人数据处理的自然人保护以及此类数据自由流动的条例并废除第95/46/EC号指令的（欧盟）第2016/679号条例（《通用数据保护条例》）。

160 欧洲网络和信息安全局（ENISA）。“从设计着手保护隐私和数据 – 从政策到工程”。2014年12月。

161 美国联邦贸易委员会。“在快速变化的时代保护消费者隐私：对企业和决策者的建议”。2012年3月。

西班牙数据保护局（AEPD）发布了一份隐私设计指南，其中强调从任何类型的处理开始就需要考虑隐私和数据保护原则。该指南还提出了处理个人数据的基本原则和策略[162]。

表4：隐私目标和隐私设计策略之间的联系

隐私保护目标	数据隐私保护策略	流程因此保护策略
无关性	最小化、抽象、分离和隐藏	
控制		控制、执行和证明
透明		告知

6.3 汲取的经验和前进方向

网络攻击、数据泄露和未经授权使用个人数据的速度呈指数增长。对于处理个人身份信息的各组织认识个人信息方面的权利和义务比以往任何时候都更重要。

本章概述了成员国在个人数据保护方面的法律变化和网络安全技术措施。内容涵盖帮助成员国遵守不断变化的数据隐私要求的最佳做法，并涉及网络安全技术在减轻风险和支持合规方面的作用。

以下是从审查成员国个人信息保护方面使用的各种网络安全技术和最佳做法得出的经验教训：

- 关于利用虚名化、隐私设计和其他技术措施创造更加安全的环境的制度性安排。
- 收集和使用个人信息的企业需要积极采取技术措施，从根本上保护个人信息。
- 各利益攸关方，包括数据主体、民间团体、学术界和行业代表，需要集体讨论技术的使用，并努力提高认识和改善安全。

[162] 西班牙数据保护署（AEPD）。《隐私设计指南》，2019年10月。

第7章 – 课题的未来

网络安全是政府和消费者等所有各方面临的一个问题。国际电联发展部门在这方面开展的工作有助于提高对风险的认识。随着世界各地的连接率和互联网使用率不断上升，保护消费者和系统依然重要。鉴于全球持续需要共享网络安全实践的信息，ITU-D第2研究组第3/2号课题管理团队认为，下个研究期继续保留关于网络安全问题的课题。本研究期内提出的主题仍然适用，并应构成下一个研究期间文稿和和工作的基础。因此，课题的总体框架应维持不变：由于安全问题涉及所有技术，第3/2号课题继续适用于所有新兴技术，本质上这些技术都可以通过设计集成在一起。

Annexes

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

Contributions on Question 3/2

Web	Received	Source	Title
2/407	2021-03-03	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/400	2021-03-01	United States	Update on Cyber Awareness Campaigns
2/385	2021-01-28	Bhutan	Survey findings on National Child Online Safety and Protection
RGQ2/278	2020-09-22	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
RGQ2/272	2020-09-22	United Kingdom	UK case study: Cyber resilience best practice for SMEs
RGQ2/268	2020-09-22	Republic of Korea	Protecting personal data in responding COVID-19 pandemic (Korea's experience)
RGQ2/261	2020-08-19	Togo	Draft text for Chapter 1 of the Final Report for Question 3/2 - Update on the status of spam and malware, including mitigation responses
RGQ2/241	2020-08-26	United Kingdom	Updated case study on securing consumer Internet of Things (IoT) devices in UK
RGQ2/235	2020-08-20	United Kingdom	UK Government Digital Service (GDS) Global Digital Marketplace Programme
RGQ2/234	2020-08-20	United Kingdom	UK case study - reporting service for phishing emails
RGQ2/216	2020-07-27	Brazil	Brazilian National Cybersecurity Strategy (E-Ciber)
RGQ2/215	2020-07-27	Brazil	#SafeConnection (#ConexãoSegura) Awareness Campaigns
RGQ2/214	2020-07-27	Brazil	Brazilian National Cyberdrill - Cyber Guardian Exercise
2/344	2020-02-11	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/342	2020-02-11	Republic of Korea	Korea's major amendment to data protection law and its implication
2/341	2020-02-11	Republic of Korea	Implementation plan for strengthening national cybersecurity of Korea

(continued)

Web	Received	Source	Title
2/338	2020-02-11	Co-Rapporteur for Question 3/2	Draft table of contents (V1) for the Final Report of Q3/2
2/336	2020-02-11	United Kingdom	Case study of best practices for securing customer Internet of Things in the UK
2/331	2020-02-11	Keio University (Japan)	Proposed text for consideration of security issues for ICT accessibility
2/328	2020-02-08	Deloitte (United States)	People with disabilities and the Internet of Things
2/325	2020-02-08	Democratic Republic of the Congo	La sécurité numérique en République Démocratique du Congo
2/322	2020-02-07	Welchman Keen (Singapore)	Enhancing capacity and capability for critical national infrastructure in the Pacific Island Nations
2/321	2020-01-08	Sudan	WSIS project for consideration by Question 3/2
2/305	2020-01-15	Mexico	Perception on security and trust from Mexican users on fixed and/or mobile Internet
2/287	2020-01-07	China	Forum on network security technology development and international cooperation
2/286	2020-01-07	China	National Network Security Publicity Week and network security industrial park
2/272	2020-01-02	Niger	Cybersecurity best practices: case study and recommendation
2/264	2019-12-27	Russian Federation	Protecting children from information harmful to their health and development. Experience of the Russian Federation
RGQ2/TD/13 +Ann.1 (Rev.1)	2019-10-08	Forum of Incident Response and Security Teams (FIRST)	Introduction to incident response for policy makers
RGQ2/196	2019-09-24	Silensec Africa Limited (Kenya)	Using cloud-based cyber ranges and competence frameworks for the delivery of cyber drills
RGQ2/179	2019-09-23	China	China's practice in protecting children's personal information
RGQ2/175	2019-09-19	United Kingdom	Follow up to "case study for the use of Active Cyber Defence on UK Government networks"
RGQ2/156 +Ann.1-3	2019-09-04	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
RGQ2/155	2019-08-23	United Kingdom	Case study of best practices for ransomware risk mitigation in the UK

(continued)

Web	Received	Source	Title
RGQ2/153 +Ann.1-2	2019-08-22	United States	Enhancing the resilience of the Internet and communications ecosystem against botnets and other automated, distributed threats
RGQ2/151	2019-08-22	United States	NIST Framework for Improving Critical Infrastructure Cybersecurity V1.1
RGQ2/146	2019-08-21	Senegal	Overview of the National Cybersecurity School with a regional focus
RGQ2/143	2019-08-23	Brazil	The adoption of the Brazilian General Data Protection Law
RGQ2/135	2019-07-30	Bhutan	Cybersecurity initiatives in Bhutan
RGQ2/134	2019-07-29	State of Palestine, which participates in ITU under Resolution 99 (Rev. Dubai, 2018)	Government Data Exchange
RGQ2/118	2019-06-21	Democratic Republic of the Congo	Securing information and communication networks: Best practices for developing a culture of cybersecurity
2/201	2019-03-08	Côte d'Ivoire	Survey of online activities and Internet use by children in Côte d'Ivoire
2/199 (Rev.1)	2019-03-06	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/174	2019-02-07	Côte d'Ivoire	Mapping of cybercrime threats in Côte d'Ivoire
2/173	2019-02-07	Côte d'Ivoire	Presentation of Platform for Combatting Cybercrime (PLCC)
2/172	2019-02-07	NRD Cyber Security (Lithuania)	National and sectorial CSIRT developments as means to strengthen cybersecurity environments, 2019 update
2/168	2019-02-07	Republic of Korea	2019 Comprehensive Cybersecurity Plan for the private sector
2/167	2019-02-07	Symantec Corporation (United States)	The importance of cyber threat intelligence in the definition of national cybersecurity strategies
2/165	2019-02-06	Mexico	Fixed and/or mobile Internet users' perception of cybersecurity
2/156	2019-02-05	China	Work experiences in personal information protection
2/155	2019-02-05	China	Design of evaluation index for network security capability
2/154	2019-02-05	China	Experience of Internet governance with the coordinated participation of the whole of society

(continued)

Web	Received	Source	Title
2/152	2019-02-01	Benin	Cybersecurity in the era of the digital economy in Benin
2/141	2019-01-15	Chad	Digital dividend
2/140	2019-01-15	Chad	Vulnerability of connected TVs
2/136	2019-01-15	Chad	Status of cybersecurity in the Republic of Chad
RGQ2/TD/1	2018-09-24	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for ITU members
RGQ2/79	2018-09-18	Bhutan	Challenges, issues and recommendations from Bhutan: developing country perspective
RGQ2/75	2018-09-18	Namibia	Enforcement of cyber security challenged by cloud services
RGQ2/55	2018-09-10	United Kingdom	Case study for the use of Active Cyber Defence on UK government networks
RGQ2/47	2018-08-31	BDT Focal Point for Question 3/2	Information on two publications issued in 2017: regional review of national activities on child online protection in Europe; and mobile identification: implementation, challenges, and opportunities
RGQ2/39 +Ann.1	2018-08-20	High-Tech Bridge SA (Switzerland)	Cybersecurity awareness and other educative activities to members
RGQ2/32	2018-08-16	Guardtime AS (Estonia)	Towards cyber resilience - the role of national cyber exercises
RGQ2/30	2018-08-15	Brazil	Survey proposal
RGQ2/26	2018-08-14	NRD Cyber Security (Lithuania)	National and sectoral CSIRT developments as means of strengthen cybersecurity environments
RGQ2/25	2018-08-14	Proge-Software (Italy)	Data Privacy and Cloud.be compliant
2/91	2018-04-24	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/84	2018-04-23	Japan	Proposal for workshops in 2018-2021 study period
2/82	2018-04-23	Iran University of Science and Technology (Islamic Republic of Iran)	KOVA Project: A best practice for COP implemented in Iran
2/75	2018-04-14	A.S. Popov Odessa National Academy of Telecommunications (Ukraine)	ITU Regional Workshop for Europe and CIS on Cybersecurity and Child Online Protection. Conclusions and Recommendations

(continued)

Web	Received	Source	Title
2/74	2018-04-13	Korea Telecom (Republic of Korea)	Study topics for Question 3/2 in the current study period
2/71	2018-04-11	G3ict	Spammers and phishers who target persons with disabilities
2/66	2018-04-08	Algérie Télécom SPA (Algeria)	Proposals on the content of the (Question 3/2) final report
2/49	2018-03-15	Burundi	Current situation with regard to the Burundian Penal Code in relation to efforts to combat cybercrime
2/41	2018-02-28	Burundi	Cybersecurity, Internet Exchange point and e-commerce in Burundi

Incoming liaison statements for Question 3/2

Web	Received	Source	Title
RGQ2/242	2020-08-31	Council Working Group on Child Online Protection	Liaison statement from the Council Working Group on Child Online Protection (CWG-COP) to ITU-D SG2 on the outcome of the 15th and 16th Meetings of CWG-COP
RGQ2/174	2019-09-18	ITU-T Study Group 17	Liaison statement from ITU-T SG17 to ITU-D SG2 Q3/2 on vulnerability of TVs
2/182 +Ann.1	2019-02-11	ITU-T Study Group 17	Liaison statement from ITU-T SG17 to ITU-D Study Group 2 Question 3/2 on Cybersecurity in Africa (overview and outlook), from Democratic Republic of Congo
RGQ2/62	2018-09-14	ITU-T Study Group 17	Liaison statement from ITU-T SG17 to ITU-D SG2 Q3/2 on collaboration and liaison representative with ITU-D Question 3/2
RGQ2/43	2018-08-27	ITU-T Study Group 13	Liaison statement from ITU-T SG13 to ITU-D SG1 Q3/1 and ITU-D SG2 Q3/2 on inter-sector coordination
RGQ2/3	2018-05-11	ITU-T JCA-IMT2020	Liaison Statement from JCA-IMT2020 to ITU-D Study Groups 1 and 2 on invitation to update the information in the IMT2020 roadmap
2/73	2018-04-13	ITU-T JCA-AHF	Liaison Statement from ITU-T JCA-AHF to ITU-D Study Group 1 Q7/1 and Study Group 2 Q3/2 on JCA-AHF recent meeting reports
2/69	2018-04-09	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Q3/2 on collaboration and liaison relationship with ITU-D Study Group 2 Question 3/2
2/68	2018-04-09	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Q3/2 on best practices in Benin and Senegal

(continued)

Web	Received	Source	Title
2/67 (Rev.1)	2018-04-09	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Q3/2 on new work item X.framcdc "Framework of the creation and operation for a Cyber Defense Center"
2/62	2018-04-03	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Question 3/2 on new work item X.framcdc "Framework of the creation and operation for a Cyber Defense Center"
2/46	2018-03-05	ITU-T JCA-IMT2020	Liaison Statement from ITU-T JCA-IMT2020 to ITU-D study groups on invitation to update the information in the IMT2020 roadmap
2/23	2017-11-24	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Question 3/2 on an ongoing work item on technical framework for countering telephone service scam
2/10	2017-11-22	ITU-T Study Group 20	Liaison Statement from ITU-T SG20 to ITU-D study groups on work on the combat of counterfeit ICT devices and mobile device theft

Annex 2: List of lessons learned received on Question 3/2

Web	Received	Source	Title
SG2RGQ/272	2020-09-22	United Kingdom	UK case study: Cyber resilience best practice for SMEs

The UK Government provides targeted support to small and medium-sized enterprises (SMEs) to help them navigate complicated standards to better understand how to mitigate cyberrisk. This support is designed specifically for organizations who are not aware of the cyberthreat and have limited resources, both financially and in terms of technical capability. Lessons learned include the following:

- Clear and consistent cyberrisk management messaging is crucial. Critically, **awareness campaigns** should not just explain what businesses need to do and how they can actually carry out the action by pointing to government advice, guidance and support, but should draw attention to why they should do it.

- **Advice and guidance** is most effective when it is non-technical, size-specific and easy to access. Government and law enforcement should use national, regional and local networks, and work in partnership with key industry bodies, to identify levers and business touchpoints that can be used to amplify messaging, and ensure advice and guidance reaching SMEs.

- The creation of a government-backed **certification scheme** can be an effective intervention to support SMEs to improve their cybersecurity. The certification scheme can:

  - be quickly and effectively delivered by a single supplier if the government can outline the technical controls and/or minimum standards that should be covered;
  - evolve to continue to meet the needs of SMEs and address the changing threat landscape;
  - better ensure organizations remain compliant through having a certification expiry date and requiring annual recertification.

Web	Received	Source	Title
SG2RGQ/235	2020-08-20	United Kingdom	UK Government Digital Service (GDS) Global Digital Marketplace Programme

Challenges

A range of interconnected challenges face governments in relation to traditional approaches to public procurement of ICTs, which is typically:

- neither understanding nor meeting the needs of users
- task oriented, risk averse and inflexible
- isolated from what happens:
  - ‘before’ (strategic planning, investment appraisals, early market engagement)
  - ‘after’ (service delivery, monitoring and evaluation, supplier relationship management)
- hidden from public scrutiny due to the poor quality, inconsistency, incompleteness and poor availability of data.

User-centred design approaches

Since GDS was established in 2011, it has incubated, embedded and mainstreamed new standards-based approaches to government transformation.

These approaches were first conceptualized by the Government Design Principles,[163] published in April 2012.

Since then, GDS and the government and UK public sector more broadly have been incrementally applying these principles to redesign and improve services, organizational structures, governance approaches, etc. This includes public procurement.

Social Purpose Digital Commissioning

Focus on culture, mindset, collaboration and capability, by:

- understanding users’ needs
- being clear about the problems you are trying to overcome (e.g. legacy ICT, system vulnerabilities, capability and capacity, governance and accountability, etc.) to meet users’ needs
- being outcome-oriented (rather than solution-oriented), experimental and flexible, making small incremental investments to try out different approaches to address users’ problems, learning quickly and iteratively
- being multidisciplinary and collaborative coalition builders, advocating for systemic change through communities of practice
- engaging throughout the end-to-end lifecycle of delivery - the ‘before’ and ‘after’ of procurement
- being open to public scrutiny through deliberative participation of civil society, enabled by structured, quality, consistent, complete and published open data.

[163] UK Government. Guidance. Government Design Principles. April 2012.

Web	Received	Source	Title
SG2RGQ/215	2020-07-27	Brazil	#ConexãoSegura (#SafeConnection) Awareness Campaigns

The campaign around personal data protection on the Internet reinforced the importance of telling consumers how to protect themselves in the digital environment. The interactions of consumers on digital media and on the website revealed that many of them have a number of doubts about what is fraud or scam - especially when it involves cash prizes, in addition to not knowing what to do when they are victims of these situations. It is also important to advise people not to post or publish personal data (surprisingly many people do not know what can happen). In the next initiative, it would be interesting to expand the dissemination of materials further in order to reach a wider audience.

Web	Received	Source	Title
SG2RGQ/214	2020-07-27	Brazil	Brazilian National Cyberdrill - Cyber Guardian Exercise

The exercise started with two national critical infrastructure (NCI) sectors and evolved in its second edition to a broader and more complex exercise process. The exercise continues to evolve, and for its third edition (cancelled due to the COVID-19 pandemic) it was planned to include six NCI sectors and to add an international cooperation component to the exercise.

Web	Received	Source	Title
2/325	2020-02-08	Democratic Republic of the Congo	La sécurité numérique en République Démocratique du Congo

Turn cybersecurity in the Democratic Republic of the Congo into a lever for integration, protection, good governance, economic growth and social progress.

This vision will make a significant contribution to building the country’ s capacity in its digital transformation (circulation of information, data economy, growth economy, transparency and traceability, interoperability of information systems, etc.). It will allow digitalization to become a key driver for modernizing the State, promoting economic growth and fostering social progress.

Web	Received	Source	Title
2/336	2020-02-11	United Kingdom	Case study of best practices for securing customer Internet of Things in the UK

A significant proportion of IoT devices do not have basic cybersecurity features built into them. Following 18 months of collaboration with industry and experts at the UK’s National Cyber Security Centre (NCSC), the Department for Digital, Culture, Media and Sport (DCMS) published the Code of Practice (CoP) for Consumer IoT Security in October 2018. The 13 voluntary guidelines, as outlined in the 2018 CoP, provide a much-needed baseline for IoT devices that manufacturers should embed into their products to make them ‘secure by design’.

These include:

- No default passwords
- Implement a vulnerability disclosure policy
- Keep software updated
- Securely store credentials and security-sensitive data
- Communicate securely
- Minimize exposed attack surfaces
- Ensure software integrity
- Ensure personal data are protected
- Make systems resilient to outages
- Monitor system telemetry data
- Make it easy for consumers to delete personal data
- Make installation and maintenance of devices easy
- Validate input data.

These guidelines are outcome-focused as opposed to being prescriptive, which gives companies the space to come up with innovative solutions and appropriate ways to secure their products. Some devices might require enhanced security that is not included on this list and, as such, retailers and manufacturers are encouraged to secure their devices accordingly and seek solutions beyond the 13 guidelines. Action on the first three guidelines will bring largest security benefits in the short term.

Web	Received	Source	Title
2/331	2020-02-11	Keio University (Japan)	Proposed text for consideration of security issues for ICT accessibility

This document describes the consideration and implementation of cybersecurity measures for persons with disabilities, especially those with hearing difficulties, such as telecommunication relay service and remote captioning, to enhance accessibility to information and communication services.

Web	Received	Source	Title
SG2RGQ/134	2019-07-29	State of Palestine	Government Data Exchange

The central server issues certificates to security servers and provides a list of authenticated certificates to the systems connected to the Government Data Exchange. In addition, the central security server maintains encrypted activity data (hash logs) from the security servers to enable a series of e-service uses to be built subsequently, if necessary. If one of the parties to the service denies sending or receiving certain information, the service provider and user logs are compared with the encrypted copy in the central server. This method allows the integrity of security server logs to be checked, as it is impossible to change the log without it subsequently being detected.

The terms of the data-sharing process are defined by a memorandum of understanding signed by the two parties sharing the data and the Ministry of Telecommunications and Information Technology (MTIT), as third-party system operator. The memorandum includes an annex on the obligations of the parties, an annex on controls, standards and the duties and rights of each party, and an annex on the data which the two parties agree to share.

The system allows a connected ministry to determine which other connected institutions may access and read its data and the level of data that may be accessed. This is done by means of a control window on the ministry’s own security server, enabling it to grant access rights to any of its services to the institutions it wishes.

Encrypted data are shared directly through secure servers from one information system to another. They do not pass through the central system and cannot be displayed there. The central system only has statistical information on the data shared.

Using this approach, the system facilitates the secure sharing of data between institutions, enabling them to share data between one another. It has also made it easier for the public to access services currently available G2G, by only going to one institution where the service involves more than one. MTIT is currently working to develop this mechanism and to provide services to the public directly via applications being developed.

Web	Received	Source	Title
SG2RGQ/146	2019-08-21	Senegal	Overview of the National Cybersecurity School with a regional focus

- Enhancing international cooperation, particularly between developed and developing countries.
- The school’s regional nature helps to enhance cooperation among African countries.
- Covering all aspects of cybersecurity in both initial and continuing training.
- As cybersecurity is a prerequisite for the Digital Senegal 2025 Strategy (SN2025), classes have begun at the offices of the National School of Administration (ENA) while construction of the school’s own premises is being completed at Diamniadio, 20 km from Dakar.
- The school will be the final element in the system for information system security and cybersecurity already in place.
- Boosting the fight against cybercrime in Africa.

Web	Received	Source	Title
SG2RGQ/151	2019-08-22	United States	NIST Framework for Improving Critical Infrastructure Cybersecurity V1.1

The recent update process to develop Version 1.1 of the Framework demonstrates an example of a good process for stakeholder engagement to ensure the Framework remains a useful tool for managing cybersecurity risk.

Web	Received	Source	Title
SG2RGQ/155	2019-08-23	United Kingdom	Case study of best practices for ransomware risk mitigation in the UK

A recent advisory on ransomware from the National Cyber Security Centre (NCSC) recommends the following risk-mitigation techniques:

- Keep devices and networks up to date (e.g. prompt updating and patching, and regular scans)
- Prevent and detect lateral movement in your enterprise network
- Segment networks
- Set up a security monitoring capability
- Whitelist applications
- Use antivirus
- Back up files.

The full advisory and detailed list of recommendations can be found at: https://www.ncsc.gov.uk/news/ongoing-threat-organisations-ransomware

Protecting your organization from ransomware: https://www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware

Mitigating malware: https://www.ncsc.gov.uk/guidance/mitigating-malware

Unfortunately, it is not a question of ‘if’ but ‘when’ a cyberattack will occur. In the event an attack does take place, cooperation between the public and private sectors is key to understanding the threat and coordinating a quick and effective response to mitigate the impact of an attack. In the event of an attack, organizations are advised to contact the National Crime Agency, NCSC’s Cyber Incident Response, or Cyber Security Information Sharing Partnership (CiSP). NCSC led the UK’s response to the WannaCry attack and worked in collaboration with the National Crime Agency (NCA). Over the course of an incident, NCSC publishes statements and guidance for large organizations as well as home users and small businesses. Up-to-date information is announced via the NCSC Twitter account (@NCSC).

Web	Received	Source	Title
SG2RGQ/196	2019-09-24	Silensec Africa Limited (Kenya)	Using cloud-based cyber ranges and competence frameworks for the delivery of cyber drills

This contribution recommends the use of cyberrange technology (cloud-based – public or private cloud) and competency frameworks in the development and delivery of new generation cyberdrills.

Web	Received	Source	Title
2/201	2019-03-08	Côte d'Ivoire	Survey of online activities and Internet use by children in Côte d’ Ivoire

- De-dramatize prevention by banishing the anxiety-provoking approach. Internet prevention can be part of a fear culture. However, this increases the anxiety of parents who are already worried about a technology they do not understand well, thereby undermining the extraordinary learning tool that is the Internet.
- Encourage educational programmes aimed at developing best practices in content management and raising children's awareness of responsible use of the Internet.
- Put an Internet portal online in order to provide children, adolescents, parents and teachers with an educational base.
- Involve all stakeholders in community-awareness activities: government agencies, the private Internet sector, NGOs, community groups and the general public.

Web	Received	Source	Title
2/174	2019-02-07	Côte d'Ivoire	Mapping of cybercrime threats in Côte d'Ivoire

Statistics should be collected on complaints and damages (financial, moral).

Web	Received	Source	Title
2/173	2019-02-07	Côte d'Ivoire	Presentation of Platform for Combating Cybercrime (PLCC)

– Development of partnerships between bodies responsible for combating cybercrime and the police in developing countries
– Awareness-raising in schools
– Collaboration with equivalent organizations in other countries.

Web	Received	Source	Title
SG2RGQ/26 2/172	2018-08-14 2019-02-07	NRD Cyber Security (Lithuania)	National and sectoral CSIRT developments as means to strengthen cybersecurity environments (2018 +2019 update)

For national digital security success, CSIRTs should focus substantial energy on broad facilitation for developing additional independent capabilities – in industries, professional communities, education centres, research, events, meet-ups and conferences, private and internal CSIRTs.

Web	Received	Source	Title
2/167	2019-02-07	Symantec Corporation (United States)	The importance of cyber threat intelligence in the definition of national cybersecurity strategies

- Establish and adopt situation awareness and threat intelligence policies.
- Develop incident analysis and response capabilities - establish CERTs.
- Develop collaboration with the private sector and information-sharing policies (public-private partnerships).

Web	Received	Source	Title
2/152	2019-02-01	Benin	Cybersecurity in the era of the digital economy in Benin

Benin calls on ITU-D Study Group 2 to support:

- the establishment of a national CERT in Benin to enhance the level of trust in cyberspace;
- the building up of a common African security and defence policy;
- the creation of a panel of eminent personalities to reflect on Africa's role in regard to security;
- the establishment of a CERT-AFR (for Africa) along the lines of CERT-EU (for the European Union);
- a coordinated effort to avoid disparities between the strategies adopted and means deployed by Member States in terms of military cyberdefence capabilities;
- regulators and ICT authorities as they seek to:
  - adopt measures designed to enhance the security of information systems and networks;
  - create reliable digital identities;
  - protect minors and vulnerable groups; and
  - foster transparency.

Web	Received	Source	Title
SG2RGQ/25	2018-08-14	Proge-Software [SME pilot] (Italy)	Data Privacy and Cloud - be compliant

General Data Protection Regulation (GDPR)

General Data Protection Regulation (GDPR) (EU) 2016/679 governs data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA. The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying regulation within the EU. Superseding Data Protection Directive 95/46/EC, the regulation contains provisions and requirements pertaining to the processing of personally identifiable information (personal data) of individuals (formally called data subjects in the GDPR) inside the European Union, and applies to an enterprise that is established in the EU or – regardless of its location and the data subjects' citizenship – that is processing the personal data of people inside the EU. Controllers of personal data must put in place appropriate technical and organizational measures to implement the data-protection principles. Severe penalties are applied to violators.

Cloud computing

In computer science, cloud computing describes a type of outsourcing of computer services, similar to the way in which electricity supply is outsourced. Users can simply use it. They do not need to worry where the electricity is from, how it is made, or how it is transported. Periodically they pay for what they have consumed. The idea behind cloud computing is similar: The user can simply use storage, computing power or specially crafted development environments without having to worry how these work internally. Cloud computing is usually Internet-based computing. According to a paper published by IEEE Internet Computing in 2008, "Cloud computing is a paradigm in which information is permanently stored in servers on the Internet and cached temporarily on clients that include computers, laptops, handhelds, sensors, etc.".

Web	Received	Source	Title
SG2RGQ/32	2018-08-16	Guardtime AS [SME pilot] (Estonia)	Towards cyber resilience – the role of national cyber exercises

Cyberexercises are essential to achieving sustainable cyberresilience. Cyberexercises are different from training, and must be customized, realistic and engaging. Governments should consider developing a programme to govern cyberresilience, covering education, training and cyberexercises ranging from localized events to customized national-scale exercises conducted on a regular basis.

Web	Received	Source	Title
2/71	2018-04-11	G3ict	Spammers and phishers who target persons with disabilities

1. Contact the service provider to inform it of the highjacking of your e-mail address.
2. Try to give information on the spammer's/hacker's contact details with an example e-mail, e.g. by forwarding the suspect e-mail to its fraud section.
3. Ask to have your violated e-mail blocked.
4. Change your e-mail address.
5. Let your friends and contacts know you have been hacked and give them the new address.
6. Do not click on any web addresses unless you have verified it is in fact from a known source.

Web	Received	Source	Title
2/41	2018-02-28	Burundi	Cybersecurity, Internet exchange point and e-commerce in Burundi

Security of IT data and of communication networks in order to ensure high-quality services is the pillar of ICT-sector development. A legal and regulatory framework for cybersecurity in our country is an essential tool for implementing all aspects of data security. The introduction of an Internet exchange point facilitates local communications and reduces latency times and associated costs. Lastly, domain name management provides facilities for investors. Data security will thus enable us to ensure reliable e-transactions and retain our customers.

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 des Almadies
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
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792
Belvedere Harare
Zimbabwe

电子邮件： itu-harare@itu.int
电话： +263 4 77 5939
电话： +263 4 77 5941
传真： +263 4 77 1257

美洲

巴西
国际电联
区域代表处
SAUS Quadra 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： ituteguciglapa@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
Thailand Post Training Center
5th floor
111 Chaengwattana Road
Laksi
Bangkok 10210
Thailand

邮寄地址：
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Thailand

电子邮件： ituasiapacificregion@itu.int
电话： +66 2 575 0055
传真： +66 2 575 3507

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

邮寄地址：
c/o UNDP – P.O. Box 2338
Jakarta 10110, Indonesia

电子邮件： ituasiapacificregion@itu.int
电话： +62 21 381 3572
电话： +62 21 380 2322/2324
传真： +62 21 389 5521

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： itumoscow@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: 978-92-61-34105-3

9 789261 341053

瑞士出版
2021年, 日内瓦