联合国 A/76/187

大 会

Distr.: General
19 July 2021
Chinese
Original: English/Spanish

第七十六届会议

临时议程* 项目 96

从国际安全角度看信息和电信领域的发展

从国际安全角度促进网络空间国家负责任行为

秘书长的报告

目录

* A/76/150

21-10045 (C) 090921 170921

一. 导言

1. 2020 年 12 月 7 日，大会在题为“从国际安全角度看信息和电信领域的发展”的议程项目下，通过了题为“从国际安全角度促进网络空间负责任国家行为”的第 75/32 号决议。

2. 大会在该决议第 2 段中请所有会员国考虑到政府专家组报告所载的评估和建议，继续向秘书长通报它们对下列问题的看法和评估：

(a) 在国家一级为加强信息安全和促进该领域国际合作所作的努力；

(b) 政府专家组各项报告提及概念的内容。

3. 根据这一要求，在 2021 年 2 月 18 日向所有会员国发出一份普通照会，邀请各国提供有关该主题的信息。为便利会员国就上述问题提交意见，提交的截止日期定为 2021 年 5 月 31 日。

4. 截至本报告编写之时收到的回复载于下文第二、第三节。2021 年 5 月 31 日以后收到的更多答复将以来件原文发布在裁军事务厅网站上。[1] 将不印发增编。

二. 从各国政府收到的答复

澳大利亚

[原件：英文]
[2021 年 5 月 31 日]

澳大利亚欢迎有机会响应大会第 75/32 号决议的邀请，就在国际安全背景下推进网络空间负责任国家行为发表看法。这份文件是基于澳大利亚根据关于“从国际安全角度看信息和电信领域发展”的 2020 年第 74/28 号决议、2016 年第 70/237 号决议、2014 年第 68/243 号决议、2011 年的第 65/41 号决议提供的资料。

国际网络和关键技术参与战略

2021 年 4 月 21 日，澳大利亚外交部长马丽斯·佩恩发布了澳大利亚的《国际网络和关键技术参与战略》，其中阐述了澳大利亚在网络空间和关键技术方面的利益和目标。澳大利亚的总体目标是使澳大利亚、印度洋-太平洋地区、全世界在网络空间和关键技术的助力下实现安全、稳定、繁荣(http://www.internationalcybertech.gov.au/)。

该《战略》提出了澳大利亚通过在各类网络和关键技术问题上追求此目标所维护的利益。这包括我们的核心原则和价值观，即人权、法治、公平、公开竞争、安全、透明、尊重、诚信。

[1] http://www.un.org/disarmament/ict-security。

该《战略》确定了三大支柱，即价值观、安全、繁荣，以指导澳大利亚在国际网络和关键技术方面的参与：

(a) 价值观：澳大利亚在处理网络空间和关键技术问题时将始终以价值观为基础，反对利用技术破坏这些价值观；

(b) 安全：澳大利亚将始终支持国际和平与稳定，并支持安全、可信、复原能力强的技术；

(c) 繁荣：澳大利亚将始终倡导以网络空间和技术促进可持续经济增长、发展、繁荣。

2020 年 8 月 6 日澳大利亚还发布了《2020 年网络安全战略》，旨在为澳大利亚人、澳大利亚企业、澳大利亚所依赖的基本服务创建更安全的网络世界(www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf)。

推进网络空间负责任国家行为的框架

随着各国日益在网络空间施加力量和影响，澳大利亚认为制定明确的规则非常重要。“从国际安全角度看信息和电信领域的发展政府专家组”的 2010 年报告(A/65/201)、2013 年报告(A/68/98)、2015 年报告(A/70/174)确认现行国际法对维护网络空间的和平与稳定是适用的，也是至关重要的。这些报告还阐明了 11 项自愿、非约束性的负责任国家行为规范，同时确认需要制定建立信任措施和协调开展能力建设。国际法、规范、建立信任措施、能力建设加在一起为安全、稳定、繁荣的网络空间提供基础，通常被称为负责任国家行为框架。

澳大利亚积极参与了联合国最近审议网络空间负责任国家行为的两个进程。这两个于 2021 年结束的进程是：第六届政府专家组(见 A/76/135)、不限成员名额工作组(见 A/75/816)。这两个进程重申并增强了上述框架。

澳大利亚重申其承诺按照政府专家组 2010 年、2013 年、2015 年、2021 年的各次报告(A/65/201、A/68/98、A/70/174)以及不限成员名额工作组的报告(A/75/816)采取行动。

国际法

澳大利亚关于国际法如何适用于网络空间国家行为的立场载于一系列文件，包括：澳大利亚的《2017 年国际网络参与战略》(www.internationalcybertech.gov.au/about/2017-International-Cyber-Engagement-Strategy)、《2019 年国际法附录》(https://www.internationalcybertech.gov.au/sites/default/files/2020-11/2019%20Legal%20Supplment_0.PDF)、2020 年 2 月发表的关于国际法对网络空间适用的案例研究(https://www.dfat.gov.au/sites/default/files/australias-oewg-non-paper-case-studies-on-the-application-of-international-law-in-cyberspace.pdf)、澳大利亚的《2021 年国际网络和关键技术参与战略》、澳大利亚提交的关于国际法的呈件，将作为 2021 年在国际安全背景下推进网络空间负责任国家行为政府专家组报告(待发布)的附件。

多利益攸关方参与

澳大利亚认识到包括民间社会、私营部门、学术界、技术界在内的多利益攸关方社区在促进自由、开放、安全、稳定、无障碍、和平的网络空间方面具有重要作用。

为此，澳大利亚高兴地共同发起了 LetsTalkCyber 倡议(letstalkcyber.org)这个平台，供多利益攸关方向不限成员名额工作组提供意见和进行参与，也供各国、民间社会、私营部门、学术界、技术界相互开展协商。澳大利亚还进行了几轮国家多利益攸关方协商，并积极征求多利益攸关方群体的意见，以便为其在不限成员名额工作组和政府专家组进程中所持的立场提供依据。

此外，澳大利亚还建立了“四方技术网络”，以支持澳大利亚、印度、日本、美利坚合众国的政府、学术界、智库合作伙伴就网络和关键技术问题开展研究，并促进它们之间进行互动。“四方技术网络”的职能包括：产生与政策相关的研究和建议；深化和加强公众对网络和关键技术问题的了解；促进知情的公众对话。该网络于 2 月 9 日启动，发布了一系列关于国际和平与安全、互联互通、区域复原力、人权、伦理、国家安全的公开文件(www.internationalcybertech.gov.au/node/139)。

哥伦比亚

[原件：西班牙文]
[2021 年 5 月 31 日]

哥伦比亚根据大会关于从国际安全角度促进网络空间负责任国家行为的第 75/32 号决议，在考虑到政府专家组报告中所载的评估和建议的同时，高兴地向秘书长通报对以下问题的看法和评估：

- 在国家一级为加强信息安全和促进国际合作所作的努力。
- 政府专家组各项报告所提及概念的内容。

本报告以 2020 年提交的报告为基础，重点介绍了去年取得的进展，主要涉及政府专家组 2015 年报告中提出供各国审议的建议，目的是促进在信息和通信技术(信通技术)领域保持开放、安全、稳定、无障碍、和平的环境。

负责任国家行为的自愿规范、规则和原则

各国应遵循联合国宗旨，包括维持国际和平与安全的宗旨，合作制定和采取各项措施，加强信通技术使用的稳定性与安全性，并防止发生公认对国际和平与安全有害或可能对其构成威胁的信通技术做法。

我国国家数字信任和安全政策(国家经济和社会政策理事会第 3995/2020 号文件)强调承担责任的概念，其主要目标之一是促进公共部门和私营部门的公民建设数字安全能力。

哥伦比亚政府通过信息和通信技术部、国家培训局、教育部按照承担责任战略实施了一系列具体活动，包括：

- 信息和通信技术部根据“让我们谈谈数字政府”计划(2020 年到 2021 年)举办了 15 次公民数字安全意识提高会议，参与者达 4 000 多人。2020 年该部为企业家、中小微企业举办了 3 期数字安全培训班，共有 483 人参加，其中 156 人为女性。该部还就信息安全和隐私模式的具体方面举办了 2 次讲习班。

- 在“数字安全月”开展了几项活动，包括：在思科和哥伦比亚计算机应急小组支持下举办了 4 次与事件管理有关的专题讲习班；举办了 2 次关于公共实体审计和风险管理重要性的讲习班；与美洲国家组织(美洲组织)就“让我们谈谈数字政府”活动的结果举行了两次会议；在哥伦比亚举办了首届网络安全创新理事会会议；举办了题为“关于如何避免遭受网络罪犯侵害的建议”和“从法律角度看网络上的虚假信息”的讲座，目标是普通公众。作为“数字安全月”的最后一项活动，与美洲组织联合举行了第二届网络安全创新理事会会议。共有 1 040 人(包括公职人员和最终用户)参加了上述活动，45%的参与者为女性。

- 2020 年首席信息官峰会期间，公共实体的技术负责人汇聚一堂，所开展一项活动是“哥伦比亚 4.0”，举行了一场主题为“如何成功应对 COVID-19 和数字化转型，且不受黑客之害”的会议，与会者有 490 人。还举办了以“根据 MITRE ATT&CK 和 XDR 模式检测和应对威胁的最佳做法”为主题的讲习班。估计有 40%的参与者为女性。为来自 1 834 个实体(包括 131 个国家实体和 1 224 个地方实体)的约 3 196 名官员举办了与信息安全和隐私模式有关的提高认识活动。

- 信息和通信技术部发起了“数字人才”倡议，包括开展了“数字技能-网络安全培训”竞赛，以选拔哥伦比亚人员从事网络安全相关事项的培训和能力建设。为培养专门技能开办了 2 个文凭课程，即：㈠ 行政和管理人员网络安全课程，㈡ 技术人员网络安全课程。

- 国家培训局开办了以下主题的课程：计算机网络安全、数据库管理与安全、数字安全监测、设备固件编程、介绍符合《国际标准化组织和国际电工委员会第 27001 号标准》的信息安全管理系统、诊断技术在网络安全领域的应用、计算机安全管理。

- 为促进承担责任，教育部开展了与内容传播有关的活动(包括开展以社交网络利用为主题的活动，还包括与公共实体及中小微型企业共同开展宣传活动、举办讲习班)。教育部还与私营部门建立了伙伴关系，并参与了国际合作。

- 教育部开展的活动还包括：开办了一些文凭课程，使 2 216 名教师受益；将数字安全战略纳入小学生、初中生、高中生数字学习项目，使 4 093 名学生受益，其范围包括“哥伦比亚学习”门户网站，内容有 30 多条。

有一条建议是各国不应在知情情况下允许其领土被人用于利用信息和通信技术进行国际不法行为。根据该建议，哥伦比亚政府实施了下文所述的活动。

- 我们在国家数字信任和安全政策(国家经济和社会政策理事会第3995/2020号文件)中规定国家协调员发挥协调和治理机制的职能。此职能由总统经济和数字转型顾问办公室和数字安全委员会履行。数字安全委员会是合议性机构，由参与促进数字安全的各实体组成，目标是在其任务范围内从战略层面审议与数字安全有关的具体问题，包括：(1) 数字安全政策和法律；(2) 保护和保卫国家关键网络基础设施；(3) 数字安全风险管理；(4) 危机和网络威胁监测；(5) 个人资料保护；(6) 国际数字安全问题；(7) 关于数字安全的战略信息传播。

- 我国政府设立了统一的网络安全指挥所，确保政府技术基础设施和网站在国家节假日、选举等里程碑事件期间安全无虞、妥善运作。该职能的目标是：㈠ 保护公民和政府免受网络威胁；㈡ 预防和预见网络威胁，并进行司法调查；㈢ 处理网络安全事件；㈣ 确保政府和机构的稳定性；㈤ 加强软件建设。政府还制定了行动规范，以应对可能的攻击，例如对门户网站的分布式拒绝服务攻击、网络漏洞、假新闻。

- 政府与国家参议院协调开展活动，包括就如何在使用虚拟平台方面制定最佳做法开展培训。

为了以最佳方式开展合作，包括交流信息、提供互助、起诉将信通技术用于恐怖主义和犯罪的行为、采取其他合作措施应对此类威胁，哥伦比亚于2020年3月16日加入了2001年在布达佩斯通过的《网络犯罪公约》，并于2020年7月1日使其生效。目前正在努力执行该《公约》。

哥伦比亚已采取适当措施保护关键基础设施免受信通技术方面的威胁，包括加强了政府的计算机安全事件应对小组，以保护公共机构。通过这一举措，哥伦比亚旨在制定全面的解决方案，确保政府的计算机安全事件应对小组向国家各实体提供更有力、更有效的服务，为此要提高该小组在全国各地的影响力，包括发展信息技术，建设有形基础设施，增强人力资源，保证全天候服务。

哥伦比亚还提出了一些倡议，包括通过当前评估和未来计划在业务、行政、人力、科学方面不断加强能力并改进技术基础设施，以便利用资源加强国家各实体的数字安全能力。目前也在进行搬迁和优化政府计算机安全事件应急小组的项目。

有一条建议是各国应鼓励负责任地报告信通技术方面的薄弱环节，并分享现有补救措施的相关信息，以限制并有可能消除信通技术和依赖信通技术的基础设施所面临的潜在威胁。根据这一建议，哥伦比亚与美洲国家组织和经济合作与发展组织一道，鼓励负责任地报告信通技术方面的薄弱环节，并正在采取合理步骤确保供应链的健全性，防止恶意信通技术工具、技术、有害隐蔽功能的扩散。

题为“国家数字信任和安全政策”的新公共政策文件(国家经济及社会政策理事会第3995/2020号文件)确定了一些具体措施，以便制定模式，用以定期报告关键活动支助资产的所有者和运营者与相关国家政府机构之间连接点各部门的薄弱环节。许多利益相关者将参与制定这一模式，并将参照国际经验。

还有一条建议是各国不应从事或故意支持损害另一国经授权应急小组(有时称为计算机应急小组或网络安全事件应急小组)的信息系统的活动，而且各国不应利用经授权应急小组从事恶意的国际活动。就此建议，哥伦比亚认识到自身对维护安全与和平的信通技术环境负有首要责任，已根据国际法和《联合国宪章》采取措施。

哥伦比亚政府还于 2021 年 3 月发布了第 500 号决定和第 3 号总统令，为数字安全战略规定了指导方针和标准，并将安全和隐私模式确定为推动数字政府政策的要素。

2019 年第 2106 号法令第 16 条就如何简化、消除、改革不必要的公共行政手续、流程、程序颁布了规则，并规定当局必须根据信息和通信技术部发布的指导方针为电子文件管理和信息保存制定数字安全战略。

信息和通信技术部作为数字政府政策的推动者，就如何实施信息安全与隐私模式和管理信息安全风险制定了指导方针，还制定了数字安全事件管理程序以及数字安全战略指导方针和标准。

哥伦比亚就执法、情报、外交领域的各种工具采取了措施，确保在网络空间开展工作前采取一切可能的方式保卫相关网络，以阻止网络攻击、防止财产被毁坏、避免生命损失。

哥伦比亚政府在制定国家数字安全政策时将重点放在 3 个基本领域：㈠ 建设数字环境风险管理能力；㈡ 建立支持治理的机构；㈢ 对活动框架和国际最佳做法进行评估。为了落实这项政策，政府的策略是：

- 就持续改进业务、行政、人力、科学领域的能力和技术基础设施进行现状评估和未来规划。
- 为建立数字化公民参与网络制定指导方针，使各利益攸关方能够通过该网络在应对网络威胁方面进行互动和合作，从而按照国际法加强和扩大哥伦比亚的数字安全能力。
- 协调数字安全改善计划准则的制定工作，目的是使综合社会保障系统在处理、管理、交换信息方面增强能力，因为该系统构成关键性网络基础设施。
- 在国家事件管理模式下制定准则，就如何管理风险和解决数字安全事件规定特殊规则，据以处理、管理、交换来自综合社会保障系统的信息。这些规则必须纳入数字安全委员会制定的一般事件管理程序。
- 协调纳入技术、法律、组织等方面的适当机制，以便在发生网络安全事件时收集必要的数字证据，从而处理、管理、交换来自综合社会保障系统的卫生子系统的信息。
- 就建立综合社会保障部门计算机安全事件应对小组一事设计、制定、提交计划草案。

- 就建立情报部门计算机安全事件应对小组一事设计、制定、提交计划草案，以利于确保国家数字安全。

- 就建立国家级别数字安全事件统一中央登记处一事制定提案。此举是为了分析事件类型，也是为了定期评估是否需要在战略和资源上将事件管理工作置于优先地位。该登记处应收集各利益攸关方关于此主题的现有报告，并应简化信息的发送，建立安全的传递手段，确保各方之间交换信息时保守机密、妥善使用。

哥伦比亚谋求保护公民在获取和使用信息方面的宪法权利和自由。

哥伦比亚已采取必要立法措施将下列行为定为刑事犯罪：㈠ 故意及未经授权进入整个或部分计算机系统；㈡ 故意及未经授权损坏、删除、恶化、更改或隐藏计算机数据；㈢ 蓄意及未经授权以技术手段截取计算机数据；㈣ 制作、传播或传播儿童色情制品。

哥伦比亚正在就国家和国际关键基础设施制定明确定义，同时正在确定哪些部门的产品或服务符合关键基础设施的标准，并且保持关键资产清单。我国正在与国际社会分享这些定义，将其作为一项建立信任措施。

哥伦比亚还正在努力建立危机解决网络，供请求支持的相关公共部门利益攸关方开展互动。此外，我国还计划协同国际社会建立“在政策和技术层面”相互联系的网络。在这方面，哥伦比亚已采取下述行动：

- 设计了国内和国际网络安全演习，通过联合网络安全演习定期测试与其他国家沟通、回应援助及减轻风险请求的能力(特别是沟通渠道、协议、程序)。

- 参与了 CyberEx 框架内的活动和国际电信联盟网络的 CyberDrills 演练，并与联合网络司令部协调开展了国家危机模拟演习。

- 使用了预先建立的国家多方利益攸关方危机解决网络，在此类网络行动期间借助了国家和非国家行为者在减轻风险方面提供的专门知识，遵循了与报告国内和国际两级事件有关的最佳做法。

- 与各类协会一起开展了活动。自从黑客团体在网络空间的社会抗议活动中对政府和私营公司发动攻击以来，哥伦比亚软件和信息技术行业联合会一直代表一些公司与政府合作开发具体的数字安全解决方案。在此项合作中，该联合会与政府开会讨论了联合会可在哪些领域为政府提供支持，并为此在成员公司中就情报和监测能力开展了调查。

哥伦比亚政府协同美国打击了针对关键基础设施的恶意网络行动。

自愿建立信任措施

我国国家警察总局加强了与相关方面的合作，包括为就恶意使用信通技术行为交换信息和协助调查设立了协调中心，通过刑事调查局网络警务中心和国际刑

事警察组织(国际刑警组织)与国家政府数字安全委员会的成员实体开展合作，共同处理网络安全三个方面的问题，即：预防、调查、计算机取证。

因此，2020、2021 年开展了下述活动：实施了 32 次反网络犯罪行动，逮捕了 219 名网络犯罪人员；通过全天候虚拟 CAI 服务处理了 14 072 起网络安全事件；针对 7 139 个含有儿童性虐待材料的网站、1 648 个非法赌博网站提出了取缔要求；发布了 454 份新闻简报。

哥伦比亚为巩固我国的网络安全和网络防御能力，还促进有关方面积极合作，实施了由哥伦比亚网络安全能力中心领导的网络岗哨制度。

哥伦比亚网络安全能力中心一直在执行《网络安全综合战略》，以确保中央司法警察与 51 个地方刑事侦查单位之间积极协调，使侦查技术标准化，并使开展积极合作的工具和机制实现标准化。

根据总检察长办公室的报告，网络犯罪自 2009 年以来一直在增多，2019 年急剧增多。2018 年发生网络犯罪 22 238 起，2019 年发生 24 197 起，增幅达 9%。这一趋势在 2020 年更趋严重：2020 年 1 月 1 日至 12 月 31 日发生了 35 346 起网络犯罪，增幅达 70%。因此，我国的网络犯罪案件数量在疫情期间大幅度增加。

总检察长办公室通过永久性沟通渠道与网络警务中心交换信息。该中心是根据《网络犯罪公约》第 35 条设定的全天候联系人。

为了改善这两个实体之间的合作，哥伦比亚国家警察总局网络安全能力中心就网络警务中心的能力为总检察长办公室负责处理网络犯罪问题的部门举办了培训。

如前所述，哥伦比亚颁布的国家经济和社会政策理事会第 3995/2020 号文件要求增强网络安全、改进网络防御政策、加强国际合作。我国还希望通过统一指挥所制度等危机应对机制改善国家级网络安全利益攸关方之间的信息共享与合作，并开展更加强有力、有效、及时的协调。

在合作方面，如果其他国家请求协助调查与信通技术有关的犯罪行为或调查为恐怖主义目的使用信通技术的行为，或其请求协助防范源自哥伦比亚的恶意信通技术活动，则总检察长办公室将按照国内法和国际法以及总检察长办公室 2020-2024 年战略指南优先调查此类网络犯罪行为(该指南是总检察长办公室制定的路线图，其中全面阐述了今后的工作规划)。因此，该办公室将制定战略，以加强和协调处理此类案件的调查人员和检察官的调查能力。

自 2009 年第 1273 号法颁布至今的每月网络犯罪统计数据可在总检察长办公室网站题为“总检察长办公室的公开数据：搜索和下载档案”的部分查阅，其参数包括：相关行为按《哥伦比亚刑法》规定属于何犯罪类型、总检察长办公室收到犯罪报告的年份或事件发生的年份、事件发生在何部门、诉讼的状况及阶段、受害者或嫌疑人的性别及年龄组。该数据库还有信息表明所举报的犯罪行为是否已被提出指控、是否已定罪、是否已发出逮捕令、或案件是否已因事件不构成犯罪或未发生而结案。

总检察长办公室设在我国主要城市的各个国家级网络犯罪小组负责处理、分析、保存网络犯罪的数字证据，并负责展开调查。此类犯罪行为包括利用计算机进行盗窃，也包括制作与散布儿童色情制品。相关犯罪行为按事发地点确定属于哪个小组的管辖范围。在此类调查期间，各小组按规定进行面谈和检查、发出禁止离境令、进行核实、实施搜查、扣押物品、逮捕嫌犯、陪同被捕者参加各种审讯。各小组还按规定支持其管辖范围内的所有政府机构在所有需要从设备或互联网网站中提取和保存数字证据的刑事案件中实施此类行动(相关刑事案件包括杀人案件、与 14 岁以下未成年人发生性行为案件、涉及 18 岁以下未成年人的色情案件，有时甚至包括诽谤案件。

总检察长办公室国际事务局负责处理所有法律援助请求，其中大部分涉及援引《网络犯罪公约》。该局已采用了《跨境请求电子证据实用指南》中建议的标准和筛选规则。此文件由联合国毒品和犯罪问题办公室、联合国反恐怖主义执行局、国际检察官协会联合编写，已在美洲组织支持下翻译成西班牙文。

国家警察总局作为《网络犯罪公约》规定的全天候联系单位，通过哥伦比亚网络安全能力中心成为主要的国际合作实体之一，其相关行动包括将欧洲联盟执法合作署、国际刑警组织等重要机构作为网络安全联系单位，还包括加强了参与执行《公约》的机构。

哥伦比亚意图通过该全天候联系单位与《网络犯罪公约》其他 65 个缔约国和 13 个观察员方展开合作，加快处理司法协助请求的速度。

以下信息涉及下述建议：鉴于信通技术的发展速度和威胁的范围，有必要增进共识、加强合作，为此应努力在联合国主持下定期举行广泛参与的机构对话，并通过双边、区域、多边论坛以及其他国际组织定期举行对话。

哥伦比亚继续积极参加联合国等国际论坛主持的多边对话，尤其是讨论网络空间负责任国家行为以及国际安全背景下信息和通信领域发展方面的问题。

在现今前所未有的全球互联互通环境下，各国保持着复杂的相互依存关系，共同面临着无法单独解决的共同问题。因此，各国必须选择在网络安全方面开展国际合作，因为信息技术和媒体的传播和使用影响到整个国际社会的利益。所以促进为和平目的使用信通技术、防止因使用信通技术而产生冲突符合所有国家的利益。有鉴于此，各国应当：

- 以计算机安全事件应对小组领导的国际合作为基础，提高各国开展合作、采取集体行动的能力，促进将信通技术用于和平目的，助力建设对国际安全至关重要的信通技术能力。
- 为私营部门、学术界、民间社会组织的参与建立机制，从而为所有国家都参与的国际安全背景下的信息和电信领域建设作出贡献。

关于在双边组织、多边组织、区域组织中实施自愿合作措施这项工作，哥伦比亚政府为了确保有效开展自愿合作和增加信任，以支持各国共同努力打击国内国际的信通技术威胁，通过信息和通信技术部采取了下述行动：

- 参加了拉丁美洲和加勒比电子政务领导人网络的网络安全圆桌会议等区域方案，并继续与美洲组织开展合作。

- 自 2017 年以来参与了由美洲组织网络安全方案负责协调的、花旗基金会负责资助的网络安全职业道路项目。该项目旨在为来自巴西、哥伦比亚、哥斯达黎加、多米尼加共和国、秘鲁的 18 至 25 岁低收入家庭年轻人提供网络安全领域的培训，促进其职业发展。

- 制定了“女网络安全员”倡议，目的是通过提高妇女对网络安全相关事项的了解，为妇女促进和创造教育空间与工作机会。信息和通信技术部通过这一倡议培训了 350 多名女性安全专家，她们将成为哥伦比亚获资格认证的一级女性数字安全专家群体的一部分，未来将组成“哥伦比亚女性网络安全工作队”，使该国成为此类倡议的区域领导者。

- 在网络安全创新理事会主持下举办了对话，期间由区域专家和设计思维专家牵头举行了 2 次活动，参与者为公共部门、私营部门、工会、学术界的高级管理人员，目的是促进本区域网络安全方面的创新、提高参与者的认识、传播最佳做法。此类创新理事会根据美洲组织网络安全计划与思科之间所订协议成立，在美洲组织协助下举行会议。

鉴于平民私有财产是网络攻击的主要对象，哥伦比亚政府承诺采取集体行动加强互联网安全，鼓励技术公司为保护平民提供技术援助。为此，我国政府通过信息和通信技术部实施了“我信赖信通技术”方案，目标是促进数字技能的发展，从而安全地应对使用互联网和信通技术方面的风险，同时促进对互联网的使用和责任感，并将此作为创造积极数字影响的机会。该方案面向 6 岁至 28 岁的男性和女性人员，通过举行虚拟和面对面工作会议讲授不同的战略，帮助参加者培养风险识别技能，促进数字共存和数字社会活动，推动利用技术工具在互联网上宣传有积极意义的共同事业。

此外，哥伦比亚政府还通过信息和通信技术部向请求计算机安全事件应对小组给予支持的公共实体提供信息安全方面的专门培训，并且正在扩大网络安全研究的范围，同时还在业务、行政、人力、科学上加强相关的能力，以及改善有形基础设施和技术基础设施。例如，我国政府采取了以下行动：

- 制定了一份指南，为相关实体实施贯穿各领域的信息安全和隐私保护规则提供咨询和帮助。该指南遵循以下列要素为基础的数字政府政策：㈠ 信息安全和隐私保护模式；㈡ 数字安全风险模式，用于为政府行政部门各实体管理风险、制定控制方法提供指南。

- 为促进对数字安全政策承担责任制定了战略。为此举办了讲习班，通过讨论提高了认识，还开发了互动工具和培训课程。

- 政府的计算机安全事件应对小组向所有国家实体提供了基本的主动和被动的安全管理服务，包括就网络威胁和漏洞发布警报和警告，对事件

进行处理、分析、反应、协调，在所有数字安全工作者和官员中培养数字安全文化，从而提高其安全意识。

- 政府的计算机安全事件应对小组通过其成套服务向国家实体提供援助和支持，以改善技术基础设施安全流程，加强网络安全事件管理，提高数字安全意识。政府的计算机安全事件应对小组由专门技术人员组成，负责为预防和管理网络安全事件实施和制定活动。

信息和通信技术安全和能力建设方面的国际合作与援助

总检察长办公室指出，为了促进跨国界合作以弥补跨国界关键基础设施的薄弱环节，必须增强本区域打击网络犯罪的能力。因此，哥伦比亚寻求发展战略伙伴关系，参加了各种论坛。例如，我国已正式成为《网络犯罪公约》缔约国，参与了联合国各相关工作组，并与其他国家签署了打击网络犯罪的谅解备忘录。

此外，哥伦比亚为了开展合作与协调，正在与美洲各计算机安全事件应对小组构成的网络进行协作。这些小组通过此平台就数字威胁交换信息、开展合作。

哥伦比亚还参加国际信息交流项目，例如向该区域其他国家与金融部门有关的政府和监管实体(包括中美洲银行、保险公司及其他金融机构主计长理事会、拉美太平洋联盟)发布公告和预警。

在总检察长办公室推动下与其他国家签署了一些谅解备忘录，以打击网络犯罪和相关犯罪活动。

为进一步开展能力建设，包括通过取证和采取合作措施应对犯罪份子或恐怖分子使用信通技术问题，我国在提升技术和能力方面作出了努力，但进展不快，原因是许可证、设备、培训费用高昂。

有一条建议是，为了建设信通技术安全能力，可考虑制定双边和多边合作倡议，以现有伙伴关系为基础加强信通技术安全能力，从而改善环境，以利于各国和主管国际组织(包括联合国及其机构、私营部门、学术界、民间社会组织)在应对信通技术事件方面有效开展互助。根据该建议，哥伦比亚政府通过信息和通信技术部担任拉丁美洲和加勒比电子政务领导人网络执行委员会主席。该委员会汇集了本地区 34 个国家政府的数字事务主管部门，宗旨是解决网络安全问题。

该委员会拟以开展各种活动，以促进对网络安全状况的了解，并就如何提高拉丁美洲和加勒比电子政务领导人网络成员国和本区域的网络安全水平提出措施建议，请该网络批准。这些活动包括：

- 美洲开发银行和美洲组织就网络安全成熟度开展研究。
- 以 SIM3 模型测定计算机应急小组和计算机安全事件应对团队的成熟度。
- 将网络安全指南、程序、良好做法存档。
- 为决策者举办关于网络安全问题的活动。
- 制定区域网络安全战略。

- 制定本区域处理敏感数据的自愿良好做法(改进跨境数字签名的使用和互操作性)。
- 研究本网络成员国计算机安全事件应对团队的现状。
- 建设部门计算机安全事件应对小组，本区域各计算机安全事件应对小组间开展协作。
- 开展网络安全能力建设。
- 开展计算机安全事件应对小组的能力建设。
- 建设恶意软件信息共享平台(美洲各计算机安全事件应对小组)。
- 进行区域数据保护框架分析。

此外，哥伦比亚政府还与美洲组织以及信息和通信技术部商定后采取步骤，通过以下方式为哥伦比亚制定一系列数字安全治理模式建议，同时就识别与管理数字安全风险的方法制定指南：

- 为这两个拟提议的产品收集信息来源和参考资料。
- 为这两个产品分析最佳方法，包括采用适用于数字安全的治理模型进行基准研究。
- 分析本地环境(机构、利益攸关方等)。
- 制定治理模式的拟议原则和目标。
- 批准提议的目标，并就治理模式向多个利益攸关方征求意见。
- 确定利益攸关方对治理模型的期望。

哥伦比亚为批准关于治理模式的拟议原则和目标，也为了解利益攸关方的关切点，于 2020 年 10 月 30 日在数字安全委员会正式会议期间举行了第一次工作组会议。代表国家网络安全生态系统中多个利益攸关方的 80 多人出席了会议。

哥伦比亚政府为了建立一个不仅与其他国家而且与国内私营部门开展业务合作的平台，以应对和解决大规模网络安全事件和危机，正在国防部领导下努力落实国家经济和社会政策理事会第 3995/2020 号文件所载行动计划中规定的以下目标：

(a) 通过改善数字安全来加强对数字技术的信任，包括开展能力建设和修订数字安全治理框架，从而使哥伦比亚成为在未来的数字世界中具有包容性和竞争力的社会。

(b) 采用的模式强调新技术并需要实施国家网络安全事件管理系统所依据的技术，从而协调各机构开展工作，及时管理网络安全事件，并为我国所报告的网络安全事件建立官方统计数据来源。

(c) 使网络安全事件和漏洞定期报告机制标准化，以完成相关的识别和评估，传达给利益攸关方，从而为我国政府进行决策提供信息。

国际法对使用信息和通信技术的适用

哥伦比亚认为，国际法(特别是《联合国宪章》，且包括国际人权法以及在适用范围内适用的国际人道法)既适用于“虚拟”领域，也适用于“实物”领域，但有一项谅解，即国际人道法仅适用于武装冲突局势的虚拟或实物领域。

国际法(尤其是《联合国宪章》)对于维护和平与稳定以及促进开放、安全、稳定、便捷、和平的信通技术环境是适用的，而且是必要的。因此，主权平等原则以及国家主权、和平解决争端、不干涉别国内政等其他国际法原则是各国更安全地使用信通技术的基础。

概念

哥伦比亚认为，鉴于信通技术应用的特殊性和新颖性，为了促进在法律、技术、政治层面上更深入地理解信通技术应用与国际和平与安全相关联的概念，应继续在多边论坛上根据“从国际安全角度看信息和电信领域的发展不限成员名额工作组”2021 年 3 月协商一致通过的最后报告所提出的结论讨论上述概念。

为了深入理解国际法如何应用于网络空间，应当开发能力建设工具，帮助各国制定共同词汇、扩展知识范围，从而能为应对网络空间的挑战调整国际法律框架，并就如何在虚拟领域应用国际法达成共识。

必须继续执行政府专家组和不限成员名额工作组的建议。

还必须建立在联合国主持下进行定期机构对话的全球机制，以便在这方面取得进展，并继续开展和加强区域一级当前开展的工作。

因此，哥伦比亚正在支持并共同发起一项倡议，即制定关于在国际安全背景下负责任地使用信通技术的行动纲领，作为永久性、包容性、协商一致、注重行动的国际文书，用以促进在国际安全背景下负责任地使用信通技术。

丹麦

[原件：英文]
[2021 年 5 月 28 日]

在丹麦，和世界上许多地方一样，数字解决方案是日常生活的一部分，有助于推动经济增长。作为世界上数字化程度最高的国家之一，丹麦必须推进一个全球、开放、自由、稳定、和平和安全的网络空间，在这个空间里，人权和基本自由以及法治得到充分应用。

为加强信息安全和促进该领域国际合作而在国家一级所做的努力

丹麦已采取多项措施加强其信息安全并促进网络空间的国际合作。

《2018-2023 年防御协议》划拨了 14 亿丹麦克朗，用于加强网络安全和网络防御，从而增强丹麦的复原力。《2018-2021 年丹麦国家网络和信息安全战略》采取进一步措施，加强网络和信息安全，确保系统和协调的努力。丹麦通过 25 项举措和 6 项有针对性的战略，解决了迄今为止被定义为关键部门(能源、金融、运输、医疗保健、电信和海事)的问题，增强了其数字基础设施的技术弹性，提高了公民、企业和当局的知识和技能，并加强了网络安全方面的协调与合作。

作为 2018-2021 年国家网络和信息安全战略的一部分，在上述六个关键部门设立了专门的网络和信息安全单位。此外，国家战略为部门专门单位和网络安全中心设立了一个论坛，重点是分享在网络和信息安全方面的工作经验。数字化局以及丹麦安全和情报局也参加了论坛。

为拥有足够熟练的人员来检测和处理针对丹麦的网络攻击，特别是涉及关键基础设施的攻击，网络安全中心进一步开发和实施了自己的强化网络学院。除了学院，网络安全中心还支持网络安全领域的教育和研究。

除了这些努力之外，数字化局还开发并执行了一些关于网络和信息安全的课程、学习材料和活动，对象是首席执行官和网络专家以及公职人员。

作为 2018-2021 年国家网络和信息安全战略的一部分，数字化局开发了 sikkerdigital.dk 网站，为公民提供关于网络和信息安全的指导、文章和学习工具以及关于不同威胁的知识。除了该网站，数字化局还与各城市和地区合作，开展了关于安全数字行为的全国性活动。

丹麦还成立了公私合营的网络安全委员会，就如何加强网络安全和改善当局、企业和研究人员之间的知识共享向政府提出建议。随着 2018-2021 年丹麦国家网络和信息安全战略的出台，丹麦还加强了国际网络参与，在布鲁塞尔派驻了网络专员；在外交部任命了一名国际网络协调员；任命了一名网络安全顾问到硅谷的技术大使办公室；并加入了位于塔林的北大西洋公约组织(北约)合作网络防御卓越中心。这使丹麦能够加强参与联合国、欧盟、北约和欧洲安全与合作组织(欧安组织)等多边网络论坛。

丹麦政府目前正在制定一项新的 2022-2024 年国家网络和信息安全战略。该战略将在当前努力的基础上，通过针对公共和私营部门以及丹麦公民的倡议，进一步加强网络和信息安全，并扩大现有努力。

同时，丹麦与北约和欧盟的伙伴和盟友合作，继续参与打击网络攻击和影响行动等混合威胁。在 2019 冠状病毒病(COVID-19)大流行期间，鉴于攻击和行动增加，联合国、欧盟、北约和欧安组织内部开展了持续外交努力，以不断促进自由、开放、稳定、和平和安全的网络空间。此外，丹麦是网络与信息安全合作小组和计算机安全信息响应小组网络的积极成员，也是欧盟网络安全局的理事会成员。

丹麦强调，正如国际社会所表明的那样，网络空间牢牢扎根于现有的国际法，政府专家组 2013 年和 2015 年的共识报告已证明这一点。现有的国际法，包括整

个《联合国宪章》、国际人道主义法和国际人权法都适用于各国在网络空间的行为，对于维护和平与稳定以及促进开放、安全、和平和可利用的信息和通信技术(信通技术)环境至关重要。丹麦还强调，2015 年政府专家小组报告中阐述的 11 项自愿的、不具约束力的负责任国家行为规范十分重要，是对现有国际法的补充和派生。

尽管各国和国际社会做出了努力，国家和非国家行为体进行恶意网络活动的能力和意愿仍在增强。这一问题应得到全球关注。根据国际法，网络空间中的恶意活动可能构成不法行为，且正在破坏稳定并有逐步升级的风险。丹麦仍决心防止、制止和应对恶意活动，并寻求加强这方面的国际合作。丹麦将与欧洲联盟一道呼吁国际社会加强国际合作，支持建立一个全面实施人权、基本自由和法治的全球、开放、稳定、和平与安全的网络空间。

政府专家组各项报告所述概念的内容

现有和新出现的威胁

丹麦认识到，网络空间为增加福利、促进可持续经济增长和提高我国公民的生活质量提供大量机会。然而，我们对数字解决方案的依赖也带来一定的挑战和脆弱性。

丹麦对国家和非国家行为体在网络空间的恶意活动增多以及通过网络盗窃知识产权的行为增加表示关切。这些行为威胁到经济增长和国际社会的稳定。

对全球、自由、开放、安全、稳定与和平的网络空间的需求从未像在 COVID-19 大流行期间那样明显。信息和通信技术能够实现世界需要的沟通、协作和知识共享，以管理这一大流行病。

但在当前的 COVID-19 危机中，我们见证到恶意行为体会利用任何机会，即使是全球大流行病。这包括干扰关键基础设施，包括抗击这一大流行病所必需的医院，以及通过网络窃取知识产权。任何阻碍关键基础设施能力的企图都是不可接受的，并会危及人们的生命。丹麦特别感到震惊的是，最近影响信通技术产品和服务的安全性和完整性的活动有所增加，这可能会产生系统性影响。这是不可接受的，必须受到所有国家的强烈谴责。此外，各国必须尽职尽责，对源自其领土的恶意信通技术活动采取迅速和坚定的行动。

此外，正如政府专家组和不限成员名额工作组以前的报告所确认的那样，鉴于信通技术的独特性质，联合国及其会员国在国际安全背景下处理网络问题所采取的办法必须保持技术中立。这符合现有国际法适用于新领域的概念和联合国的认可，包括新兴技术的使用。

国际法如何适用于信息和通信技术的使用

丹麦坚决支持以有章可循的国际秩序为基础的多边体系，以应对恶意使用信通技术带来的现有和潜在威胁。

国际社会已经明确表示，网络空间牢牢扎根于现有的国际法，政府专家组2013年和2015年的共识报告也证明了这一点。丹麦着重指出，包括整个《联合国宪章》、国际人道主义法和国际人权法在内的现行国际法适用于各国在网络空间的行为。丹麦感到高兴的是，大会今年早些时候以协商一致方式结束了这项工作，核可了从国际安全角度看信息和电信领域的发展不限成员名额工作组的最后报告。现在所有会员国都必须履行承诺。

主权、不干涉和禁止使用武力是国际法的基本原则，各国违反这些原则可能构成国际不法行为，各国可以根据国家责任规则采取反制措施并寻求获得赔偿。在加强对这些基本原则的共同理解和解释方面仍有余地，丹麦支持政府专家组和不限成员名额工作组的工作，以及其他国际和区域举措(如推动网络空间负责任国家行为的新行动纲领)为实现这一成果而开展的工作。

重要的是，各国不应利用主权原则在本国境内限制或违反国际人权法。人权法既适用于线上，也适用于线下，其中既包括各国以尊重的方式避免采取侵犯人权行为的消极和积极义务，也包括确保人民能够行使其权利和自由的义务。

如《丹麦军事手册》所述，根据适用的国际法，网络空间行动与使用常规军事能力没有什么不同。这个问题也反映在2019年的国家军事网络空间行动联合理论中，该理论指出，军事领导人有义务在进行网络空间行动时纳入对遵守国际法的考虑。因此，包括审慎、人道、军事必要性、相称性和区分等原则在内的国际人道主义法适用于国家在网络空间的行为，并通过在武装冲突时期为其合法性设定明确的界限，完全成为保护性的。丹麦愿与欧盟一道强调指出，国际法不是助长冲突，而是保护平民和限制不成比例影响的一种方式。

现有的国际法，加上政府专家组2015年报告中阐述的11项自愿性非约束性的负责任国家行为规范，为各国提供了关于网络空间负责任行为的框架。丹麦呼吁所有国家遵守这一框架并执行其建议。

由于现行国际法适用于网络空间，丹麦既不呼吁也不认为有必要为网络问题制定新的国际法律文书。然而，对于现有国际法如何适用于网络问题，仍有加强共同理解的空间。希望现任政府专家组和新的不限成员名额工作组的工作和建议将有助于进一步澄清，从而促进国家遵守，并促进更大的可预测性和降低局势升级风险。

负责任国家行为规范、规则和原则

丹麦与欧洲联盟及会员国一道，鼓励所有国家在联合国大会、特别是第70/237号决议再三认可的工作的基础上再接再厉，并进一步执行这些在预防冲突中发挥重要作用的商定规范和建立信任措施。

作为对现有国际法的补充和衍生，政府专家组在2010、2013和2015年连续发表的报告中阐述的负责任国家行为的规范、规则和原则具有巨大的价值。丹麦将继续以国际法为指导，并遵守这些自愿的规范、规则和原则。应通过围绕最佳做法加强合作和提高透明度，进一步执行这些规范。

摩尔多瓦共和国

[原件：英文]
[2021 年 5 月 24 日]

信息技术、信息资源和电子通信系统已成为个人、社会和国家所有活动领域中不可缺少的一部分。信息技术有助于社会秩序的根本变革，并在国家、区域和国际各级推动建立综合的信息社会。因此，信息技术已跨越了国家边界或国家社区的法律框架。

除了现代技术无可争议的好处之外，信息空间也容易受到一些安全威胁。因此，它助长了不忠诚的竞争、间谍活动、大规模的错误信息、宣传、恐怖主义和有组织犯罪，传播各种形式的仇恨和煽动暴力，特别是基于性别、种族、国籍、族裔血统、语言、宗教、政治派别和其他标准的仇恨和煽动，这些问题仍然被低估，很少得到补救或反击。

提高信息安全水平，为公共和私人行为体的某些活动创造有利条件，包括为信息系统的简单用户创造有利条件，是国家政策的基本优先事项，以确保法治国家的信息安全。这些行动的实现意味着需要最新的全面监管框架，该框架将涵盖信息安全领域的主要问题。在这方面，摩尔多瓦共和国已批准《信息安全战略》和实施该战略的活动计划。因此，该战略的目的是确保在信息空间中保护基本权利和自由、民主和法治。

对风险、威胁和脆弱性的分类，以及确保信息安全的活动的系统化，有助于提高网络空间的信任度，这一事实反映在摩尔多瓦共和国的信息安全战略中。

该战略的目的是在法律上将优先领域与职责和能力相结合，在安全领域以网络复原力、多媒体多元化和机构融合为基础，确保国家一级的信息安全，以保护摩尔多瓦共和国的主权、独立和领土完整。

因此，该战略为识别、抵制和应对信息安全威胁提供了具体而明确的机制，以及实现其实施目标的最后期限。

该战略所包含的机制和目标旨在创建和更新规范框架，落实将面对国内外挑战的技术性能和方案组成部分，培训工作人员，并加强与国家和国际主管机构的合作。

在这方面，该战略规定建立一个针对信息安全威胁的综合沟通和评估系统，并制定可操作的应对措施。这涉及到创建/指定一个实体作为国家网络安全事件应对中心，该中心将成为主管公共当局、个人和法律实体报告网络安全事件的唯一机构。建立国家计算机应急小组将加强摩尔多瓦共和国境内的小组网络，确保对事件作出快速反应。

此外，考虑到不断监测和确保高度网络安全的必要性，该战略规定对涉及国家利益的信息技术基础设施进行审计，并实施国际信息安全标准。

此外，该战略为摩尔多瓦共和国的特殊通信网络和限制访问的信息提供保护机制。通信系统、信息系统和数据传输网络是为国家重要数据的存储、处理和进一步传输而设计的，因此需要在保护和发展方面采取具体办法。

加密保护手段的数量不断增加和加密算法的复杂性使得有必要确保对信息保护手段的进口、认证和使用进行控制。因此，该战略要求对技术和加密信息保护手段进行认证，开发信息保护手段的进口监测系统，使加密信息保护领域的本国法律框架与欧洲法律框架相一致，并建立关于技术和加密信息保护手段的数据库。

此外，互联网全球网络的自由接入，色情和极端主义数据的存在，以及难以确定上传数据的来源和准确性，使得有必要为用户、特别是儿童制定保护机制，使其免受网络空间中任何形式的虐待。

有必要对互联网空间进行评估，以确定参与制作和传播对摩尔多瓦共和国信息安全有影响的在线媒体内容的实体和(或)个人，以便查明、抵制和应对信息媒体空间的信息安全威胁。

此外，为了发展战略沟通机制，促进摩尔多瓦共和国的国家利益，并确保信息媒体空间的安全，该战略规定开展一项全面研究，以检测和评估信息安全系统中媒体组成部分的易受攻击因素，并创建一个战略传播信息资源，其中包含有关安全事件和检测到的虚假信息和(或)操纵企图的信息。

此外，值得一提的是，该战略包含在信息安全和打击网络犯罪领域开展国际合作所必需的目标。

批准了 2019 年至 2024 年期间的信息安全战略，确定了包括在国际伙伴的协助下逐步实现的一些目标和措施。

尽管摩尔多瓦共和国正试图在国家一级采取若干措施加强其信息安全能力，但我们评估，在国际一级，网络空间的局势正变得越来越复杂，恶意的国家行为体进行复杂的网络攻击，干涉其他国家的选举进程，破坏重要的基础设施，实施“供应链”式的网络间谍攻击，所有这些都违反了联合国决议。

与此同时，非国家网络行为体利用“恶意软件即服务”工具，充分利用信息系统漏洞进行犯罪，以获取经济利益。

上述问题导致人们不愿意接受新技术，阻碍了信息技术的良好发展。

新加坡

[原件：英文]
[2021 年 5 月 24 日]

新加坡坚定致力于在网络空间建立基于规则的国际秩序，它将成为会员国之间互信和信心的基础，并将促进经济和社会进步。为尽享数字技术的惠益，国际社会必须依托可以适用的国际法、界定明确的负责任国家行为规范、强有力的建

立信任措施和协调一致的能力建设，开发一个安全、可信、开放和可互操作的网络空间。关于此类法律、规则和规范的讨论必须继续在联合国这一各国享有平等发言权的唯一普遍、包容的多边论坛进行。

新加坡参加了2019年至2021年期间从国际安全角度促进网络空间负责任国家行为政府专家组和最近结束的根据大会第73/27号决议设立的不限成员名额工作组。我们继续致力于为联合国制定和执行网络安全规范和规则的工作作出建设性贡献，并将继续积极参与联合国今后的进程。我们认为，联合国未来的网络安全讨论必须考虑到广泛的意见，特别是来自特别容易受到网络冲突影响的小国和发展中国家的意见。为此，联合国未来关于网络安全的任何进程都应是开放、包容和协作的，以进一步加强国际合作，并在推动网络空间负责任国家行为方面取得进展。新加坡与爱沙尼亚是电子政务和网络安全之友小组的共同主席，新加坡将继续利用这一平台提高对网络挑战的认识，分享最佳做法并促进联合国的能力建设。

新加坡认为，各国需要促进提高对现有自愿非约束性负责任国家行为规范的认识并协助落实这些规范。新加坡支持在必要时进一步完善这些规范。例如，跨境关键信息基础设施的保护是所有会员国的共同责任，可将其视为此类关键基础设施的一个特殊类别，并应纳入现有的一套规范，因为信通技术对此类基础设施的威胁可能对区域和全球产生破坏性影响。[2]

区域组织可以发挥重要作用。东南亚国家联盟(东盟)在2018年4月发表的第一份东盟领导人关于网络安全合作的声明中重申需要在网络空间建立基于规则的国际秩序。2018年9月，第三届东盟网络安全部长级会议与会者决定原则上赞同政府专家组2015年报告所述11项规范，并将重点开展关于落实这些规范的区域能力建设。2019年10月，第四届东盟网络安全部长级会议与会者决定设立一个工作级别的委员会，以考虑制定一项长期区域行动计划，确保有效落实这些规范，包括在各计算机应急小组间合作、保护关键信息基础设施和网络安全互助等领域。2020年第五届东盟网络安全部长级会议的与会者重申，东盟承诺制定一项行动计划，以适当速度为所有东盟成员国绘制规范的实施路线图。与会者还一致认为，迫切需要保护国家和跨境关键信息基础设施。

能力建设对于确保各国发展成功执行负责任国家行为规范及其国际法义务的能力至关重要。作为这一努力的一部分，新加坡于2016年设立了东盟网络能力计划，以支持东盟国家在网络政策以及操作和技术问题上的能力建设。到目前为止，东盟网络能力方案已经培训了来自东盟成员国的600多名官员。作为该计划的延伸，东盟-新加坡网络安全卓越中心于2019年启动，承诺提供3 000万美元，为东盟高级官员提供政策和技术方案。卓越中心已于2020年4月开始运作。尽管由于COVID-19大流行的影响，旅行受到限制，但卓越中心继续在网上提供培训方案，并在2020年组织了七个虚拟能力建设方案。

[2] 跨境关键信息基础设施是由私营公司拥有并跨越国界运行但不受任何单个国家管辖的关键信息基础设施。

新加坡还在联合国-新加坡网络方案下共同组织了一次讲习班，以提高东盟成员国对网络规范的认识。此外，新加坡与裁军事务厅合作，开发了一个向所有联合国会员国开放的旗舰在线培训课程。该课程旨在促进加深对信息和通信技术的使用及其对国际安全的影响的理解。我们仍然致力于与联合国会员国，特别是小国和发展中国家分享我们的经验和专门知识。

在国家一级，新加坡继续在以下三个方面加强其系统和网络的网络安全，即建设有抵御力的基础设施、创建更安全的网络空间和发展有活力的网络安全生态系统：

(a) 建设有抵御力的基础设施。新加坡网络安全局在 2019 年推出了《运营技术网络安全总计划》，以此作为新加坡持续努力的一部分，目的是加强其关键信息基础设施部门在提供基本服务方面的安全性和复原力。该总计划旨在改善跨部门的反应，以减轻运营技术环境中的网络威胁，并通过概述涵盖人员、流程和技术领域的关键举措，加强关键信息基础设施所有者和操作运营技术系统的组织的能力，加强与业界和利益攸关方的伙伴关系。2021 年，网络安全局将制定并启动一项关键信息基础设施供应链方案，涉及的利益攸关方包括政府机构、关键信息基础设施所有者及其供应商。该方案将为所有利益攸关方提供建议流程和良好做法，以管理供应链中的网络安全风险；

(b) 创建更安全的网络空间。作为新加坡提升国家网络安全态势的努力的一部分，网络安全局于 2020 年启动了《加强网络空间安全总计划》，以：㈠ 保护核心数字基础设施；㈡ 保障网络空间活动；㈢ 增强网络知识人口的权能。总计划概述了 11 项举措，旨在增加企业和组织对安全设计的采用，以及提高终端用户的网络安全意识和良好的网络卫生习惯。其中一项举措是针对网络连接的智能设备的网络安全标签计划。网络安全标签计划于 2020 年作为一项自愿计划推出，以让市场和发展商有时间了解该计划对其的惠益。网络安全标签将提供嵌入产品中的安全级别指示。消费者可利用网络安全标签上的信息选择安全等级更高的产品。网络安全标签计划旨在激励制造商开发和提供其网络安全特性得到承认并有所改进的产品；

(c) 发展有活力的网络安全生态系统。新加坡认识到，加强网络安全涉及建立网络生态系统和鼓励行业内创新。此外，日益需要培养一批能够在组织中承担网络安全领导角色的人才。网络安全局已与新加坡的政府机构、协会、行业伙伴和学术界合作，扩大和发展网络安全队伍。新加坡网络人才计划旨在吸引和培养从小就展露才华的网络安全爱好者，并帮助网络安全专业人员加深技能。目标是在三年内接洽至少 20 000 人，加强新加坡的网络安全人才输送。

瑞士

[原件：英文]
[2021 年 5 月 28 日]

为加强信息安全和促进该领域国际合作而在国家一级所做的努力

瑞士在国家、区域和全球层面采取了一系列措施，旨在推进更加稳定、开放和自由的网络空间。

《2020-2023 年瑞士外交政策战略》[3] 列出了总体纲要和优先事项，包括瑞士继续参与建立一个以国际法为基础、围绕人民及其需求的开放和安全的数字空间。瑞士还致力于巩固日内瓦作为全球领先数字中心的地位。瑞士首项《数字外交政策战略》(2021-2024 年)[4] 以外交政策战略为基础，提出了旨在保证开放、自由和安全的数字空间的关键原则。

2018-2022 年第二项《保护瑞士免受网络风险国家战略》建立在 2012 年第一项《保护瑞士免受网络风险国家战略》所概述的战略目标之上。[5] 这两项战略都承认信息和通信技术(信通技术)作为社会、经济和政治活动不可或缺的驱动力的重要性，并为采取全面、综合和整体的办法应对基于信通技术的威胁奠定了基础。瑞士寻求改善对网络风险和新出现威胁的早期检测，提高关键基础设施的复原力，并普遍减少网络风险。这些战略的基本原理是需要树立网络安全文化，各级政府之间以及公共和私营部门之间需要分担责任，并需要采取基于风险的方法。这些战略主张在政府层面加强协调，促进公私伙伴关系，并在国际舞台上加强合作。无论是国家还是国际层面的合作，都被定义为瑞士应对网络威胁的方法的基石之一。国家网络安全中心成立于 2019 年，是企业、学术界、公众和政府机构的联系点。在联邦网络安全代表的领导下，网络安全中心还帮助提高网络安全意识。

2020 年 9 月，联邦委员会通过了新的《数字瑞士战略》。[6] 该战略确定了政府、学术界、私营部门和民间社会之间合作的若干行动领域，以塑造社会的数字化转型，使瑞士的每个人都能从中受益，并确保所有人都能获得数字化转型带来的机会。

2021 年 3 月，联邦国防部通过了《2021-2024 年网络防御战略》。[7] 该战略旨在预测和早期发现网络威胁和恶意活动，预防和归因针对瑞士利益的网络事件，教育和培训文职和军事人员，以及增强关键基础设施的网络复原力。

---

[3] 可查阅 www.eda.admin.ch/eda/en/fdfa/foreign-policy/implementing-foreign-policy/aussenpolitische strategie.html。

[4] 可查阅 www.eda.admin.ch/eda/en/fdfa/fdfa/aktuell/newsuebersicht/2020/11/digitalaussenpolitik-strategie.html。

[5] 可查阅 www.ncsc.admin.ch/ncsc/en/home/strategie/strategie-ncss-2018-2022.html。

[6] 可查阅 www.digitaldialog.swiss/en/。

[7] 可查阅 www.newsd.admin.ch/newsd/message/attachments/66203.pdf。

在保护关键基础设施方面，瑞士采取了分散处理办法。与保护关键基础设施有关的任务被分配给联邦民防办公室、联邦国家经济供应局和联邦情报局等联邦各部门和办公室，因此并不局限于一个机构。

自《保护瑞士免受网络风险国家战略》通过以来，旨在将恶意网络活动归于犯罪人的能力得到了进一步发展。查明犯罪人是一个整体方法，包括分析网络事件的技术特征，考虑到地缘政治背景，并利用整个情报范围来获得相关信息。瑞士已确定跨机构标准化程序，以公开归因(政治归因)对瑞士国家安全构成威胁的网络事件。根据国际法对网络事件进行法律归因的标准构成了本评估的一部分。

2019 年 1 月，瑞士建立了“网络防御园区”，[8] 负责进行研究，以预测和监测技术驱动的发展可能带来的威胁，提出解决方案，并培训网络专家。该园区汇集了来自联邦国防采购办公室、工业和研究机构的专家。

在与私营部门和学术界的外联和接触方面，瑞士促进了各种举措。例如，为打击间谍和扩散活动，自 2004 年以来，联邦情报局利用其预防和提高认识运动方案“Prophylax”，向公司、大学和研究机构提供可能的预防措施，以识别和应对非法间谍和扩散活动。

政府专家组各项报告所述概念的内容

关于威胁评估，直接针对关键基础设施的恶意网络活动会造成严重损害，并对医疗保健等基本服务的运作产生负面影响。近年来，一些瑞士联邦机构和私营公司已成为国家支持的恶意网络活动(网络间谍)的受害者。这些恶意网络活动的最终目的通常是为了获得经济、政治和军事优势。在 2020 年期间，瑞士的关键基础设施主要受到出于经济动机的攻击的影响。瑞士预计，未来犯罪集团的勒索软件攻击以及由国家进行、赞助或纵容的网络行动将会增加。此外，恶意网络活动可能会对瑞士产生意想不到的影响，并导致附带损害。随着威胁行为体继续开发技术和工具来破坏和操纵合法软件，对供应链的攻击尤其令人担忧。

瑞士积极参加了关于国际网络稳定的第六届政府专家组(2019 年至 2021 年)和不限成员名额工作组(2019 年至 2021 年)，并为其做出了贡献，旨在加强执行联合国关于网络空间负责任国家行为的框架。瑞士深信，适用包括人权法和国际人道主义法在内的国际法、自愿非约束性规范、建立信任措施和能力建设是确保和维护国际网络安全的关键。瑞士常驻纽约联合国代表担任不限成员名额工作组主席。在他的主持下，工作组于 2021 年 3 月商定了一份协商一致的成果报告(A/75/816)。

瑞士与国际电信联盟合作，特别是参与其关于全球网络安全问题议程利用准则的协商，目的是与联合国一级的其他进程建立一致性。

瑞士致力于推动欧洲安全与合作组织(欧安组织)在促进网络稳定方面的作用，并积极参加其网络安全问题非正式工作组。自欧安组织制定和执行建立信任措施

[8] 见 www.ar.admin.ch/en/armasuisse-wissenschaft-und-technologie-w-t/cyber-defence_campus.html。

的任务以来，瑞士通过欧安组织和欧安组织通信网维护的平台，在非正式工作组定期会议上分享关于国家结构、组织和政策的信息，提高了本国网络状况的透明度。瑞士还与德国一道，继续参与实施第 3 号建立信任措施所载的信息和协商机制。

瑞士是欧洲委员会《网络犯罪公约》的缔约国，认为该公约的执行和实际应用对打击网络犯罪至关重要。瑞士正在参加关于该公约第二项附加议定书的谈判，该议定书旨在加强国际合作。

在双边方面，瑞士与各国就网络相关问题定期举行政治磋商。

瑞士于 2019 年加入自由在线联盟，成为其第 31 个成员。瑞士坚信，人们在网下享有的权利在网上也须受到保护。自由在线联盟是加强所有利益攸关方参与的一项关键举措，以便在互联网时代保护人权和基本自由。瑞士还在财政上支持自由在线联盟的努力。

2019 年，瑞士启动了关于国际法如何在网络空间适用的法律专家对话。2021 年，瑞士将继续这一努力，促进对国际法如何适用的共同理解，重点是国际人道主义法在网络空间的适用。

2018 年，瑞士启动了关于网络空间负责任行为的日内瓦对话，为讨论有关国际网络稳定的作用和责任提供了一个多利益攸关方平台。自 2020 年以来，日内瓦对话一直专注于企业在执行国际层面商定的规范方面的作用。

国家网络安全中心最近启动了一个跨机构流程，以制定整体政府方法，以协调和负责任的方式披露新发现的网络漏洞。这一流程使发现硬件、软件和数字服务中的漏洞的研究人员能够向该中心报告该漏洞。披露的目的是为了在漏洞被恶意利用之前填补漏洞(例如打补丁)。

瑞士参加了一系列国家和国际演习，如“锁定盾牌”，以测试国家能力、程序和决策过程。

瑞士是全球网络专门知识论坛的创始成员之一，并支持各种网络能力建设项目。瑞士还在财政上支持旨在加强外交官和非政府代表参与和促进联合国有关国际网络稳定进程的能力的倡议。

土耳其

[原件：英文]
[2021 年 5 月 31 日]

信息和通信技术(信通技术)已成为当今社会和经济生活的重要组成部分。这些技术用于包括公共和私营部门、关键基础设施和个人在内的广泛网络，并已在土耳其和世界各地广泛使用。因此，信通技术对可持续增长和发展起着重要作用。然而，我们越多地使用技术，我们就越依赖它，并容易受到它带来的风险的影响。由于网络威胁，个人、公司、关键基础设施和国家都遇到了严重的问题。

土耳其重点采取必要措施改善国家网络安全。运输和基础设施部是负责制定土耳其国家网络安全政策及制定战略和行动计划的机构。在这方面，土耳其公布并实施了国家网络安全战略、2013-2014 年行动计划和 2016-2019 年国家网络安全战略和行动计划。土耳其制定了 2020-2023 年国家网络安全战略和行动计划，之前所有相关利益攸关方都参加了由运输和基础设施部协调的研究小组。

2020-2023 年国家网络安全战略和行动计划于 2020 年 12 月 29 日在政府公报中公布，包括以下主要战略目标：

- 保护关键基础设施和提高复原力
- 国家能力建设
- 有机的网络安全网络
- 新一代技术的安全性(物联网、5G、云计算等)
- 打击网络犯罪
- 发展和培育国内和国家技术
- 将网络安全纳入国家安全范畴
- 改善国际合作

此外，隶属于信息和通信技术局的国家计算机应急小组自 2013 年以来一直在协调土耳其的网络事件应对工作。除了网络威胁检测和网络事件应对，包括事件发生之前、期间和之后，该小组还确保实施防范网络威胁和网络威慑的措施。

国家计算机应急小组与网络安全有关的主要重点领域是：

- 网络能力建设
- 技术措施
- 收集和传播威胁情报
- 保护关键基础设施

在改善国家网络安全的背景下，自 2013 年以来，为关键部门或基础设施(如能源、卫生、银行和金融、水管理、电子通信和关键公共服务)建立了 14 个部门计算机应急小组和 1 803 个机构计算机应急小组。所有的计算机应急小组在国家小组的协调下，每周七天，每天 24 小时运作，以减轻网络危机，打击网络威胁。国家计算机应急小组使用检测和预防工具进行监测，并使用报告工具与有关各方共享信息。国家计算机应急小组为土耳其境内的所有计算机应急小组开发了信息共享平台，以便发布警报、警告和安全通知，提供了高效和安全的沟通渠道。

国家计算机应急小组组织和支持向若干社区开放的网络安全培训课程、夏令营和竞赛。此外，国家小组还为计算机应急小组提供关于恶意软件分析和日志分

析等主题的培训。过去四年中，逾 5 000 人接受了国家小组在网络安全不同领域的培训。

此外，在信息和通信技术局内设立的学院向公众提供有关网络安全和其他相关领域的在线培训，以促进土耳其人力资源的专业知识。培训内容可查阅该学院的官方门户网站(www.btkakademi.gov.tr/portal)。

土耳其的一些组织、机构、大学、非政府组织和私营部门实体也在全国范围内组织关于网络安全、保护关键基础设施和其他相关主题的研讨会、会议和培训。

一年一度的互联网安全日是提高认识的活动之一，其主要目标是自觉和安全地使用互联网。官方安全网络门户(www.guvenlinet.org.tr/)提供了互联网帮助热线和网站安全网，家庭可在此查找有效使用互联网的建议。

土耳其还采取措施应对日益加剧的数字安全风险，以确保网络安全，并在 2019 冠状病毒病(COVID-19)大流行范围内采取措施。

国家计算机应急小组一周七天、每天 24 小时地工作，对利用 COVID-19 大流行趋势的恶意软件、网络钓鱼攻击和其他网络威胁进行分析。通过指挥和控制中心，确定并防止这些网络威胁的恶意链接，以保护关键基础设施和公民。在此范围内，编制网络情报报告，并与有关各方共享。还编写和发布了指导方针，包括以下内容：

- 远程连接的安全原则
- 保护用户免受网络钓鱼攻击
- 与 COVID-19 相关的虚假申请
- 设置和使用视频会议和会议软件的安全原则

土耳其在许多组织中发挥了重要作用，或成为创始成员，或为网络安全和信息安全问题的合作努力作出贡献。在这方面，土耳其重视在众多领域与各国和各组织分享信息。国家网络应急小组是事件应对和安全小组论坛、可信引导者、国际电信联盟(国际电联)、北大西洋公约组织(北约)多国恶意软件信息共享平台、网络安全共同进步联盟和伊斯兰会议组织计算机应急小组的成员。自 2015 年 11 月以来，土耳其还作为赞助国参加了北约合作网络防御卓越中心的工作。此外，在网络安全方面正在进行双边和多边合作，例如与许多国家签署谅解备忘录。此外，土耳其积极参与和协助国际组织进行的研究，这些组织包括联合国、北约、欧洲安全与合作组织(欧安组织)、经济合作与发展组织(经合组织)、二十国集团、突厥语国家合作委员会以及区域军备控制核查和实施协助中心——安全合作中心等。

网络安全演习是合作和防范的另一项重要活动。在国家和国际一级开展的这类活动有助于加强网络空间和测试应对潜在网络威胁的措施。自 2011 年以来，运输和基础设施部组织了四次国家和两次国际网络安全演习。最近于 2019 年 12 月 19 日，运输和基础设施部与信息和通信技术局在安卡拉共同举办了 2019 年“网络盾牌”演习，这是一次国际性的网络安全演习。2019 年“网络盾牌”演习

得到了国际电联和网络安全共同进步联盟的支持。此外，土耳其参与并促进国际网络安全演习，如北约“锁定盾牌”、北约“网络联盟”和北约“危机管理”演习。与其他能力建设和指导研究一样，国际网络安全演习对于提高全世界的防范水平和网络事件应对能力建设仍然至关重要。

网络空间方面的国际和平与安全需要在加强国际合作基础上开展进一步研究。可清楚地看到，国际法以及政府专家组、不限成员名额工作组的报告和相关研究报告中所述的规范和规则有助于提高网络空间的安全性。

此外，改善合作和支持信息共享机制对打击网络威胁至关重要，需要给予应有的重视。

此外，土耳其意识到执行国际法、网络空间负责任国家行为规范的重要性以及开展有效国际合作的必要性。土耳其决心采取必要步骤确保实现这些目标，加强国家和国际层面的网络安全仍将是土耳其的关键优先事项之一。

乌克兰

[原件：英文]
[2021 年 5 月 31 日]

对现有信息的分析表明，在针对我国的“混合”战争条件下，对国家安全的主要威胁之一是俄罗斯联邦旨在破坏宪法秩序、侵犯乌克兰主权和领土完整以及使我国社会政治和社会经济局势恶化的破坏性信息行动和特别心理行动。有目的地散布虚假信息和错误信息，以及进行武装侵略，不仅对乌克兰，而且对整个世界都构成了紧迫威胁，因为上述行为对其他国家公民的意识造成影响，扭曲乌克兰的形象，形成仅对俄罗斯有利的舆论。

侵略国正越来越多地采取旨在降低我国信息安全水平的措施，创建对国家机构和信息空间施加影响力的手段，以加强自身地位，同时形成对自己有利的外国舆论，并向乌克兰国家机构施压，以使其做出有利于自己的决定。为达到上述目的，在乌克兰的信息和媒体空间系统地开展了宣传，并在互联网上开展宣传，特别是误导性宣传，包括利用社交网络、信息传播者、电子资源和特别制作的信息产品。

为了对我国施加这种负面的信息影响，俄罗斯联邦建立了一个推广宣传内容的强大系统，其中包括一个由信息平台(博客、网站)、受控媒体和互联网资源、聚合器和新闻集中器、发布内容的博主和舆论领袖、新闻机构和公关公司组成的网络，以便在顶级新闻源中发布宣传信息。俄罗斯还广泛使用软件机器人网络来迅速传播错误信息和反乌克兰的信息，目的是操控公众意识。俄罗斯方面用来传播错误信息的信息空间关键主体是世界领先的社交网络(脸书、Instagram、推特)，由于俄罗斯的社交网络 VKontakte 和 Odnoklassniki 在乌克兰被禁，因此这些网络的受众迅速增长。有一种倾向是使互联网乌克兰方面的用户转向广泛使用消息服务(Telegram、WhatsApp、Viber 等)，原因是可以保持匿名，宣传效率高，内容可进一步大规模传播，以及有大量互动和反馈。

视频托管服务(YouTube、Yandex.Video、RuTube、Video@Mail.Ru)也被用来传播错误信息，因为拥有照片及视频托管服务的公司根据所在地的国家法律运作。俄罗斯宣传者对此加以利用，在这些网络平台上创建并发布对乌克兰信息安全构成威胁的内容。由于这些消息来自美国和欧洲的主机，因此内容可以在互联网上自由传播。

此外，侵略国正在努力不断发展受控信息资源的网络。特别是，我国暂时被占领土上的占领当局正在采取系统措施，目的是创建新的信息平台，增加电视频道数目，扩大电视和无线电广播的覆盖范围，包括在乌克兰当局控制的领土内。除了传播反乌克兰的内容外，俄罗斯占领当局还安装了强大的转播设备，用以压制干扰乌克兰国内的电视和电台广播信号，办法是在乌克兰用来向暂时被占领土居民传播客观信息的频率上播放所谓“白噪音”。此举对以下方面尤其产生影响，即乌克兰国内最大传媒集团(Inter Media Group、StarLightMedia、Media Group Ukraine、1+1)的电视频道卫星信号编码，以及采用数字标准的国家电视和电台广播在乌克兰领土的覆盖情况不能令人满意。因此，乌克兰边境地区的居民不断受到来自俄罗斯联邦主要宣传频道上危害性内容的影响。暂时被占领土上的运营商和提供商的运营是另一个负面影响因素，这些运营限制了当地居民获取互联网上乌克兰方面的内容，使得向乌克兰暂时被占领土居民提供立场性内容变得复杂化。非营利组织 RIPE 网络协调中心(荷兰)违反欧洲法律，为克里米亚和顿巴斯占领区所谓互联网提供商的业务注册 IP 地址。为了使该组织的活动符合乌克兰现行法律，乌克兰外交部和乌克兰驻荷兰王国大使馆正在国家间采取适当措施。

此外，俄罗斯联邦利用苹果和谷歌的服务传播错误信息，目的是操纵互联网乌克兰方面的用户。特别是，应用商店(App Store)和 Play 商店(Play Market)有法人和个人开发的移动应用程序，但根据 2020 年 5 月 14 日第 184/2020 号乌克兰总统令颁布的 2020 年 5 月 14 日国家安全与国防委员会关于适用、取消和修正个人特别经济和其他限制性措施(制裁)的决定，对这些法人和个人适用了特别经济和其他限制性措施(制裁)。上述软件产品的功能使其具备访问乌克兰境内被禁网络资源的技术能力。

尽管乌克兰已做出一切努力加强信息安全并阻止错误信息的传播，但信息侵略是信息领域的最大威胁之一，迫切需要协助国际社会和国际机构充分反击俄罗斯联邦的信息侵略行为，这些行为不仅针对乌克兰，而且也涉及其他国家，俄罗斯站在其立场上在信息空间采取具有破坏性影响的行动。

直到最近，为了施加破坏性信息影响并实现干涉我国内政以及在开展国际合作和实施国内进程中强加条件的企图，俄罗斯联邦采用了以下方式，即利用相关联的乌克兰政党和运动，直接秘密资助在我国境内活动的民间机构和经济实体，通过在乌克兰东部的军事侵略施加强大压力，或阻止国际支持并阻止乌克兰加入欧洲联盟和北大西洋公约组织(北约)，以及通过受控的信息资源开展信息运动、运作和行动。

但出现了一种稳定趋势，即俄罗斯联邦调整针对乌克兰的所谓“信息战”的进一步战略的方向，转向从所谓“第三”国的立场来执行针对我国的破坏性措施，

以此来掩盖其参与组织和实施上述措施的行为。一方面，这是欧洲联盟和美国因俄罗斯联邦干涉乌克兰内政、吞并克里米亚自治共和国以及在顿涅茨克州和卢甘斯克州暂时被占领土上的武装冲突而对其实施经济制裁的结果。另一方面，这也是因为乌克兰方面采取了措施，以打击侵略国对乌克兰信息空间和公民意识的破坏性影响，减轻信息传播的负面后果，提升我国人民的爱国热情和自我意识水平。

特别是，施加信息影响的行动和干涉乌克兰内政的行为增加。俄罗斯联邦正在从北约和欧洲联盟成员国的立场开展情报活动和颠覆活动，其中包括为了俄罗斯的利益在国家和地方当局和管理机构、各政党和运动、专家和博客社区、智囊团、广告和咨询公司、捐助方、非政府组织和舆论领袖中招募并资助游说者，以及创建受控媒体、互联网资源和公关公司。

通过欧洲联盟内所谓“俄罗斯世界”小组中的亲俄欧洲政客，俄罗斯联邦正试图将克里米亚全民投票合法性的思想合法化并将其强加于国际社会，为其武装侵略乌克兰做辩护，从而实现解除对俄制裁和俄罗斯重返世界政治体系的目标。目前，亲俄分支活跃在一些欧洲国家。这些政治力量的大多数代表都是为了侵略国在本国境内外的利益而进行游说的人，他们散布亲俄观点，传播俄罗斯的说辞，并采取威胁乌克兰国家利益的信息措施。

俄罗斯联邦做出调整，从“第三”国的立场组织和开展具有破坏性信息影响的特别信息运作和行动，其表现形式是煽动其他国家与乌克兰的历史性矛盾和对乌克兰的领土主张，在乌克兰少数民族中挑动分裂分子和自治表示。一方面，这使我国与邻国之间的关系复杂化，俄罗斯联邦正是从这些国家的立场出发开展此种破坏性活动的；另一方面，这也成为这些国家宣布其对乌克兰某些土地的领土主张的理由。与此同时，俄罗斯表面上与这一进程拉开距离，从而避免乌克兰和国际社会直接指责其干涉我国内政和直接威胁乌克兰与其他国家的睦邻友好关系，以处于对乌克兰国内政治局势有影响力的地位。

有鉴于此，乌克兰将继续采取综合措施，确保国际安全背景下网络空间的负责任行为，同时呼吁国际社会提供支持并开展联合努力，以便妥善应对俄罗斯联邦的“混合”战争。

为了确保电子数字签名立法改革得到落实，使立法与欧洲议会和欧盟理事会 2014 年 7 月 23 日关于内部市场电子交易的电子身份识别和信任服务的第 910/2014 号条例(欧盟)(废除了欧洲议会和欧盟理事会第 1999/93/EU 号指令)的规定相一致，乌克兰最高拉达于 2017 年 10 月 5 日通过了关于电子信任服务的《第 2155-VIII 号法》，该法于 2018 年 11 月 7 日生效。

该法的主要目的是在乌克兰引入在欧洲联盟使用的提供电子信任服务的模式和原则，同时不破坏在乌克兰发展起来的电子数字签名领域各方之间的互动系统。该法明确规定了提供电子信任服务，包括跨境服务的法律和组织原则、电子信任服务领域关系主体的权利和义务、国家对电子信任服务领域法律遵守情况的监督(控制)程序以及电子身份识别的法律和组织原则。在制定《第 2155-VIII 号法》的规定时，乌克兰内阁通过了一些决议：

- 关于批准在公共机关、地方政府、国家所有的企业、机构和组织使用电子信任服务的程序的第 749 号决议，乌克兰内阁 2018 年 9 月 19 日通过。
- 关于批准有关《证明清单》的强制性要求的第 775 号决议，乌克兰内阁 2018 年 9 月 26 日通过。
- 关于批准合格电子信任服务机构业务终止情况下文件信息存储及移交中央管理机构程序的第 821 号决议，乌克兰内阁 2018 年 10 月 10 日通过。
- 关于批准电子信托服务领域规定和电子信托服务领域立法规定遵守情况检查程序的第 992 号决议，乌克兰内阁 2018 年 11 月 7 日通过。
- 关于批准电子信任服务领域合规评定程序的第 1215 号决议，乌克兰内阁 2018 年 12 月 18 日通过。
- 关于批准乌克兰和外国相互认可公钥证书、电子签名以及使用中央机构(负责确保在不同国家主体之间互动过程中提供有法律意义的电子服务时使用的电子信任服务和外国公钥证书在乌克兰得到承认)信息和电信系统的程序的第 60 号决议，乌克兰内阁 2019 年 1 月 23 日通过。

乌克兰特殊通信和信息保护局根据上述法律第 8 条的要求，在 2020 年 5 月 14 日的命令中核准了有关合格电子证明服务提供者及其单立注册点(2020 年 7 月 16 日在乌克兰司法部注册)信息的安全和保护要求，其中详细说明并确定执行 2018 年 11 月 7 日乌克兰内阁通过第 992 号决议批准的法律和电子信任服务领域的要求，以确保有关电子信任服务提供者和单立注册点信息的安全和保护。

目前，乌克兰正在采取措施，目的是在乌克兰与欧盟之间的《联系国协定》框架内，并根据乌克兰与欧洲联盟在第二十二届欧洲联盟-乌克兰首脑会议期间达成的协定，相互承认电子信任服务。

与此同时，有必要修订该法的某些规定，使其尽可能与第 910/2014 号条例(欧盟)的规定相一致，特别是在拟订电子身份识别领域的国家条例、改进电子签名和签章的要求以及澄清合格电子签名或签章的要求方面的规定。乌克兰内阁目前正在审议由乌克兰数字转型部和乌克兰特殊通信和信息保护局起草的一项法律草案。

此外，乌克兰内阁在 2021 年 1 月 13 日第 24 号决议中修正了管理国家特殊通信局的《乌克兰特殊通信和信息保护局条例》第 4 款，并规定了根据 2017 年 5 月 24 日《第 2068 号法》批准的乌克兰政府与北约之间关于保护受限访问信息的行政安排的第 7 条设立的安全认证机构的职能。

乌克兰特殊通信和信息保护局通过建立国家认证程序，保护用于交换北约限制访问信息的通信和信息系统的安全，采取措施执行北约关于这些问题的条例。

作为促进国际合作和提高信息安全专业人员认识的一部分，乌克兰特殊通信和信息保护局参加了欧洲联盟委员会技术援助和信息交换文书(TAEIX)国际会议和 FireEye 研讨会。

为了加强信息安全，在关键基础设施中不断引入信息安全审核系统，具体情况如下：

- 拟订对关键基础设施的独立信息安全审核员的要求。
- 拟订信息安全审核员认证/再认证程序，以及信息安全审核员专业培训的特殊目的评估制度，并对信息技术安全“审核”中的关键基础设施目标的独立信息安全审核结果进行分析。

同时，为了落实信息保护领域的国家政策，乌克兰特殊通信和信息保护局工作人员对法律所要求的国家信息资源和信息在网络空间的技术保护的状况实施国家管制措施。

此外，乌克兰特殊通信和信息保护局采取了若干行动，为以下法案做准备并确保其获得通过：

- 根据乌克兰《宪法》第 107 条、国家安全基本原则法第 2 条第二部分以及乌克兰关于 2020 年 9 月 14 日国家安全和国防委员会决定的第 391/2020 号总统令，为乌克兰网络安全战略草案(2021-2025 年)编写了详尽提案。
- 支持乌克兰内阁通过 2019 年 6 月 19 日关于批准关键基础设施的网络保护一般要求的第 518 号决议，该决议在关键信息基础设施网络保护国家政策拟订和实施框架内发起，旨在与欧洲联盟和北约的相关标准协调一致，创建一个关于网络安全的监管和术语框架，并根据国际标准统一信息安全和网络安全领域的规章。
- 乌克兰内阁通过了关于某些关键基础设施问题的第 1109 号决议和关于某些关键信息基础设施问题的第 943 号决议，这些决议的拟订考虑到了欧洲联盟立法的要求，特别是欧洲议会和欧盟理事会关于采取措施使欧盟网络和信息系统共同达到较高安全水平的 2016 年 7 月 6 日第 2016/1148 号指令(欧盟)，以及关于欧洲关键基础设施的识别和指定以及加强保护的必要性评估的 2008 年 12 月 8 日欧盟理事会第 2008/114/EC 号指令。
- 2020 年 11 月 11 日，乌克兰内阁通过了关于批准法律要求的关键信息基础设施、国家信息资源和信息网络保护状况审查程序的第 1176 号决议，允许对法律要求进行保护的信息基础设施、国家信息资源和信息进行监管。

乌克兰计算机应急小组不断采取措施，与外国小组合作，解决与消除网络攻击对关键信息基础设施的影响有关的问题，分析网络事件相关数据，为网络安全

设施所有者提供预防、检测和消除网络事件后果的实际援助，拟订有关打击现代类型网络攻击和网络威胁的建议并在其官方网站上发布，提供有关网络威胁和防范这些威胁的适当方法的信息。

大不列颠及北爱尔兰联合王国

[原件：英文]
[2021 年 5 月 31 日]

联合王国欢迎大会第 75/32 号决议邀请所有会员国向秘书长通报它们对从国际安全角度促进网络空间负责任国家行为相关问题的看法和评估意见。我们鼓励所有参与从国际安全角度看信息和电信领域的发展相关讨论的国家利用这个机会和后续机会。

网络空间不尊重国界。作为一个负责任的网络大国，联合王国将努力影响网络空间的未来管理框架，同时维护现有规则，并建立在从根本上由技术塑造的世界中的积极行为规范的共识。

联合王国认识到，未来十年，人工智能、网络和数据等领域的快速技术变革将重塑我们的社会。各国必须共同努力应对最大的全球性挑战，包括共同致力于促进自由、开放、和平与安全的网络空间，并在全世界形成一支向善的力量，捍卫数字社会中的民主和人权。

我们将推动接受和遵守这些规则和规范，并将与广泛的各类伙伴和利益攸关方协调合作，为建立一个保护开放社会并促进创新、发展和增长的网络空间提出令人信服的理由。我们还将通过开展国际能力建设为正在应对数字化挑战的国家提供支持，以便树立其参与国际辩论和增强自身的网络安全能力的信心。

联合王国欣见顺利完成两个同时开展的联合国进程，即从国际安全角度看信息和电信领域的发展不限成员名额工作组和从国际安全角度促进网络空间负责任国家行为政府专家组。不限成员名额工作组提供了一个包容各方的进程，代表了所有会员国和其他利益攸关方的不同意见，同时我们相信，政府专家组的报告将提供许多国家所要求的网络空间负责任国家行为初步框架详细指南。

国家一级为加强信息安全和促进这一领域的国际合作所作的努力

2021 年 3 月 16 日，联合王国发表了《竞争时代全球化的英国：安全、国防、发展和外交政策综合审查》，[9] 介绍了政府对今后十年联合王国在世界上的作用的愿景以及到 2025 年将采取的行动。此次审查确定，需要随着国际秩序在网络空间和空间领域等今后前沿领域的发展来塑造这一秩序，在这些领域开展经济、社会和军事活动的可能性正在迅速扩大。我们将积极确保有效的问责和监督，以保护民主价值观，同时反对过度扩大国家控制的范围。

[9] www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy。

联合王国还将在 2021 年通过一项新的全面的网络战略，取代之前的 2016-2021 年国家网络安全战略。正如上述综合审查所预示的那样，该战略的基础将是，必须对网络问题采取“整体政府”办法。根据这项战略，我们将采取以下优先行动：

- 加强联合王国的网络生态系统，以便能就网络采取全国一体的办法，同时深化政府、学术界和产业界之间的伙伴关系。
- 建设一个有复原力的繁荣的数字联合王国，公民在网上感到安全，并相信自己的数据受到保护。
- 在微处理器、安全系统设计、量子技术和新的数据传输形式等对网络力量至关重要的技术方面处于领先地位。
- 促进自由、开放、和平与安全的网络空间，同时与其他政府和产业界合作，并利用联合王国在网络安全方面的思想领导地位。
- 识别、扰乱和威慑对手。

通过这些战略，我们将与其他政府合作并与产业界建立伙伴关系，以确保网络空间的管理规则和规范增强集体安全、促进民主价值观和支持全球经济增长，遏制数字独裁主义的蔓延。联合王国将维护网络空间的法治：体现负责任的国家行为和塑造国际最佳做法，同时鼓励合规行为，遏制袭击行为，并追究其他各方对不负责任的国家行为的责任。如有必要，我们将拟订规则，以便进攻性网络工具的开发和使用能够根据国际法负责任地进行。

此外，我们将：

- 为了子孙后代，对可访问、可互操作的全球互联网进行保护。
- 确保与线下环境中一样，线上环境中的人权得到保护。
- 确保新技术的设计和部署从一开始就体现透明度和问责。
- 支持数据的国际流动，实现安全、可信和可互操作的跨境数据交换，同时维持数据保护标准。

联合王国认为，网络外交是其网络领导力的一个关键要素，其官员网络遍及六大洲。除了网络安全能力建设方案外，我们还启动了与 20 个国家的跨政府对话。通过开展上述工作，我们将继续发展伙伴关系，更有力地倡导建立自由、开放、和平与安全的网络空间，应对并遏制国家主导的恶意网络活动。

我们继续参加各种专门开展网络安全问题讨论的全球和区域论坛，包括联合国不限成员名额工作组和联合国政府专家组、欧洲安全与合作组织(欧安组织)、国际电信联盟和全球网络专门知识论坛。

如果联合王国认为追究国家对恶意网络行为的责任符合其最大利益，并且可进一步履行其对网络空间明确性和稳定性的承诺，那么它有能力开展这项工作而且也确实开展了这项工作。我们仍认为，决定追究国家对恶意网络活动的责任，

而且至关重要的是将其公之于众，归根结底是各国的一项政治决定。各项声明和其他相关信息可在 www.gov.uk 和 www.ncsc.gov.uk 在线查阅。

2020 年，联合王国成立了国家网络部队。联合王国是公开确认正在发展此种能力的几个国家之一。国家网络部队开展有针对性、负责任的进攻性网络行动，以支持联合王国的国家安全优先事项，同时汇集国防和情报能力。与外交、经济、政治和军事能力相结合的网络行动示例可能包括：

- 干扰手机，防止恐怖主义分子与联络人联系。
- 帮助防止网络空间被用作欺诈和儿童性虐待等严重犯罪的全球平台。
- 使联合王国的军用飞机免遭武器系统的攻击。

联合王国致力于根据联合王国法律和国际法，以负责任的方式使用其网络能力。过去的网络行动一直根据现行法律运作，今后的网络行动也将继续根据现行法律运作，其中包括 1994 年的《情报机构法》和 2016 年的《调查权力法》。这确保了联合王国的网络行动是负责任、有针对性和相称的。

所有会员国都同意，促进为和平目的使用信息和通信技术(信通技术)符合所有国家的利益。联合王国再次确认，信通技术本身并不构成“威胁”。相反，只有当各国(或其他行为体)选择将信通技术用于“不符合国际和平与安全的目的”或被视为将其用于此目的时，才会出现威胁或风险。在此背景下，进一步推进有关各国如何理解在网络空间采取行动时国际法适用问题的讨论，是提高透明度、可预测性和稳定性的实际步骤。

关于联合王国在网络安全方面的办法，包括国际合作办法的最新信息，可查阅 www.gov.uk/government/cyber-security 和 www.ncsc.gov.uk。

政府专家组各项报告所述概念的内容

联合王国欢迎会员国在两个进程中重申了 2010 年、2013 年和 2015 年的前三份政府专家组协商一致报告，其中确认国际法适用于网络空间，并建立了一个负责任国家行为的框架，该框架由一套以能力建设为基础的、自愿和不具约束力的规范和建立信任措施组成。2021 年的新报告将是对这些文书的重要贡献。

联合王国认为，所有国家适当执行现有报告所述框架的全面内容，为我们增强网络空间稳定性的努力提供了一个实实在在的起点。普及并落实累积评估和建议将是向前迈进的切实步骤。因此，需要以行动为导向的实际办法。

现有和新出现的威胁

关于不断发展的趋势，在 2019 冠状病毒病(COVID-19)大流行期间，袭击者在选择目标时利用了此次危机，其目标包括医院和与卫生相关的其他关键基础设施。恶意行为体蓄意以参与国家和国际 COVID-19 应对行动的组织为目标。这些组织包括医疗保健机构、医药公司、学术机构、医学研究组织和地方政府。这类

行为体经常以组织为目标，以便收集大量个人信息、知识产权和与国家优先事项相一致的情报。

勒索软件已经成为联合王国国家网络安全中心处理的最频繁和最具破坏性的一类事件。在 2020 年的年度审查中，[10] 我们注意到该中心处理的事件是上一年的三倍以上。在联合王国，在各机构努力开展在线学习、招生和考试程序管理工作的同时，影响教育部门的勒索软件攻击也出现激增。攻击者不断加大要让对方付出的代价，在受害者不愿支付赎金时就威胁要公开泄露被盗数据。我们还看到攻击者越来越精明老练，他们长时间在网络上，寻找价值最高的数据进行加密，并寻找在线备份资料，以便对资料恢复设置障碍。

国际法如何适用于信息和通信技术的使用

联合王国申明，所有现行国际法，包括尊重人权和基本自由以及将国际人道法适用于武装冲突中的网络行动，都是我们在网络空间负责任行为的共同承诺的一部分。与国际法在线下环境中对国家活动的适用方式相同，国际法在网络空间中也全面适用。

在这方面，我们欢迎红十字国际委员会呼吁所有国家重申国际人道法适用于武装冲突期间开展的网络行动。同从事任何其他领域的活动一样，国家从事网络行动也受到国际法的管辖。将国际人道法适用于武装冲突中的网络行动既提供了保护，也带来明确性。这样做有助于减缓此种冲突，并确保适用旨在最大限度地减少冲突的人道主义后果的现行原则和规则。

但我们认为，各国都需要更进一步，阐明我们自己对国际法如何适用于网络空间的认识。联合王国于 2018 年开展了这项工作，当时的前任总检察长英王室法律顾问杰里米·赖特议员阐述了联合王国有关国际法适用于网络空间的立场。这是政府大臣首次正式提出联合王国的观点。

我们还认识到需要进行国际法方面的能力建设，包括为此开展与我们对国际法适用的理解有关的、可能的工作。这一领域的能力建设可以对各国在未来谈判中形成自己的立场和捍卫本国利益的能力产生切实影响，并确保我们不会在无意中以这种方式加深数字鸿沟。

负责任国家行为准则、规则和原则

2019 年 9 月，联合王国向不限成员名额工作组提交了“关于按照联合国政府专家组 2010 年、2013 年和 2015 年报告的商定成果，努力执行网络空间负责任国家行为准则的非正式文件”。[11] 这份文件仍是联合王国努力执行负责任国家行为

[10] www.ncsc.gov.uk/news/annual-review-2020。

[11] https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/uk-un-norms-non-paper-oewg-submission-final.pdf。

准则的一个有效指南。我们欢迎联合王国网络问题多利益攸关方咨询小组提交一份补充文件，[12] 其中就利益攸关方如何推动落实准则，以支持各国提出了建议。

联合王国认为，准则必须得到落实才能有效。以下是落实工作的关键因素：

- 提高政府和利益攸关方社区的认识，帮助就准则的价值形成共识，并促进采用准则。
- 为支持落实准则提供资源。落实准则可以而且应该成为国家网络安全战略的一个要素。2019 年，仅有 40%的国家有这种战略。联合王国继续支持一系列国家开展国家网络能力建设工作。
- 提供关于落实准则的最佳实践指南。联合王国认为，政府专家组的报告将提供许多国家所要求的网络空间负责任国家行为初步框架详细指南。上述非正式文件和补充文件也有助于建立这一领域的最佳做法。

建立信任措施

联合王国认为，各国应重点关注落实现有的建立信任措施，而不是拟订新措施。与私营部门、学术界和民间社会组织一道，区域组织在普及和落实以往政府专家组的建议方面可发挥重要工具的作用。但建立信任措施的落实仍然有限，使框架的潜在效力出现重大空白。

联合王国积极参加欧安组织网络建立信任措施非正式工作组。我们通过了关于能力建设的欧安组织建立信任措施 5，承诺支持在欧安组织国家中予以落实。2019 年，我们主办了一次基于网络情景的讨论，以便在 40 个成员国之间就建立信任措施的认识和执行工作进行演练。2020 年和 2021 年，联合王国担任欧安组织安全委员会主席，并借此主办了两场以网络为重点的活动。

能力建设

联合王国是双边网络能力建设的一个主要捐助国。我们认为，联合国可以利用其召集力加大对网络安全能力建设工作的关注，支持协调一致的良好做法。为了最大限度地提高效率和效力，重要的是让所有利益攸关方参与，避免现有工作出现重复。全球网络专门知识论坛已经成为能力建设的有效协调机制。独立的能力审查工具、最佳实践指南和网络安全事件响应小组社区中的事件应对和安全小组论坛等组织，在实现这一目标方面也发挥重要的推动作用。

2019-2021 年期间，联合王国是妇女参与国际安全和网络空间研究金方案的一个发起国。我们尤为自豪的是，通过这一方案为妇女更多参与不限成员名额工作组作出了贡献。

[12] www.un.org/disarmament/wp-content/uploads/2019/12/efforts-implement-norms-uk-stakeholders-12419.pdf。

定期机构对话

联合王国是一项行动纲领提案的提案国，该提案旨在促进联合国关于网络空间负责任国家行为的包容性定期机构对话。我们支持就制定和确立这一提案进一步开展工作。

三. 从国际组织收到的答复

欧洲联盟

[原件：英文]
[2021 年 5 月 31 日]

网络空间，尤其是全球开放互联网已经成为我们社会的支柱之一。它提供了一个推动互联互通和经济增长的平台。欧洲联盟及其成员国支持以法治、人权、基本自由和民主价值观为基础的全球、开放、稳定和安全的网络空间，该空间为全球带来社会、经济和政治发展。

随着互联网越来越深入我们的生活，我们在现实世界中面临的许多问题同样出现在网络空间。网络空间越来越多地被用于政治和意识形态目的，而且国际上的两极分化加剧，正在对有效的多边主义造成阻碍。全球开放互联网以及整个供应链技术控制方面的地缘政治紧张关系，使威胁状况更加复杂。恶意地以关键基础设施为目标，是一个重大的全球风险。对互联网的限制和互联网上的限制以及恶意网络活动的增加，包括影响信息和通信技术(信通技术)产品和服务的安全和诚信的活动的增加，威胁到全球开放网络空间，以及法治、基本权利、自由和民主。欧洲联盟及其成员国经常对这种恶意活动表示关切，这些活动破坏基于规则的国际秩序，增加冲突风险。

国家一级为加强信息安全和促进这一领域的国际合作所作的努力

欧洲联盟及其成员国大力支持上述开放、自由、稳定和安全的网络空间的愿景，并为此推进和实施一个包容、多层面的网络空间冲突预防和稳定的战略框架，包括通过双边、区域互动和多方利益攸关方参与。作为这一战略框架的一部分，欧洲联盟努力增强全球复原力，推动和促进对网络空间基于规则的国际秩序的共同理解，并制定和实施切实可行的合作措施，包括国家间的区域建立信任措施。加强全球网络复原力是维护国际和平与稳定的一个关键要素，可以降低冲突风险，成为应对经济和社会数字化相关挑战的一种手段。全球网络复原力可降低潜在犯罪人出于恶意滥用信通技术的能力，加强各国有效应对网络事件并从中恢复的能力。

2013 年题为“开放、安全和有保障的网络空间”的网络安全战略[13] 以及下文引用的后续政策文件、文书和战略，体现了欧洲联盟关于如何最好地预防和应对

[13] 见向欧洲议会、欧盟理事会、欧洲经济和社会委员会和区域委员会提交的题为“欧洲联盟网络安全战略：开放、安全和有保障的网络空间”的联合通报。

网络中断和攻击的全面愿景。上述各项政策文件、文书和战略旨在促进欧洲联盟的价值观，确保为数字经济的增长创造条件。某些具体行动旨在增强信息系统的网络复原力，减少网络犯罪，加强欧洲联盟国际网络安全政策和网络防御。

2015 年 2 月，欧洲联盟理事会在其关于网络外交的理事会结论[14] 中强调，必须进一步制定和实施欧洲联盟网络外交的共同和全面方法，促进人权和欧洲联盟基本价值观，确保言论自由，促进性别平等，推动经济增长，打击网络犯罪，减轻网络安全威胁，防止冲突，并为国际关系带来稳定。欧洲联盟还呼吁加强互联网治理的多利益攸关方模式，并在第三国加强能力建设。此外，欧洲联盟认识到与关键合作伙伴和国际组织互动合作的重要性。欧洲联盟还强调要在网络空间和国际安全领域适用现行国际法，并强调了行为规范的相关性以及互联网治理作为欧洲联盟网络外交共同和全面办法组成部分的重要性。

根据对 2013 年网络安全战略的审查，欧洲联盟与成员国和欧盟各相关机构充分合作，同时尊重其权限和责任，以协调一致的方式进一步加强了欧盟的网络安全架构和能力。2017 年，题为“复原力、威慑和防务：为欧盟建设强有力的网络安全”的联合通报[15] 阐述了挑战的规模和在欧洲联盟层面设想的措施范围，以确保欧洲联盟更好地准备应对不断增加的网络安全挑战。

对这些挑战的关切，推动了欧洲联盟针对恶意网络活动发展联合外交应对框架——网络外交工具箱。[16] 国家和非国家行为体通过恶意网络活动追求其目标的能力和意愿不断增强，这应该引起全球关注。根据国际法，此类活动可能构成不法行为，并可能导致不稳定和连带效应，增加冲突风险。欧洲联盟及其成员国致力于通过和平手段解决网络空间的国际争端。为此，欧洲联盟联合外交应对框架是欧洲联盟网络外交方法的一部分，有助于预防冲突、减轻网络安全威胁并使国际关系更加稳定。该框架鼓励合作，促进缓解当前和长期威胁，并从长计议，影响恶意行为体的行为。它还与欧洲联盟危机管理机制，包括协调应对大规模网络安全事件和危机蓝图进行适当协调。欧洲联盟及其成员国促请国际社会加强国际合作，支持一个全球、开放、稳定、和平和安全的网络空间，在这个空间里，人权、基本自由和法治完全适用。欧洲联盟及其成员国决心继续努力防止、阻止、遏止和应对恶意活动，争取加强这方面的国际合作。

2020 年 12 月，欧洲联盟进一步概述了其在复杂威胁环境中实现网络安全数字转型的战略。[17] 欧洲联盟的数字十年网络安全战略旨在促进和保护一个以人权、基本自由、民主和法治为基础的全球、开放、自由、稳定和安全的网络空间。该

[14] 《欧盟理事会关于网络外交问题的第 6122/15 号结论》。

[15] 见向欧洲议会和欧盟理事会提交的题为“复原力、威慑和防务：为欧盟建设强有力的网络安全”的联合通报。

[16] 《欧盟理事会关于欧盟打击恶意网络活动的联合外交应对框架(“网络外交工具箱”)的第 10474/17 号结论》。

[17] 见向欧洲议会和欧盟理事会提交的题为“欧盟数字十年网络安全战略”的联合通报，以及《欧盟理事会关于欧盟数字十年网络安全战略的第 7290/21 号结论》(2021 年 3 月 22 日)。

战略包含了具体建议，以便处理复原力问题，预防、威慑和应对网络威胁，推进全球开放网络空间。防止滥用技术、保护关键基础设施和确保供应链的完整性也使欧洲联盟能够遵守联合国关于负责任国家行为的准则、规则和原则。

欧洲联盟的国际网络空间政策促进对欧洲联盟核心价值观的尊重，界定负责任行为准则，倡导在网络空间适用现行国际法，同时协助欧洲联盟以外国家进行网络安全能力建设，促进网络问题国际合作。欧洲联盟继续与国际伙伴合作，推动和促进一个全球、开放、稳定和安全的网络空间，在这个空间中，国际法特别是《联合国宪章》得到尊重，不具约束力的负责任国家行为准则、规则和原则得到自愿遵守。为促进有效的多边辩论以推动网络空间的和平与安全，显然需要推进联合国网络空间负责任国家行为框架。欧洲联盟与联合国 53 个会员国一道，提议制定一项推进网络空间负责任国家行为的行动纲领。在大会认可的现有文书的基础上，行动纲领为联合国内部的合作和最佳做法交流提供一个永久性平台。它提供促进能力建设方案的机会，这些方案根据受益国确定的需求拟订。它还在联合国内部提供一个体制机制，以改善与私营部门、学术界和民间社会等其他利益攸关方就以下方面开展的合作，即履行各自的责任，以维护一个开放、自由、安全、稳定、无障碍与和平的信通技术环境。

政府专家组各项报告所述概念的内容

现有和新出现的威胁

欧洲联盟及其成员国认识到，网络空间为经济增长以及可持续和包容性发展提供重大机遇。然而，网络空间的最新发展带来了不断演变的挑战。

欧洲联盟及其成员国对网络空间恶意行为增加感到关切，其中包括国家和非国家行为体出于恶意目的滥用信通技术，以及借助网络盗窃知识产权的行为增加。这种行为破坏和威胁经济增长以及全球社会的诚信、安全和稳定，并可能导致不稳定和连锁效应，增加冲突风险。

随着 2019 冠状病毒病(COVID-19)大流行的持续，欧洲联盟及其成员国观察到针对成员国及其国际合作伙伴(包括医疗保健部门合作伙伴)的重要运营商的网络威胁和恶意网络活动。欧洲联盟及其成员国尤其感到震惊的是，最近影响信通技术产品和服务安全及诚信的活动增加，可能会产生系统性影响。

欧洲联盟及其成员国谴责网络空间的这种恶意行为，强调将继续支持增强全球网络复原力。任何阻碍关键基础设施能力的企图均不可接受，会危及生命。恶意使用信通技术破坏了互联网和信通技术使用给整个社会带来的好处，表明一些行为体随时准备切实危及国际安全与稳定。任何行为体都不应在网络空间进行不负责任和破坏稳定的活动。

欧洲联盟及其成员国促请每个国家根据国际法以及联合国政府专家组 2010 年、2013 年和 2015 年的协商一致报告，尽职尽责，对从其境内开展此类活动的行为体采取适当行动。欧洲联盟及其成员国再次强调，各国不应在知情的情况下

允许其领土被用于以信通技术开展国际不法行为，还应响应他国的适当请求，减少源自其领土的恶意网络活动。

此外，正如联合国政府专家组和不限成员名额工作组以往报告所确认的那样，鉴于信通技术的独特性，欧洲联盟在国际安全背景下解决网络问题的方法必须保持技术中立。这符合现有国际法适用于新领域，包括新兴技术的使用的概念和联合国在此方面的认可。

欧洲联盟及其成员国只能支持在充分尊重适用的国际法和准则，特别是《联合国宪章》，以及国际人道法和人权的前提下，开发和使用技术、系统或信通技术促成的服务。

国际法如何适用于信息和通信技术的使用

欧洲联盟及其成员国大力支持以尊重规则的国际秩序为基础的有效多边体系，该体系在应对网络空间当前和未来的全球挑战方面取得成果。

真正普遍的网络安全框架只能基于现行国际法，包括整个《联合国宪章》、国际人道法和国际人权法。欧洲联盟及其成员国重申，现行国际法适用于网络空间的国家行为，这是 2010 年、2013 年和 2015 年联合国政府专家组报告以及 2015 年报告第 28(a)至 28(f)段所确立的原则和不限成员名额工作组所确认的。

国际人道法等国际法，包括预防原则、人道原则、军事必要性原则、相称原则和区别原则，适用于网络空间的国家行为，是完全保护性的，为其合法性设定了明确界限，也适用于冲突背景。欧洲联盟强调，它坚信国际法不是冲突的促成因素；相反，国际法界定了指导军事行动的规则，以限制其影响，特别是为了保护平民。

此外，相关国际文书所载的人权和基本自由必须在线上和线下得到同等尊重和维护。欧洲联盟及其成员国欢迎联合国人权理事会[18] 和大会也确认了这些原则。

有鉴于此，欧洲联盟及其成员国不呼吁，也不认为有必要在现阶段为网络问题制定新的国际法律文书，因为已经有了国际法律框架。

欧洲联盟及其成员国重申，支持继续开展对话与合作，以促进对现行国际法适用于各国使用信通技术的共同认识，并重申支持努力在法律上澄清现行国际法如何适用，因为这将有助于维护和平、预防冲突和确保全球稳定。

我们继续支持目前为促进现行国际法在网络空间的适用所作努力，包括交流在网络空间适用现行国际法的信息和最佳做法。我们承诺继续通报各国在国际法如何适用于各国使用信通技术方面的立场，因为此举将增强透明度，并促进全球更好地了解各国的办法，这对维护长期和平与稳定，以及减少网络空间行为引发冲突的风险至关重要。应进一步关注提高对现行国际法适用性的认识并开展能力建设工作，将其作为促进网络空间稳定和防止冲突的手段。

[18] A/HRC/RES/20/8。

负责任国家行为准则、规则和原则

欧洲联盟及其成员国鼓励所有国家在联合国大会、特别是其第 70/237 号决议再三认可的工作的基础上再接再厉，继续推进这项工作，并进一步巩固不限成员名额工作组的工作，巩固推动落实商定准则和建立信任措施的工作，这些准则和措施在预防冲突中发挥重要作用。

正如联合国政府专家小组在 2010 年、2013 年和 2015 年的历次报告中所阐述的那样，欧洲联盟及其成员国在使用信通技术时将遵循现行国际法，遵守负责任国家行为的自愿准则、规则和原则，并在网络空间中执行这些准则、规则和原则。我们认为，切实可行的办法应该是鼓励在分享最佳做法方面加强合作和提高透明度，包括在有关政府专家组现有准则如何适用的最佳做法方面，并为此利用相关举措和区域组织和机构等框架，以促进提高认识并有效执行商定的负责任国家行为准则。

建立信任措施

在网络空间建立国家合作和互动的有效机制是预防冲突的重要组成部分。事实证明，区域论坛是一个相关的平台，可以为有共同关切和共同利益的行为体创造对话与合作的空间，以便从区域角度有效应对挑战。

在欧洲安全与合作组织、东南亚国家联盟地区论坛、美洲国家组织和其他区域场合制定和实施网络建立信任措施，包括合作和透明度措施，将提高国家行为的可预测性，降低信通技术事件可能引起误解、局势升级和冲突的风险，从而促进网络空间的长期稳定。

信息和通信技术安全和能力建设方面的国际合作与援助

为防止冲突，减少滥用信通技术造成的紧张局势，欧洲联盟及其成员国的目标是增强全球复原力，特别是发展中国家的复原力，以此应对与经济和社会数字化相关的挑战，并降低潜在犯罪人恶意滥用信通技术的能力。复原力可加强各国有效应对网络威胁并从中恢复的能力。

欧洲联盟及其成员国支持一系列有针对性的方案和举措，以协助各国发展应对网络事件的技能和能力，并支持通过直接互动、双边接触或通过区域和多边机构开展互动，推动交流最佳做法的举措。

欧洲联盟及其成员国认识到，促进适足的保护能力和更安全的数字产品、流程和服务将有助于建立一个更安全、更值得信赖的网络空间。我们认识到所有相关行为体在这方面参与能力发展的责任，并进一步呼吁加强与主要国际伙伴和组织的合作，以支持第三国的能力建设。欧洲联盟及其成员国特别重视加强网络空间的国际安全与稳定，并为此鼓励和促进就网络空间的负责任国家行为采取具体行动，加强网络能力建设合作，包括在联合国促进机制、例如行动纲领的支持下，推动符合受益国所确定需求的能力建设方案。