联合国 A/75/123

大 会

Distr.: General
23 June 2020
Chinese
Original: Arabic/English/French/
Spanish

第七十五届会议

暂定项目表* 项目 98

从国际安全角度看信息和电信领域的发展

秘书长的报告

目录

* A/75/50。

20-08285 (C) 070820 180820

一. 导言

1. 2019 年 12 月 12 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 93 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 74/28 号决议。

2. 在第 74/28 号决议第 2 段中，大会请所有会员国考虑到从国际安全角度看信息和电信领域问题发展政府专家组的报告中所载评估和建议，继续向秘书长通报其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中所述概念的内容。

3. 根据这一要求，在 2020 年 1 月 27 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。由于当前仍在持续的冠状病毒病(COVID-19)危机，为便于会员国就上述议题提出看法，将原定的 2020 年 5 月 15 日提交截止日期延长至 2020 年 5 月 31 日。

4. 截至本报告编写之时收到的回复载于第二和第三节。2020 年 5 月 31 日之后收到的其他答复将以来件原文语言登载于裁军事务厅网站(www.un.org/disarmament/ict-security)。

二. 从各国政府收到的答复

亚美尼亚

[原件：英文]
[2020 年 5 月 13 日]

亚美尼亚高度重视在完全遵守国际法原则和准则和《联合国宪章》的基础上建立开放、自由、稳定、安全的网络空间。鉴于网络空间具有全球性，必须保护在线人权和自由，特别是意见和表达自由，其中包括寻求、接受和传递信息的权利。与此同时，使用信息和通信技术和网络环境带来的挑战广泛多样。因此，国际社会应团结一致地采取对策，防止滥用信息通信技术，为和平、合作使用信息通信技术做出贡献。有鉴于此，亚美尼亚正在积极参与国际合作平台，以提高网络空间的透明度、可预测性和稳定性，降低使用信息和通信技术所带来威胁的风险。

亚美尼亚充分致力于全面贯彻执行欧洲委员会《网络犯罪公约》及其关于将通过计算机系统犯下具有种族主义和仇外性质的行为定为刑事犯罪的附加议定书。自 2019 年以来，亚美尼亚一直积极参与实施欧洲联盟和欧洲委员会的联合“网络东方”项目，旨在提高网络适应力、刑事司法和电子证据方面的能力。同样，亚美尼亚正在秉诚执行欧洲安全与合作组织(欧安组织)建立信任措施(常设理事会第 1202 号决定)，以减少使用信息和通信技术带来的威胁。2019 年 7 月，亚美尼亚接待了欧安组织跨国威胁司的专家小组，以评估在调查和起诉网络犯罪方面的国家能力。2019 年 11 月，欧安组织跨国威胁司在埃里温举办联席圆桌会议，

与亚美尼亚利益攸关方讨论上述评估结果。根据专家的评估报告和圆桌会议的结论，欧安组织跨国威胁司编写了一份专门针对这一专题的概念说明，这项工作日后可能变成一个项目。

政府专家组2013年和2015年报告的内容和调查结果表达了参与政府专家组报告编写的联合国少数会员国的立场，因此，这无助于制定一套所有会员国都能接受的普遍、全面规范。同样，我们认为，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作为一个包容透明的会员国间讨论平台，可以就使用信通技术方面负责任国家行为的规则、规范和原则拟定一份所有会员国都能接受的全面综合清单。

澳大利亚

[原件：英文]
[2020年5月29日]

澳大利亚欢迎有机会响应大会第74/28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题为“从国际安全角度看信息和电信领域的发展”2016年第70/237号决议、2014年第68/243号决议和2011年的第65/41号决议提供的资料。

总体而言，从国际安全角度看信息和电信领域的发展问题政府专家组2010年(A/65/201)、2013年(A/68/98)和2015年(A/70/174)的报告确认，现行国际法、特别是整个《联合国宪章》对于维护和平与稳定以及对于促进开放、安全、稳定、可及、和平的信息和通信技术环境是适用的，也是必不可少的。这些报告还阐明了负责任国家行为的自愿、非约束性规范，同时确认需要制定建立信任措施和协调开展能力建设。这些措施(国际法、规范、建立信任措施和能力建设)加在一起通常被称为负责任国家行为框架，为安全、稳定和繁荣的网络空间提供依据。

澳大利亚再次承诺将按照政府专家组2010年、2013年和2015年多次提出的报告(A/65/201；A/68/98；A/70/174)采取行动。澳大利亚正在积极参加第六届政府专家组和首届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(分别根据第73/266号决议和第73/27号决议设立)的工作。

国际法

澳大利亚在《国际网络参与战略》(2017年)中阐述了对国际法如何规范网络空间国家行为的立场，并在《2019年国际法补编》加以补充(均可查阅外交和贸易部网站：www.dfat.gov.au/sites/default/files/application-of-international-law-to-cyberspace.pdf。

2020年2月，澳大利亚发表了题为“国际法在网络空间的适用问题案例研究”的非正式文件(可查阅不限成员名额工作组网站：https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/australian-international-law-case-

studies-final-5-february-2020.pdf；外交和贸易部网址：www.dfat.gov.au/sites/default/files/australias-oewg-non-paper-case-studies-on-the-application-of-international-law-in-cyberspace.pdf)。

执行情况

大会在 2015 年呼吁所有会员国“将政府专家组 2015 年报告作为其使用信息和通信技术的指南”(见第 70/237 号决议)，有鉴于此，澳大利亚发表了一份综述，说明了澳大利亚遵守和实施 2015 年政府专家组报告中国际法、负责任国家行为准则、建立信任措施和能力建设等四大支柱的情况(可查阅不限成员名额工作组网站：https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf；澳大利亚外交和贸易部网站：https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/international-security-and-cyberspace)。

2015 年政府专家组报告阐明了最佳做法方面的活动，许多国家正在或已经予以实施。澳大利亚鼓励所有国家根据 2015 年政府专家组报告(适用国际法、执行负责任国家行为准则、建立信任措施和能力建设)对正在进行的活动进行评估，并找出差距以及填补这些差距所需的能力(如果适用)。澳大利亚与墨西哥和其他 24 个国家一道，谨向不限成员名额工作组(根据第 73/27 号决议设立)提出一项建议，即对各国执行大会第 70/237 号决议的情况进行一次调查(可查阅不限成员名额工作组的网站：https://front.un-arm.org/wp-content/uploads/2020/04/final-joint-oewg-proposal-survey-of-national-implementation-16-april-2020.pdf和外交和贸易部网站：www.dfat.gov.au/sites/default/files/joint-oewg-proposal-survey-of-national-implementation-april-2020.pdf)。

性别平等

正如妇女与和平与安全议程所确认的那样，妇女受到冲突和对国际和平与安全的威胁的影响有所不同而且十分独特。澳大利亚赞扬联合国裁军研究所最近就军备控制、不扩散和裁军外交中的性别平衡问题提出了题为“仍然落后于曲线”的报告，其中指出，第一委员会的女性外交官比例是大会所有主要委员会中最低的。“妇女参与国际安全和网络空间研究金”是澳大利亚、大不列颠及北爱尔兰联合王国、加拿大、荷兰和新西兰等国政府提出的一项联合倡议，旨在促进妇女更多地参与联合国与网络空间负责任国家行为相关的国际安全问题的讨论。澳大利亚将继续采取切实步骤，支持妇女积极有效地参与国际安全和裁军方面的多边讨论。

波斯尼亚和黑塞哥维那

[原件：英文]
[2020 年 5 月 11 日]

波斯尼亚和黑塞哥维那在国家一级为加强信息安全和促进该领域国际合作所作努力的情况介绍

本报告基于从以下波斯尼亚和黑塞哥维那机构收集的数据：波斯尼亚和黑塞哥维那安全部、波斯尼亚和黑塞哥维那国防部、波斯尼亚和黑塞哥维那运输和通信部、联邦警察署、塞族共和国内政部以及塞族共和国科技发展、高等教育和信息社会部。在报告发送之前向波斯尼亚和黑塞哥维那安全部提交数据的相关机构是：布尔奇科特区警察局和联邦运输和通信部。

波斯尼亚和黑塞哥维那签署了与信息和网络安全有关的国际协定和公约。其中最突出的是《网络犯罪公约》和《联系国协定》。《公约》于 2001 年 11 月 23 日在布达佩斯开放供签署，波斯尼亚和黑塞哥维那主席团在 2006 年 3 月 25 日举行的第八十九届会议上作出批准该文件的决定。据此，波斯尼亚和黑塞哥维那有义务通过打击网络犯罪的立法和其他必要措施，在重罪惩治、数据获取、处理和存储方面与《公约》的其他签署国协调一致。

在涉及《公约》所涵盖的主题方面，波斯尼亚和黑塞哥维那可适用以下立法：

- 《波斯尼亚和黑塞哥维那刑法》，《波斯尼亚和黑塞哥维那政府公报》(第 3/03 号)
- 《刑事诉讼法》，《波斯尼亚和黑塞哥维那政府公报》(第 3/03、32/03、36/03、26/04、63/04、13/05、48/05、46/06、76/06、29/07、32/07、53/07、76/07、15/08、58/08、12/09、16/09、93/09 和 72/13 号)
- 《波斯尼亚和黑塞哥维那联邦刑法》，《波斯尼亚和黑塞哥维那联邦政府公报》(第 36/03、21/04、69/04、18/05、42/10、42/11、59/14、76/14、46/16 和 75/17 号)
- 波斯尼亚和黑塞哥维那联邦刑事诉讼法，《波斯尼亚和黑塞哥维那联邦政府公报》(第 35/03、37/03、56/03、78/04、28/05、55/06、27/07、53/07、09/09、12/10、08/13 和 59/14 号)
- 《塞族共和国刑法》，《塞族共和国政府公报》(第 64/17 和 104/18 号)
- 《塞族共和国刑事诉讼法》，《塞族共和国政府公报》(第 53/12、91/17 和 66/18 号)
- 《布尔奇科特区刑法》，《布尔奇科特区政府公报》(第 33/13、26/16、13/17 和 50/18 号)
- 《布尔奇科特区刑事诉讼法》，《布尔奇科特区政府公报》(第 33/13、27/14 和 3/19 号)

国家一级

波斯尼亚和黑塞哥维那安全部出于上述考虑并意识到网络空间可能出现的风险，开展了以下活动。

根据波斯尼亚和黑塞哥维那安全部的提议，波斯尼亚和黑塞哥维那部长会议在 2017 年 3 月 8 日举行的第九十三届会议上通过了“关于成立波斯尼亚和黑塞哥维那各机构计算机应急小组的决定”，并在《波斯尼亚和黑塞哥维那政府公报》(第 25/17 号)上公布，从而成立了计算机应急小组，隶属波斯尼亚和黑塞哥维那安全部信息技术和电信系统司。

根据上述决定第 4 条，波斯尼亚和黑塞哥维那安全部需要调整其内部组织，系统安排工作岗位，以使计算机应急小组进入正常运作。2017 年底收到了机构内部机构改革和制度化时按照程序提出的所有必要意见，这些意见以及已经编制的所有文件都是积极正面的。

为了使计算机应急小组进入正常运作，波斯尼亚和黑塞哥维那安全部对其内部组织和工作岗位的系统安排作出必要变动修改和修正，并提交波斯尼亚和黑塞哥维那部长会议通过。目前，正在等待波斯尼亚和黑塞哥维那部长会议批准拟议规则手册。在获得批准后，波斯尼亚和黑塞哥维那安全部将启动波斯尼亚和黑塞哥维那机构计算机应急小组的技术和业务组建工作。内部组织的拟议变动包括在信息技术和电信系统部这个新设立的司增设 5 个职位。

波斯尼亚和黑塞哥维那安全部计划在业务、体制和技术上加强计算机应急小组，旨在实现该机构的战略目标(与波斯尼亚和黑塞哥维那有关机构开展协调与合作、消除和减少未经授权访问波斯尼亚和黑塞哥维那各机构信息和通信技术系统的安全事件所产生的后果、通过坚持不懈提高波斯尼亚和黑塞哥维那各机构信息和通信技术系统的可靠性、努力预防和尽量减少发生安全事件的可能性、协助行政人员处理安全事件等)，从而根据“决定”第 6 条开展活动，并在波斯尼亚和黑塞哥维那建立计算机应急小组网络。

此外，根据波斯尼亚和黑塞哥维那安全部的提议，波斯尼亚和黑塞哥维那部长会议在 2017 年 7 月 6 日举行的第 107 届会议上通过了关于统一波斯尼亚和黑塞哥维那网络安全领域立法的分析报告，并责成波斯尼亚和黑塞哥维那安全部加紧起草波斯尼亚和黑塞哥维那网络安全战略。

因此，目前正在开展活动，协调各实体和机构对战略文件模式的意见，使之与《欧洲联盟网络信息安全指令》保持同步，同时与波斯尼亚和黑塞哥维那的宪政组织保持一致。

在欧洲安全与合作组织(欧安组织)的主持下，成立了一个非正式工作组。该小组由波斯尼亚和黑塞哥维那主管机构和有意参与的机构的代表组成，并起草了《关于波斯尼亚和黑塞哥维那战略网络安全框架的指导方针》。

此外，波斯尼亚和黑塞哥维那安全部正在参与为起草波斯尼亚和黑塞哥维那防止和打击恐怖主义新战略开展的活动，其中应涵盖利用数字环境开展这些活动。

波斯尼亚和黑塞哥维那安全部积极参与欧洲委员会网络犯罪公约委员会的工作。

根据波斯尼亚和黑塞哥维那安全部的提议，波斯尼亚和黑塞哥维那部长会议在 2016 年 11 月 10 日举行的第 80 届会议上通过了“关于设立实施网络犯罪领域能力建设项目部际工作组(iPROCEEDS)的决定”(在波斯尼亚和黑塞哥维那政府公报(第 14/17 号)上颁布)。

2016 年 1 月，欧洲联盟和欧洲委员会就一个东南欧国家打击网络犯罪领域能力建设区域项目(iPROCEEDS)签署一份协议，重点是没收网络犯罪收益。项目为期 42 个月。该项目由欧洲联盟和欧洲委员会提供资金，而实施工作由欧洲委员会布加勒斯特网络犯罪办公室负责。有人提议，代表波斯尼亚和黑塞哥维那的项目组由司法部对这一罪行拥有管辖权的机构组成：检察官办公室、警察、金融情报部门等。根据上述安排，这一工作组已经成立。

此外，波斯尼亚和黑塞哥维那安全部负责协调 iPROCEEDS-2 项目小组成员，该项目小组成立于 2020 年 1 月，负责在东南欧和土耳其打击互联网犯罪收益和收集电子证据。该项目将以 iPROCEEDS 项目实施期间取得的成果为基础，集中在以下项目领域提供有针对性的支持：(a) 在充分尊重基本权利和自由、包括保护隐私和个人数据的前提下，就收集电子证据和获取数据开展立法；(b) 与欧洲联盟和欧洲委员会的个人数据保护标准保持一致；(c) 推动网络犯罪和网络安全政策和战略；(d) 在网络犯罪和犯罪收益调查方面开展机构间和公共-私营部门合作；(e) 针对网上欺诈和其他网络犯罪罪行的公众举报制度；(f) 关于网络犯罪和电子证据以及相关金融调查和反洗钱措施的司法培训；(g) 在调查网络犯罪和网上犯罪收益方面开展机构间合作和信息共享。该项目为期 42 个月。

波斯尼亚和黑塞哥维那安全部成功地发挥了执行欧安组织建立信任措施的联络方作用。在此期间开展的一些活动包括成功地就波斯尼亚和黑塞哥维那网络安全的现状提出报告和提供信息、参加根据常设理事会第 1039 号决定组成的部际工作组的工作并参加七次通信检查、在 2019 年 5 月主办关于网络安全和信通技术安全的次区域培训等。此外，我们在几个当地会议和讲习班的组办方面向欧安组织提供了人员和知识方面的支持。

此外，波斯尼亚和黑塞哥维那已被列入题为“东南欧打击网络犯罪刑事司法人员的能力建设”的区域项目。该项目由德国和美利坚合众国政府提供资金，是由欧安组织跨国威胁司与该区域各国(阿尔巴尼亚、波斯尼亚和黑塞哥维那、黑山、科索沃、[1] 塞尔维亚和北马其顿)和欧安组织外地特派团的代表合作开展的。该项目的主要目的是教育和培训负责处理网络和与网络有关的有组织犯罪案件的专家。该项目在 2017-2019 年期间进行，在制定解决网络犯罪和网络安全威胁问题、加强打击网络犯罪和应对网络安全威胁的现有能力的全面综合战略框架等方面

[1] 这一称谓不影响对地位问题的立场。

作出贡献。波斯尼亚和黑塞哥维那安全部在该项目中是波斯尼亚和黑塞哥维那的协调机构。

波斯尼亚和黑塞哥维那国防部正在开展活动，以便到 2023 年在其管辖范围内建立一个高效、可持续的网络安全系统。迄今，国防部于 2017 年 10 月 4 日通过了《国防部门网络安全战略》。这一战略的详细实施计划于 2017 年 12 月 27 日获得通过。安全目标的重点是，防止安全事件，应对安全事件，对波斯尼亚和黑塞哥维那国防部门在网络安全领域工作的人员进行教育和认证，以及提高最终用户对通信和信息系统安全的认识。为落实上述几点，波斯尼亚和黑塞哥维那国防部已经起草或通过了某些执行文件。

此外，波斯尼亚和黑塞哥维那国防部已着手设立波斯尼亚和黑塞哥维那国防部计算机应急小组。

波斯尼亚和黑塞哥维那国防部有义务在北大西洋公约组织和平伙伴关系范围内实施关于网络防御的伙伴目标 G7300，该目标要求：(a) 通过政策、程序和其他文件，切实将网络防御纳入行动和行动规划进程，并实施网络空间的国际条例、风险交换的安全措施以及在网络安全领域的国家和国际机构间网络威胁评估；(b) 设立一个常设计算机应急小组；(c) 建立能力，确保波斯尼亚和黑塞哥维那国防部及其武装部队在信息和信息系统方面的机密性、可用性和真实性；(d) 开展外地专家和最终用户的教育和培训方案；(e) 通过组织国家网络演习和研讨会，以及波斯尼亚和黑塞哥维那国防部和波斯尼亚和黑塞哥维那武装部队派工作人员参加国际网络演习和研讨会，落实教育方案。

根据波斯尼亚和黑塞哥维那运输和通信部的提议，并与波斯尼亚和黑塞哥维那安全部合作，波斯尼亚和黑塞哥维那部长理事会在 2017 年 3 月 22 日举行的第 95 届会议上通过了 2017-2022 年波斯尼亚和黑塞哥维那各机构信息安全管理政策。

波斯尼亚和黑塞哥维那运输和通信部目前正在与波斯尼亚和黑塞哥维那安全部一道，根据欧洲联盟《关于网络和信息系统安全的 2016/1148 号指令》，起草和统一一项关于信息安全及网络和信息系统安全的法律。该部还与牛津大学全球网络安全能力中心、世界银行和全球网络安全发展中心等共同编写了一份能力成熟度报告，以评估波斯尼亚和黑塞哥维那网络安全的人力水平。

关于今后的活动，波斯尼亚和黑塞哥维那运输和通信部计划提出一项关于电子交易保密服务的电子身份验证法，并起草一项波斯尼亚和黑塞哥维那信息社会发展战略。

实体一级

波斯尼亚和黑塞哥维那联邦

联邦警察署已经认识到网络安全的重要性，因此在 2015 年成立一个打击网络犯罪部门。该部门和法医分析中心有足够的工作人员、知识和设备。这个打击网络犯罪部门有 10 名专家，而法医分析中心是欧洲法医科学研究所网络的成员。此外，该机构还与联合国儿童基金会、国际埃玛乌斯组织和救助儿童会一起，积

极参与实施在波斯尼亚和黑塞哥维那数字环境中防止儿童性剥削和性虐待的项目。此外，该机构在实施 iPROCEEDS、“东南欧刑事司法人员打击网络犯罪和网络导致犯罪的能力建设”等上述项目方面发挥重要作用，并在实施新的 iPROCEEDS-2 项目方面发挥关键作用。

波斯尼亚和黑塞哥维那联邦在 2018 年通过了“关于成立波斯尼亚和黑塞哥维那联邦各机构计算机应急响应工作组的决定”，目标和宗旨与前述两个机构相同。

塞族共和国

塞族共和国内政部表示，已经开展一些活动，使该实体内的立法与欧洲联盟的立法保持一致，并为此通过了 2017-2021 年期间发展方向和 2017-2019 年期间执行发展方向的行动计划。此外，还通过了 2017-2021 年期间信息和通信技术发展方案，其中包含一项侧重于改进和整合信息通信系统的目标。有鉴于此，对塞族共和国警察和内政法进行更新，从而建立了执行《欧洲联盟关于内部市场电子交易的电子身份识别和信托服务的第 910/2014 号条例》和《关于网络和信息系统安全的第 2016/1148 号指令》的机制。

根据塞族共和国内政部的提议，通过了《关键基础设施安全法》(《塞族共和国政府公报》(第 58/19 号))，从而为执行《第 2008/114/EC 号指令》和《欧洲联盟网络信息安全指令》提供依据。通过这种方式，建立了立法能力，并确立了该实体用于应对任何事件包括与网络有关事件的关键基础设施的定义。

此外，该机构还参与了以下项目：2015 年“加入前援助文书”项目、“提高波斯尼亚和黑塞哥维那执法机构间信息交流的质量和安全”、“刑事司法人员打击网络犯罪和网络导致犯罪的能力建设”、iPROCEEDS 和 iPROCEEDS-2。该部还在与其他机构和法律主体进行安全数据交换基础设施方面开展筹备工作，并根据《欧洲联盟关于内部市场电子交易的电子身份识别和信托服务的指令条例》中定义的安全机制提供服务。此外，有关建立现有信息安全机制的文件正在起草中。

与波斯尼亚和黑塞哥维那所有其他执法机构一样，塞族共和国内政部还有一个专门负责打击高科技犯罪的单位，与国际刑事警察组织、欧洲联盟执法合作署、欧洲联盟刑事司法合作署、联合国毒品和犯罪问题办公室、欧安组织、欧洲联盟执法培训局、美国大使馆、国际刑事调查培训方案、国际警察协会、联合国儿童基金会和许多其他大使馆和国际组织开展合作。合作领域包括教育、培训、知识和数据交换等。

在增设确保波斯尼亚和黑塞哥维那网络安全的机构方面，塞族共和国实体于 2011 年通过了《信息安全法》(《塞族共和国政府公报》(第 70/11 号))，其中规定了基本信息安全规则。根据这项法律，在原塞族共和国信息社会机构(即现在的科学和技术发展、高等教育和信息社会部)中设立了塞族共和国的信息安全部门，即计算机应急小组。该机构的任务是：协调预防，防范计算机安全事故，保护公共机构、法人和自然人的网络基础设施。在过去两年中，该机构成立了塞族共和国政府安全行动中心，目的是从信息安全角度保护相关基础设施。对操作人员的培

训也已进行，并开始了三班倒的工作。该机构致力于受到相关国际组织的认可或和成为其成员。

加拿大

[原件：英文和法文]
[2020 年 5 月 7 日]

在网络安全方面，加拿大：

- 致力于促进国际稳定以及自由、开放、安全的网络空间
- 认为国际法适用于各国使用信息和通信技术，并可以加强网络空间的稳定
- 鼓励各国尊重商定的网络空间国家行为准则，包括从国际安全角度看信息和电信领域的发展问题政府专家组在 2015 年报告中提出的并获得大会认可的各项准则
- 认为务实的建立信任措施是加强网络空间稳定的行之有效的方法

在国家一级，加拿大在许多方面作出积极努力：

- 2018 年 6 月，政府由加拿大公共安全部门牵头，发布了《加拿大国家网络安全战略》。该战略旨在加强伙伴关系，以确保联邦政府内外重要网络系统的安全，在加拿大人和加拿大企业在线连接时给予保护。该战略还寻求更好地发现不断变化的网络威胁并采取应对措施。该战略立足于三个高级别目标：(a) 安全、有复原力的加拿大系统；(b) 创新型、具有适应能力的网络生态系统；(c) 领导力、治理和协作。加拿大正在通过《2019 年国家网络安全行动计划》贯彻落实该战略的目标，并在该计划中阐述了在五年内采取的具体举措。
- 在执行《国家网络安全战略》过程中，加拿大建立了加拿大网络安全中心，将政府的网络安全行动单位合并为一个面向公众的组织。作为加拿大的国家计算机应急响应小组，网络中心是向政府、关键基础设施所有者和运营商、私营部门及加拿大公众提供专家建议、指导、服务和支持的统一来源。
- 《2018 年国家网络安全战略》还包括为新成立的国家网络犯罪协调股提供资金。该股隶属加拿大皇家骑警，为加拿大所有警察机构提供服务，并将与公共和私营部门合作伙伴合作。该股将于 2023 年全面投入运作，负责协调和理顺网络犯罪调查，实现加拿大和国际多重管辖的目标。
- 加拿大皇家骑警在 2018 年也获得资金，用于增强调查情报方面的行动能力，在支持打击国内和国际网络犯罪活动的行动方面加强专门技术知识。

在国家一级，加拿大在许多方面作出积极努力：

- 加拿大正在多个国际论坛中与国际社会、志同道合的国家和盟国进行接触，以加强国际网络安全环境。例如，加拿大继续推动制定国际法以及

尊重网络空间方面的商定国家行为准则，包括政府专家组 2015 年报告中提出的并获得大会认可的准则。加拿大还积极参与从国际安全角度看信息和电信领域发展问题不限成员名额工作组正在进行的工作，并酌情就政府专家组正在进行的讨论发表意见。加拿大希望，不限成员名额工作组将促进商定准则的贯彻落实，解决网络安全中涉及性别的问题，等等。

- 在联合国多边论坛上，加拿大始终致力于推动制定准则和标准，并敦促各国尊重其人权义务。这包括打击利用信息和通信技术实施的暴力侵害妇女和女童行为，并确保她们在线下和线上环境中的安全和人格完整。加拿大寻求以各种途径推进这些目标，包括在人权理事会牵头通过一项关于消除数字环境中暴力侵害妇女和女童行为的决议。

- 加拿大在 2017 年题为“强大、安全、参与”的国防政策指导下，正在努力遏制和应对恶意网络活动，包括利用其网络能力支持军事行动。加拿大武装部队的现役网络人员必须遵守与其他军事人员相同的严格要求，包括相关的国内和国际法律和义务以及接战规则。

- 在 2018 年 6 月的夏洛瓦峰会上，七国集团领导人宣布创建快速反应机制。该机制的任务是协调七国集团的努力，通过信息共享和分析，发现和应对我们民主国家面临的各种不断变化的威胁，包括故意传播虚假信息，并确定协调应对的机会。该机制旨在消除民主制度面临的各种广泛威胁，造福于七国集团成员和整个国际社会。

正在进行的其他一些国际努力包括：

- 自 2015 年以来，加拿大承付了逾 400 万美元，用于支持网络安全能力建设项目。加拿大还资助美洲的女外交官参加不限成员名额工作组，将此作为妇女参与网络研究金方案的一部分，该方案旨在促进妇女切实参与联合国网络问题谈判。

- 加拿大支持北大西洋公约组织加强联盟和盟国的网络防御。

- 加拿大一直致力于在欧洲安全与合作组织、美洲国家组织、东南亚国家联盟区域论坛等各种论坛上执行建立信任措施。

- 加拿大是自由在线联盟的积极成员，该联盟是一个促进在线人权的国际多边组织，加拿大担任人工智能和人权问题多方利益攸关方专责小组的主席。

加拿大继续致力于推进全球努力，以确保网络空间的安全与稳定，造福所有人。

哥伦比亚

[原件：西班牙文]
[2020 年 5 月 29 日]

根据大会题为“从国际安全角度促进网络空间负责任国家行为”的第 74/28 号决议，在考虑到从国际安全角度看信息和电信领域的发展政府专家组报告中所载的评估和建议的同时，哥伦比亚高兴地向秘书长通报其对以下问题的看法和评估：

- 国家一级努力加强信息安全和促进国际合作。
- 政府专家组各项报告提及概念的内容。

导言

哥伦比亚总体上赞成建立一个确保网络中立的自由、开放和安全的数字环境，因此认为，必须继续优先重视基于国际法以及现有规范和协定的能力建设与合作，并在网络空间执行建立信任措施。

哥伦比亚在控制论领域作出重大努力，加强最高级别的机构间协调，以确保更安全的网络空间。

根据 2016 年通过的数字安全公共政策，国家政府成立了由相关实体参加的数字安全委员会，协调努力应对潜在的国家网络安全危机。该委员会由一名国家协调员即现任负责经济事务和数字转型的总统顾问领导。信息和通信技术部担任其技术秘书处。

这些机构协调努力，审查和更新与数字安全有关的政策和法律，审查国际议程，确保数字环境中的国防和安全，以指导旨在减轻和打击网络攻击、保护国家关键基础设施以及加强人力、各种技术和实际能力的活动，如下所示：

- **哥伦比亚计算机应急小组**。国防部内设有一个机构，其目的是协调必要的活动，以保护关键的国家基础设施免受威胁或破坏国家安全和国防的网络安全紧急情况的影响。它负责应对计算机安全事件。
- **国家军队联合网络司令部**。负责指导、规划、协调、整合、实施和同步开展联合网络行动的监督机构。其任务是实施网络防御措施，并在战略层面开展军事网络行动，以确保国家安全和网络空间防御，包括关键基础设施方面的协调。
- **网络警察中心哥伦比亚网络安全能力中心**。刑事调查局和国家警察国际刑事警察组织内的一个司，负责制订刑事调查战略、方案和项目，以确保数字安全、网络安全和保护本国民众在网络空间中分发的信息和数据。
- **网络安全事件响应小组**。哥伦比亚设有政府、金融、部门和私人响应小组。在区域一级，在美洲国家组织(美洲组织)框架内，哥伦比亚是旨在加强区域传播警告的美洲计算机安全事件响应小组半球网络成员。

哥伦比亚赞同，有必要加强国家间的协调与合作，以便审议威胁以及应对威胁的可能合作措施。尤其重要的是，不仅要以转让知识、技术和最佳做法的形式，而且要以联合协调行动的形式加强国际合作。

对于技术不太先进的国家，还必须订立协议，以确保网络空间不会因对这些国家的潜在影响而成为不断升级的冲突的舞台，无论这些国家成为网络行动的目标，还是因缺乏足够的预防能力被用作“代理国”而成为受害者。

在这些国家，对关键网络基础设施的任何损害都会产生巨大影响，不仅是因为对信息和通信技术(信通技术)的依赖以及转向使用连接到互联网的技术实现工业流程的自动化，还因为缺乏对风险和威胁的认识，以及缺乏加强对这类基础设施的公司的数字安全的管理所需的资源。

因此，应将缺乏能力视为一个风险因素，也需要建立国际合作机制，审查风险和进行能力建设。

此外，缺乏与关键活动相关的风险分类以及预防和保护措施，对在数字安全领域不太先进的国家来说，这是一种风险。缺乏数字安全治理框架，进而阻碍机构间和国际协调，这也构成风险。

除了新威胁或由于令人眼花缭乱的技术发展而在未来可能出现的威胁外，必须采用跨国办法处理网络空间负责任国家行为以及信息和电信安全问题，以便有效地应对威胁。需要共同努力确保及时传播信息，包括负责任地交换脆弱性方面的信息，并有效应对潜在威胁。

哥伦比亚重申十分愿意继续加强协调与合作，审议当前和潜在的威胁以及为应对这些威胁而可能采取的措施，包括合作。

负责任国家行为的自愿规范、规则和原则

哥伦比亚完全同意政府专家组报告、特别是以政府专家组前任工作为基础的 2015 年报告中提出的概念、考量、解释和建议，2015 年报告提出的建议同年受到大会的欢迎，成为会员国使用信通技术的指南。

近期的努力应侧重于广泛传播和执行这些建议。哥伦比亚认为目前不需要制订一份具有约束力的文书。

为加强各国执行建议的能力，国际合作也很重要。

哥伦比亚重申愿意遵循联合国宗旨，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。

在这方面，哥伦比亚于 2019 年 9 月 23 日支持美利坚合众国编写的关于促进网络空间负责任国家行为的声明，其中反映了若干国家的共同承诺，即合作更有效应对和威慑恶意、干扰性、破坏性和破坏稳定的网络活动，确保加强网络空间的问责和稳定。声明强调，网络空间负责任国家行为必须以国际法为指导，遵守和平时期负责任国家行为的自愿规范，并实施切实的建立信任措施。

哥伦比亚还支持法国政府于 2018 年 11 月 12 日发起的《网络空间信任与安全巴黎呼吁》倡议；该倡议推动制定加强网络空间安全的共同原则，并得到各国、私营企业和民间社会组织的支持。

此外，哥伦比亚支持法国和新西兰政府于 2019 年 5 月发起的《消除网上恐怖主义和暴力极端主义内容的克赖斯特彻奇呼吁》倡议。

哥伦比亚已在国家一级制定公共政策，载于国家经济和社会政策委员会的文件中。2011 年，哥伦比亚正式努力确认网络安全和网络防御是国防的基石。为此，国家经济和社会政策委员会题为“网络安全和网络防御政策指南”的第 3701 号文件，其总体目标是加强国家能力，应对网络领域国家安全和国防威胁(网络安全和网络防御)，创造网络空间得到保护的环境和条件。在 3 个主要领域取得进展：(a) 建立侧重于处理网络安全事件的机构，并发布加强国家应对网络空间威胁能力的准则；(b) 建立信息安全培训机制，扩大相关研究范围；(c) 加强网络安全法律。

2016 年，政府发布了国家经济和社会政策委员会题为“国家数字安全政策”的第 3854 号文件，着重实现以下 4 个主要目标：(a) 加强体制框架；(b) 提高各利益攸关方的能力，帮助其识别、管理、解决和减轻在线社会经济活动中的数字安全风险；(c) 促进分摊责任；(d) 将风险管理办法纳入各利益攸关方的在线活动。

自 2019 年以来，政府一直在制订有关数字信任与安全的公共政策，其目标包括评价和更新数字安全治理框架，以完善数字安全治理框架。该政策规定建立国家网络安全事件管理系统，目的如下：(a) 协调机构努力，确保及时管理网络安全事件；(b) 作为该国报告网络安全事件统计数据的官方来源；(c) 对定期报告事件和脆弱性的机制进行标准化，以便能够识别、评估并传达给各利益攸关方；(d) 为国家政府的决策提供信息。我们正计划实施支持该系统的技术。系统中的信息将由国家安全机构实时查阅。

在安全事项上进行国际合作，并利用创新、科学和技术加强国防部门的能力，这已被纳入国防与安全政策准则的战略转型目标。

哥伦比亚在通过战略国际伙伴关系实现共同安全的框架内，在网络安全和网络防御领域开展外交活动。例如，哥伦比亚作为北大西洋公约组织的全球伙伴进行知识交流，并正根据个别伙伴关系合作方案，加强国家军队的能力及其应对威胁和保护网络空间的协调努力。

哥伦比亚还根据国际最佳做法和标准，为私营部门、公共部门和公私混合部门制订有关建立和运作计算机安全事件响应小组的准则，以确保对影响国家利益的网络安全事件进行业务管理；促进与美洲和欧洲的计算机安全事件响应小组成员在数字安全、网络安全和网络防御方面的合作、协作和国际援助；交流经验和最佳做法。

联合网络指挥部方面将参加伊比利亚美洲网络防御论坛，以推进合作，分享经验教训，加强管理网络空间跨国风险和威胁的能力，并参加国家和国际演习。

通过哥伦比亚网络安全能力中心，网络警察中心将进行分析，发布预防警报，参与与管理网络安全事件相关的活动，并启动对网络犯罪的调查。

通信监管委员会有以下目标：(a) 建立各种机制，促进通信服务提供商和哥伦比亚计算机应急小组之间在数字安全方面的合作；(b) 将有关信息安全事件的部门信息集中在负责管理此类信息的实体内；(c) 向应急小组提供必要的信息，以管理事件并提高相关认识，使各利益攸关方受益。

为此，通信监管委员会发布了 2018 年第 5569 号决定，其中规定，各电信网络和服务提供商必须实施信息安全管理系统，并调整流程，以确保数据的完整性、保密性和可用性。

应该指出的是，经济合作与发展组织在《数字安全风险管理促经济和社会繁荣》文件中所提出的建议已在数字安全政策中得到考虑。

经济合作与发展组织在该文件中指出，数字安全风险管理应从界定经济和社会目标或设计具体活动着手，以便可在风险管理阶段评估与活动相关的风险水平，并确定对经济和社会目标的任何潜在影响。

随后，在风险处理阶段，各利益相关方应通过决定是否应承担、降低、转移或避免风险，确定应如何修改策略，以增加活动成功的可能性并维持既定目标。为了降低风险，他们可以选择和实施安全措施，或考虑采取创新和准备措施。

因此，一旦发生信通技术事件，哥伦比亚将考虑所有相关信息，包括所发生事件的大背景，信通技术环境中归责方面的困难，以及后果的性质和范围。

关于事件的特征及其必须向主管当局报告的问题，通信监管委员会在 2018 年第 5569 号决定中对信息安全事件类别进行界定时，也考虑到国际标准化组织和国际电工委员会制定的 27000 系列标准(特别是第 27035-1 号标准中界定的类别)中规定的准则和最佳做法。根据该决定，当信息安全事件发生时，通信网络和服务提供商在事件得到遏制、杜绝和恢复后必须向哥伦比亚计算机应急小组发送电子报告。

根据有关各国不应蓄意允许他人利用其领土使用信通技术实施国际不法行为的建议，哥伦比亚通过数字安全委员会预防和应对全国所有类别和类型的网络安全事件。该委员会的成员包括各国家网络安全实体，如哥伦比亚计算机应急小组、联合网络指挥部、网络警察中心和政府的计算机安全事件响应小组。

哥伦比亚寻求在国际一级开展合作，促进信息交流、互助、起诉使用信通技术从事恐怖主义和犯罪行为以及采取其他合作措施应对威胁。

在这方面，国家经济和社会政策委员会正在制订的关于数字信任和安全的新文件规定建立和实施网络信息交流系统，旨在促进传播在国家和国际两级数字环境中互动的各利益攸关方间达成折衷的各项指标。该系统将与单一的数字安全事件中央登记处保持一致。

总检察长办公室将根据双边和多边协议利用国际合作渠道。然而，需要建立一个安全的技术渠道或网络服务，使其能够直接从互联网服务提供商咨询和获取信息，其中大多数信息是私密的，以便及时发送、接收、交换、考虑和回应司法协助请求。

在目前的机制下，反应时间很慢，阻碍刑事诉讼。当收到回应时，调查通常处于不可行的阶段，即在诉讼程序中使用结果是不可行的。

国家情报局一直在与某些国家的情报机构协调，制订及时交换行动信息的程序，并要求提供与需要调查或确认的具体事件有关的补充信息。

这种协调涉及与在事件或活动历史必须相关的网络空间确定的事件或趋势有关的补充信息，以便监测在网络空间活动的敌对行为体。

哥伦比亚宪法法院发布了一些判决，涉及以下建议：在确保安全使用信通技术方面，各国应遵守人权理事会关于在互联网上增进、保护和享有人权的第 20/8 和 26/13 号决议以及大会关于数字时代的隐私权的第 68/167 和 69/166 号决议，保证充分尊重人权，包括表达自由权。

例如，法院在 2019 年第 SU-420 号统一判决中裁定，在哥伦比亚，表达自由适用于互联网的方式与其他通信媒体是相同的，结论是社交网络不能确保成为诽谤的场所；虽然无法对发布内容进行事前许可或授权，但表达自由具有一定的优先权地位并不意味着没有限制；因此，行使这项权利的人必须承担对第三方产生任何影响的后果。

通信监管委员会方面发布了 2017 年第 5111 号决定，其中确立了通信服务用户权利保护计划，修订了 2016 年第 5050 号决定第一章第二部分，并提出其他规定。根据通信服务用户权利保护计划，网络和电信服务提供商必须使用适当的技术工具，以防止其网络中的欺诈行为，并定期核实这些机制的有效性。如用户提交与欺诈指控案件相关的请求、投诉、索赔或上诉，提供商必须进行相关调查。

为了确定促进数字安全和能力建设所需的法律和监管改革，新的数字信任和安全政策规定进行评估，以确定哪些文书需要在以下领域进行调整：(a) 信通技术安全；(b) 保护和捍卫隐私权、表达自由等网上人权；(c) 负责任地报告脆弱性；(d) 数据保护；(e) 保护消费者；(f) 风险和事件管理；(g) 事故响应中心或其他相关实体；(h) 设立部门计算机安全事件响应小组。这项评估将顾及各利益攸关方，并确定如何进行必要的调整。

根据有关各国应采取适当措施保护本国关键基础设施免受信通技术威胁的建议，哥伦比亚正寻求通过与各相关利益攸关方协调，为信通技术部门制订一项关键基础设施安全和防御计划，为该部门各组织提供一般性指导方针。该文件将是朝着努力加强和协调保护此类基础设施迈出的第一步。

哥伦比亚将参与国际合作，并回应其他国家就减轻恶意信通技术活动提出的要求。例如，哥伦比亚于 2020 年 3 月 16 日加入了《网络犯罪公约》。哥伦比亚采取步骤确保供应链的完整性，以便最终用户能够对信通技术产品的安全抱有信心。

关于负责任地报告信通技术脆弱性，并分享关于这些脆弱性的现有补救办法的相关资料，以限制并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，新的数字信任和安全政策规定制订程序，以促进负责任地报告国家实体的信息系统和技术基础设施中的脆弱性，以便相关实体能够补救这些脆弱性。

此外，国家政府还通过国家经济和社会政策委员会 2016 年第 3854 号文件发布关于成立计算机应急小组和网络安全事件响应小组的准则。

自愿建立信任措施

哥伦比亚坚定致力于继续制订和采取有关增强网络空间信心和安全的措施；并通过美洲组织在区域一级开展相关工作。

2017 年 4 月，加拿大、智利、哥伦比亚、墨西哥和美国牵头通过关于在美洲组织美洲反恐怖主义委员会设立网络空间合作与建立信任措施工作组的决议。2018 年 2 月，哥伦比亚当选为工作组主席。2019 年 4 月在智利举行的工作组第二次会议上，智利接替哥伦比亚担任主席。

美洲组织在网络安全领域采取的建立信任措施如下：

1. 提供有关国家网络安全政策的资料，如国家战略、白皮书、法律框架和各成员国认为相关的其他文件；

2. 确定在政策层面能够讨论半球网络威胁影响的国家联络点；

3. 如没有联络点，在外交部内指定联络点，以便促进网络安全和网络空间方面的国际合作与对话工作；

4. 通过为公私营部门官员举办网络外交讨论会、会议、讲习班等活动，发展和加强能力建设；

5. 促进将与网络安全和网络空间有关的主题纳入外交部和其他政府机构的外交官和官员的培训课程；

6. 通过设立工作组、其他对话机制和各国签署协议，促进在网络外交、网络安全和网络空间方面的合作和交流最佳做法。

特别是与网络外交相关的建立信任措施是通过美洲组织作出的重要贡献。

可以通过网络外交找到应对网络安全挑战的方法。这不仅需要促进各国积极参与关于网络安全的国际辩论，这一目标反过来又涉及向外交官员提供相关培训，而且还需要确保专家积极参与多边论坛。

应考虑促进有广泛参与的定期机构对话，扩大和支持计算机应急小组和网络安全事件响应小组之间合作的做法。

关于拟议建立一份细清的联络点详单，应在不同层面指定联络点，例如，在政治和外交层面指定一个联络点，在技术层面指定其他联络点(决策者、总检察长办公室、计算机应急小组等)。

必须确定由谁来管理资料并确保资料更新。应考虑制订一项规程，规范对包括数据库在内的资料进行明确和公开的管理。

关于在技术和政策层面确定国家联络点以处理严重的信通技术事件，信息和通信技术部已明确确定负责处理数字安全各个层面的个人。可以与有需要的任何机构共享相关数据

信息和通信技术部还有一个名录，其中载有国家实体的首席信息技术官和首席信息安全官以及各利益攸关方的联络信息，后者各利益攸关方参与了有关数字安全准则的讨论，并参与了政府计算机安全事件响应小组在事件管理各阶段的协调活动。

关于发展和支持双边、区域、次区域和多边磋商的机制和进程，以加强国家间建立信任，减少信通技术事件可能引起的误解、升级和冲突的风险，哥伦比亚将积极参加各种国际论坛，

特别是参加联合国(在纽约、维也纳和日内瓦)举行的辩论，以及主要在美洲组织框架内举行的区域机制和活动。

在拉美太平洋联盟数字议程小组方面，在美洲的美洲组织网络安全事件响应小组网络的支持下，哥伦比亚将参加拉美太平洋联盟成员国间网络威胁信息交流项目。在这方面，成员国的网络安全事件响应小组间的信息交流技术平台自 2020 年 1 月 23 日开始运行。哥伦比亚国家节点由哥伦比亚计算机应急小组运作。

在双边层面，哥伦比亚和智利两国外长于 2019 年 3 月 21 日就网络空间、网络安全、网络防御、网络犯罪和网络情报签署了谅解备忘录。哥伦比亚的参与实体包括总统经济事务和数字转型问题咨询办公室、信息和通信技术部、国防部、国家警察的哥伦比亚网络安全能力中心、国家情报局、总检察长办公室、司法部和外交部。

2020 年 4 月 15 日，哥伦比亚和秘鲁两国政府专家以虚拟形式交流数字安全领域的经验。双方就国家政策和战略进行信息交流，并就今后处理与信通技术有关的安全事件的支助活动建立一个沟通渠道。

哥伦比亚还参加美洲组织和思科公司倡导的网络安全创新理事会，作为该区域公私部门主要领导人、民间社会和学术界在促进创新、提高认识和传播与网络安全有关的最佳做法方面进行合作的论坛。这些论坛是对落实网络空间建立信任措施的重要贡献，还可以支持在国家和国际两级实施更有效的数字安全政策。

有关网络安全事项的国际请求一般通过外交部预防犯罪协调办公室提出。

关于加强合作，包括在恶意使用信通技术和提供调查协助方面建立信息交流协调中心，必须注意到各国政府当局和实体正在努力拟订国家事件管理规程，以便促进及早协调努力，处理可能威胁到经济和社会秩序或国家安全的网络安全事件。这一规程的实施至关重要，因为它注重确定事件、检查事实、考虑威胁和确定适当的遏制或纠正方法。

总检察长办公室内设有 3 个负责处理与网络犯罪有关问题的小组，在发现恶意使用信通技术时请求司法协助所引起的调查中提供专家支持和协助。

这些小组如下：(a) 打击有组织犯罪检察官办公室；(b) 公民安全问题检察官办公室；(c) 技术调查局。除了在调查中提供协助外，这些专家组还在总检察长办公室内推广与网络犯罪和数字证据有关的新趋势和最佳做法。

总检察长办公室国际事务局在各专门检察官和该办公室各网络犯罪小组的支持下开展与网络犯罪有关的调查。

美国司法部就与司法协助请求有关的问题提供了培训。在美国，请求当局必须符合某些证据基准和标准，才能查阅所存储的电子通信。具体地说，请求当局必须提供按时间顺序排列的明确事实，表明有合理理由相信电子记录对正在进行的调查是相关和重要的。他们还必须证明有合理和可靠的事实，而不仅仅是推定的事实，其中表明有人犯了罪，且电子邮件或社交网络账户包含与正在调查的罪行相关的信息。

同样，在国际合作框架内，国家情报局应各国的直接请求进行双向协调调查和查询。

信息和通信技术安全和能力建设方面的国际合作与援助

对哥伦比亚来说，能力建设是技术问题方面一个关键问题。

数字安全风险管理是国家、私营部门和学术界可以共同努力的领域，应考虑到为此目的而设立的合作和国际援助机制。

必须让各不同利益相关方参与网络安全问题的分析，他们在确定和采取预防性安全措施以及事件响应和应急措施方面所提供的协助非常宝贵。

各国必须首先确定需要加强能力的领域。为此，各国可以采用国际上开发的标准化成熟度模型作为依据。

各国应在此基础上制订计划，其中包括业务、行政、人力和科学能力以及有形和技术基础设施的发展，这些计划也是为负责网络安全和关键部门的机构和实体制订的。同样，作为加强能力的一部分，必须定期更新国家关键网络基础设施目录和相关保护计划及其相互之间的协调机制。

由于这是关乎我们所有人的问题，因此有必要致力于创建与数字安全有关的教育内容，以便将其纳入各级教育的学术课程和非正规课程。

鉴于在应对事件和处理短期网络安全问题方面建立了互助程序，包括快速援助程序，哥伦比亚已建立国家事件应对模式，其中确定全国各地发生的事件的管理规程，因此，网络实体可根据其权力和职能采取行动。

具体地说，政府为加强国家实体的数字生态系统而设立了计算机安全事件响应小组，向各实体免费提供服务。服务目录包含三种类型的服务：积极主动式、

反应式和安全管理。其中包括网站可用性监测、脆弱性分析、安全事件监测、对事件管理和应对的支持以及提高对事件管理的认识。

政府的计算机安全事件响应小组与其他国家网络实体(哥伦比亚计算机应急小组、联合网络指挥部和网络警察中心)协调，以管理国家实体的事件，并通过数字安全委员会参与制订战略，以解决影响普通公民和国家数字安全的问题。

为了促进跨界合作应对跨越国界的关键基础设施脆弱性，总检察长办公室还与该区域各国协调战略，以便在知道关键基础设施可能受到攻击或遭到破坏的国家调查中及时简化信息交流。

信息和通信技术部通过政府的计算机安全事件响应小组与计算机应急小组和网络警察中心进行协调，通过各种国际来源核实信息，从而得以在必要时加快采取缓解和调查行动。

关于制订与信通技术安全有关的能力建设举措可持续性战略，国家经济和社会政策委员会 2016 年第 3711 和 3854 号文件所载的各种公共政策文书载有能力建设方面的准则和建议。此外，信息和通信技术部和国防部等还宣布加强应对能力的其他行政和法律措施。

例如，在这方面，哥伦比亚政府与美洲组织缔结了合作协定，通过这些协定，双方合力开展技术合作，通过以下两个基本领域的举措，支持更新数字安全准则，并加强网络风险管理的技术能力和技能：(a) 政策制订和传播；(b) 能力建设。

总检察长办公室通过国际事务局遵循各多边组织颁布的加强网络空间安全的指导方针和建议，旨在确保妥善管理网络犯罪调查，从而尽可能减少有罪不罚现象。

为了促进国家网络能力，国家情报局决定为情报部门设立计算机安全事件响应小组，作为处理该部门活动和事件的协调机制，促进有关活动和事件技术信息的传播，并对网络事件进行调查。

哥伦比亚还优先考虑提高对信通技术安全的认识以及国家计划和预算中的能力建设，目的是在发展和援助规划中给予安全应有的重视。在这方面，除了已经提出的数字安全公共政策之外，还制订提高认识方案，目的是就信通技术安全对各机构和公民进行教育和通报相关情况。

信息和通信技术部努力制订一项以能力建设为重点的方案，并通过订立合作协定，举办信息安全和信息技术管理方面的课程并颁发文凭和证书，让国家和地方各级政府机构的 1 134 名公务员从中受益。

其中值得注意的是“让我们谈谈数字政府”方案，各公共实体的 250 多名信息技术官员和安全人员通过该方案参加一个关于安全和数字风险管理能力建设的小组讨论。

有 40 名信息技术领导参加了在佩雷拉市举行的公职人员网络挑战赛。他们还参加一个网络安全挑战赛，参与应对网上可能出现的挑战和情况。这次活动是由美洲组织在一家跨国网络安全公司 Trend Micro 的支持下举办的。

在“加强数字安全，区域更美好”讲习班方面，包括公共实体方面的信息技术领导和安全人员在内的 1 400 多名官员参加了在哥伦比亚 24 个城市举行的 25 次会议。

区域培训在美洲组织的支持下得到加强。例如，荷兰王国资助的题为“海牙进程：国际安全行动与网络空间”的课程已举办多次。2019 年，上述课程在哥伦比亚举办；哥伦比亚官员接受了培训，来自拉丁美洲和加勒比地区负责网络安全事务的代表也参加了培训。课程专题包括所有涉及网络行动学术背景的主权、管辖权、尽职原则、使用武力、国际人权法、海洋法、和平协议及其他相关专题。

关于法医技术以及为应对将信通技术用于恐怖主义或犯罪目的而采取的合作措施方面的能力建设，哥伦比亚政府主办了由美洲国家组织、反恐怖主义委员会执行局、联合国毒品和犯罪问题办公室、国际检察官协会、国家数字安全协调机制以及哥伦比亚信息和通信技术部组织的拉丁美洲区域讲习班，内容涉及从私营通信服务提供商获取电子证据，作为在跨界调查中防止恐怖主义和有组织犯罪的一部分。参加讲习班的有来自拉丁美洲 13 个国家的代表(刑事侦查警察和其他政府机构的官员)，他们接受了以下方面的培训：获取跨界数字证据事项；美国、加拿大和欧盟的立法执行情况；紧急披露请求；编写司法协助请求等问题，以加强在防止恐怖主义和有组织犯罪方面的国际合作。

在过去 3 年中，总检察长办公室批准从计算机犯罪小组和计算机取证小组借调刑事侦查人员，参加美洲组织和拉丁美洲和加勒比因特网地址注册机构等组织的重要讨论会和培训班，并与熟悉和牵头涉及技术(作为犯罪手段或目的)的调查的检察官合作。

此外，还在私营实体和当地大学的支持下举办各种关于打击网络犯罪和改进技术的培训课程，如数字证据分析硬件和软件方面的规程和培训等，以便将案件联系起来并发现犯罪模式。

国家情报局计划与情报部门的计算机安全事件响应小组协调，在穿透测试和脆弱性分析、数字信息的取证分析和恢复、恶意软件和网络制品分析、应用程序分析、开放源码实验室和网络现象研究方面进行能力建设。

针对关于制订能力建设区域办法的建议，铭记文化、地域、政治、经济或社会性质的具体问题，以便促进采取适合各自具体情况的办法，信息和通信技术部通过数字政府局安全和隐私问题小组，一直在实施信息安全和隐私模式，以便汇集使国家和地方两级的实体能够应对网络威胁的各种工具，建立一种安全文化，使人们能够在应对影响跨国组织的网络威胁时提高对局势的了解。

此外，负责犯罪政策的当局一直在制订一项涵盖各种不同形式犯罪问题的国家计划。

国家情报局正在努力建设国家情报界在安全交换信息方面的能力。在这方面，正与总统府合作署协调制订一个为加勒比国家提供保护和良好做法管理方面的培训和能力建设的项目。

如前所述，为建设信通技术安全能力着想，哥伦比亚参加了双边和多边合作倡议，以期改善提供有效互助以应对信通技术事件的环境。

信息和通信技术部还一直在制订与国际一级的安全公司和网络实体合作的战略，以便在战略、战术和行动层面共享威胁情报。

国际法对各国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》以及包括国际人权法和国际人道主义法，既适用于“虚拟”世界，也适用于“实体”世界。

哥伦比亚赞同时任秘书长在 2015 年政府专家组报告序言中的表述：“只有通过国际合作，才能实现网络空间的稳定与安全，而国际法和《联合国宪章》原则必须成为这一合作的基石。”

因此，哥伦比亚认为，国际法的一般概念可适用于网络空间，但需要根据虚拟业务性质作出调整。

考虑到对网络空间国际法相关问题的各种可能解释，这并不妨碍编写关于在网络空间适用国际公法的指南或手册。

在这方面，与《网络犯罪公约》有关的做法可能是非常有益的，因为该公约有指导说明指导其条款的执行，并使其与技术的发展保持一致。这被认为是可以效仿的好做法。

考虑到大会建议并欢迎载于政府专家组报告中的一套负责任国家行为的国际规则、规范和原则，哥伦比亚的当务之急必须是加快执行这些规则、规范和原则。哥伦比亚认为目前不需要一份具有约束力的文书。

还应强调，哥伦比亚遵守承诺和既定保障措施。

概念

鉴于信息和传播技术应用的特殊性和新颖性，应当继续在多边方案的背景下讨论概念的发展，这被认为是在法律、技术和政治层面上更深入地理解与国际和平与安全有关的概念所必需的。

这些讨论对于调整国际法律框架以应对网络空间挑战，并对于能够就如何在这一虚拟空间中适用国际法达成共识，是至关重要的。在这方面，哥伦比亚同意政府专家组在其 2015 年报告中提出的结论，并准备在联合国与其他代表团进行更详细的讨论。

这是确保适当使用信通技术的唯一途径，而信通技术对于应对国际社会目前面临的挑战以及防止以违背《联合国宪章》宗旨和原则、包括充分维护国际和平与安全的方式使用信通技术至关重要。

破坏性使用新技术提供服务正推动信息社会中建立新型的关系，而这种关系的基础是信息的安全处理和个人数据的特殊保护，从而鼓励促进技术进步的好处及其对社会和经济发展的贡献。

因此，必须加强各国政府的领导，以便根据应对数字安全风险的最佳国际做法建立新的愿景，同时考虑到支持各国负责任行为的原则，促进各国参与国际数字安全讨论论坛，并鼓励各国以透明和可预测的方式对待同行，从而减少数字安全问题中的误解、升级和冲突的风险。

最后，实施负责任利用数字环境的战略和措施有助于通过在尊重的基础上创造有利于数字共存的条件开展建设和平，包括支持表达自由和适当使用网络语言，以期最大限度地发挥信通技术的好处，支持调整适应数字未来。

丹麦

[原件：英文]
[2020 年 5 月 29 日]

像世界其他地方一样，丹麦越来越多地通过互联网连接起来。数字解决方案是日常生活的一部分，有助于推动经济增长。作为世界上最数字化的国家之一，丹麦必须推进一个全球、开放、稳定、和平和安全的网络空间，在这个空间里，人权和基本自由以及法治得到充分应用。

在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

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，从而增强我们的复原力。《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安全。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。此外，还将《欧盟网络与信息安全指令》完全转入丹麦法律中。

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建立了一个论坛，重点是分享它们在信息和网络安全方面的工作经验。数字化局和丹麦安全和情报局也参加了论坛。

为了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。网络学院在 2019 年有 15 名毕业生，现在受雇于该中心的情况中心。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。例如，2019 年，网络安全中心与哥本哈根设计和技术学院、奥尔堡大学、丹麦南方大学、哥本哈根商学院和丹麦技术大学合作，举办了第一个网络安全暑期学校。

2019 年，成立了一个公私网络安全理事会，以鉴定国家当局和私营部门的工作，加强数字民主，并提高对数字化和新技术带来的威胁和机遇的认识。

根据《2018-2021 年丹麦国家网络和信息安全战略》，丹麦还通过在布鲁塞尔派驻网络专员加强了其国际网络参与；在外交部任命一名国际网络协调员；任命一名网络安全顾问到硅谷的技术大使办公室；并加入了塔林的北约合作网络防御英才中心。这使得丹麦得以加强在联合国、欧盟、北约和欧安组织等多国网络论坛上的参与。丹麦还是网络与信息安全合作小组的现任成员，也是欧盟网络安全局的成员。通过参与这些论坛，丹麦一贯促进全球、开放、稳定、和平和安全的网络空间。

此外，丹麦在欧盟 5G 工具箱的开发中发挥了积极作用。该工具箱旨在基于一套共同的措施，确定欧洲对 5G 的协调方法，旨在减轻 5G 网络的主要网络安全风险。

丹麦强调，正如国际社会已经表明的那样，正如政府专家组 2013 年和 2015 年的协商一致报告所证明的那样，网络空间牢牢植根于现有国际法。现有国际法，包括整个《联合国宪章》、国际人道主义法和国际人权法，适用于国家在网络空间的行为。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准则十分重要，是对具有约束力的国际法的补充。

尽管我们共同努力，国家和非国家行为者进行恶意网络活动的能力和意愿仍在增加。这应该是全球关注的问题。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。

政府专家组报告中提到的概念内容

现有和新出现的威胁

如前所述，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。

丹麦对国家和非国家行为体在网络空间的恶意活动上升以及利用网络空间侵犯知识产权表示关切。这些行为威胁到经济增长和国际社会的稳定。

对开放、安全、稳定、可进入与和平的网络空间的需求，从未像 COVID-19 大流行期间那样突显出来。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者会利用任何机会——即使是全球大流行病。其中包括干扰抗击大流行病必不可少的医院等关键基础设

施。这是不可接受的，必须受到所有国家的强烈谴责。此外，各国必须进行尽职调查，并迅速而坚定地采取行动，打击源自其领土的恶意信通技术活动。

国际法如何适用于信通技术的使用

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。

国际社会明确表示，网络空间牢牢植根于现行国际法，政府专家组 2013 年和 2015 年的协商一致报告也已证实这一点。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。

主权、不干涉和禁止使用武力是国际法的基本原则，各国违反这些原则将构成国际不法行为，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——以及其他国际和区域倡议——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 年以来的国家军事网络空间行动联合理论中，该理论指导军方领导人在开展网络空间行动时应考虑遵守国际法。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。

现行国际法——并辅之以 2015 年政府专家组报告中所阐明的 11 项关于负责任国家行为的自愿不具约束力的准则——为各国提供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。

由于已经有一个关于网络问题的国际法律框架，丹麦既不呼吁也不认为有必要就网络问题制定新的国际法律文书。但在加强对该框架如何适用的共同理解方面仍有空间。希望本政府专家组和不限成员名额工作组的工作和建议将有助于澄清问题，从而促进亟需的国家遵约。最终促进提高可预测性并降低升级风险。

负责任国家行为准则、规则和原则

丹麦与欧盟及其成员国一道，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准则和建立信任措施。

作为对具有约束力的国际法的补充，政府专家组 2010、2013 和 2015 年连续发表的报告中所阐明的负责任国家行为准则、规则和原则具有巨大价值。丹麦将继续以国际法为指导，并遵守这些自愿准则、规则和原则。应通过围绕最佳做法加强合作和提高透明度，进一步执行这些准则。

法国

[原件：法文]
[2020 年 5 月 29 日]

法国欢迎有机会对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 74/28 号决议作出回应，并愿提供以下信息。

1. 对网络安全问题的总体评估

法国首先愿重申其不使用“信息安全”一词，而是更倾向于使用“信息系统安全”或“网络安全”的说法。法国认为信息本身并非潜在脆弱性的来源。“网络安全”一词更为准确，因为这个词是指信息系统面对源于网络空间的事件时的抵御能力，这些事件可能导致存储、处理或传输的数据以及这些系统提供或接通的相关服务在可用性、完整性或机密性方面受到威胁。

法国认为，数字空间必须继续作为自由、交流和增长的空间而存在，促进我们社会的繁荣和进步。过去 30 年来，法国一直在推动这种开放、安全、稳定、可访问、和平的网络空间，这样的网络空间蕴藏着经济、政治和社会机遇，但如今却因新型恶意做法的演变而受到威胁。数字空间的特殊性(包括相对匿名性、获取恶意工具的成本和难度较低、脆弱性的存在以及某些工具的扩散)使一些行为体得以从事间谍活动、非法贩运、扰乱稳定和破坏活动。虽然一些低力度威胁并非国家安全问题，而是某种形式的犯罪，但对国家信息系统、关键基础设施或企业使用这些工具可能会造成严重后果。

目前，与网络安全有关的问题是支配国际关系的权力战略和权力关系的组成部分；网络安全既是优先事项，又是重要政治问题。法国认为，各国必须保持在网络空间和其他地方合法使用暴力的垄断地位。然而，数字技术作为一种新的冲突工具和领域的传播，给私营部门、特别是一些系统行为体带来维护国际和平与安全的关键作用和前所未有的责任。

2. 法国在国家和国际两级在网络安全领域做出的努力，以及法国对政府专家组报告中提到的概念实质的看法

多年来，法国一直在奉行维护、发展和促进开放、安全、稳定、无障碍、和平的网络空间的政策和积极外交，并应对国际稳定与安全面临的威胁。

法国参加的前五个从国际安全角度看信息和电信领域的发展政府专家组的工作，促使在共同原则的定义和对网络空间的集体理解方面取得进展，特别是在国际合作、标准和国际法的应用等领域取得进展。

法国在国际合作、能力建设以及促进和发展建立信任措施方面采取的行动

法国在双边、欧洲和国际三级促进在网络安全问题上的国际合作。

为了加强欧洲联盟的网络抵御力，法国正在帮助制定用于预防和解决事件的自愿合作框架。该框架尤其以制定用于伙伴间开展合作的共同业务规范和程序为基础；这些标准和程序是通过泛欧洲演习进行测试的。法国还参与开发了“网络工具箱”；该工具箱根据与网络事件有关的预防、合作、稳定和应对措施、特别是限制性措施，为欧洲联合采取外交手段应对网络攻击提供了一个框架。法国还在参与发展“旋风”(CyCLONe)网络，以便在发生网络危机时组织欧洲国家网络安全机构之间的业务合作，并参加联合演习，为应对网络危机做准备，以补充这些机构的计算机应急小组之间的合作。

在北大西洋公约组织内部，在法国倡议下，盟国在 2016 年 6 月华沙峰会上通过了一项关于网络防御的承诺，即《网络防御承诺》，每个成员国在该文件中承诺将适当份额的资源用于加强其网络防御能力，从而改善联盟的整体安全。

法国积极参与欧洲安全与合作组织(欧安组织)的网络安全问题非正式工作组，继续推动执行欧安组织在该领域制定的 16 项建立信任措施。具体而言，法国与其他参与国一道，正在试行关于确保关键基础设施安全的建立信任措施 15。

法国还认为，与网络安全有关的许多挑战应通过多利益攸关方办法解决，以便考虑到非国家行为体的作用和具体责任。在 2018 年发布的《巴黎网络空间信任与安全呼吁》中，法国强调必须加强多利益攸关方办法。法国认为，民间社会、学术界、私营部门和技术界拥有对制定相关网络安全政策非常有用的专门知识和资源。2018 年 11 月 12 日，共和国总统在联合国教育、科学及文化组织举行的因特网治理论坛上提交了《巴黎呼吁》，[2] 证明法国在推动安全、稳定和开放的网络空间方面发挥积极作用。《巴黎呼吁》作为世界上最大的多利益攸关方网络安全倡议，现在得到了 78 个国家和 1 000 多个非国家实体的支持。该文件旨在促进规范数字空间的某些基本原则，包括在网络空间中适用国际法和人权法、负责任国家行为、国家对合法暴力的垄断权以及承认私人行为体的特定责任。

法国还支持全球网络空间稳定问题委员会制定标准和政策提案，以加强国际安全与稳定，并指导网络空间中负责任国家行为。载有该委员会结论的报告提交给了第二届巴黎和平论坛。

法国正在努力确保二十国集团按照《巴黎呼吁》，解决数字经济中的竞争和新监管方法以及数字安全的治理等基本问题。

法国还在经济合作与发展组织(经合组织)内部参与相关工作。它目前担任经合组织数字经济中的安全和隐私问题工作组主席，并希望设法解决私营行为体的责任、保证产品和服务的安全以及负责任的漏洞披露等问题。

[2] 可查阅：https://pariscall.international/en。

在能力建设领域，由于各国网络和社会高度连通，法国认为，只有在每个国家都有足够能力保障本国信息系统安全的情况下，才能确保所有人都享有网络安全。因此，它正在以双边或多边方式加强其合作伙伴的网络安全能力。此类改进合作的努力有益于所有各方，使我们能够通过与同行接触和向他们学习做到与时俱进，促进有关利益攸关方彼此增进知识和专业技能并建立信任。近年来，法国还向伙伴国家的国内安全部队派遣了网络安全方面的国际技术专家。例如，法国正在与塞内加尔合作，继续开展达喀尔国家网络安全学校的各项活动；该学校面向整个区域，于 2018 年底启用。该项目的宗旨是优先为西非的网络安全专业人员和高级官员提供可调整的短期培训课程。

负责任行为标准的定义：一项重大成就

法国通过其国家学说、治理安排和法律建立了一套机制，以实行政府专家组报告、特别是 2015 年报告(A/70/174)中建议的行为规范。下文提供的信息旨在说明法国设法实施这些规范的方式，但这些方式不是详尽无遗的。

规范(a)：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，加强信息和通信技术(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。

法国针对这一规范采取了一系列措施，特别是为此巩固了以防御、预防、复原力与合作为重点的国家网络安全战略。在 2018 年 2 月发布的我们对网络防御的战略评估中，[3] 确立了危机管理理论，澄清了我们的目标。法国的模式得到了确认，即对负责进攻能力的机构和执行防御任务的机构进行区分，并强烈肯定了发展对网络空间的信心及其稳定这一外交目标。

法国还在与各合作伙伴就网络安全问题建立双边战略对话。上文提到，它还积极参加许多区域和国际合作与协调论坛。

法国还认识到，它有能力在严格遵守国内法和国际法的情况下，在网络空间开展防御性和进攻性军事行动，以保障国家主权。为了确保透明度和一致性，它在 2019 年发布了几份文件，其中包括与进攻性网络战相关的军事理论，以及一份关于适用于网络空间军事行动的国际法白皮书，从而使尽可能多的人能够了解其理论。这种澄清和分享国家愿景的愿望应该能够限制误解和不确定性，从而有助于巩固对网络空间的信心及其透明度。法国鼓励所有其他国家也这样做。

规范(b)：一旦发生信通技术事件，各国应考虑所有相关信息，包括所发生事件的大背景，信通技术环境中归责方面的困难，以及后果的性质和范围。

法国制定了以下在发生与技术有关的事件时可实行的危机管理程序及国家机构和政策：

[3]可查阅：www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf。

- 一个部际危机小组，在发生重大危机时加以部署；
- 一个每月开会的网络危机协调中心，由技术或业务层和高级别的部际战略层组成，其成员在更广泛的背景下分析网络事件，评估其后果，并可能考虑归责问题。对法国来说，确定攻击的责任方并决定公开归责结果，是主权权力。

法国已经制定评估事件的方法，包括采用严重程度表来帮助决策者进行分析和采取行动。在确定事件的严重程度时，法国除其他外，会考虑其对以下方面的影响：

- 国家的利益和主权，以及民主
- 国内安全和民事安全
- 人和环境
- 经济

还可以考虑其他标准，诸如意图、危险性、归责、规模和是否重复发生。

规范(c)：各国不应蓄意允许他人利用其领土使用信通技术实施国际不法行为。

为确保其领土不被用来实施恶意行为，法国：

- 已经要求至关重要的运营商，即国家关键基础设施运营商(见第 2013-1168 号法)和基本服务运营商(见第 2018-133 号法)加强其信息和通信系统的安全；
- 《刑法》第 323-1 条已经将未经授权侵入第三方信息安全系统的行为定为犯罪行为；
- 已经通过第 2018-607 号法，加强国家网络安全局查明对关键基础设施运营商产生影响的网络事件的能力；
- 已经通过第 2016-1321 号法鼓励负责任地披露漏洞；根据该法，向国家网络安全局通报数字产品或服务漏洞的个人受到保护，不会受到法律诉讼。

规范(d)：各国应考虑如何最好地合作交流信息，相互协助，起诉使用信通技术从事的恐怖主义和犯罪行为，并采取其他合作措施应对此类威胁。各国可能需要考虑是否需要在这方面制定新的措施。

除了上文提供的有关合作的信息外，法国还制定了一系列措施，以改善与其伙伴的合作，以防止利用信息技术从事犯罪和恐怖主义行为，特别是为此加入了《网络犯罪公约》(《布达佩斯公约》)和支持消除网上恐怖主义和暴力极端主义内容的克赖斯特彻奇呼吁。

在技术层面，国家网络安全局继续与许多国家的对口单位建立伙伴关系，鼓励分享关键数据，诸如关于产品和服务的漏洞或故障的信息。此外，国家网络安全局

的政府计算机应急小组还积极参与若干多边网络(事件应对和安全小组论坛、欧洲计算机安全事件应对小组工作队、欧洲政府计算机应急小组和欧洲联盟计算机安全事件应对小组网络)，通过这些网络与世界各地的计算机应急小组保持联系。

规范(e)：各国应在确保安全使用信通技术方面遵守人权理事会关于在互联网上增进、保护和享有人权的第 20/8 号和第 26/13 号决议，以及大会关于数字时代的隐私权的第 68/167 号和第 69/166 号决议，保证充分尊重人权，包括表达自由权。

法国极为重视在互联网上必须尊重和增进人权以及个人在线上线下必须享有同等权利的原则。自 1978 年以来，国家信息技术与自由问题委员会一直是负责确保尊重人权和基本自由、特别是隐私权和表达自由的权力机构。

法国还参与通过相关欧洲法规，在考虑到竞争力需求和数字技术潜力的同时，继续保护成员国的公民和企业(包括隐私权和个人数据保护、保护关键基础设施以及打击网上恐怖主义内容)。在 2016 年通过欧洲议会和理事会关于在处理个人数据和此类数据的自由流动方面保护自然人的 2016 年 4 月 27 日(EU)第 2016/679 号条例，通过欧洲议会和理事会关于在整个欧盟范围内对网络和信息系统采取高度共同安全措施的 2016 年 7 月 6 日(EU)第 2016/1148 号指令，以及支持法国加强欧洲联盟网络安全署的管辖权过程中，这一愿望得到了明确体现。最后，法国正在努力确保欧洲联盟通过其产业政策支持先进的研发能力，以促进部署可靠且经过独立评估的数字安全技术和服务。法国还积极参与起草欧洲联盟关于线上和线下表达自由的人权准则，该准则于 2014 年 5 月 12 日获得理事会通过。

在欧洲委员会，法国支持采取行动保护互联网上的人权。例如，法国支持于 2014 年 4 月通过欧洲委员会的部长委员会起草的《互联网用户人权指南》，其中特别强调表达自由、获取信息、结社自由、隐私权、保护个人数据和防止网络犯罪；这些权利和自由在线上和线下同样适用。

在联合国，法国支持通过人权理事会关于促进保护和享受互联网人权的所有决议，以及大会关于数字时代的隐私权的第 68/167 号决议。

在 2018 年 11 月举行的第二届巴黎和平论坛上，法国总统埃马纽埃尔·马克龙及其他 11 位国家元首和政府首脑还宣布，在非政府组织“无国界记者组织”已经开展的工作的基础上，发起一项关于信息与民主的政府间倡议。该倡议现在由法国和德国发起的多边主义联盟主持。

规范(f)：一国不应违反国际法规定的义务，从事或故意支持蓄意破坏关键基础设施或以其他方式损害为公众提供服务的关键基础设施的利用和运行的信通技术活动。

本着这一规范的精神，如上所述，法国在《刑法》第 323-1 条中将未经授权侵入第三方自动数据处理系统的行为定为犯罪行为。

法国还在其理论的公开部分、包括其 2019 年关于适用于网络空间行动的国际法的白皮书中明确规定，国际人道主义法完全适用于在武装冲突背景下开展的以及与武装冲突有关的网络行动，下文将结合国际法进行更详细的讨论。

规范(g)：各国应考虑到大会关于创建全球网络安全文化及保护重要的信息基础设施的第 58/199 号决议和其他相关决议，采取适当措施，保护本国关键基础设施免受信通技术的威胁。

如上所述，法国制定了保护关键基础设施的监管框架，要求至关重要的运营商加强其运营的关键信息系统(即所谓至关重要的信息系统)的安全(2013 年 12 月 18 日第 2013-1168 号法)，并加强国家网络安全局查明事件的权限和能力。至关重要的运营商还必须加强其安全措施，并使用国家网络安全局核准的检测系统。法国鼓励开展公私合作，以发展关键基础设施保护，并确定有效、适当的框架。

规范(h)：各国应对关键基础设施遭到恶意使用信通技术行为破坏的另一国提出的适当援助请求作出回应。各国还应回应另一国的适当请求，减轻源自其领土的针对该国关键基础设施的恶意信通技术活动，同时考虑到适当尊重主权。

例如，为了遵守这一规范，法国通过国家网络安全局的技术伙伴关系建立了一个基于信任的合作网络，该网络除其他外，使计算机应急小组之间能够通过常设联络点进行联系。

为了组织危机管理，法国还设立了一个常设的部际威胁分析、准备和协调机制，该机制的形式是网络危机协调中心。具体而言，该中心使各部门之间能够顺利交换信息，以改善国家协调并回应这些需求。

法国还根据《网络犯罪公约》建立了一个全天候的联络点网络，以便能够实施数据冻结。

在欧安组织，法国一直参与将根据常设理事会第 1106 号决定中的建立信任措施 8 设立的联络点名单投入运转，并支持各种努力，以确保每个国家根据常设理事会第 1202 号决定中的建立信任措施 13 建立适当的交流和信息渠道。

规范(i)：各国应采取合理步骤，确保供应链的完整性，以便最终用户能够对信通技术产品的安全抱有信心。各国应设法防止恶意信通技术工具及技术的扩散以及有害隐蔽功能的使用。

法国鼓励制定该行业的规范和标准，特别是通过《巴黎呼吁》予以鼓励。它还主要通过二十国集团的数字经济工作队以及经合组织，在各种论坛上促使启动有关这一主题的国际工作。

法国还在国家网络安全局领导下，推动使用第三方认证原则，以确保市场提供最高级别的安全。这一进程正由国家认证中心在国家网络安全局试行。法国还推动在欧洲联盟一级设立此类证书。

为了加强打击扩散恶意工具和技术的努力，法国还支持将侵入软件列入《关于常规武器和两用物品及技术出口控制的瓦森纳安排》的两用物品清单。

规范(j)：各国应鼓励负责任地报告信通技术的漏洞，分享关于这些漏洞的现有补救办法的相关资料，以限制并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。

如上所述，法国已采取各种步骤，允许负责任地披露计算机漏洞，并通过国家网络安全局开展了技术层面的合作，该机构定期与其对口单位及合作伙伴交流有关漏洞和可采用的解决方案的信息。

规范(k)：各国不应开展或蓄意支持损害另一国授权应急小组(有时称为计算机应急小组或网络安全事件应急小组)信息系统的活动。一国不应利用授权的应急小组从事恶意的国际活动。

1988 年 1 月 5 日关于计算机欺诈的第 88-19 号法(即所谓的《Godfrain 法》)，是法国第一部惩罚计算机犯罪和黑客行为的法律。该法将以欺诈方式进入或停留在全部或部分自动数据处理系统中的行为定为犯罪行为。

法国的治理模式将进攻能力与防御能力和任务区分开来，确保了这一原则得到尊重。政府计算机应急小组的任务包括协调和调查对网络事件的应对情况，不仅包括政府、而且也包括法律规定的关键基础设施和基本服务运营商的应对情况，为此帮助这些运营商建立必要的保护级别，检测网络和系统中的漏洞，必要时在合作伙伴的帮助下组织应对此类事件，并参加一个值得信赖的计算机安全事件应急小组网络。

包括《联合国宪章》在内的国际法适用于网络空间：政府专家组确认的另一项原则

法国认为，集体网络安全框架的出现只能以遵守国际法的规则为基础。因此，它认为现阶段不需要制定一项新的具有法律约束力的国际文书来专门应对网络安全挑战。现行国际法适用于网络空间，就像适用于其他领域一样，必须得到尊重。

正如政府专家组在其 2013 年报告中得出的结论，国际法原则和规则适用于各国在网络空间的行为。即使考虑到网络空间的具体特征，如匿名和私人行为体的作用，国际法也为负责任地控制国家在这种环境中的行为提供了必要的手段。

主权原则适用于网络空间。因此，法国根据其国际法义务，重申对其领土上或在其管辖下的信息系统、个人和网络活动行使主权。国家实体或在国家指挥或控制下行事的非国家行为体使用进攻性电子手段未经授权渗透法国系统或在法国领土上产生了效果，可构成对主权的侵犯。

各国可以采取的应对可能网络攻击的措施的范围，取决于攻击效果的严重程度。因此，网络行动可以理解为《联合国宪章》第二条第四款禁止的使用武力。是否越过了这一门槛并不取决于所使用的电子手段，而是取决于网络行动的效果。如果其效果与常规武器相似，网络行动就可构成使用武力。法国认为，如果一国或在一国控制或指示下行事的非国家行为体实施的重大网络攻击的范围或影响达到足够的门槛(如重大生命损失、重大物质损害、关键基础设施出现缺陷并有重大后果)，该攻击可构成《宪章》第五十一条规定的“武装侵略”，因此有正当理

由要求自卫。根据必要性和相称性的原则，自卫权可以通过常规或电子手段行使。把网络攻击定性为《宪章》第五十一条所列“武装侵略”是一项政治决定，应根据国际法确立的标准逐案作出。

法国还确认，国际人道主义法完全适用于在武装冲突背景下实施的以及与武装冲突有关的网络行动。进攻性的网络行动目前是与常规军事行动结合进行的。

尽管这些行动是非物质性质的，但仍受国际人道主义法地理适用范围的制约；换句话说，其效果限于国际武装冲突参与国的领土，或者在非国际武装冲突的情况下，限于发生敌对行动的领土。法国武装部队开展的网络战进攻行动必须遵守以下国际人道主义法原则：

- 区分民用资产和军事目标的原则。禁止不以特定军事目标为目标的网络攻击，也禁止使用不能以特定军事目标为目标的网络武器实施的网络攻击。某些数据虽然是无形的，但可能属于受国际人道主义法保护的平民资产。根据这一原则，必须对战斗人员或有组织武装团体的成员同平民加以区分。除非平民直接参与敌对行动以及除非在他们参与敌对行动期间，一般平民和单个平民不得成为攻击的目标。在武装冲突中，任何身为冲突一方的武装部队成员的网络战斗人员、参与针对另一方的网络攻击的有组织武装团体的任何成员或通过电子手段直接参与敌对行动的任何平民，都可能成为常规攻击或网络攻击的目标；

- 相称原则和预防原则。在此类行动中，必须时刻保持警惕，保护人员和平民资产免受敌对行动的影响。附带损害必须与预期的具体和直接军事优势相称。网络空间的相称原则要求考虑到武器的所有可预见的影响，此外还要考虑到这些影响是直接的(如对目标系统的损害或服务中断)还是间接的(如对受攻击系统控制的基础设施的影响，以及对受系统故障或破坏或数据更改和损坏影响的人的影响)，条件是这些影响与攻击有充分的因果联系。按照这一原则，也禁止使用在时间和空间方面无法控制的网络武器。

武装力量部 2019 年 9 月 9 日发表的关于适用于网络空间行动的国际法的报告以及同年发表的法国军事理论关于进攻性网络战的公开内容提供了这一信息。

法国认为，对于其基础设施涉嫌被恶意用于损害另一国利益的国家的义务，在国际一级达成共识至关重要。这里的目的是澄清应尽义务原则适用于网上领域；该原则规定，每个国家都有义务“不故意允许其领土被用于有悖其他国家权利的行为”。[4] 因此，各国不应故意允许其领土被用于通过电子手段实施并被国际法禁止的行为，必须采取一切可以合理预期的措施，确保其领土不被非国家行为体用来实施此类行为。法国已将对私人行为体应对事件能力的监管确定为一个重要的工作领域，这可能有助于通过限制对第三方造成不利影响的行动，确保应尽义务

[4] 《科孚海峡案，1949 年 4 月 9 日判决，1949 年国际法院案例汇编》，第 4 页。

原则得到尊重。[5] 更好地理解该原则如何适用于这一领域的挑战，将加强各国间的合作，以期保护某些关键基础设施，消除通过第三国发动的重大网络攻击。

格鲁吉亚

[原件：英文]
[2020 年 5 月 29 日]

格鲁吉亚政府在促进安全、具有复原力、有保障和可靠的电子政务解决方案和发展整个信息社会的同时，密切考虑每一个机会，以落实从国际安全角度看信息和电信领域的发展政府专家组关于推进在网络空间负责任国家行为的建议。格鲁吉亚希望积极促进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提供的原则和准则，并为此目的建立专门的国家机制。

本文件概述格鲁吉亚网络安全和信息安全发展的重要最新情况，以及在国家一级为加强信息安全和促进国际合作而做出的努力。

格鲁吉亚继续致力于发展其网络安全态势，使其网络安全状况在国际舞台上处于比较先进的地位。格鲁吉亚的地缘政治条件显然提高了其网络安全发展努力的重要性。2019 年 10 月 28 日，格鲁吉亚总统办公厅、法院、各市议会、国家机构、私营部门组织和媒体的网站、服务器和其他操作系统遭到了大规模网络攻击。这次网络攻击的目标是格鲁吉亚的国家安全，目的是通过扰乱和瘫痪各个组织的运作来伤害格鲁吉亚公民和政府机构。格鲁吉亚当局进行的调查，再加上通过与我们的合作伙伴合作收集的信息，得出结论认为，这次网络攻击是由俄罗斯联邦武装部队总参谋部主要司策划和实施的。上述事件再次证实了格鲁吉亚政府努力在国家一级加强网络安全的重要性，并再次表明需要加强网络安全方面的国际伙伴关系。

格鲁吉亚利用其所有资源成为网络空间中一个更强大、更有保障和更安全的国家。具体而言，格鲁吉亚政府努力增强信息社会中每个目标群体的能力，使其拥有应对网络威胁所需的知识和经验。格鲁吉亚的治理模式为公共和私人组织提供了集体和独立的能力，通过共同分享资源来确保国家的网络安全和相关可持续能力。此外，格鲁吉亚作为值得信赖的网络安全合作伙伴，得到国际合作伙伴的赞誉和支持。

格鲁吉亚政府正在积极努力提供一个开放、安全、有保障的网络空间。网络安全是格鲁吉亚政府国家安全政策的战略方向，使其更加发达和更具复原力正在受到政治上的高度关注。政府认为自己有权为本国的信息社会、数字经济和电子治理创造一个有利的环境；政府承担建立相关战略、机构-组织和法律-监管框架的责任，支持公民以及公共和私营部门在电子环境中安全、有保障地行使职能，同时考虑到他们正在安全地利用在线空间。

[5] 这种监管应依据与私营行为体可自行采取的应对事件措施有关的风险分析，其基本原则应为政府专家组的工作提供信息参考。

加强网络安全领域的双边、区域和国际合作一直列在格鲁吉亚政府政治议程的重要位置。格鲁吉亚是区域和国际两级伙伴关系以及多边形式伙伴关系(欧洲联盟、北大西洋公约组织(北约)、欧洲安全与合作组织(欧安组织)、联合国、东部伙伴关系、欧洲委员会、欧洲联盟执法合作署、国际刑事警察组织、欧洲警察学院、欧洲联盟网络安全署)的典范。格鲁吉亚积极参加与网络安全有关的国际项目和会议。

在过去几年中，开展了以下合作和伙伴关系倡议：

- 格鲁吉亚在过去十年中采取的旨在加强网络安全的步骤是积极的，所实施的改革和正在进行的进程在国际一级得到了积极评价。在东部伙伴关系中，格鲁吉亚在网络安全发展方面排名靠前，处于领先地位，这就是为什么该区域各国参与能力建设、信息和最佳做法交流等方面的多项活动，而格鲁吉亚在这些活动中发挥着区域网络安全中枢的作用。

- 格鲁吉亚-北约在网络安全领域的合作正处于发展阶段。格鲁吉亚正在积极与北约成员国合作，单独和集体参加在北约赞助下管理的各个项目。这还包括格鲁吉亚参加战略或技术学习倡议。北约(总部和联络处)协助格鲁吉亚网络当局在格鲁吉亚各地开展针对不同目标群体的系统和持续的提高认识和培训活动。格鲁吉亚定期向北约-格鲁吉亚委员会介绍其网络安全成就和举措，并利用《北约网络防卫承诺》紧密指导自己。

- 格鲁吉亚和欧洲联盟。通过《欧洲联盟促进格鲁吉亚安全、问责和打击犯罪》五年期方案，格鲁吉亚在网络犯罪、网络和混合威胁处理、边界管理、民事保护和安全部门监督等领域得到了欧洲联盟的援助。格鲁吉亚加强了在《欧洲联盟共同安全和防务政策》平台框架内的合作；该平台呼应该组织经国际确定的战略目标，并总体上通过发展格鲁吉亚的国防能力，支持巩固其国家安全。

- 格鲁吉亚和欧安组织。格鲁吉亚认为，通过网络安全领域的建立信任措施，在伙伴国家之间建立可信赖的网络具有重大价值。格鲁吉亚各联络人积极参与欧安组织的网络安全平台及其倡议。

- 格鲁吉亚和英国两国政府签署了《网络安全合作谅解备忘录》。其目的是加强相互合作，分享最佳做法，并更好地对接关于不同网络安全主题的办法。

- 格鲁吉亚和东部伙伴关系各国。数据交换局继续在《欧盟促进数字：提高东部伙伴关系各国的网络复原力》方案范围内与东部伙伴关系各国合作。“东部网络”项目帮助格鲁吉亚和其他东部伙伴关系国家提高东部伙伴关系各国的网络复原力、刑事司法和电子证据等能力，以更好地应对网络犯罪。重点是改善法律和政策框架；加强司法和执法当局的能力以及机构间合作；以及引入高效的国际合作机制，以增加在刑事司法、网络犯罪和电子证据等事项上的信任，包括服务提供者和执法部门之间的信任。

- 格鲁吉亚继续在民主和经济发展组织框架下加强与邻国的区域合作。2019 年，格鲁吉亚代表参加了在基辅民主与经济发展组织所在地举办的会议。

- 计算机应急小组是格鲁吉亚司法部数据交换局的一个附属单位；该局签署了大量合作备忘录，与欧洲和东欧伙伴关系各国(即立陶宛、罗马尼亚、摩尔多瓦、乌克兰和白俄罗斯)的相应组织交流知识和经验。格鲁吉亚正在积极参加国际网络演习和研究方案；在这些演习和方案中，格鲁吉亚在观察得到的成果方面经常处于领先地位。

在实践中，格鲁吉亚凭借在该领域所拥有的丰富国家知识，将国际上最好和最相关的专门知识视为在建立其战略、法律、体制和能力建设等支柱方面进行合作以及开展网络文化转型进程的宝贵指导和机会。

在网络安全领域各部门机构的积极合作下，[6] 2019 年在格鲁吉亚拟订了国家网络安全战略及其行动计划第三稿。[7] 国家安全委员会办公室在这一进程中发挥了协调作用。与此同时，来自私营部门、学术界和民间社会的相关利益攸关方也参与了相应的工作。在格鲁吉亚努力使其国家框架与相应的欧洲-大西洋机制相匹配的同时，外国专家和志同道合的本国咨询人为战略发展进程提供了大量建议。在起草国家网络安全战略及其行动计划方面，特别重要的是联合王国向格鲁吉亚相关网络安全行为体提供的援助。格鲁吉亚政府将在 2020 年批准国家网络安全战略及其行动计划草案。有关文件将接受 2020 年 1 月在国家安全委员会设立的常设机构间委员会的审查；该委员会的职责是协调拟订安全领域的国家一级概念性文件。随后，文件草案将由国家安全委员会提交格鲁吉亚政府批准。

格鲁吉亚继续加强执行网络领域的法律和监管框架。格鲁吉亚实施了处理网络安全的全面信息和通信技术立法和监管框架，并通过了保护个人和组织在数字环境中的权利的立法。各项法律处理对关键信息基础设施的保护、互联网服务提供商的责任、事件报告义务和电子交易的安全。下一步，格鲁吉亚已经制定宏伟的计划，使其网络安全法律框架与欧洲联盟关于网络和信息系统安全的指令相匹配。也就是说，在 2019 年期间，负责机构已经启动了与欧洲联盟的合作进程；到今年年底，将开发结对卡片，目的是帮助格鲁吉亚开展协调统一进程。作为结对项目的一个结果，格鲁吉亚将更新其《信息安全法》，其中除其他重要方面外，将明确界定网络安全治理框架、《指令》的权限以及网络安全在战略、业务和战术层面的作用和责任。

格鲁吉亚还启动了另一个宏伟的进程，设计和采用与欧洲联盟相匹配的关键信息基础设施保护模式。在 2019 年期间举办了几次讲习班，以便讨论网络领域关键基础设施的识别并与之合作的适当制度。格鲁吉亚为关键信息基础设施制定

[6] 数据交换局(司法部)、网络安全局(国防部)、行动技术局(国家安全局)。

[7] 2020-2023 三年期间预计。

了相关的整套方法和问卷。这一进程涉及与来自不同部门和商业领域的私人拥有关键行业的代表进行讨论。

目前，所有被界定为关键信息基础设施的组织都在实施信息安全政策和网络安全规定。负责国家机构协助这些实体执行信息安全政策和网络安全要点，提供建议、专门知识和培训，并为此开展更全面的活动，诸如信息安全审计、渗透测试及其他信息和网络安全服务。在作为关键信息系统一部分的机构中已经启动了用于实施信息安全管理系统的各种项目。这些实体在采用信息安全政策、承担资产管理任务和政策审查方面得到支持。同时，政府通过立法和附则(以国际标准化组织 27 000 系列标准为基础)制订信息安全标准和程序，并为政府和私营机构代表举办信息安全培训课程。下一个目标是根据欧洲联盟关于网络和信息系统安全的指令，制定并采用关于关键信息基础设施保护的法律规定，保证有关网络和信息系统安全的扩大法律规定适用于关键信息基础设施保护。

格鲁吉亚政府成功地利用公私多个利益攸关方平台作为一种工具，在所有利益攸关方之间建立信任，分享信息和知识，落实新的倡议，并使私营部门能够参与政策和战略制定进程。领导公私合作进程的数据交换局在 2019 年期间与金融、能源和电信部门举办了多次讲习班和会议，以便加入关键基础设施确定进程的筹备协商。私营利益攸关方是关于战略、政策、法律、监管和能力建设倡议中横向项目的所有主要协商进程的一部分。

格鲁吉亚针对不同的目标群体开展系统和持续的提高认识和培训活动，以培养网络专业素质和精通程度。通过格鲁吉亚国家组织的参与，开展了旨在提高民众网络卫生知识水平的大规模提高认识运动；此外，目前正在积极管理针对网络安全领域各种目标群体的学习——再培训方案。年复一年，格鲁吉亚的网络安全能力成熟度因各种不同的倡议和教育方案而得到提高，格鲁吉亚政府一直而且目前也在非常积极地努力提高公共部门雇用的网络安全专业人员的资质。因此，他们的专业素质很高，其中许多人拥有国际公认的、享有盛誉的证书(SANS 研究所、信息系统审计与监督协会、国际标准化组织)。

最后，格鲁吉亚将继续积极参加关于互联网治理的国际对话和其他有关集体网络安全的国际倡议。

洪都拉斯

[原件：西班牙文]
[2020 年 4 月 17 日]

关于从国际安全角度就网络空间所采取的措施的报告

洪都拉斯国家警察局正在国际标准化组织 27001(国际信息安全标准)的背景下采取各种内部步骤，以期创造一种与共和国总统办公室推动的数字政府倡议相一致的工作文化。这些步骤的重点是根据其信息安全手册负责任地使用互联网资源；该手册明确说明了为保护我们人员的不同业务活动以及减少导致我们的系统可能成为攻击或恶意行为受害者的漏洞而制定的政策。

国家警察局在网络空间方面采取的一些措施如下。

1. 制定信息安全政策

信息安全政策确立了标准和准则，以确保适当使用旨在保护警察局的信息技术和实物资源的技术工具，以此作为履行其宪法使命的关键投入，并通过有效应用最佳做法和控制措施，保证不断改进、管理和保护这一使命，并保证所有信息的机密性、可用性和完整性。

2. 培训班

洪都拉斯国家警察局通过警察远程信息技术局，持续为业务和行政人员举办网络空间提高认识培训班。警察局还参加特殊活动，就网络欺凌、社会工程、假新闻、网络犯罪和网络安全等问题提供培训。

3. 建立一个本地网络

我们的内联网网页“Poliweb”，用来随时向我们的工作人员通报网络犯罪的最新趋势、发布有关我们环境中的网络安全事态发展的重要通讯，以及宣传根据信息安全手册制订的保护计算机安全的政策。

这种内部连接使国家警察局的所有内部业务都可以通过我们的本地网络或内联网进行，从而最大限度地降低了我们的用户访问未知网站的风险，并节省了互联网资源和带宽。

4. 事件管理和调查

信息安全团队对机构数据网络进行持续监测，并查明我们的用户可能因不适当的互联网冲浪或试图规避我们的限制而造成的设备中的漏洞和设备面临的威胁。同时，正在采取措施调查和管理机构网络中的计算机事件。信息安全部的信息管理科和事件管理科负责分析可能使机构系统和信息面临风险的已知漏洞。这些漏洞可通过以下正规程序进行适当的管理和修复：

- 增补与软件提供商、版本、当前部署状态和负责软件的官员相关的信息资产数据清单。
- 每年进行两次漏洞分析。
- 维护有关新漏洞的最新信息。
- 制定一个对已知漏洞采取修复和补救措施的时间表。
- 在部署到生产环境之前测试漏洞补救的修复或修补情况。

5. 审计

通过年度审计计划，核实为正确使用计算机设备和警察互联网连接而颁布的政策的遵守情况。

其中一些限制如下：

- 禁止在计算机上安装虚拟专用网络。
- 禁止使用各种隐名浏览器，如 Tor、I2P、DuckDuckGo 和 Whonix。
- 禁止使用社交网络(特殊的局除外)。
- 禁止使用数字电视和视频回放网站等高消费流播网站。
- 禁止储存个人文件和安装与工作无关的软件。

信息系统以及服务器、网络设备和其他技术服务要保留审计记录(日志)，其中尽可能包括：

- 使用者身份查验。
- 交易的日期和时间。
- 进行交易的设备的 IP 地址和名称。
- 交易类型。
- 交易识别。
- 所查阅、修改或删除的数据。
- 连接尝试失败次数。
- 系统配置中的更改。
- 特权的更改或撤销。
- 所访问的文件。
- 来自控制系统的警报。
- 使保护机制失效。

6. 杀毒软件

杀毒软件保持活动状态，作为防范恶意软件的另一层保护；它为我们提供反“网络钓鱼”功能、防范零日攻击、反勒索软件功能以及持续更新的安全补丁。

7. 防火墙管理

网络分段和授权是通过“防火墙”周边安全软件进行的，该软件可以阻止企图侵入我们网络的行为，并统计我们使用者的登录次数，识别网站浏览量和登录到不同机构系统的次数。

8. 加密通信

在应对国家安全紧急情况和国家警察局内部协调方面，我们拥有最先进的安全加密无线电通信系统，以保障我们通信的完整性。

所有采取的措施都在改善对机构信息的保护，并促进防止网络攻击的努力，同时铭记，我们没有对我们的系统采取保护措施。目前没有绝对安全的系统，但通过采取其中一些措施，我们正在缩小漏洞差距，通过识别和阻止网络攻击来确保治理网络空间。

匈牙利

[原件：英文]
[2020 年 5 月 15 日]

对国际安全背景下网络空间相关问题的整体理解

2019 年 12 月，大会通过了一项关于从国际安全角度促进网络空间负责任国家行为的决议。在该决议中，大会请会员国继续向秘书长通报他们对在国家一级为加强信息安全和促进这一领域的国际合作而做出的努力的看法和评估意见，以及从国际安全角度看信息和电信领域的发展政府专家组报告中提到的概念的内容。

匈牙利欢迎在联合国第一委员会定期讨论负责任国家行为的志原规范、规则和原则、建立信任措施和国际法的持续进程，以及设立其他政府专家组。

2018 年，匈牙利分别支持大会第 73/266 号和第 73/27 号决议，这两项决议设立了从国际安全角度推进网络空间负责任国家行为问题政府专家组和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，作为以后应对使用信息和通信技术所带来的威胁的重要步骤。

匈牙利首次也加入了这些谈判，只是我们非常感兴趣地关注了以往几个政府专家组的工作，包括在 2013 年通过我们的第一个《国家网络安全战略》过程中。不限成员名额工作组自成立以来，匈牙利分别派其常驻欧洲安全与合作组织(欧安组织)代表(也是欧安组织网络安全问题非正式工作组主席)以及外交和贸易部网络问题协调员作为代表出席了该工作组第一次和第二次正式会议。匈牙利还积极参加关于不限成员名额工作组主席报告草稿的协商。总体而言，匈牙利与欧洲联盟的立场一致。

匈牙利坚决支持以基于规则的国际秩序为支撑的有效多边体系，这样的体系在应对网络空间全球挑战方面取得了成果。我们参与并支持不同的政府间和多个利益攸关方倡议就是一个很好的例子。匈牙利重申，正如政府专家组 2010 年、2013 年和 2015 年的协商一致报告所确认的那样，现行国际法适用于网络空间中的国家行为。然而，国家和非国家行为体不遵守国际法义务仍然是对国际和平与安全以及我国国家主权的重大威胁，无论是在现实世界还是在网络空间都是如此。因此，我们需要能够威慑和防止常规和非常规攻击。

对裁军议程的支持

匈牙利赞同秘书长对恶意使用信息和通信技术的情况日益增多表示的关切，因此支持将促进和平的信息和通信技术环境作为秘书长 2018 年 5 月宣布的《裁军议程》中的一个关键优先事项。作为对我们高度参与的认可，联合国裁军事务

厅已将匈牙利确定为《议程》行动 31 的支持者，该行动的目的是促进问责和遵守网络空间的新规范。

匈牙利支持秘书长为防止网络事件升级而进行的斡旋，支持自愿网络规范付诸实施，并支持旨在弥补会员国之间网络知识差距的进一步协作。

网络安全是关系到国家安全的问题

2020 年 4 月，政府通过了匈牙利新的《国家安全战略》(附于第 1163/2020(IV.21.)号政府决定之后；根据新的战略，需要对我们现有的《国家网络安全战略》进行审查。新的《国家安全战略》概述了自 2012 年以来安全威胁格局发生的变化。其主要目标之一是查明、探讨和应对信息和通信技术迅速发展带来的安全挑战。

人们普遍预计，网络攻击的数量和复杂程度将持续增长。因此，匈牙利政府将与其他利益攸关方合作，尽其所能加强能力，以防范针对我国重要信息基础设施的恶意网络攻击，并进一步提高公众的网络卫生意识。

处理错误信息和虚假信息在线上和线下传播造成的挑战是一个关键的优先事项，在我们继续与冠状病毒病(COVID-19)大流行作斗争的今天更是如此。在国家紧急状态下，虚假信息可能会造成特别严重的破坏。

发展攻击性和防御性网络能力必须与一个国家根据国际法承担的义务相一致。否则，使用攻击性信息和通信技术能力可能会助长数字空间的军事化。

我们认为，能够威胁国家安全和稳定的网络能力被视为一种武器，使用这种武器可以达到武装攻击的门槛，作为自卫手段，各国也可以对此作出强力反应。考虑到信息和通信技术环境中查找原因方面的挑战，公共当局在发生信息和通信技术事件时应谨慎行事，考虑到所有相关信息，包括事件的大背景以及后果的性质和程度。

国际合作和其他多利益攸关方倡议

作为欧洲联盟的成员，匈牙利积极参与开发欧洲联盟自己的网络外交工具箱，以便欧洲联盟能够协调应对源自欧洲联盟以外的针对其机构及其成员国的恶意网络活动。我们强调国际合作的重要性，支持加强与我们的战略合作伙伴、盟友和其他国际组织的对话。

任何一个国家或组织都不可能单独成功地应对当代的安全威胁。这使得伙伴关系、特别是欧洲联盟-北大西洋公约组织(北约)的合作在今天比以往任何时候都更加重要。别无选择，只能在未来几年继续并进一步深化这一合作。对抗混合威胁(包括网络安全威胁)肯定是这两个组织应该重点努力的主要领域之一。

预计在未来几年，网络空间中的冲突将进一步加剧，技术先进国家与发展中国家之间的能力差距将进一步扩大。2016 年 7 月，盟国重申了北约的防御性任务，并确认网络空间是北约必须捍卫的行动领域。2018 年 7 月，盟国再次宣布北约准备继续适应不断变化的网络威胁格局，这一格局受到国家和非国家行为体、

包括国家支持的行为体的影响。北约成员国同意在盟国自愿的条件下，将主权网络效应纳入强有力的政治监督框架。北约重申了联盟的防御性任务，宣布决心部署包括网络能力在内的全方位能力，以威慑、防御和反击全方位的网络威胁。北约致力于进一步发展与所有盟国工业界和学术界的伙伴关系，通过创新跟上技术进步的步伐。

匈牙利对网络安全的承诺并不是新事物。2001 年在布达佩斯达成了第一项也是唯一项关于打击网络犯罪的国际协议，称为欧洲委员会《网络犯罪公约》，又称《布达佩斯公约》；该公约此后一直作为制定打击网络犯罪的综合国家立法的指导方针和国际合作的框架。2004 年第 LXXIX 号法批准了该条约。匈牙利除了是《布达佩斯公约》的缔约国外，还积极推动第三国加入该公约。

作为我国的一个贡献，自 2017 年以来，匈牙利常驻代表一直担任根据常设理事会第 1039 号决定设立的欧安组织非正式工作组的主席；该决定的内容涉及制定建立信任措施，以减少使用信通技术引起的冲突风险。匈牙利支持旨在加强联合国各进程与欧安组织等其他相关区域组织之间合作的努力。在区域层面，我们强调执行欧安组织通过的一套建立信任措施的重要性。我们还赞成在不限成员名额工作组范围内阐述区域建立信任措施的全球化问题。不过，我们的重点应该是以同样的效力落实每一项区域建立信任措施。

匈牙利是少数几个拥有专门的网络外交工作人员的国家之一。外交和贸易部网络问题协调员负责双边和多边关系中关于网络空间问题的国际外联活动，其中包括联合国、欧洲联盟、欧安组织和其他相关多利益攸关方倡议，诸如全球网络专门知识论坛。网络外交是我们国际合作的一个相对较新的领域，我国政府在应对恶意网络活动时可以借助网络外交。

匈牙利帮助第三国开展能力建设努力。作为这些努力的一部分，网络安全在匈牙利的国际发展合作政策、特别是对非洲伙伴国家的政策中也发挥不可或缺的作用。为此，匈牙利一直在信息技术安全领域向乌干达提供发展援助，目的是帮助乌干达面对二十一世纪的挑战。网络安全领域是匈牙利最近通过的《非洲战略》及其《2020-2025 年期间国际发展合作战略》中规定的关键合作要素。

除了参加不同政府间谈判以外，匈牙利政府还支持多利益攸关方的倡议，诸如“网络空间信任与安全巴黎呼吁”，响应在制定网络空间的国家行为规范、规则和原则方面开展更深入合作的呼吁。我国政府与数十个匈牙利私营部门组织一起参与这些努力。匈牙利也支持消除网上恐怖主义和暴力极端主义内容的克赖斯特彻奇呼吁，这些内容对人权和我们的集体安全有不利影响。

匈牙利也认为，非政府组织(民间社会、学术界、私营部门以及信息和通信技术界)拥有各种技术专长和/或必要资源，能够在各自的作用和责任中为发展安全和可持续的网络空间作出贡献。各国在促进这种协调与协作方面发挥着牵头作用。

印度尼西亚

[原件：英文]
[2020 年 5 月 31 日]

国家一级为加强信息安全和促进国际合作所作的努力

印度尼西亚有超过 1.7 亿互联网用户，占其总人口的 65%。信息和通信技术为印度尼西亚提供了对实现可持续发展目标至关重要的机会。另一方面，网络空间中的挑战也在增加。2019 年，印尼遭受了超过 2.2 亿次网络攻击，阻碍了人们对网络空间的有益利用。

印度尼西亚正在积极采取多种措施，通过加强机构基础设施、能力建设和国际合作的法律和政策方面，最大限度地发挥数字潜力和应对网络威胁。

国家层面的努力

2017 年，成立了国家网络和加密局，作为印度尼西亚负责网络安全事务的中央机构。国家计算机应急响应小组是在该局下设立的，负责快速应对针对政府或私人基础设施的网络事件。印度尼西亚 34 个省的每个中央和区政府机构也成立了计算机安全事件响应小组，以处理网络事件并从网络事件中恢复。

在加强国家法律和政策框架方面，印度尼西亚颁布了《信息和电子交易法》以及《2017-2019 年国家电子商务路线图》，其中包括努力确保电子和数字交易的安全。印度尼西亚的《网络防御准则》是通过 2014 年国防部第 82 号条例颁布的。印度尼西亚的国家标准化系统也采用了信息和通信技术安全国际标准，即 ISO/IEC27001 标准和 ISO 15408 标准。

印度尼西亚的网络安全法已被设定为 2020 年的优先法案，立法程序目前正在进行中。印度尼西亚目前还在起草 2020-2024 年国家网络安全战略，该战略涵盖五大支柱：网络复原力、加强法律框架、网络技术能力、支持数字经济增长以及国家和国际合作。

印度尼西亚还致力于继续加强国内合作，特别是与国有企业、私营部门和行业的合作，以支持创建包容型网络安全文化。自 2018 年以来，印度尼西亚政府发起了网络安全扫盲运动，以促进安全的互联网接入、打击恶作剧和网络欺凌、社交媒体道德、负责任的使用和对家长的引导，以确保儿童的互联网安全。

国际层面的努力

印度尼西亚通过其多重举措，继续推进相互合作、最佳做法和能力，以帮助建立起最终可普遍采用的关于网络安全的有效机制。

在全球多边参与方面，印度尼西亚积极参与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，包括以不结盟国家运动裁军工作组协调员的身份参加。印度尼西亚目前还是从国际安全角度看信息和电信领域的发展政府专家组的 25 个成员之一。

在区域一级，印度尼西亚参加东南亚国家联盟(东盟)框架内的建立信任措施，为此除其他外，支持在其政治安全和经济共同体支柱下处理网络问题的东盟部门机构中设立联络点，并开展信息交流、定期网络安全协作和成员国对话。东盟还通过成立跨支柱协调委员会，加强在网络安全问题上的合作。通过东盟区域论坛，关于网络安全背景下建立信任措施的讨论已扩展到东盟以外，还涉及到其他国家及合作伙伴。

此外，印度尼西亚还与各国及合作伙伴保持双边对话与合作。印度尼西亚将继续有效地推进各项努力，加强负责任国家行为，促进开放、安全、稳定、无障碍与和平的信息和通信技术环境。

政府专家组各项报告所述概念的内容

国家和非国家行为体、包括代理人滥用网络空间，对国际和平与安全以及国家政治、经济和社会领域的稳定构成风险。在应对冠状病毒病(COVID-19)大流行的多层面影响方面，国际上目前也正在出现向信息和通信技术的重大转变。恶意的网络行为体可能特别会试图利用信息和通信技术系统以及信息在网络空间的传播。

相互理解、合作、协作、建立信任措施、援助和能力建设对于加强网络空间的安全与稳定至关重要。在这方面，双边、区域和全球努力都必须得到支持，并被视为相辅相成，而不是相互竞争。

印度尼西亚支持根据 2015 年政府专家组的报告，继续讨论和执行非约束性规范。印度尼西亚重申，联合国和区域组织在促进讨论和执行关于网络安全的 11 项准则、建立信任措施和能力方面，特别是在缩小和弥合国家之间的数字差距方面，发挥了关键作用。

印度尼西亚认为，自愿和不具约束力的规范是负责任国家行为的重要框架。虽然在不受管制的网络空间问题上的差距需要解决，但印度尼西亚鼓励创建更多的国家和习惯做法。

印度尼西亚对讨论在网络空间适用现有国际法、包括特别法的可能性持开放态度。印度尼西亚强调，使用网络空间应符合国际法律原则，特别是与充分尊重主权、不干涉、和平解决争端、人权和《联合国宪章》有关的原则。

印度尼西亚支持所有国家在大会宣布不将网络空间军事化，因为这破坏国际和平与安全，违背各国根据国际法享有的权利和承担的义务。

印度尼西亚强调要扩大理解和深化接触，那些还没有充分参与网络安全讨论和措施的国家和区域更要这样做。

爱尔兰

[原件：英文]
[2020 年 5 月 30 日]

爱尔兰欢迎有此机会对秘书长根据第 74/28 号决议第 2 段提出的要求做出回应，即在国际安全背景下推进网络空间负责任国家行为。爱尔兰也支持欧洲联盟提交的案文。

信息和通信技术(信通技术)惠益社会和国家，便利通信、教育、创新和经济活动的进行，并促进了繁荣。但在一个日益相互联系的世界里，滥用这些强大的技术也可能产生非常不利的影响，恶意网络活动的上升，包括在当前的大流行病期间，是爱尔兰主要关注的问题。这项活动影响到公民及其对体制的信任和信心。在社会和国家层面也能感受到它的影响，它可能导致社会和国家层面的冲突或使冲突升级。

联合国仍然是应对滥用信通技术和恶意网络活动相关挑战的首要论坛，这些挑战影响到联合国议程的所有三大支柱：和平与安全、人权和可持续发展。作为一个拥有重要信息和通信技术部门的经济体，作为一个对联合国有着坚定承诺的国家，爱尔兰将继续支持联合国促进和推进网络空间负责任国家行为。爱尔兰还将继续与联合国和国际合作伙伴积极协作，为开放、自由、安全和有保障的网络空间提供支持，促进网上言论自由、结社和集会自由，降低冲突风险，促进和平，并确保网络空间的社会和经济效益惠及所有的人，包括给可持续发展目标提供支持。我们认为，只有在多层面经由多个利益攸关方的参与，才能保证在应对所面临的挑战方面取得持续进展，我们为此将致力于在全国范围内采取各种举措，包括 2019 年在政府资助下建立的爱尔兰网络集群，该集群汇聚行业、学术界和政府的多个利益攸关方，以讨论和促进在网上教育和职业发展机会方面的合作并提高这方面的认识，促进爱尔兰网络安全部门的创新。我们还将致力于在国际上也奉行该做法，并就此欢迎联合国及其他论坛为促进更广泛的合作与对话而采取的举措，包括通过从国际安全的角度来看信息和电信领域的发展问题不限成员名额工作组采取的举措。爱尔兰还支持在国际安全范围内推进网络空间负责任国家行为的政府专家组会议

爱尔兰对网络问题的做法仍然基于我们对包括《联合国宪章》、国际人道主义法和国际人权法在内国际法的可适用性及其中心地位所持承诺。爱尔兰还欢迎大会在 2015 年达成的共识，即所有各国都应在 2015 年政府专家组报告指导下使用信通技术，该报告列出了 11 项自愿和不具约束力的负责任国家行为规范。我们认为，这些规范与国际法相结合，辅之以建设网络复原力和促进更多获取信通技术的能力建设措施和旨在减少武装冲突风险的建立信任措施，可以给推进国家在网络空间的积极行为提供一个强有力的框架。信通技术能力建设举措也有助于解决仍然存在的全球数字鸿沟，改变人民和社区的生活，促进繁荣，协助并便利包括在性别等领域落实可持续发展目标。

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

爱尔兰 2019-2024 年国家网络安全战略

在一个相互关联的网络空间中，所有各国都必须确保在国内和全球建立抵御网络相关风险的能力。爱尔兰 2019 年至 2024 年国家网络安全战略提出了这方面的关键行动和目标。[8] 该战略给联合国促进负责任国家网络空间行为及维护国际和平与安全的目标提供支持，保护爱尔兰、爱尔兰人民及本国重要基础设施免受网络安全的威胁。这也是爱尔兰在国际上致力于支持自由、开放、和平与安全的网络空间的根本原因。爱尔兰网络安全政策执行机构是国家网络安全中心，该中心推动就网络问题展开对话并与国际伙伴机构及其他利益攸关方进行合作，提升对网络空间的信任度和网络空间安全，从而为联合国网络议程做出贡献。

爱尔兰网络安全战略的主要目标包括：

- 继续提高爱尔兰检测、应对和管理网络安全事件的能力
- 识别和保护国家重要基础设施，增强抵御网络攻击的能力
- 提高公共部门信息技术系统的抵御力和安全性，以更好保护公民所依赖的服务及其数据
- 投资于教育举措，为劳动力在信息技术和网络安全方面的职业提升做好准备
- 提高企业对其在网络、设备和信息安全方面所负责任的认识，推动爱尔兰网络安全研发工作，包括为此促进在新技术上的投资
- 继续与国际伙伴和国际组织开展合作，以确保网络空间仍然是开放、安全、统一和自由的，有能力促进经济和社会发展，给可持续能力建设提供支撑
- 为在确保基本网络安康做法上提高个人的总体技能和认识水平，并通过信息和培训向其提供支持。

《国防白皮书》

爱尔兰《国防白皮书》(2015 年公布，[9] 2019 年更新[10])注意到国内和国际恶意网络活动带来的危险，包括对关键基础设施和关键服务的危险，并认识到网络问题又是如何被滥用以破坏包括人类尊严、自由和民主等核心价值观的。《国防白皮书》和《国家网络安全战略》继续是爱尔兰据此参与有关信通技术和网络问题工作的依托。

[8] 可查阅 www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf。

[9] 可查阅 https://assets.gov.ie/21963/f1e7723dd1764a4281692f3f7cb96966.pdf。

[10] 可查阅 www.gov.ie/en/publication/a519cf-white-paper-on-defence-update-2019/。

双边、区域和多边做法

爱尔兰在与其他国家的双边交往以及在区域和多边论坛上与其他国家的交往时，继续促进关于信通技术和网络问题的对话。

爱尔兰欢迎欧洲安全与合作组织(欧安组织)和世界各地其他区域组织在促进信任和建立信任措施方面所做工作。

爱尔兰支持促进网络空间信任、安全与和平的国家和非国家倡议，包括《网络空间信任与安全巴黎呼吁》。爱尔兰还支持《消除网上恐怖主义和暴力极端主义内容的克赖斯特彻奇呼吁》。爱尔兰是由合力推进互联网自由的 31 个国家组成的自由在线联盟的成员。

爱尔兰还提交了一份寻求加入塔林合作网络防御卓越中心的意向书，目的是与志同道合的伙伴合作一道携手应对网络安全挑战。爱尔兰将作为参与编撰方(作为非北约成员国)加入该中心。

在欧洲联盟(欧盟)促进国际合作

爱尔兰继续就网络问题在欧洲联盟充分发挥积极作用，并与其欧洲联盟伙伴密切合作，利用网络外交倡议和欧洲联盟网络外交工具箱等手段，推动形成一个有助于预防冲突的向世界开放、自由、稳定和安全的网络空间。在网络抵御力的能力建设方面，爱尔兰还参与了欧洲防卫局的一些举措。

在联合国促进国际合作

爱尔兰在联合国层面上支持国际安全背景下的信息和电信领域发展问题政府专家组的工作(另见下文)，并为国际安全背景下的信息和电信领域发展问题不限成员名额工作组作出了积极贡献。爱尔兰常驻联合国大使还在 2020 年 5 月 22 日举行的安全理事会关于网络稳定、预防冲突和能力建设的阿里亚办法会议上发言，强调爱尔兰致力于与联合国合作在该领域广泛开展各项活动，包括利用信通技术和网络空间实现可持续发展目标，特别是有关性别的目标。

政府专家组报告所提及的概念的内容

一般原则

爱尔兰支持以基于规则的国际秩序为依循，采取技术中立和多边方式促进全球网络安全。爱尔兰认为，利益攸关方(包括民间社会、学术界、技术和行业代表)的参与及其所做贡献丰富了不限成员名额工作组在近期会议上的讨论。这些利益攸关方在就信通技术领域未来发展向各国提供咨询并直接维护一个安全稳定的网络空间上的作用日益重要。爱尔兰认为，让利益攸关方更多参与今后关于网络问题的会议及其他讨论既重要又有必要，应该将其固定为正式的安排。

现存的和新出现的威胁

爱尔兰国家网络安全战略承认，信通技术对经济和社会发展影响日增并且积极，但也强调，网络犯罪和知识产权盗窃有增无减，虚假信息泛滥，国家对攻击

性网络能力的利用有所上升。冠状病毒病(COVID-19)大流行让我们依托信通技术以灵活、可靠的方式工作和通信并维持经济活动的情况得到彰显。然而，这一流行病也让恶意行为者的活动暴露于世人面前，他们利用技术和人的弱点实施网络犯罪，或传播虚假信息，散布混乱、制造不信任和分裂。爱尔兰特别关切地注意到最近针对卫生、医疗和相关服务的网络攻击。这种对医疗保健和其他基本服务的攻击危及生命。爱尔兰与其欧洲联盟伙伴一道谴责这些行为，并呼吁各国根据国际法以及政府专家组 2010 年、2013 年和 2015 年经协商一致形成的报告，尽职尽责，在其领土上开展此类活动的行为者采取适当行动。

国际法

爱尔兰坚信包括《联合国宪章》、国际人道主义法和国际人权法在内的国际法可适用于网络空间并在这方面享有中心地位。无论是线上还是线下，人权和基本自由都必须得到尊重。鉴于现有的国际法律框架，爱尔兰概述了其保留意见，包括在不限成员名额工作组最近的会议上，呼吁起草一项新的法律文书。然而，爱尔兰欢迎正在进行的为促进加深就对各国使用信通技术适用现行国际法形成更大共识的对话。

各国负责任行为规范、规则和原则

爱尔兰支持 2015 年政府专家组报告中关于负责任国家行为的自愿非约束性规范、规则和原则，并欢迎大会以协商一致方式商定报告应就使用信通技术向各国提供指导。这些规范促进提升全球信通技术环境的稳定和安全，并能有助于维护国际和平。爱尔兰的国家网络安全战略和爱尔兰政策反映了这些规范、规则和原则，包括与可持续能力建设有关的规范、规则和原则。爱尔兰在联合国呼吁进一步制定指导方针，说明如何切实执行和落实这些为所有各会员国一致认可的现有规范。

建立信任措施

爱尔兰在双边、区域和多边会议和论坛上，包括在全球和平与安全、可持续发展和人权的背景下，积极促进和推动关于信通技术和网络安全问题的讨论。爱尔兰承认，包括巴黎呼吁等区域组织以及国家和非国家利益攸关方倡议在提高信任和信心方面开展的广泛工作，并大体支持设立关于建立信任措施最佳做法分享机制的提议，以给今后的倡议提供支持。

能力建设措施

爱尔兰国家网络安全战略列有进一步采取可持续能力建设措施的承诺。爱尔兰还重视采取力求建设所有各国抵御恶意网络活动能力并减少脆弱性的多边和多个利益攸关方做法，保护关键基础设施，并让信通技术得以惠及所有各国。爱尔兰还认为，至关重要的是，所有各国和主要利益攸关方都有能力参与关于网络问题的全球讨论。在这方面，爱尔兰很高兴于 2019 年 12 月 2 日至 4 日主办了不限成员名额工作组非正式闭会期间会议，该会议将各国和各利益攸关方汇聚在一起，其中包括非政府组织和民间社会的代表、技术专家、研究人员和学术界以及

私营部门。爱尔兰还大力支持为解决性别数字鸿沟问题所做努力。爱尔兰欢迎强化今后关于联合国能力建设的讨论和倡议与可持续发展目标、妇女及和平与安全议程之间的联系。

意大利

[原件：英文]
[2020 年 5 月 29 日]

导言

意大利赞同欧洲联盟在其就该报告提交的意见中所述立场，并愿向秘书长提供有关意大利的以下信息。

对于本报告，意大利将不考虑“信息安全”一词，因为在意大利法律制度中不使用该词。而是使用了诸如“网络安全”或“网络和信息系统安全”等其他表述，因此这些表述更为可取。言论自由-无论是在线上还是线下-均为意大利基本法所承认，也为意大利 1978 年批准的《公民及政治权利国际公约》第 19 条所承认。

根据载有关于国家网络空间保护及信息和通信技术安全准则的 2017 年 2 月 17 日意大利总理令，“网络安全”一词是指经由适当的物理、逻辑和程序性安全措施确保对网络空间实施保护，目的是防止和应对涉及不当获取和传输数据、修改或非法销毁数据或不当控制、损坏、毁损或阻碍网络和信息系统或其组件正常运行的蓄意或偶然事件。

同样，根据转引欧洲联盟网络和信息系统安全指令的第 65/2018 号法令的定义，“网络和信息系统安全”一词是指，对于以所存储、传输或处理的数据以及对经由该网络或信息系统而可获得或访问的相关服务的可用性、真实性、完整性或保密性为攻击目标的任何行动，网络或信息系统具有在一定保密级别上加以抵制的能力

在国家一级加强网络安全的努力：体制和规范框架

2013 年 12 月，意大利通过了网络空间安全国家战略框架，该框架注意到信息和通信技术(信通技术)的使用所造成的日益增加并且不断变化的威胁，其目的是加强意大利的网络能力和复原力。根据 2017 年 2 月 17 日上述总理令予以通过并于 2017 年 3 月最新发布的下述国家行动计划确定了实施《战略框架》的若干行动、项目和优先事项。

该总理令界定了国家网络安全架构及其治理，在安全情报部内部设立了一个网络安全管理委员会，负责预防和防备国家网络危机，协调公共和私营部门根据总理的决定所开展的应对和复原活动。

网络安全管理委员会由一个秘书处和一个联合委员会组成，联合委员会由安全情报司负责网络事务的副司长担任主席，成员包括情报界(安全情报司、对外情报和安全局以及内部信息和安全局)、总理军事顾问、外交和国际合作部、内政部、

司法部、国防部、经济和财政部、经济发展部、民防司和数字意大利局的代表。每当讨论危及机密信息系统的事件时，安全情报司中央保密办公室的代表都会加入委员会。

在国家发生网络危机时，该委员会还可能包括来自卫生部、基础设施和运输部以及消防部门的代表。总理可根据国家安全委员会提供的信息，在网络事件因其规模、强度或性质而无法由单个相关部门处理但需要由经网络安全管理委员会确保采取联合和协调做法时，宣布发生网络危机的情况。

在《总理令》之后还有其他法律，即：

- 第 65/2018 号法令，该法令转用欧洲联盟网络和信息系统安全指令，并指定安全情报司担任网络和信息系统单一联络点；

- 国家网络安全周界(第 133/2019 号法律)于 2019 年 11 月生效，适用于履行基本职能或为实施被视为对意大利国家利益至关重要的活动提供基本服务的国家公共和私营实体。根据“国家安全渐进优先”原则，公共和私营实体被纳入“周界”。该法律涵盖上述实体拥有或运营的可能影响国家安全的网络、信息技术系统和服务。它包含以下内容：

  - 事件通知，目的是确保信息即刻发送给预防、防备和管理网络事件相关负责机构，即均属于安全情报司的网络安全管理委员会和计算机安全事件响应小组；

  - 涵盖组织问题、流程和程序包括信通技术采购的安全措施；

  - 对属于特定类别并与周边资产/实体相关的信通技术产品和服务进行的技术筛选。根据该法，任何希望购买这些物品的经营者都应通知国家评估和认证中心，该中心则可进行初步评估、提出条件并要求进行硬件或软件测试。在后一种情况下，相关的招标和合同应列入一项暂停取消政策的条款，该条款涉及国家评估和认证中心规定的要求或测试的积极结果；

  - 对公共和私人行为者进行检查和制裁的活动分别由部长理事会主席和经济发展部长实施。

如果出现与网络、信息技术系统和服务有关的严重和紧迫的国家安全风险，总理可指示部分或全部关闭/暂停在网络或系统上安装的或与已交付服务有关的一个或多个设备或产品。该决定须经共和国安全部际委员会事先审议，根据相称性原则，在消除或减轻威胁所绝对必需的时期内有效。

- 已经转化为第 41/2019 号法律(第 1 条)的第 22/2019 号法令，是对已经转化为“关于国防和国家安全部门以及能源、运输和通信部门战略相关活动特殊持股权力”的第 56/2012 号法律的第 21/2012 号“黄金权力”法令的补充，它把基于 5G 技术的宽带电子通信服务列入对国防和国家安全具有战略重要性的活动。根据最新规定，合同或协议，凡涉及为规

划、执行、维护和管理基于 5G 技术的宽带电子通信服务相关网络而购置货物或服务，或涉及购置助益上述执行或管理的“高强度技术组件”，只要事关非欧洲联盟实体，就须通知在部长理事会主席团内设立的“黄金权力”委员会。做出此项规定的考虑是，如果国家评估和认证中心发现存在可能危及网络及其数据完整性和安全性的漏洞，就应当允许行使否决权或设置包括更换产品和设备在内的具体规定和条件，对于这些规定和条件可加以修改或可与其他措施结合使用。

网络防御

2015 年《国际安全与防卫白皮书》承认，需要对网络领域提供保护和防御，包括为此建立“特定的防御作战能力……以维护政治、经济和社会结构的稳固性。”根据国防部 2019-2021 年多年规划文件，必须保护和防御网络空间，以免其受到对网络或计算机服务和关键基础设施的攻击。国防部近年来进行了一系列改革，以加强其保护、抵御能力和态势。

除其他外，意大利国防部于 2017 年设立了联合网络行动指挥部，这是一个负责规划、开展和实施网络行动的军事指挥部，目的是发现和消除对意大利境内国防部和意大利境外行动区网络、系统和服务的威胁和攻击。

联合网络行动指挥部最近已被纳入新成立的网络组成指挥部，目的是建立一个更直接的指挥链，并确保国防部门(空军、陆军和海军)内所有相关网络安全部门之间的效率和协调。网络组成司令部为意大利联合行动总部提供支持，其任务是开展防御行动，以保护意大利国防部及其军事机构免受网络事件和攻击的影响。

此外，网络组成司令部：

- 负责国防部网络的网络安全和网络防御，通过负责监测网络活动、预防和管理影响国防部门的事件和紧急情况的计算机应急小组确保网络安全和网络防御；
- 目前正在开展一项研究，以完全按照国际法和国际人道主义法来界定战区的法律框架。此类研究旨在界定最低标准和接触规则，以通过在网络空间开展的活动为行动提供支持。之所以需要有一个法律框架，主要是鉴于以往几年开展的众多国家与国际活动和演习，包括在北大西洋公约组织(北约)框架内开展的活动和演习。

在联合网络行动指挥部内建立了一个网络实验室，旨在开发调查网络漏洞和组织培训活动的工具。

其他活动包括初步测试以确立在意大利武装部队电信学院开展技术网络培训的网络范围并与许多意大利大学在网络安全领域开展合作。

为促进网络安全领域国际合作所做努力，包括在政府专家组报告方面

根据《意大利宪法》第 10 条，“意大利的法律制度符合公认的国际法规则”。

因此，意大利致力于根据欧洲联盟的立场及上述意见促进在网络空间适用包括整个《联合国宪章》在内的现有国际法；遵守 2015 年从国际安全角度来看信息和电信领域发展的政府专家组和以前各小组所确立的负责任国家行为规则、规范和原则；制定建立信任措施和能力建设方案；以及基于多利益攸关方模式的互联网治理。

意大利支持关于执行合作措施以减少影响网络空间稳定的风险和建立信任、能力和互信的《网络空间信任与安全巴黎呼吁》。意大利也是《消除网上恐怖主义和暴力极端主义内容的克赖斯特彻奇呼吁》的签署国之一。

促进与第三国的能力建设活动是我国国家网络安全战略的一部分，并根据 2018 年 6 月 26 日欧洲联盟一般事务理事会第 3629 次会议通过的“关于欧盟外部能力建设准则的理事会结论”进行。与第三国的能力建设活动主要侧重于分享信息和最佳做法，特别是在计算机安全事件对策以及教育和培训方面。

参加国际论坛和支持遵守网络空间负责任国家行为规范也是意大利国家网络安全战略的一个重要组成部分。在我们的双边和多边对话和/或磋商中，也酌情讨论了网络安全领域的国际合作，包括在政府专家组报告方面。意大利积极促进加强网络空间合作的主要多边论坛有联合国、欧洲联盟、北约、欧洲安全与合作组织(欧安组织)、欧洲委员会和七国集团。

关于后者，2017 年 4 月 10 日和 11 日，意大利主办了七国集团外交部长级会议，会议通过了《关于网络空间负责任国家行为的七国集团宣言》。《宣言》呼吁所有各国对信通技术的使用应当依循联合国从国际安全角度来看信息和电信领域发展的政府专家组逐渐累积的多份报告。

在 2018 年意大利担任欧安组织主席期间，意大利积极支持参与国在信息和通信安全领域落实欧安组织建立信任措施，特别是在 2018 年 9 月 27 日和 28 日在罗马举行的 2018 年整个欧安组织的网络/信通技术安全会议间隙期间，组织了一次关于在国际网络事件中使用这些措施的场景讨论。2019 年，意大利在担任欧安组织亚洲联络小组主席期间，于 2019 年 9 月 2 日和 3 日在东京组织举办了第二十届亚洲欧安组织会议，主题是“如何在数字时代实现全面安全：欧安组织及其亚洲伙伴的观点”。意大利还协助开展了一些关于网络/信通技术领域能力建设的欧安组织项目，例如 2019 年 2 月 7 日和 8 日在雅典举行的“关于信息和通信技术(信通技术)在区域和国际安全背景下作用的次区域培训”。

意大利积极参与从国际安全角度看信息和电信领域发展的不限成员名额工作组的活动，并支持目前政府专家组和以前各小组开展的工作。意大利还回顾，大会第 70/237 号决议欢迎以往政府专家组在其 2013 年和 2015 年报告中的结论，并呼吁会员国对信息和通信技术的使用依循 2015 年报告。

最近在意大利外交和国际合作部内设立了一个处理网络安全和网络政策的部门，旨在进一步加强和促进我们在该领域的外交行动和国际合作。

日本

[原件：英文]
[2020 年 5 月 31 日]

日本欢迎有此机会对秘书长根据大会第 74/28 号决议第 2 段提出的要求做出回应，即在国际安全背景下推进网络空间负责任国家行为。

1. 在国家一级为加强信息安全和促进该领域国际合作所做努力

在国家一级为加强信息安全所做努力

日本已经为数据利用奠定了法律基础，包括《推进公共和私营部门数据利用的基本法》和经修订的《个人信息保护法》。政府还采取了这样一项政策，即通过网络空间与现实空间高度融合打造以人为本的社会，既能实现经济发展，又可解决社会问题。在这类情况下，网络空间目前正在积累由真实空间中的传感器和设备生成的大量数据并对这些数据进行分析。此外，在多个领域均可看到周期性出现和发展的这样一种现象，即真实空间提供了经由数据使用而增值的新产品和新服务。网络空间和现实空间不再是相互独立而是彼此互动的实体，因此之故，无法认为它们是独立的，应当将它们视为一个单一的不间断演变的有机实体。

网络空间和真实空间的统一极大增加了让社会富足起来的潜力。同时，这也增加了恶意行为者滥用网络空间的机会。真实空间中经济和社会损失或损害的风险预计将呈指数级扩散和加速增加。尤其是，冠状病毒病(COVID-19)的暴发似乎正在加速人类日益依赖信息和通信技术(信通技术)的趋势，同时加剧了恶意使用信通技术造成的风险和问题。人们越来越担心网络攻击和利用危机进行恶意网络活动的报道，包括攻击医疗机构和当局的勒索软件，以及针对医学研究设施的分布式阻断服务攻击。在这些情况下，必须确保作为经济社会基础的网络空间的安全，同时，必须确保网络空间的自主持续演进和发展，以实现社会的可持续进步和财富。

最近出现了这样一种趋向，即某些国家应对网络威胁的做法是，强调国家依恃其主导地位进行管控。然而，国家加强对网络空间的管控的后果是，自主、可持续的发展可能受到阻碍。因此，对所有各利益攸关方自主开发的当今网络空间，必须予以尊重，要确保网络安全，就必须与这些利益攸关方主动携手合作。基于这一认识，并考虑到 2020 年及以后各年的理想状况，日本在网络安全措施方面将会竭尽全力，明确阐述网络安全基本愿景，确定需要解决的新问题，并迅速落实相关措施。

在国家一级为促进国际合作所做努力

由于网络空间事件的影响很容易超越国界，海外网络事件总是会影响日本。日本将与世界各国政府和私营部门开展合作，以确保网络空间的安全，努力实现国际社会的和平与稳定以及日本的国家安全。为此，政府将积极促进国际讨论，努力就网络相关问题分享信息并形成共识。政府还将与外国分享专门知识，推动开展具体的合作与协作，凡有必要则将采取行动。此外，政府会积极参与国际讨论，以解决 2019 冠状病毒病暴发后出现的网络安全相关问题。

关于分享专门知识和协调政策，政府将通过关于网络安全的双边对话和国际会议，交流关于网络安全政策和战略以及应对系统的信息，并将利用这些知识规划日本网络安全政策。我们还将加强我们在网络安全政策方面与在网络安全方面有着相同基本原则的战略伙伴的合作与协作。

关于事件应对方面的国际协作，政府将分享关于网络攻击和威胁的信息，并加强计算机应急小组之间的合作，以便在事件发生时能够做出协调一致的回应。政府还将通过联合培训和参与国际网络演习，努力提高协调应对能力。此外，政府将通过适当的国际合作对事件做出适当回应。

鉴于网络相关国际合作所涉外交方面的情况，我们所持的承诺由三个支柱组成：法治、建立信任措施和网络空间能力建设。

促进法治对于国际和平与稳定及日本的国家安全均有重要意义。日本的立场是，包括《联合国宪章》在内的现行国际法也适用于网络空间，日本将积极促进讨论现行国际法的个别和具体适用以及规范的发展和普遍适用。关于打击网络犯罪的措施，日本警察厅及其他相关部委和机构将利用《网络犯罪公约》、司法协助条约和国际刑事警察组织(国际刑警组织)等框架，与国际组织以及外国执法机构和安全情报机构开展国际调查合作和信息共享，以此协作进一步促进国际伙伴关系。

日本将努力在各国之间建立信任，以防止网络攻击的发生。由于网络攻击具有匿名性和保密性，而可能会无意中加剧国家间的紧张并使局势恶化。为防止出现此类意外和不必要的对抗，必须在和平时期加强国际沟通渠道，为应对发生超越国界的事件做好准备。还有必要通过在双边和多边协商中开展积极的信息交流和政策对话，在国家间增强透明度并建立信任。政府还将与其他国家合作，考虑建立一个网络空间问题协调机制。在这方面，日本热切推动建立信任措施，包括发起设立和共同主持东南亚国家联盟(东盟)网络安全领域区域论坛闭会期间会议，同时主要在亚太地区稳步实施能力建设援助。

在能力建设方面，随着跨境相互依存的加深，日本不可能单凭一己之力确保和平与稳定。全球协同减少和消除网络安全漏洞是确保日本国家安全的关键。从这一观点来看，协助其他国家开展能力建设可以确保在这些国家并依赖于这些国家关键基础设施的日本居民的生活和日本公司的活动保持稳定性，并可确保这些国家网络空间使用的健康发展。同时，能力建设也直接关系到确保所有网络空间的安全，有助于改善包括日本在内的整个世界的安全环境。此外，在网络犯罪领域，日本是第一个批准《网络犯罪公约》的亚洲国家，并在推动该公约方面发挥了积极作用，该公约是亚洲地区通过能力建设协助打击网络犯罪的重要法律框架。

2. 政府专家组各项报告所述概念的内容

日本认为，所有各国均考虑到由政府专家组确定的以下概念是有效和有意义的。

恶意网络行为对国际社会的影响

为了将信通技术的迅速发展灵活纳入我们的生活，并防止恶意网络行为造成的损害，我们应该认识到，预见网络空间现有和潜在威胁以及国际社会可能受到这些威胁的影响的重要性。

落实自愿非约束性负责任国家行为规范

为了最大限度地减少恶意网络行为的影响并对恶意网络行为实施人形成威慑，我们应该回顾协商一致的政府专家组报告的重要性，包括报告所述自愿和非约束性负责任国家行为规范。我们应该与有关地区性组织合作开展深入讨论，以切实有效利用这些重要努力。

促进执行自愿非约束性负责任国家行为规范，并就相关建立信任措施和能力建设开展合作

为进一步加强各国在国际安全背景下开发和维护自由、公平、安全的网络空间所做努力，我们应该重申，各国都有消除网络空间安全漏洞并防止利用恶意网络行为牟利的强烈愿望。这方面，小组成员应始终鼓励所有各国稳步执行建立信任措施等自愿非约束性负责任国家行为规范，并通过包括下一个政府专家组和不限成员名额工作组进程等开展合作，给各国能力建设工作提供支持，以执行上述规范和建议。

墨西哥

[原件：西班牙文]
[2020 年 5 月 29 日]

信息技术以及电信方面新发展让可持续发展和实现基于权利、公平与包容的世界有了更多的可能性。整个国际社会都有义务确保为了共同的利益和平利用这些技术。

联合国关于网络空间稳定、网络安全和网络空间治理的讨论，特别是从国际安全角度来看信息和电信领域发展的政府专家组关于推进网络空间负责任国家行为的报告，为逐步实现开放、自由、稳定和安全的网络空间奠定了基础。

根据这些先例，墨西哥政府提交本报告的前提是：大会通过的决议有其价值，以及唯有多边做法方能长期确保对网络空间的合法与和平利用、数字环境中的适应力、信息技术作为可持续发展的推动力量的潜力以及网络空间中的人权保护。

1. 信息技术在在国家一级为加强信息安全和促进该领域国际合作所做努力

墨西哥政府建立了以信息安全为重点的以下国家协调机制和应对机构：

(a) 信息安全专门委员会

机构间合议机构，负责制定适用于国家安全机构的信息安全政策，并确保加以适当执行。墨西哥侧重国家安全、公共安全、电信、金融部门和外交政策的联

邦机构均派代表参加了该委员会。委员会采取的举措例如包括设计和更新国家网络安全战略、举行计算机安全事件应对演习及开展信息安全相关提高认识活动。

(b) 国家网络安全事件应对中心

该机构隶属于新成立的墨西哥国民警卫队，负责监测墨西哥战略技术基础设施的完整性。该中心设有专职预防和调查使用计算机从事非法行为的单位，对网络实施监测以查明犯罪行为，并开展旨在减少和减轻对网络安全的威胁和攻击风险的活动。它还实施网络安全相关科技发展计划。

(c) 敏感信息安全事件应对小组

旨在有效应对金融部门信息安全事件的协调机制。总检察长办公室、墨西哥的国家金融主管机构和金融部门的工会均参与了该机制，其目的是有效应对直接影响金融部门的事件。

在国家一级，墨西哥近年来采取了以下举措来加强信息安全：

墨西哥政府通过安全和公民保护部主办一年一度的国家网络安全周。该活动的目的是，鼓励就促进网络安全展开对话，并促成相关部门间合作，以确保有一个安全和有抵御力的数字环境。该活动还旨在通过会议、小组讨论、培训、讲习班、网络研讨会和娱乐活动提高对信息技术和数字安全的认识。

自 2018 年以来，墨西哥政府与美洲国家组织(美洲组织)和趋势科技公司合作，主办了名为“妇女面临的网络挑战”的年度活动。该活动的目的是，在在与防范和应对网络安全威胁相关的活动中促进性别平等，并加强相关机构的能力。

2019 年，通信和运输部举行了网络安全工作组会议，来自该部全国各地的数字包容中心的 5 000 多人参加了会议。这些会议侧重于查明电信和广播服务使用方面的高风险行为。从会议中收集的信息被用作关于 2019 年墨西哥用户网络安全习惯的报告的素材。

根据该报告所载调查结果，在美洲组织和联合王国政府支持下，开发了一个模拟器。模拟器这一工具，能让用户在交互式环境中体验模拟网络安全威胁，以评估其应对此类威胁的能力，并就最佳保护方法提出建议。

为协助推进国际合作和网络空间负责任国家行为，墨西哥参加了以下多边和区域论坛、机制和倡议：

(a) 联合国大会第一委员会

墨西哥参加了根据大会第 73/27 号决议设立的从国际安全角度来看信息和电信领域发展的不限成员名额工作组。

此外，墨西哥的一名政府专家参加了根据大会第 73/266 号决议设立的从国际安全角度推进网络空间负责任国家行为政府专家组。

墨西哥努力确保这两个机构的运作互为补充，并认识到这两个机构都将在大会以协商一致方式通过的以往政府专家组工作及其报告基础上继续努力。

(b) 数字技术之友小组

墨西哥十分重视在数字技术相关活动上的规划与合作，特别是促进积极利用信息和电信技术以协助实现可持续发展目标和具体目标的活动。因此，自 2019 年 11 月以来，墨西哥协同芬兰和新加坡共同担任数字技术之友小组的主席，该小组的目的是，促进与所有利益攸关方的包容性对话，以审议数字技术与可持续发展之间的联系，并讨论相关跨领域国际合作。

(c) 联合国秘书长数字合作高级别小组

根据数字合作高级别小组的建议，墨西哥与联合国促进性别平等和增强妇女权能署(妇女署)一道，牵头举行了一次小组讨论，旨在确定执行关于数字包容和相关指标的建议 1(c)和 1(d)的具体步骤。

(d) 国际电信联盟

墨西哥参加了由国际电信联盟协调的信息安全和网络安全相关举措，例如全球网络安全议程和全球网络安全指数。

墨西哥认为《全球网络安全议程》是一项重要举措，有助于逐步建立一个更安全并且更有抵御力的数字环境，其根本意义在于让包括国家、私营部门、民间社会和学术界在内所有各利益攸关方都有了参与的机会。

(e) 美洲国家组织

墨西哥积极参与美洲组织美洲反恐怖主义委员会的网络安全方案，该方案促进了该区域的政策制定、能力发展、研究和外联。

国家网络安全事件应对中心在美洲组织美洲反恐怖主义委员会网络安全方案的框架内，参加了美洲计算机安全事件应对小组网络。

墨西哥还参加了美洲组织美洲反恐怖主义委员会网络空间合作和建立信任措施工作组。该小组成立于 2018 年，通过其工作，采取了以下建立信任措施：

- 提供关于诸如国家战略、白皮书、法律框架和各成员国认为有关的其他文件等国家网络安全政策的信息。
- 确定能够讨论半球网络威胁所涉影响的政策层面的国家联络点。
- 如果外交事务所涉各部未设有联络点，则指定促进网络安全和网络空间国际合作与对话的联络点。
- 通过针对公共和私营部门官员的网络外交研讨会、会议和讲习班等活动，逐步开展和加强能力建设。
- 推动把网络安全和网络空间相关主题纳入外交官和外交事务所涉各部及其他政府机构的官员的培训课程。
- 建立工作组及其他对话机制及签署国家间协议，以推动网络外交、网络安全和网络空间方面的合作并交流这方面的最佳做法。

(f) 网络专业知识全球论坛

墨西哥自 2015 年以来参加了这个致力于网络安全能力建设的论坛。墨西哥感兴趣的领域有：预防网络攻击、数据保护、预防网络犯罪(包括儿童色情及类似犯罪)、电子政务举措和数字战略、保护关键基础设施、和平利用信息和通信技术及互联网，以及国际法对网络空间的可适用性。

(g) 事件应对和安全小组论坛

国家网络安全事件应对中心是事件应对和安全小组论坛的成员，它是一个汇集世界各地网络安全事件应对小组并促进其相互间合作的全球论坛。经由该论坛得以开展并加强研究，并将研究结果连同其他国家网络安全政策一并用于查明和定位网络攻击的可能实施者。

2. 政府专家组报告所提及的概念的内容

根据政府专家组以往报告所载声明，墨西哥认为国际法适用于网络空间。为了维护这一原则，墨西哥政府在国家一级采取了支持其下述立场的各种举措：适用国际法是指《联合国宪章》、国际人权法、国际人道主义法、习惯国际法适用规范和相关判例法。

根据政府专家组以往报告，墨西哥认识到区域机构的潜在作用和贡献，特别是在执行建立信任措施方面。因此，墨西哥政府鼓励其国家机构考虑执行政府专家组报告中所述并在美洲组织工作中得到进一步发展的建立信任措施。

墨西哥十分重视政府专家组报告中强调的能力建设的概念，这一概念不仅指信息安全领域国家能力建设，还指需要利用已被证明有助于国际和平与安全的各种形式的国际合作。能力建设确保各国和所有其他利益攸关方得以更好应对网络安全威胁，并推动对网络安全相关问题达成共识。

在本报告所述期间，墨西哥政府还力求在侧重于信息技术、电信、网络安全、网络空间治理、数字合作和技术变革相关问题的联合国系统各团体、论坛、机构和倡议间实现协同增效，目的是提高一致性，避免工作重复，并善用资源以利合作。

新加坡

[原件：英文]
[2020 年 4 月 27 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的网络空间。关于此类法律、规则和规范的讨论必须继续在所有各国享有平等发言权的唯一普遍、包容的多边论坛联合国进行。

新加坡参加了从国际安全角度推进网络空间负责任国家行为政府专家组和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。新加坡重申它认为这两个平台互为补充，并再次表示将继续为这两个进程做出建设性贡献。这两个进程取得成功的前提是，必须本着建设性合作、共识、相互尊重和相互信任的精神开展工作。新加坡与爱沙尼亚同为电子政务和网络安全之友小组的主席，作为共同主席，新加坡将致力于争取所有各国均支持这两个进程的工作。新加坡认为，由新加坡网络安全局局长戴维·科主持的不限成员名额工作组非正式闭会期间协商会议有助于促进会员国、私营部门、民间社会、学术界和技术界就一系列实质性问题进行互动式交流。

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。新加坡支持需要时对此类规范加以完善。举例说，超国家关键信息基础设施[11] 可被视为此类关键基础设施的一个特殊类别，保护此类设施是所有会员国的共同责任，可被纳入现有的一套规范。

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。

能力建设对确保各国逐步建立成功实施负责任国家行为规则和规范的能力至关重要。作为该努力的一部分，新加坡 2016 年建立了一个 1 000 万新元的东盟网络能力方案，以给东盟在网络政策、战略和技术问题上的能力建设提供支持。迄今为止，来自东盟成员国的 170 名官员在该方案下接受了培训。作为东盟网络能力方案的延伸，新加坡于 2019 年 10 月启动了耗资 3 000 万新元的东盟-新加坡网络安全英才中心，以进一步支持东盟国家的网络安全政策制定、战略制定以及技术和业务能力，并与国际伙伴进行更密切接触。

新加坡还在联合国-新加坡网络计划下共同组织了一次研讨会，以提高东盟成员国对网络规范和网络场景政策规划的认识。此外，新加坡与裁军事务厅合作开发了一个向联合国所有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(信通技术)的使用及其对国际安全的影响的理解。新加坡还在新加坡合作计划下推出了几门网络安全培训课程。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、创建更安全网络空间和发展有活力网络安全生态系统：

[11] 超国家关键信息基础设施是由私营公司拥有并且跨国界运营但不受任何单个国家管辖的关键信息基础设施。

(a) *建设有抵御力的基础设施*。新加坡网络安全局制定了《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。总计划旨在改善跨部门应对措施，以减轻运营技术环境中的网络威胁，并加强与行业和利益相关方的合作伙伴关系。运营技术网络安全总计划提出了涵盖人员、流程和技术等领域的关键举措，旨在提高关键信息基础设施所有者和使用运营技术系统各组织的能力。

(b) *创建一个更安全的网络空间*。作为为更好保护网络空间和提高网络安康水平所做努力的一部分，新加坡将在 2020 年为联网智能设备引入网络安全标签计划。网络安全标签计划将会自愿推出，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。消费者可以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) *开发一个有活力的网络安全生态系统*，新加坡认识到，加强网络安全涉及逐步建立网络生态系统并在行业内部鼓励创新。此外，越来越需要培养一批能够在组织中担任网络安全领导角色的人才。自 2015 年成立以来，网络安全局一直与新加坡的政府机构、协会、行业合作伙伴和高等院校合作，以拓宽和壮大网络安全工作人员队伍。网络安全局正在牵头开展一项新的国家网络人才计划，以吸引和从小培养崭露才华的网络安全爱好者，并帮助网络安全专业人士提高技能。新加坡政府网络人才计划的目标是争取在三年内达到至少 20 000 人。

土耳其

[原件：英文]
[2020 年 5 月 22 日]

为加强信息安全和促进国际合作而在国家一级所做努力

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。在此背景下，在交通和基础设施部的协调下，通过让所有相关利益攸关方参与研究小组，制定了国家网络安全战略和行动计划。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》。土耳其一直在制定下一个国家网络安全战略和行动计划，该计划涵盖 2020-2023 年，并将很快予以公布。

土耳其下一个国家网络安全战略和行动计划的主要战略目标是：

- 保护关键基础设施并提高其抵御力

- 能力发展
- 新技术的安全性(物联网、5G、云计算等)
- 打击网络犯罪
- 开发和促进使用本国技术
- 有机网络安全网络
- 改善国际合作。

此外，自 2013 年以来，隶属于信息和通信技术管理局的土耳其国家网络应急小组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响应(包括事件发生前、发生期间和发生后)，国家网络应急响应小组还负责实施针对网络威胁的预防措施，并确保网络威慑。它在网络安全方面的主要重点领域是：网络能力建设、技术措施、威胁情报收集和共享以及关键基础设施保护。

在改善国家网络安全背景下，自 2013 年以来，还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 个部门网络应急小组，并建立了 1 299 个机构网络应急小组。它们都在国家小组的协调下一周七天、一天 24 小时运作，以减轻网络风险和打击网络威胁。

国家网络应急小组组织并支持面向多个社区的网络安全培训课程、夏令营和竞赛。此外，它还为网络应急响应团队提供在诸如恶意软件分析、日志分析等领域的培训课程。在过去三年里，国家网络应急小组已经对 4 500 多人进行了网络安全不同方面的培训。

技术措施研究包括早期检测、警报和预警活动。为此，土耳其开发了检测和预防系统。这些系统在提高土耳其国家网络安全水平方面发挥了巨大作用。

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

此外，每年都组织一次安全互联网日，开展有意识地安全使用互联网的宣传活动。已经开通互联网帮助热线和网站安全网(https://www.guvenlinet.org.tr/)，家庭可以在此寻找有效使用互联网的建议。

随着信通技术在个人之间的传播，个人信息或数据已成为网络攻击者的一个有吸引力的目标。个人数据的隐私和保护也是主要的安全问题之一。在这方面，关于保护个人数据的第 6698 号法律于 2016 年生效，目的是保护隐私。

土耳其在许多组织中发挥了重要作用，要么是创始成员，要么就是为网络安全和信息安全问题上的合作努力做出贡献。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。土耳其国家网络应急小组是事件相应和安全小组论坛、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和网络安全共同进步联盟的成员。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英才中心。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，这些组织包括如北约、联合国、欧洲安全与合作组织、经济合作与发展组织、20 国集团、突厥语国家合作委员会和区域军备管制核查和执行援助中心的安全合作中心。

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管理局在土耳其安卡拉共同举办了 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互进联盟的支持。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。

土耳其还批准了《网络犯罪公约》，该公约涵盖各种犯罪，如通过互联网和其他计算机网络实施的犯罪、与计算机有关的欺诈、儿童色情制品和侵犯网络安全等，这些犯罪现已被纳入土耳其的国家立法。

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。可以清楚地看到，国际法以及政府专家组报告和相关研究报告所述规范和规则有助于建立一个更安全的网络空间。

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

此外，应予考虑的另一点是，需要就新一代技术(物联网、5G、云计算等)的安全提供指导)。会员国合作编写的新一代技术指南或基线安全建议将有助于提高应对随之而来的新的网络威胁的准备水平。此外，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。

乌克兰

[原件：英文]
[2020 年 5 月 29 日]

自俄罗斯联邦对乌克兰的混合侵略开始以来，出现了新的威胁和挑战，其中利用网络影响机制损害乌克兰国家安全占据了重要位置。

乌克兰在使用信息和通信技术(信通技术)方面对国际法所持承诺继续毫不动摇，并仍然坚定不移地全力支持政府专家组报告所载结论和建议。国际法首先是指维护国家主权平等、不使用或不威胁使用武力侵犯国家领土完整、不干涉他国内政以及尊重人权和基本自由。

为了组织有效行动以对付网络空间的威胁和对网络空间行为实施法律监管，在扼要阐述完善国家一级对付这种威胁的行动系统的同时，通过了一些条例，主要是经国家安全和国防委员会批准的《乌克兰网络安全战略》；关于乌克兰网络

安全战略的决定(由乌克兰总统 2016 年 3 月 15 日第 96 号法令颁布)和 2017 年 5 月 5 日《关于维护乌克兰网络安全基本原则的法律》。

应对网络威胁的另一个机制是利用 2014 年 8 月 14 日《乌克兰制裁法》的规定，通过对参与旨在损害乌克兰国家安全的措施的一些法律实体和个人采取限制性措施，而有可能对已查明威胁做出快速反应。

今天，对乌克兰国家电子信息资源和关键基础设施的网络保护是根据《关于维护乌克兰网络安全基本原则的法律》进行的。该法律对网络安全主体的权力、任务和职能的界定有助于建立一个统筹全局的网络安全体系。

在这方面，制定网络安全和网络防御领域公共政策的基本原则是制定符合国际做法和标准的监管框架。为执行这项任务，尤其采取了以下措施：

- 乌克兰政府关于批准关键基础设施网络保护一般要求的决议获得通过；该决议所界定的网络安全做法考虑到信息安全领域国际标准的要求，并执行了欧洲联盟的指令，从而使国家成为全球安全领域的平等参与者
- 乌克兰政府的决议草案已经拟定
  - 关于批准对关键信息基础设施、国家信息资源和信息提供网络保护状况的审查程序，网络保护要求由法律规定
  - 关键基础设施指定程序的批准
  - 关于批准关键信息基础设施清单编制程序、将关键信息基础设施纳入关键信息基础设施及其形成和运作国家登记册，同时考虑到欧洲议会和理事会关于整个欧盟网络和信息系统高度共同安全措施的(EU)第 2016/1148 号指令的要求
  - 批准《网络安全实体和关键信息基础设施所有者(管理者)在发现、预防和停止网络攻击和网络事件以及消除其后果方面采取联合行动的议定书》。

为加强信息的技术和密码保护系统，经调整乌克兰法律以适应欧洲联盟的立法要求，提出了在信息保护领域进行改革的路线图；为实施这一路线图，乌克兰制定了一项关于信息安全、通信和信息系统的法律草案。

有效完善国家网络安全系统的关键要素之一是审查网络安全的状况。将基于审查结果，制定新的国家网络安全战略或调整现有战略，以改善网络安全实体监管框架，为国家信息资源和关键基础设施网络保护措施筹集资源，改善网络安全人力资源培训系统，制定在该领域开展公私合作的新做法，加强网络安全主体间的信息交流及其在解决安全问题方面的互动。

此外，为加强信息安全，促进这一领域的国际合作，国家特种通信局提供了：

- 乌克兰政府计算机应急小组的运作，小组得到了网络事件应对小组论坛的认可，并与来自 96 个国家的其他小组进行互动

- 由国家控制网络空间保护以及国家信息资源和信息的技术保护的条件，并依法对这种保护作出规定
- 使用欧洲安全与合作组织网络安全通信网，参加国家联络点会议
- 提高公众认识，并为国家网络安全系统主题举办关于网络安全的实用研讨会
- 与执法机构互动，及时通报网络攻击
- 根据乌克兰全国标准化委员会的 ISO/IEC 27001:2015，协调、组织和实施对关键基础设施的通信和技术系统的审计，对信息安全进行审计。

鉴于当前的挑战和威胁，乌克兰网络防御领域法律机制的形成旨在：

- 加强网络和信息系统的安全，其主要目的应该是有效保护信息和数据，确保网络和系统的稳定、功能连续，以及网络事故后检测、应对和尽量减少恢复的有效性；
- 实施风险管理系统
- 为提供资源创造条件，包括网络安全领域的人力资源
- 加强关键基础设施的运营和网络复原力
- 建立国家信息资源保留制度，确保技术信息得到保护，这对关键基础设施的运作至关重要
- 通过加入相关协定(关于承认信息技术安全领域通用标准证书的安排)，加入共同标准委员会，这将确保乌克兰的认证产品纳入欧盟国家和该领域其他领先国家承认的登记册
- 确保管理重要信息基础设施的机构负责人严格遵守国家信息资源保护、信息加密和技术保护(包括个人数据保护)领域的立法要求
- 利用公私合作和利益相关方互动的机会，解决网络防御和网络安全问题
- 提高互联网上的行为文化水平
- 积极参与国际社会的相关倡议，加入主要国际组织的相关结构。

在 2015 年至 2020 年，乌克兰国家安全和国防委员会每年通过“关于适用个人特别经济和其他限制性措施(制裁)”的决定，经乌克兰总统颁布相关法令后执行。

此外，乌克兰安全局作为网络安全的主要主体之一，根据法律规定的权限，正在采取措施改善网络空间的国内监管框架。特别是，定期开展工作，旨在确定执行《乌克兰关于网络安全基本原则法》所需的条例。

正在采取措施，将《乌克兰关于网络安全基本原则法》的规定落实到管理乌克兰安全局活动的监管框架。

不过，尽管采取了这些措施，改进信息和网络安全领域监管框架的问题今天仍然具有现实意义。

具体而言，安全局的一些立法举措长期以来一直由前一届议会的乌克兰最高拉达审议，但没有得到乌克兰议员的审议(加强对网络犯罪刑事责任的追究、划分对乌克兰安全局和国家警察各自的调查权限、确定不遵纪守法的责任)。

《网络犯罪公约》的规定尚未充分执行。

乌克兰最高拉达于 2005 年 9 月批准了 2001 年 11 月 23 日《欧洲委员会关于网络犯罪的公约》。《公约》条款规定了侵犯计算机数据和系统的保密性、完整性和可用性的刑事责任，即：非法访问；非法拦截；数据干扰；干预系统；滥用资金。也即，《公约》这些条款涵盖了危害关键基础设施可持续运行的罪行。

然而，《网络犯罪公约》的一些条款目前没有在国家立法中得到执行，这限制了执法机构侦查和预防网络犯罪的活动。具体而言，它们需要执行《网络犯罪公约》关于紧急存储已储存的计算机数据、紧急存储和部分披露关于信息流动、提交、搜索和扣押已储存计算机数据程序的信息，收集关于实时信息移动的数据的规定(第 16-20 条)，以及乌克兰《刑事诉讼法》修正案，单独设立一个证据类别，即刑事诉讼中的数字证据。

目前，最高拉达执法委员会工作组中乌克兰安全局代表正在起草乌克兰“关于执行《网络犯罪公约》的某些法案的修正案”的法律，以便在乌克兰立法中使公约条款标准化，改进乌克兰《刑事诉讼法》的条款，建立打击网络犯罪的有效法律机制，包括：

- 授权业务单位负责人、调查员、检察官向计算机数据所有人(电信运营商和提供商、其他法律实体和个人)发出强制指令，要求紧急存储解决犯罪所需的计算机数据，最长 90 天
- 应执法机构的请求，规定向电信运营商和提供商提供必要信息的要求，以确定服务提供商和信息传输的路线
- 采用有效机制，在刑事诉讼中使用电子(数字)形式的证据
- 《乌克兰产品总分类》和《乌克兰电信法》修正案和(或)《乌克兰电子通信法》草案，确保建立法律机制，暂时限制对张贴在某一(确定的)信息资源(服务)上的信息或计算机数据的访问，并确定其实施程序。

2020 年 2 月 4 日，乌克兰最高拉达撤销了乌克兰《电子通信法》草案(第 2264 号)，去年年底，乌克兰安全局通过最高拉达数字转换委员会向其提交了意见和建议。

2020 年 2 月 5 日，在乌克兰最高拉达登记了一份标题相同的法律草案(“关于电子通信”)和一个几乎相同的编纂团队，编号为第 3014 号。根据初步分析，新的法律草案也不包含有助于全面执行《网络犯罪公约》规定的条款。

今年，为解决网络安全领域的当前问题，乌克兰安全局支持提出一项立法举措，由最高拉达第九届会议审议若干法案；这些法案通过后，将根据《乌克兰网络安全基本原则法》为安全局奠定法律基础。

特别是，国家警察调查人员与负责调查在使用计算机、系统、计算机网络和电信网络、国家信息资源和重要信息基础设施领域所犯罪行的安全当局之间的法律区别，以及加强这些犯罪的处罚。

执行关于预防、侦查、制止和披露在网络空间犯下的危害人类和平与安全的罪行的任务，执行旨在打击网络恐怖主义和网络间谍活动的反情报和行动调查措施，需要修订乌克兰“反情报”法的部分内容，充实乌克兰安全局各机构、分支机构和雇员的职能和权力。

此外，建立国家关键基础设施保护体系的原则和方向尚未在立法层面上确立，国家关键基础设施也未在规章制度层面上界定(《关键基础设施实体清单》和《关键信息基础设施实体清单》尚未形成)。

去年，政府批准了《关键基础设施网络保护的总要求》(乌克兰内阁 2019 年 6 月 19 日第 518 号决议)。在没有国家《关键基础设施清单》和《关键信息基础设施清单》的情况下，这项法律无效，其存在是由《乌克兰关于网络安全基本原则法》规定的。

国家关键基础设施不确定，使分配给乌克兰安全局和其他网络安全行为体的网络安全和网络安全任务的执行复杂化。

2019 年 12 月 23 日，乌克兰最高拉达数字转换委员会就“乌克兰国家网络安全和网络防御，包括在关键基础设施领域”这一主题强调，需要确保制定和通过《关键基础设施及其保护法》，加快通过乌克兰内阁法案，执行《乌克兰关于网络安全基本原则法》条款。

在 2020 年 2 月 19 日举行的最高拉达数字转换委员会会议上，分别听取了适用《乌克兰关于网络安全基本原则法》和通过实施该法律所需的条例的问题。

仍然存在一个实际问题是，在减少国内机构、组织和企业对外国软件的严重依赖方面仍未制定法规，而这些软件可能包含故意植入的漏洞和未记录的功能。

据乌克兰安全局专家称，这需要在信息化领域制定一项国家进口替代计划，一套支持国内软件生产商的措施，以及创建：

- 关键信息基础设施的经核实的软件供应商登记册，准备将其列入/排除在特定登记册之外的程序
- 推荐在关键信息基础设施中使用的专有软件的登记册
- 免费软件的国家存储库，加强国家程序的实施，以便转交公共权力，并管理其使用。

此外，为了建立一个立法程序，立即有效地应对信息和通信技术领域里对乌克兰国家利益和安全的现有和潜在威胁，采取措施，限制使用侵略国经济实体开发/制造的所有形式的所有权软件(包括反病毒软件)和电信设备的关键基础设施，需要对《乌克兰制裁法》进行适当修正。

造成负面影响的另一个因素是国内立法不完善，缺乏一个法律界定的机制来阻止用户访问互联网资源，删除包含非法信息的内容。

还应指出，乌克兰安全局在加强信息和网络安全领域开展国际合作措施。根据乌克兰网络安全战略，主要优先事项和方向是：

- 发展网络安全领域的国际合作
- 支持网络安全领域符合乌克兰国家利益的国际倡议
- 深化乌克兰与欧盟和北约的合作，加强乌克兰的网络安全能力
- 参与在欧洲安全与合作组织主持下的网络空间建立信任措施。

特别是，乌克兰安全局在其职权范围内，参与欧洲联盟和欧洲委员会为东部伙伴关系国家开展的联合项目“网络东方”的活动，旨在执行立法和政策决定，实施《布达佩斯网络犯罪公约》的规定。“网络东方”项目由欧盟邻里和扩大谈判总局与欧洲委员会网络犯罪办公室共同实施。

乌克兰安全局代表强调，向国际伙伴通报乌克兰在网络安全领域的最新成就，以及根据欧安组织常设理事会在信通技术使用和信通技术领域的第 1039、1106 和 1202 号决定执行某些建立信任措施的重要性，通常参加欧安组织信通技术工作组会议。此外，乌克兰安全局还在实现第 1202 号决定第 8 号建立信任措施的框架内，确定了一个技术联络点，在专业一级开展计划内和计划外的沟通检查活动。

乌克兰安全局还加入了欧安组织项目，其主要目的是详细分析网络安全领域的国家治理结构，根据第 1202 号决定的规定，执行乌克兰在信通技术/网络安全领域的建立信任措施。

此外，根据分配给乌克兰安全局的任务，在乌克兰-北约网络安全信托基金的支持下，获得了必要的设备，成立了乌克兰安全局网络安全情况中心，旨在：

- 预防、侦查、制止和侦查在网络空间犯下的危害人类和平与安全罪
- 开展反情报和行动搜索措施，打击网络恐怖主义和网络间谍活动
- 验证关键基础设施对可能的网络攻击和网络事故的准备情况
- 打击其后果可能威胁国家重大利益的网络犯罪
- 调查对国家电子信息资源、关键信息基础设施的网络事件和网络攻击
- 确保应对国家安全领域的网络事件。

乌克兰安全局还利用恶意软件信息共享平台及威胁共享“乌克兰优势”，就网络威胁、网络攻击和网络事件的信息交流开展合作，这是乌克兰安全局与关键基础设施、其他企业、机构、组织(无论所有权如何)以及个人之间就改善用户信息、电信和信息及电信系统安全问题进行合作的公开提议，根据相关协议或其他法律依据，他们有权确保对其给予保护。

阿拉伯联合酋长国

[原件：阿拉伯文]
[2020 年 5 月 31 日]

关于阿拉伯联合酋长国努力加强信息安全和促进国际网络安全合作的国家报告

导言

阿拉伯联合酋长国非常重视网络安全。防范利用信息和通信技术对基础设施、政府服务和个人构成严重威胁的攻击，是维护国家安全的关键。因此，阿拉伯联合酋长国努力创建一个综合系统，确保重要部门的安全，增强用户信心并激励创新。

在国家一级为加强网络安全所做的努力

启动了一项国家网络安全战略，目标是创造一个安全、灵活的数字环境，让个人实现自己的抱负，让企业成长。战略的目标包括五个主要领域：

1. 实施全面的法律和监管框架，应对网络犯罪，保护当前和新兴技术，使中小企业能够保护自己免受网络威胁；

2. 制定网络安全领域的综合提高认识和能力建设方案，鼓励在使用技术方面的安全做法，发展网络安全人员有效应对攻击和保护系统和服务的技能；

3. 制定有效的国家计划，以便在全国范围内对网络安全事件做出快速、协调的反应；

4. 保护重要部门的数字基础设施；

5. 加强地方和全球网络安全伙伴关系。

2006 年，阿拉伯联合酋长国通过了《信息技术犯罪法》，其中含许多条款，保护在基于信息和通信技术的媒体上发表和传播的私人材料，惩罚滥用此类媒体的行为。

阿拉伯联合酋长国多年来还启动了许多方案和举措来加强网络安全，包括建立国家计算机应急小组。小组向政府机构提供一系列服务，例如对基础设施进行 24 小时监测和检查，以便发现和直接应对任何异常活动或攻击；有效的网络安全事件响应；以及网站和移动电话应用程序的安全评估，以消除可能被利用或导致信息泄露的漏洞。小组还通过各种平台(包括其网站、社交媒体和邮件名单)向政府机构和个人提供定期安全咨询和重大网络攻击报告。

为确保国内所有重要部门采用最佳网络安全做法，建立了一个信息安全保障系统，为提高信息安全资产和支持系统的最低保护水平设定基准要求。

除了政策和技术系统之外，还需要加强人员的专业发展，提高他们对如何建设性和安全地使用信通技术的认识，使他们成为抵御网络攻击对其国家和家庭的威胁的第一道防线。考虑到这一点，启动了国家网络安全意识和能力建设方案，在社会中培养网络安全文化和国家网络安全能力。根据网络专业人员倡议，网络安全专业人员参加为期一个月的培训课程。还建立了一个提供同一领域课程的虚拟学院。定期为社会不同阶层举行公共宣传运动和活动。

考虑到儿童在线保护，卡通人物“萨利姆”在以轻松简单的方式向儿童传达安全使用技术的原则方面取得了巨大进展。除了与教育部合作建立的数字安全课程和启动“萨利姆”网站之外，还组织了数以千计的互动讲习班，通过讲故事教育儿童，其中让儿童担任主角。这些举措还让儿童通过网络安全大使倡议参与提高认识活动，通过该倡议，他们获得了在同龄人中传播信息的工具，并鼓励对这一问题采取安全、合理的方法。

努力加强国际网络安全合作

阿拉伯联合酋长国非常清楚，要实现最佳网络安全水平和应对攻击和风险的能力，需要国际合作和严肃的态度。因此，它努力积极参与所有国际网络安全论坛，其中一些将在下文提及。

阿拉伯联合酋长国是国际电信联盟(国际电联)成员，并与其他成员国合作，通过相关的研究委员会和工作组寻找解决方案，确定最佳网络安全做法。它感到高兴的是，它的一些专家在联盟中担任重要职务，例如担任国际电联理事会儿童在线保护工作组组长，这突出表明阿联酋致力于支持在这些重要问题上的全球努力。

阿拉伯联合酋长国派代表参加伊斯兰合作组织计算机安全事件响应小组，该小组通过制定方案、手册和其他关于机构和个人安全风险的基本材料来提高网络安全意识。小组还积极参与阿拉伯区域网络安全中心和海湾合作委员会国家计算机应急中心委员会。

除了与国际论坛和组织合作之外，阿拉伯联合酋长国还热衷于加强与友好国家的双边网络安全合作，签署谅解备忘录和协议，规范国家之间的信息和专门知识交流以及应对网络攻击的合作。

对政府专家组报告中提到的概念内容的看法

阿拉伯联合酋长国谨感谢政府专家组关于从国际安全角度看信息和电信领域发展的报告。它同意专家组的结论，即各国必须努力防止有害的信通技术做法，合作应对网络攻击，支持基于透明度和联合行动的对话，支持数字基础设施的全球发展，并就网络安全立法、战略和系统的发展进行协商。

三. 从国际组织收到的答复

欧洲联盟

[原件：英文]
[2020 年 5 月 20 日]

网络空间，尤其是全球开放的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。欧盟及其成员国支持一个全球、开放、稳定、和平和安全的网络空间，在这个空间里，人权和基本自由以及法治都得到充分适用，以期实现自由民主社会的福祉、经济增长、繁荣和完整。

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同样问题也在网络空间中出现。在国际背景下，一些国家似乎接受了网络空间中由政府高度控制的愿景，这引起了对侵犯人权和基本自由的关切。国家和非国家行为者的恶意网络活动也在增加，令人担忧。欧盟及其成员国经常对这种破坏注重规则的国际秩序并增加冲突风险的恶意活动表示关切。

(a) 在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，推进和实施一个包容、多层面的网络空间预防冲突和稳定的战略框架，包括通过双边、区域和多方利益攸关方的参与。作为这一战略框架的一部分，欧盟努力加强全球复原力，推进和促进对基于规则的网络空间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重要因素，可以降低冲突风险，并作为应对与我们经济和社会数字化相关的挑战的一种手段。全球网络复原力降低了潜在犯罪人恶意滥用信通技术的能力，加强了各国有效应对网络事件并从中恢复的能力。

题为“开放、安全和有保障的网络空间”的网络安全战略[12] 以及下文引用的其他后续政策文件，代表了欧盟关于如何最好地预防和应对网络中断和攻击的全面愿景。这些措施旨在促进欧盟价值观，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中强调，[13] 必须进一步制定和实施欧盟网络外交的共同和全面方法，促进人权和欧盟基本价值观，确保言论自由，促进性别平等，促进经济增长，打击网络犯罪，减轻网络安全威胁，防止冲突，并为国际关系提供稳定。欧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，欧盟认识到与关键合作伙伴和国际组织合作的重要性。欧盟还强调在国际安全领域适用现有国际法，以及行为

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

[13] 理事会关于网络外交问题的第 6122/15 号结论。

规范的相关性，还有互联网治理作为欧盟网络外交共同和全面办法的一个组成部分的重要性。

根据对 2013 年网络安全战略的审查，欧盟在成员国和欧盟各相关机构的充分合作下，以协调一致的方式进一步加强了其网络安全结构和能力，同时尊重它们的权限和责任。2017 年，关于《弹性、威慑和防务：为欧盟建设强有力的网络安全》的联合通报[14] 阐述了挑战的规模和在欧盟层面设想的措施范围，以确保欧盟更好地准备应对不断增加的网络安全挑战。

对日益增长的网络安全挑战的担忧，推动了欧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。[15] 国家和非国家行为者通过恶意网络活动追求其目标的能力和意愿日益增强，这应引起全球关注。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，欧盟联合外交应对框架是欧盟网络外交方法的一部分，有助于预防冲突、减轻网络安全威胁和提高国际关系的稳定。框架鼓励合作，促进缓解当前和长期威胁，并从长计议，影响恶意行为者的行为。它还与欧盟危机管理机制适当协调，包括协调应对大规模网络安全事件和危机蓝图。欧盟及其成员国呼吁国际社会加强国际合作，支持一个全面、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。他们决心继续努力防止、阻止、遏止和应对恶意活动，争取加强这方面的国际合作。

欧盟的国际网络空间政策促进对欧盟核心价值观的尊重，界定负责任行为的规范，倡导在网络空间适用现行国际法，同时协助欧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。

(b) 政府专家组报告中提到的概念的内容

现有和新出现的威胁

欧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。

欧盟及其成员国对网络空间恶意行为的增加感到关切，包括国家和非国家行为者出于恶意目的滥用信息和通信技术，以及网络盗窃知识产权的增加。这种行为破坏和威胁经济增长，以及全球社会的完整、安全和稳定，并可能导致不稳定和连锁效应，增加冲突风险。

最近，随着冠状病毒病(COVID-19)大流行的持续，欧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)的重要运营商的网络威胁和恶意

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

[15] 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。

网络活动。欧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都是不可接受的，并会危及人们的生命。任何行为者都不应在网络空间进行不负责任和破坏稳定的活动。欧盟及其成员国呼吁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 年协商一致的报告，尽职尽责，对从其境内开展此类活动的行为者采取适当行动。欧盟及其成员国再次强调，各国不应故意允许其领土被用于以信通技术开展的国际不法行为，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以前报告所承认的那样，鉴于信通技术的独特性，我们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的概念和联合国的认可，包括新兴技术的使用。

欧盟及其成员国只能在充分尊重适用的国际法和准则，特别是《联合国宪章》，以及国际人道主义法及其衍生原则和人权的情况下，支持技术、系统或信通技术服务的开发和使用。

国际法如何适用于信通技术的使用

欧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，其在应对网络空间当前和未来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》、国际人道主义法和国际人权法。此外，欧盟及其成员国重申，现行国际法适用于 2010 年、2013 年和 2015 年联合国政府专家组报告所承认的国家网络空间行为，以及 2015 年政府专家组报告第 28(a)至 28(f)段所确立的原则。

国际法，包括国际人道主义法，包括预防原则、人道原则、军事必要性原则、相称性原则和区别原则，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的界限，也适用于冲突时期。欧盟强调，其坚信国际法不是行为的促成因素；相反，国际法界定了军事行动的规则，以限制其影响，特别是保护平民。

此外，相关国际文书所载的人权和基本自由必须在网上和网下得到同等尊重和维护。欧盟及其成员国欢迎联合国人权理事会[16] 和大会也确认了这些原则。

出于这些原因，欧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。

欧盟及其成员国重申，支持继续开展对话与合作，促进对现行国际法适用于各国使用信通技术的共同理解，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。

[16] A/HRC/RES/20/8。

我们继续支持目前的努力，促进现行国际法在网络空间的适用，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，因为它促进了透明度，促进了全球对国家方法的理解，这对维护长治久安，减少通过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，将其作为促进网络空间稳定和防止冲突的手段。

负责任国家行为的规范、规则和原则

欧盟及其成员国鼓励所有国家巩固和推进联合国大会一再认可的工作，特别是第 70/237 号决议，进一步执行这些在预防冲突中发挥重要作用的商定准则和建立信任措施。

欧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，在网络空间中执行这些准则、规则和原则，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。我们认为，切实可行的前行道路应鼓励加强合作和透明度，分享最佳做法，包括关于如何通过相关举措和框架(如区域组织和机构)，应用联合国政府专家组现行规范的最佳做法，促进提高认识，有效执行商定的负责任国家行为规范。

建立信任措施

在网络空间建立有效的国家合作和互动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，可以为有共同关切但有共同利益的行为者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、东盟区域论坛、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，降低因信通技术事件而可能产生的误解、升级和冲突的风险，从而促进网络空间的长期稳定。

信通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，欧盟及其成员国旨在加强全球复原力，特别强调发展中国家，以此应对与经济和社会数字化相关的挑战，降低潜在犯罪人出于恶意滥用信通技术的能力。复原力加强各国有效应对网络威胁并从中恢复的能力。

欧盟及其成员国支持一系列有针对性的方案和举措，以帮助各国发展应对网络事件的技能和能力，并支持通过直接接触、双边接触或通过区域和多边机构进行接触，来交流最佳做法的举措。

欧盟及其成员国认识到，促进足够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。