联合国 A/77/92

大 会

Distr.: General
8 June 2022
Chinese
Original: Arabic/English/Russian/
Spanish

第七十七届会议

暂定项目表* 项目 94

从国际安全角度看信息和电信领域的发展

# 从国际安全角度看信息和电信领域的发展以及促进使用信息和通信技术时的负责任国家行为

## 秘书长的报告

目录



* A/77/50。

22-08761 (C) 110722 270722

# 一. 导言

1. 2021 年 12 月 6 日，大会在关于“从国际安全角度看信息和电信领域的发展”的议程项目 95 下，通过了题为“从国际安全角度看信息和电信领域的发展以及促进使用信息和通信技术时的负责任国家行为”的第 76/19 号决议。

2. 在第 76/19 号决议第 6 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的发展不限成员名额工作组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的国际合作所做的努力；

(b) 不限成员名额工作组报告和政府专家组报告中提到的概念的内容。

3. 根据这一要求，2022 年 1 月 24 日向所有会员国发出一份普通照会，请各国提供有关该主题的信息。

4. 在提交报告时收到的答复载于文件第二和第三节。2022 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]
[2022 年 5 月 31 日]

### 在国家一级为加强信息安全和促进该领域的国际合作所做的努力

亚美尼亚政府成立了一个数字化委员会，以促进数字技能的发展以及公共行政系统和经济的数字化。根据 2021 年的数据，讨论了近 25 个方案和战略文件，在数字身份识别、官方文件认证、电子许可证、启用个人和公共通知、采用统一电子司法系统，以及数字议程上的若干其他问题方面正在持续开展工作。

亚美尼亚共和国于 2021 年 2 月 11 日批准了一项数字化战略。该战略设想通过引进和开发创新技术、网络安全、数据政策、电子服务和电子政务系统，协调数字化进程，界定共同标准和数字环境，以及促进私营经济部门使用数字技术的举措，并制定和实施促进公众使用电子工具的方案，实现政府、经济和社会的数字化转型。

计划在 2021-2025 年亚美尼亚数字化战略框架内采取以下举措：

(a) 进行信息安全领域的立法和规范性法律修订；

(b) 阐述公共开放数据政策概念；

(c) 对边境村庄居民进行网络安全培训(目前为国家雇员开设网络安全课程)；

(d) 建立国家网络安全中心。特别是，正在考虑引入网络安全标准、创建国家快速反应小组和开展提高网络素养的公共宣传活动的可能性。

高技术产业部计划制定一项全面的政策和行动计划，以克服网络安全领域的挑战，其中将包括创建网络安全中心的进程，以及在自然灾害、紧急情况和戒严期间建立风险管理和快速反应机制。

该部强调与私营部门密切合作、机构间合作、国际经验本土化和遵守国际网络安全标准、国家间合作和加入国际安全机构的重要性。

亚美尼亚正在与国际和区域组织一道发展网络安全领域的政策和能力，具体包括亚美尼亚相关机构参加各种专题研讨会、会议和培训。

亚美尼亚共和国是《欧洲委员会网络犯罪公约》缔约国。最近，亚美尼亚启动了签署《<欧洲委员会网络犯罪公约>关于加强合作和披露电子证据的第二附加议定书》的国家程序。

亚美尼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的工作。该工作组的独特设计是为信息和通信技术领域的新标准奠定基础。

欧洲委员会网络东方项目内正在进行的合作旨在建设亚美尼亚政府机构专家应对网络犯罪威胁的能力。

亚美尼亚还重视在欧洲安全与合作组织信息和通信技术领域建立信任措施的框架内持续努力，这有助于在该领域建立透明度、可预测性和稳定性。

同时，与超国家公司的合作值得注意。亚美尼亚境内设有领先的信息技术公司，如 Synopsys、Mentor Graphics、National Instruments、Microsoft、VMware、D-Link、Oracle、Cisco 等。微软和思科定期提供合作或参加论坛，支持亚美尼亚政府在网络安全和防御方面的最新发展。

## 澳大利亚

[原件：英文]
[2022 年 5 月 31 日]

澳大利亚欢迎有机会响应大会第 76/19 号决议的邀请，就推进网络空间负责任的国家行为向秘书长提供意见。本文件以澳大利亚根据大会以往决议提供的信息为基础，[1] 包括最近于 2021 年 5 月提供的信息(见 A/76/187)。澳大利亚鼓励所有国家积极主动地定期向秘书长提供最新情况，以提高透明度，增进对彼此努力促进网络空间负责任的国家行为的了解。

### 网络空间中负责任的国家行为框架

综合来看，从国际安全角度看信息和电信领域的发展政府专家组 2010 年、2013 年和 2015 年的报告[2] 确认，现行国际法对于维护网络空间的和平与稳定是适用的和必不可少的。报告还阐述了负责任的国家行为的 11 项自愿、不具约束

[1] 第 65/41、第 68/243、第 70/237、第 74/28 和第 75/32 号决议。

[2] 分别为 A/65/201、A/68/98 和 A/70/174。

力的规范，同时承认需要建立信任措施和协调能力建设。这四项原则合在一起，通常称为网络空间中负责任的国家行为框架。

澳大利亚感到高兴的是，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 月的报告(A/75/816)显示了对该框架的普遍承诺，该报告是由联合国所有 193 个会员国谈判并核可的。澳大利亚还高兴地有一名主要专家参加了关于从国际安全角度促进网络空间负责任的国家行为的第六届政府专家组，其就如何执行该框架提供了进一步的实际指导(见 A/76/135)，大会随后在第 76/19 号决议中对此表示欢迎。

澳大利亚重申致力于按照政府专家组和工作组的各项报告行事。澳大利亚仍然积极参与根据第 75/240 号决议设立的 2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，是法国和埃及关于制定一项行动纲领的提案的坚定共同提案国。澳大利亚支持制定一项行动纲领，为在联合国主持下就网络问题进行持续讨论和采取实际行动提供一个永久、包容和透明的论坛。

为透明起见，澳大利亚不久将公布一份关于其如何执行和遵守负责任的国家行为的 11 项自愿、不具约束力的规范的最新情况。虽然规范不能取代或改变国际法(具有约束力)规定的国家义务或权利，但澳大利亚重申，11 项规范是对国际法的补充，为在使用信息和通信技术方面什么是负责任的国家行为提供更多具体指导。澳大利亚还将在不久的将来，利用联合国裁军研究所的国家调查，通过联合国裁军研究所网络政策门户网站，公布其对我国执行联合国网络事务情况的初步自我评估。澳大利亚向所有国家推荐国家调查，并鼓励各国也考虑公开其自我评估。调查联合国建议的执行情况有几个好处。也即，各国可以确定它们如何实施该框架，实施中可能存在的差距以及实施中的任何障碍。这反过来又可能有助于制定有针对性的合作和能力建设方案，这可能有助于克服已查明的任何能力差距和(或)执行障碍。

### 国际法

澳大利亚鼓励所有国家继续研究国际法如何适用于网络空间的国家行为，并保持立场透明。我们重申，即使观点不同，就国际法在网络空间如何适用的问题增进对彼此立场的理解，也可以提高可预测性，减少误判风险；因为误判可能导致国家行为升级。澳大利亚进一步重申，当各国履行和遵守其国际法律义务，在必要时开展合作，维护国际法和确保追究违法行为时，国际法最为有效。

澳大利亚欢迎政府专家组 2021 年报告(A/76/135)所载的结论，即国际人道法适用于武装冲突情况下的网络活动。

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已在一系列文件中阐述：

- 澳大利亚 2021 年提交的文件载于《政府专家组中参与政府专家提交的关于国际法如何适用于各国使用信息和通信技术问题的国家自愿贡献正式汇编》(A/76/136)；

- 2021 年国际网络和关键技术参与战略；
- 2020 年网络空间国际法应用个案研究(提交给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)；
- 2019 年国际法补编；
- 2017 年国际网络参与战略。

澳大利亚除参与联合国关于国际法如何适用于网络空间的进程之外，还努力在区域论坛上参与此类讨论。在这方面，澳大利亚在 2021 年底亚非法律协商组织关于网络空间国际法的第五十九届会议上发表了声明。

### 威慑和应对不负责任的国家行为

澳大利亚不容忍网络空间中有害于国际和平与稳定或违背联合国所有会员国商定的框架的活动。澳大利亚鼓励国际社会揭露恶意网络活动，追究行为者的责任。澳大利亚有一项政策：如果来源已知，并且符合我国利益，将公开指认恶意网络活动。这项政策不针对任何一个国家。迄今为止，澳大利亚已经 13 次公开指认恶意网络活动。最近，2022 年 5 月 10 日，澳大利亚与美利坚合众国和欧洲联盟一道，将一系列针对乌克兰的破坏、扰乱和损害稳定的网络活动归咎于俄罗斯政府。

### 多利益攸关方参与

澳大利亚感谢 2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组组长布尔汗·加福尔作出建设性努力，就非政府利益攸关方今后参与工作组的一套透明和平衡的方式达成共识。澳大利亚期待这些模式在将于 2022 年 7 月举行的工作组第三次实质性会议上正式通过。澳大利亚坚定支持多利益攸关方参与讨论网络空间中负责任的国家行为。网络空间十分独特：私营部门、技术界、民间社会和学术界在其技术管理和治理中发挥着至关重要的作用，而多利益攸关方群体可以提供视角，帮助我们更好地了解新出现的网络威胁、其影响以及如何应对这些威胁。澳大利亚对一些国家试图阻碍利益攸关方参与这一进程感到失望，我们认为这违背了成立工作组的精神。澳大利亚认为，工作组有可能对许多利益攸关方产生深远影响，包括对社区和个人的直接影响；应对来自网络空间的威胁需要我们利用所有相关利益攸关方的经验、专门知识和资源。因此，澳大利亚欢迎商定模式，认为这是朝着透明度和包容性迈出的一步。

### 网络中的女性

正如妇女与和平与安全议程所确认，妇女和女童受到冲突和危机的独特和不成比例的影响，在国际和平与安全进程中代表不足(并被排除在外)。正如裁研所题为“仍然落后：军备控制、不扩散和裁军外交中的性别平衡”的报告所指出，第一委员会的进程远远落后于联合国其他委员会在实现性别均等方面取得的进展。裁研所的数据显示，在第一委员会的辩论中，27%的发言者是女性。在讨论更专业议题的论坛上，这一比例平均降至 20%。

为解决这一问题，澳大利亚与加拿大、荷兰、新西兰、大不列颠及北爱尔兰联合王国和美国一道，于 2020 年 2 月发起了妇女参与国际安全和网络空间研究金方案，为处于职业生涯早期至中期的女外交官提供多边谈判、网络政策和国际法方面的培训，赞助前往纽约加入其本国代表团，参加审议网络空间负责任的国家行为的联合国会议，包括工作组会议。

澳大利亚感到高兴的是，通过该研究金，许多人员得以加入其国家代表团参加工作组第一届和第二届会议，为工作组和推动妇女与和平与安全议程做出了重大贡献。在 2021 年 12 月举行的工作组第一届会议上，37%的发言者是女性。在 2022 年 3 月举行的第二届会议上，43%的发言者和一半的关于国际法问题发言者是女性。

## 阿塞拜疆

[原件：英文]
[2022 年 5 月 31 日]

近年来，阿塞拜疆通过了几项新法案，确保信息安全。除此之外，还通过了发展概念、战略路线图、国家战略和国家方案，并经阿塞拜疆总统法令和命令，建立了与各国的合作。

由于需要优先考虑关键信息基础设施的安全，通过了一项规范性法案，以加强这一领域的安全。根据这些基础设施的重要性对其进行分类，确定一般和特殊的安全要求，这在上述法律中得到了考虑；预计将通过采用适当方法进行持续管控。

根据阿塞拜疆总统命令，信息安全协调委员会于 2018 年成立。

为维持重要信息基础设施的安全，根据 2021 年 4 月 17 日阿塞拜疆总统令确定了机构间的权力划分。

为增强这一领域的人力资本，数字发展和运输部网络学院组织了各种培训班，并提供国家和国际证书。

在欧洲联盟和欧洲委员会的网络东方和网络安全东方联合方案框架内，国际专家为阿塞拜疆相关国家机构代表举办了关于保护个人数据、网络犯罪和电子证据的虚拟研讨会。

阿塞拜疆几个国家机构的代表参加了在韩国国际协力团赠款方案框架内举办的首次网络安全认证培训。

除上述之外，还与各国计算机应急小组开展了协商和合作举措。

在国际电信联盟的 2020 年全球网络安全指数中，阿塞拜疆在世界上排名第四十，在独立国家联合体中排名第三(仅次于俄罗斯联邦和哈萨克斯坦)。

由于 2019 冠状病毒病(COVID-19)大流行疫情期间网络威胁数量增加，以及查明的方案和技术设备的薄弱环节，关于防范网络威胁的方法的相关通知和信息已发布在 www.cert.az 和社交网络上。

# 古巴

[原件：西班牙文]
[2022 年 5 月 31 日]

滥用信息和电信技术仍然是国际社会非常关切的问题，因此需要解决这一领域日益增长的威胁。

我们谴责滥用媒体平台，包括社交媒体和电台广播，将其作为干涉主义的工具，通过宣扬仇恨言论、煽动暴力、颠覆、破坏稳定、传播假新闻和出于政治目的歪曲事实，作为发动战争，或是威胁使用武力或使用武力的借口，这违反《联合国宪章》的宗旨和原则以及国际法。

在这方面，我们反对美国政府针对古巴部署的非常规战争手段，包括利用新信息技术和其他数字平台来破坏我国的稳定和信誉。

我们重申，作为一项宪法特权，各国有权利和义务打击传播可能被解释为干涉他国内政或有害于促进国家和民族间和平、合作和友好关系的虚假新闻或歪曲新闻。

我们不能忽视这样一个事实，即网络攻击能力和行动的不断发展会将网络空间变成一个新的冲突场所。我们反对将恶意使用信息和通信技术等同于“武装攻击”概念，以此企图为行使《联合国宪章》第五十一条规定的自卫权进行辩护。

我们反对蓄意利用这些技术来破坏其他国家的重要基础设施，包括其信息系统，或以其他方式阻碍对各国社会稳定和安全至关重要的关键基础设施的使用和运行。

联合国是最重要的多边论坛，也是解决会员国对信息和通信技术安全和使用的关切的主要平台。在这方面，根据大会第 75/240 号决议设立的 2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组是会员国以透明平等方式讨论网络安全问题的唯一包容性机制。

我们重申上述工作组的重要性，并希望这一政府间进程将有助于以具有约束力的规范填补现有的法律真空，从而通过一项关于国际安全背景下的信息和通信技术的全面法律文书。

建立信任措施是一个有益的工具，但这种措施本身并不能保证信息和通信技术严格用于和平目的，因为在这一领域不存在这种具有法律约束力的文书。

古巴作为不结盟国家运动的成员，再次呼吁发达国家和相关国际实体根据请求向发展中国家提供援助与合作，包括通过财政资源、能力建设和技术转让，同时考虑到每个受援国的具体需求和特点。

我们反对实施单方面胁迫性措施，如同美国政府对古巴实施的经济、商业和金融封锁一样，这些措施阻碍或限制普遍获得、以及和平利用和享有信息和通信技术、造福我国人民。

# 丹麦

[原件：英文]
[2022 年 5 月 31 日]

在丹麦，如同在世界许多地方一样，数字解决方案是日常生活不可或缺的一部分。它们既是基本社会活动的平台，也是经济增长的主要驱动力。然而，随着我们的社会和我们的数字基础设施越来越相互关联，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。这应引起全球关注，根据国际法，网络空间中的恶意活动可能构成不法行为，有逐步升级的风险，进而威胁国际安全和稳定。俄罗斯无端非法入侵乌克兰，包括对关键基础设施的网络攻击，尤其令人关切，完全不可接受，因为这违反了国际法，破坏了网络空间负责任的国家行为框架。

作为世界上数字化程度最高的国家之一，丹麦仍然决心预防、遏制和应对恶意活动，并为此加强国际合作。丹麦与欧洲联盟一道，力求加强国际合作，支持一个全面、开放、稳定、和平和安全的网络空间，让人权、基本自由和法治得到充分实施。在这方面，丹麦强调各国必须遵守网络空间负责任的国家行为框架，该框架支持基于规则的国际秩序，确认国际法的适用性，遵守负责任的国家行为的自愿规范，以及制定和实施切实可行的建立信任措施。大会所有成员一再申明，该框架是国际社会努力遏制网络空间不计后果和不负责任的国家行为、避免最具破坏性的网络攻击和潜在升级的基石。因此，我们呼吁包括俄罗斯联邦在内的所有会员国履行承诺。

## 在国家一级为加强信息安全和促进该领域的国际合作所做的努力

迄今为止，丹麦已采取若干步骤来加强其网络安全和信息安全，促进网络安全方面的国际合作。《2018-2023 年丹麦国防协议》拨款 14 亿丹麦克朗用于加强网络安全和网络防御，从而加强丹麦社会抵御网络攻击的强韧和力度。

根据丹麦 2018-2021 年网络和信息安全战略，推出了 25 项举措和 6 项专门战略，目的是：

(a) 加强网络和信息安全，特别是在关键部门；

(b) 确保系统和协调的努力；

(c) 增强数字基础设施的技术复原力；

(d) 增进公民、企业和当局对网络安全的了解。

作为该战略的一部分，在六个关键部门(能源、金融、运输、保健、电信和海事)设立了专门的网络安全和信息安全单位，并为这些单位提供了分享经验的论坛。

网络安全中心也推出了自己的强化网络学院，广泛支持网络安全领域的教育和研究。同样，电子政务局针对首席执行官、网络专家和公职人员编制了若干关于网络安全和信息安全的课程、学习材料和活动。

此外，电子政务局开发了网站 www.sikkerdigital.dk，向公民提供具体的网络安全和信息安全指导，并与各市和地区密切合作，开展关于安全数字行为的全国活动。

丹麦设立了一个公私网络安全委员会，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供咨询意见。最后，根据丹麦 2018-2021 年网络和信息安全战略，丹麦还加强了其国际网络参与，更多参与多国网络论坛，如联合国、欧洲联盟、北大西洋公约组织(北约)和欧洲安全与合作组织(欧安组织)。

2021 年 12 月，政府提出了新的 2022-2024 年国家网络安全和信息安全战略。该战略通过针对公共和私营部门以及全体丹麦公民的 34 项主要举措，进一步加强网络安全和信息安全，从而巩固和扩大了目前的努力。总体而言，该战略包括四个主要目标：

(a) 首先，该战略进一步加强支持重要社会功能的关键信息和通信技术基础设施的复原力。为确保政府机构和工商业有足够的网络安全水平，启动了一系列战略行动，包括收紧对社会至关重要的政府信通技术系统管理的安全要求，以及加强警方对网络犯罪的应对措施。该战略还扩大了关键部门的数量，包括了更广泛的负责信息技术支持的重要社会职能的政府机构。除了先前在 2018-2021 年战略中提出的最低要求之外，这些关键部门的政府机构还必须遵守一些具体的安全要求。这是为了确保对重要社会职能负有特殊责任的部委能够在发生严重网络事件时迅速有效地采取行动；

(b) 第二，该战略包括若干举措，旨在加强丹麦公民的网络安全技能，增加管理层对加强网络安全的承诺。这些举措包括针对政府雇员的新的专门培训方案，以及为儿童、青年和成人提供数字扫盲所需能力的教育方案。此外，高层管理人员和领导人在优先考虑网络安全和信息安全方面面临越来越多的要求和期望；

(c) 第三，该战略加强公共和私营部门在网络安全和信息安全方面的合作。跨部门分享知识和经验的能力对于实现高水平的网络安全和信息安全至关重要。出于这一原因，将设立一条网络热线，以便于征求与网络犯罪有关的建议，还将为中小企业设立一个专门的网络安全单位，以加强网络安全中心提供指导的能力；

(d) 第四,该战略进一步加强丹麦在网络安全方面的国际努力。这包括向外交部门分配更多资源，加强丹麦对欧洲联盟、北约和联合国内部网络安全多边合作的贡献，促进与国际技术产业、学术界和智囊团的合作，以及对数字产品的出口管制。最后，该战略还包括加强国家和国际努力的举措，以建立积极的网络防御和提高威慑力。

除了作为国家网络安全和信息安全战略的一部分发起的倡议外，丹麦继续通过与北约和欧洲联盟伙伴和盟友合作，广泛地参与应对网络攻击和影响力行动等混合威胁。丹麦还为联合国、欧洲联盟、北约和欧安组织的外交努力做出贡献，以始终如一地促进自由、开放、稳定、和平和安全的网络空间。

值得注意的是，丹麦支持制定一项联合国行动纲领的想法，其可为国家和非国家行为者提供进一步合作的平台，例如，开展适应其需求的能力建设活动，或

在联合国框架下推进其国家执行努力，从而提高信息和通信技术领域的集体复原力和稳定性。

此外，丹麦还是网络与信息系统安全合作小组和网络安全事故应对小组网络的现任成员，也是欧洲联盟网络安全局理事会成员。

## 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报告和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

### 现有威胁和新出现的威胁

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们公民的生活质量带来了巨大机遇。尽管如此，我们对数字解决方案的依赖也带来了某些挑战和漏洞。

丹麦感到关切的是，国家和非国家行为者在网络空间的恶意活动有所增加，通过网络窃取知识产权的行为也有所增加。这种行动威胁到经济增长和国际社会的稳定。

国家和非国家行为者都显示其愿意利用任何机会开展恶意网络活动。这包括干扰关键基础设施和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不可接受，都会危及人的生命。丹麦尤其感到震惊的是，最近影响信息和通信技术产品和服务的安全和完整性的活动有所增加，这可能会产生系统性影响。具体而言，俄罗斯对关键基础设施进行网络攻击，作为无端非法入侵乌克兰的一部分，这是全然不可接受的，因此必须受到整个国际社会的强烈谴责。各国必须按照国际法以及政府专家组 2010 年、2013 年、2015 年和 2021 年共识报告和工作组 2021 年报告，避免使用网络攻击，尽职尽责，并对源自境内的恶意信通技术活动迅速采取坚定行动。

正如政府专家组以前各项报告以及工作组报告所承认，鉴于信通技术的独特性，联合国及其会员国在国际安全背景下处理网络问题的方法必须保持技术中立。这符合这一概念，也符合联合国承认现有国际法适用于新领域，包括新兴技术的使用。

### 国际法如何适用于使用信息和通信技术

丹麦坚决支持基于规则的国际秩序的多边体系，以应对恶意使用信通技术造成的现有威胁和潜在威胁。

正如政府专家组 2010 年、2013 年、2015 年和 2021 年共识报告以及工作组 2021 年报告第 71(b)至(g)段确立的原则所确认，国际社会非常明确地表示，网络空间牢牢植根于现行国际法。丹麦强调，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均适用于国家在网络空间的行为。因此，我们呼吁所有会员国履行承诺。

主权、不干涉和禁止使用武力是国际法的基本原则，国家违反这些原则可能构成国际不法行为，对此，国家可以根据国家责任规则采取反措施并寻求赔偿。仍有加强对这些基本原则的共同理解和解释的余地。丹麦支持政府专家组和工作

组的工作，以及其他国际和区域倡议，包括促进网络空间负责任国家行为的行动纲领，以实现这一成果。

重要的是，主权原则不应被国家用来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 年国家军事网络空间行动联合原则中，根据该原则，军事领导人在开展网络空间行动时，有义务考虑遵守国际法。因此，国际人道法，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界限，完全具有保护性。丹麦愿与欧洲联盟一道强调，国际法不是冲突的促成因素，而是保护平民和限制过度影响的一种方式。

现行国际法，加上政府专家组 2015 年报告中阐述的 11 项负责任的国家行为自愿非约束性规范，为各国在网络空间的负责任行为提供了一个框架。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。然而，在加强对现行国际法如何适用于此类问题的共同理解方面，仍有余地。丹麦希望，工作组的工作和建议将有助于进一步澄清问题，从而促进各国守规，促进更大的可预测性和减少升级风险。为此，丹麦目前正在就国际法如何适用于网络空间的国家行动制定国家立场。

### 负责任国家行为的规范、规则和原则

丹麦与欧洲联盟及其成员国一道，鼓励所有国家增进大会一再认可、特别是第 76/19 号决议认可的工作，并推进这项工作，执行在网络空间负责任的国家行为的商定规范，以及在预防冲突中发挥重要作用的建立信任措施。我们欢迎工作组内的包容性和建设性对话，以及通过一项可能的联合国行动方案进行实际合作的可能性。

政府专家组在 2010 年、2013 年、2015 年和 2021 年的报告以及工作组的报告中阐述的负责任的国家行为的规范、规则和原则是对现有国际法的补充和衍生，具有巨大价值。丹麦将继续遵循国际法，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透明度，进一步落实这些规范。

### 建立信任措施

为了交流信息、建立信任和防止冲突，在国家间建立有效的网络问题合作机制至关重要。欧安组织等区域论坛已经为具有共同关切和共同利益的行为体之间的建立信任措施和合作建立了相关平台，以便从区域角度有效应对挑战。此外，工作组本身也应被视为一项建立信任措施，因为它为所有会员国提供了一个交流信息和分享对网络问题看法的国际论坛。

丹麦与欧洲联盟及其成员国一道，鼓励国际社会进一步制定和实施建立网络信任措施，提高国家行为的可预测性，减少误解、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

为了减少恶意使用信通技术带来的风险、缓解紧张局势和预防冲突，加强我们社会的网络复原力至关重要。因此，如上所述，丹麦政府推出了大量举措，加强国家网络复原力。同样，欧洲联盟及其成员国，包括丹麦，也在开展合作，加强整个欧洲联盟的复原力，特别是通过关于网络和信息系统安全的指令来加强复原力。

除了这些努力之外，丹麦还与欧洲联盟及其成员国一道，通过一些有针对性的方案和举措，帮助提高发展中国家的网络复原力，这些方案和举措旨在发展应对网络事件的技能和能力，并促进交流最佳做法。

丹麦与欧洲联盟及其成员国一道，认识到促进更具复原力的数字基础设施将有助于建立更安全和稳定的网络空间，并鼓励所有相关行为体参与这方面的能力建设，进一步呼吁加强与关键国际伙伴和组织的合作，支持第三国的能力建设。

此外，丹麦还支持建立一个联合国机制，以促进专门针对受益国确定的需求的能力建设方案，如行动纲领,并确定促进所有利益攸关方参与执行负责任行为框架的机制。

## 埃及

[原件：阿拉伯文]
[2022 年 5 月 31 日]

### 埃及关于加强信息安全和促进国际合作的看法和建议

### 一. 国家努力

- 近期，埃及加强了能力建设工作，并根据不限成员名额工作组最后报告和政府专家组报告的建议，制定了通信和信息安全监管框架。
- 埃及国家正在采取平衡的政策，根据基于最近制定的一些法律的立法框架，跟踪和打击网络犯罪并处理互联网和社交媒体上的非法活动，这些法律包括：关于打击信息技术犯罪的第 175(2018)号法、关于监管新闻和媒体的第 180(2018)号法和关于保护个人数据的第 151(2020)号法。
- 成立了最高网络安全委员会，作为网络安全事务的主管机构和国家参考机构。作为《埃及 2030 年愿景》的一部分，启动了国家网络安全战略。它将建立一个纳入国际最佳做法的国家综合系统。它将在政府机构和私营部门之间建立国家网络安全伙伴关系，并通过建立和提高计算机应急小组和国家各部门内部形成的网络的效力，加强网络防御方案。它还将建立和发展针对特定社会群体，如学童、政府机构和老年人的网络安全意识方案，并促进科学的网络安全研究和创新。

- 已经制定了许多国家政策、治理机制和监管框架及标准，包括国家一级的基本网络安全管制、网络安全系统管制和持续网络安全监测。
- 埃及正在努力促进信息安全和能力建设方面的双边和多边国际合作。
- 已经启动了许多国家方案和举措，发布关于最新和最危险的网络漏洞的警报，提高社区意识、预防网络风险并降低其影响。
- 正在与国家机构和学术机构开展合作，以建设能力和创建合格的网络安全和信息安全人员库。

## 二. 提议

- 至关重要的是，要加强国际网络安全合作，最大限度地减少跨境网络犯罪活动，防止网络犯罪。我们还必须交流专门知识和现代技术，起诉所有非法使用互联网的行为，从而使各国能够应对这些行为。应当举办培训课程，以发展负责打击网络犯罪的安全机构的能力。
- 应采取行动，管理加密货币的流通，使其不被用于资助非法活动。还应考虑在国际刑事警察组织(国际刑警组织)设立一个打击网络犯罪的专门部门，促进参与打击此类活动的安全机构之间的信息交流。

## 俄罗斯联邦

[原件：俄文]
[2022 年 5 月 31 日]

21 世纪是信息技术突破的时代。这些技术几乎征服了生活的所有领域。国家、社会和商业的传统活动领域经历了彻底的转变。为发展经济和劳动力市场以及提高生活水平创造了新的机会。与此同时，新的技术解决方案也带来了新的挑战。

全球数字空间往往成为激烈的信息对抗、计算机攻击(包括针对关键信息基础设施的攻击)、不公平竞争和私营公司滥用权力的场所。一些主要威胁是在军事政治和其他领域使用信通技术，破坏主权、侵犯领土完整、干涉国家内政；开放源代码中恶意软件的传播；将信通技术用于恐怖主义、极端主义和犯罪目的。所有这一切从根本上改变了世界格局，加剧了对国际安全的威胁。

俄罗斯是首批敦促国际社会加入这一新领域努力的国家之一。早在 1998 年，俄罗斯就率先提出了一项联合国大会决议，题为“从国际安全角度看信息和电信领域的发展”。它呼吁开展基础广泛的合作，打击信息领域的共同威胁，主要是利用先进技术破坏国际和平与稳定的企图。由于我们的努力，信息安全已成为联合国大会的一个议程项目，通过一项相关决议已成为一项年度活动。

2004 年，在俄罗斯的倡议下，成立了政府专家组：有史以来第一个在联合国内部讨论确保信息通信技术安全问题的专门平台。政府专家组总共有六个版本。信息领域的迅速发展为将讨论提升到新的质量水平创造了条件。

2018 年，联合国大多数会员国批准了俄罗斯提出的国际信息安全决议。该文件提出了一套国家使用信息和通信技术的负责任行为的初步规则、规范和原则。还规定进一步加以发展，在联合国不限成员名额工作组框架内，在更加民主的基础上，普遍讨论信息和通信技术安全问题。该小组圆满完成了工作，以联合国所有会员国协商一致的方式于 2021 年 3 月 12 日在纽约通过了最后报告。

由于俄罗斯和志同道合的国家的努力，通过新建 2021-2025 年关于信息通信技术安全和使用的不限成员名额工作组，确保了联合国主持下的谈判进程连续而不间断。它的任务规定进一步阐述国家负责任行为的规则、准则和原则及其实施方式。要做到这一点，主要是通过就信息安全领域的威胁、国际法对各国使用信通技术的适用、建立信任措施、能力建设和加强主管机构之间的联系达成共识。不限成员名额工作组机制确保各国在讨论中发挥主导作用，也给予非政府实体参与的可能性。

俄罗斯确保国际信息安全的方法保持透明和不变。这一领域被列为俄罗斯联邦国家安全战略(2021 年 7 月 2 日俄罗斯联邦第 400 号总统令批准)的优先事项。根据国际信息安全领域国家政策的基本原则(2021 年 4 月 12 日俄罗斯联邦第 213 号总统令批准)，主要目标是促进建立规范全球信息空间的国际法律制度。

我们认为，重要的是通过具有普遍法律约束力的安排，旨在信息领域预防冲突和建立互利合作。在俄罗斯支持的特设委员会内我们提交的关于打击为犯罪目的使用信息和通信技术的公约草案，以及我们关于确保国际信息安全的联合国公约的概念，可以作为这种文书的基础。

信通技术应服务于可持续发展目标，有助于为科学研究和快速实施最先进的技术解决方案创造有利条件。正是为了在未来普遍认可和公平的法律义务框架内实施这些准则，2021 年，俄罗斯和美国发起了联合国大会第 76/19 号决议，该决议以协商一致方式获得通过，有 108 个会员国为共同提案国。

俄罗斯主张国家数字主权不可侵犯。每个国家都能够而且应该独立确定规范其信息空间和相关基础设施的参数。我们坚持互联网治理的国际化，在这一过程中保障各国的平等权利。我们认为，限制各国管理和确保全球网络中本国部分安全的主权的任何企图都是不可接受的。

我们还认为，必须在国家和国际层面采取法律措施，反对某些国家在数字领域的主导地位。必须为可靠和平等地保护信息空间所有用户的权利创造条件。没有一个国家或国家集团能够单独为互联网的运作制定原则、规则和标准。为了完成这些任务，俄罗斯主张将互联网治理的特权移交给电信和信息通信技术领域的联合国专门机构——国际电信联盟，该机构在这些问题上拥有必要的专业知识。

俄罗斯一如既往，无论是以双边形式还是在国际平台和论坛，主要是在联合国，都愿意与所有伙伴进行对话和建设性互动。

## 新加坡

[原件：英文]
[2022 年 5 月 31 日]

新加坡坚定致力于加强网络空间基于规则的国际秩序，这将成为会员国之间信任和信心的基础，促进经济和社会进步。为了获得数字技术的全部好处，国际社会必须发展一个安全、可信、开放和可互操作的网络空间，以适用的国际法、负责任的国家行为的明确规范、强有力的建立信任措施和协调的能力建设为基础。新加坡认为，至关重要的是，关于这些问题的讨论，包括关于负责任的国家行为的法律、规则和规范的讨论，应继续在联合国进行，因为联合国是所有国家都有平等发言权的唯一普遍、包容和多边论坛。

新加坡 2019 年至 2021 年期间参加了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，以及根据大会第 73/27 号决议设立的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。我们积极参与并支持主席努力建立一个面向行动的 2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，推动关于国际网络规范和网络空间负责任国家行为商定框架的讨论。我们仍然致力于为工作组进程做出建设性贡献，以进一步加强国际合作，并在推进网络空间负责任的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。

### 国家负责任行为的准则、规则和原则

新加坡认为，需要作出更多努力，提高对负责任的国家行为的现有自愿、非约束性规范的认识，并支持这些规范的实施。新加坡还支持在必要时进一步充实这些准则。例如，跨几个国家提供服务的跨界关键信息基础设施，其保护是所有会员国的共同责任，可被视为这种关键基础设施的一个特殊类别，并应纳入现有的一套规范，因为信息和通信技术(信通技术)对这种基础设施的威胁可能会产生区域和全球的不稳定影响。[3]

区域组织在支持实施现行规范框架方面可发挥重要作用。东南亚国家联盟(东盟)原则上赞同关于国家在使用信通技术方面负责任行为的 11 项自愿、不具约束力的规范，迄今仍是唯一通过这些规范的区域组织。在 2021 年举行的第六届东盟网络安全部长级会议上，与会者讨论了东盟关于执行网络空间负责任国家行为规范的长期区域行动计划的进展，该计划旨在确保有效和切实执行这些规范，包括在计算机应急小组之间合作、保护重要信息基础设施和网络安全互助等领域。2021 年 11 月，第二届东盟网络安全协调委员会核可了区域行动计划，该计划仍然是一份有活力的文件，供进一步审查。《2021-2025 年东盟网络安全合作战略》更新了《东盟网络安全合作战略》，以在东盟区域创建一个更安全、更有保障的网

[3] 跨境关键信息基础设施系私营公司拥有、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。

络空间。东盟已同意建立区域计算机应急小组，内含东盟计算机应急小组信息交流机制，以加强东盟对网络安全事件的应对。通过东盟区域论坛信通技术安全和使用联络点名录，论坛成员能够在发生网络事件时与其对应方联系。

### 能力建设

新加坡认为，能力建设是商定规范框架的一个重要支柱，因为确保所有国家都有能力执行规范框架、履行国际法义务非常重要。为此，新加坡致力于在区域和全球层面与联合国其他会员国，特别是发展中小国分享我们的经验和专门知识。

为支持区域(东盟)一级的能力建设，新加坡在 2016 年设立了东盟网络能力方案，支持东盟国家在网络政策以及业务和技术问题上的能力建设。在国际伙伴和参与者对该方案作出积极反馈后，新加坡于 2019 年 10 月宣布成立东盟-新加坡网络安全英才中心，承诺在 2023 年前的五年内投入 3 000 万美元，为东盟高级政策和技术官员开展网络安全培训方案。该中心的园地于 2021 年 10 月在新加坡国际网络周期间正式开放。迄今为止，该中心已开办了 30 多个方案，来自东盟内外的 1 250 多名高级官员参加了这些方案，并与各国政府、私营部门、学术界和非政府组织的 40 多个伙伴开展了合作。尽管由于 2019 冠状病毒病(COVID-19)大流行疫情引起的旅行限制，该中心继续开展在线培训方案，并自 2020 年 5 月以来组织了 21 次虚拟能力建设方案。

在全球一级，新加坡正在与裁军事务厅合作开展以下举措：

(a) 在联合国-新加坡网络方案下，新加坡正在与裁军事务厅合作，通过在各区域举办一系列讲习班，制定规范执行核对表。核对表将采取指南的形式，列出发展中国家可以采取的一系列行动，以执行关于负责任的国家行为的 11 项自愿、不具约束力的规范。2022 年 3 月，新加坡与东盟成员国举办了第一次规范实施讲习班，以制定核对表，重点是实施关于关键基础设施保护、漏洞报告以及保护计算机应急小组和网络安全事件响应小组的规范；

(b) 2022 年底，裁军事务厅和新加坡将共同组织联合国-新加坡网络研究金方案，该方案旨在使联合国会员国的高级政府官员具备必要的跨学科专门知识，以有效监督国家网络安全和数字安全政策、战略和运作。

### 建立信任措施

新加坡还认为，国际社会应进一步努力制定建立信任措施，支持商定的规范框架，因为此类措施有可能减少发生误解的风险，并防止和缓解网络空间的冲突。有鉴于此，新加坡支持按照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建议，建立一个业务或技术层面的国家联络点全球名录。2022 年下半年，新加坡还将与联合国裁军研究所(裁研所)合作，为国家网络联络点举行一系列桌面演练中的第一次。桌面演练将(a) 为联合国所有会员国提供一个参与实质性网络演练的机会，无论其目前的技术能力和(或)区域组织成员地位如何；(b) 提高国家网络联络点应对现实事件和网络危机的能力；以及(c) 展示拟议的联络点全球名录的效能和价值。这种演练以前在区域一级在计算机应急小组之间组织过，

但没有向所有感兴趣的联合国会员国开放，特别是那些在区域计算机应急小组网络之外的会员国。为解决这一问题，新加坡的桌面演练方案将是首次向所有会员国开放的演练。

### 国家一级的努力

在国家一级，新加坡继续在三个方面加强其系统和网络的网络安全，即建设具有复原力的基础设施、实现更安全的网络空间和发展充满活力的网络安全生态系统。

#### 建设具有复原力的基础设施

拥有和运营我们的核心数字基础设施的实体必须遵守网络安全行为守则，该守则详细规定了此类实体应采取的网络卫生措施，如保持系统和软件更新、维护关键数据的更新备份以及快速检测网络入侵。必要时还会发布警报和咨询，以补充业务守则，应对不断变化的威胁(如勒索软件)。此外，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》，作为我们努力加强新加坡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的一环。《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。安全局还推出了运营技术核心能力框架，企业可以利用该框架建立流程、结构或工作，以管理其组织内的运营技术网络安全。2022 年，安全局将启动一项关键信息基础设施供应链计划，涉及政府机构、关键信息基础设施所有者及其供应商等利益攸关方。该方案将为所有利益攸关方提供管理供应链网络安全风险的推荐流程和良好做法。

#### 创建更安全的网络空间

作为我们提高新加坡国家网络安全态势的努力的一环，网络安全局在 2020 年启动了《更安全的网络空间总计划》，以：(a) 保护新加坡的核心数字基础设施；(b) 保障网络空间活动；以及(c) 增强我们精通网络的人口的能力。《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，提高最终用户的网络安全意识和良好的网络卫生习惯。所有企业和组织都有责任保护我们更广泛的网络空间活动。为促进这一点，安全局推出了若干计划，提高利益攸关方对网络安全的认识，如针对不同企业利益攸关方的网络安全工具包。除此之外，还以“网络信任和网络要素”标志的形式对企业进行网络安全认证，以认可具有全面网络安全措施和做法的企业。

网络安全局发布了公共建议，指导企业和公众在出现与网络相关的漏洞和威胁时进行处理管控。例如，安全局就最近的 Log4Shell 漏洞发布了公开咨询，并与贸易协会和商会合作，向新加坡企业介绍如何解决该漏洞并保护其系统。此外，安全局还有处理网络犯罪的长期咨询，如劝阻受害者向勒索行为者支付赎金的公共咨询。

鉴于物联网连通广泛，但又缺乏网络安全防护，与物联网的扩展相关的网络安全风险越来越大。网络安全局利用技术标准来增进网络卫生，为产品和服务提

供保证。2020 年，安全局启动了“消费者物联网设备网络安全标签计划”。现在市场上有 150 多种贴有标签的产品。新加坡也大力提倡基于规则的国际标准，并且是根据共同标准认可安排颁发证书的国家。[4] 国际标准将有助于增进网络卫生，共同保护网络空间，降低跨境贸易壁垒。新加坡希望与志同道合的伙伴合作，为消费者物联网的安全制定一个通用的标签框架，以协调既定的国际标准和标签要求，并促进此类标准的相互承认。这将有助于最大限度地减少标准的分散，消除各国之间的重复测验，降低遵守国家法规的成本，并便利开发商进入市场。

*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的创新。鉴于网络威胁形势的快速变化，网络安全公司需要不断创新和投资新的解决方案，以保持领先地位。网络安全局通过网络安全行业创新呼吁，支持行业主导的网络安全创新。这鼓励网络安全公司开发创新的解决方案，以满足地方主要终端用户(如拥有和运营核心数字基础设施的实体和商业部门)的网络安全需求，刺激国内网络安全行业的需求。还越来越需要培养一批有才能的个人，在组织中承担网络安全领导角色。安全局与新加坡的政府机构、协会、行业合作伙伴和学术界合作，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。它的目标是在三年内接触至少 20 000 名个人，以加强新加坡的网络安全人才管道。

## 土耳其

[原件：英文]
[2022 年 5 月 31 日]

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的报告和从国际安全角度看信息和电信领域的发展政府专家组的报告所载的评估和建议，下文介绍土耳其对国家一级为加强信息安全和从国际安全的角度促进信息和电信领域国际合作所做努力的看法和评估，以及相关报告中提到的概念内容。

如上述报告所强调，在信息和通信技术环境中建设和维护国际和平、安全、合作和信任的必要性从未如此明确。特别是由于数字技术的传播及其跨界性质，随着网络威胁和犯罪的多样化和扩大，信息和通信技术安全已成为国防和国际安全的主要因素之一。因此，会员国正在加紧努力，在国家安全领域建立必要的技术基础设施、机构能力和人力资本。为了积极预防对土耳其国家安全的潜在风险，正在计划和采取必要行动，如开发网络安全和数据隐私相关技术，解决合格人力资源供应方面的差距，完成机构重组，更新法律基础设施，并确保符合不断发展的技术。此外，有必要开展合作，特别是在国际一级，以打击网络犯罪。在这方面，目标是进一步发展知识和信息共享及国际合作，以便以最有效的方式发现网络犯罪的源头和涉案罪犯。

[4] 见 www.commoncriteriaportal.org。

土耳其注重采取必要措施，以改善国家网络安全。运输和基础设施部是负责土耳其国家网络安全决策及制定战略和行动计划的机构。在此背景下，发布实施了《国家网络安全战略》和《2013-2014 年行动计划》，以及《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》，在该部协调下，所有相关利益攸关方都参加了研究小组。

2020 年 12 月 29 日的政府公报公布了《2020-2023 年期间国家网络安全战略和行动计划》，其中包括以下主要战略目标：

- 保护关键基础设施并提高复原力
- 国家能力建设
- 有机的网络安全网络
- 新一代技术的安全性
- 打击网络犯罪
- 开发和培养国内和国家技术
- 将网络安全融入国家安全
- 改善国际合作。

运输和基础设施部根据确定的实施步骤、负责机构和组织正在开展的活动以及衡量标准，对行动计划进行监测和衡量。

与此同时，信息和通信技术管理局下属的土耳其国家计算机应急小组自 2013 年以来一直在协调国内网络事件应对工作。除了检测网络威胁和应对网络事件，包括事件发生之前、期间和之后，该小组还确保针对网络威胁和网络威慑实施预防措施。

国家计算机应急小组网络安全的主要重点领域如下：

- 建设网络能力
- 技术措施
- 收集和传播威胁情报
- 关键基础设施的保护。

在改善国家网络安全的背景下，2013 年以来还成立了 14 个关键部门和基础设施(如能源、保健、银行和金融、水管理、电子通信和关键公共服务)部门计算机应急小组和 2 000 多个机构计算机应急小组。在国家小组的协调下，所有小组每周 7 天、每天 24 小时工作，以减轻网络风险和打击网络威胁。国家小组使用检测和预防工具进行监测，并使用报告工具与相关方分享信息。它为土耳其境内所有计算机应急小组开发了通信平台，以便发布警报、警告和安全通知，这提供了一个高效安全的通信渠道。

国家小组组织并支持向几个社区开放的网络安全培训课程、夏令营和竞赛。此外，它还为计算机应急小组提供恶意软件分析和日志分析等主题的培训。截至2022 年 4 月，超过 5 000 人接受了国家小组在不同网络安全领域的培训。

国家小组已得到 MITRE 公司的公共漏洞和暴露方案接受，在这方面，它为第三方软件、硬件或产品的漏洞指定公共漏洞和暴露号码，在漏洞管理方面提供流程协调。

此外，2017 年成立的信息和通信技术局培训中心 BTK 学院向公众提供网络安全和其他相关领域的在线培训，以促进增加土耳其人力资源的专门知识。培训内容可在学院的官方门户网站上获得(www.btkakademi.gov.tr/portal)。

土耳其一些组织、机构、大学、非政府组织和私营部门实体也在全国范围内就网络安全和保护重要基础设施等相关主题组织研讨会、会议和培训。

每年组织的“更安全互联网日”是信息和通信技术局的提高认识活动之一，其主要目标是自觉和安全地使用互联网。在官方的安全门户网站上，公布提供了一条互联网帮助热线和一个安全网站，家庭可以在上面找到关于有效使用互联网的建议(www.guvenlinet.org.tr)。

此外，正在为学生、教师和家长举办关于自觉和安全使用互联网的在线和面对面培训和研讨会。许多学生还使用更安全的“互联网卡车”进行学校访问，这有助于确保全国儿童和青少年直接与新技术互动，正确使用技术和互联网，提高对这一问题的认识。

土耳其还采取措施应对日益增加的数字安全风险，以确保网络安全，并在2019 冠状病毒病(COVID-19)大流行疫情期间采取了措施。

利用 2019 冠状病毒病(COVID-19)大流行疫情趋势的恶意软件、网络钓鱼攻击和其他网络威胁由国家计算机应急小组进行分析，该小组每周 7 天、每天 24 小时运作。通过指挥和控制中心，这些网络威胁的恶意链接被确定和预防，以保护重要的基础设施和公民。在此范围内，编写网络情报报告并与相关方分享。还编写和出版了若干准则，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 2019 冠状病毒病(COVID-19)大流行疫情相关的虚假申请
- 设置和使用视频会议和会议软件的安全原则。

此外，国家网络安全工作人员职业标准(第 5 级)在政府公报上公布后生效。

土耳其在许多组织中发挥了重要作用，或是作为创始成员，或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，土耳其极其重视与不同国家和组织分享信息。土耳其是国际电信联盟成员，国家计算机应急小组是事件和安全小组论坛、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。此外，正在努力开展网络安全方面的双边和多边合作，例如与许多国家签署了谅解备忘录。土耳其还支持积极参与和促进国际组织的研究，如联合国、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)、20 国集团、突厥语国家组织、经济合作组织、发展中八国经济合作组织以及区域军备控制核查和实施协助中心——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。这种国家和国际一级的演习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，在土耳其进行了五次国家和两次国际网络安全演习。最近，2021 年 10 月 12 日和 13 日，与交通和基础设施部以及信息和通信技术局合作，在公共机构和组织的参与下，举行了国家网络盾牌 2021 演习。此外，该部和该局于 2019 年 12 月 19 日在安卡拉共同组织了 2019 年国际网络盾牌演习。这次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，土耳其继续参与和促进各种国际网络安全演习，如北约“锁定盾牌”、北约“网络联盟”和北约“危机管理”演习。除了其他能力建设和指导研究之外，国际网络安全演习对于提高全世界的准备水平和建设网络事件应对能力仍然至关重要。

国家信通技术政策领域的另一个重要机构是土耳其总统数字转型办公室。

数字转型办公室开展的最重要和最杰出的研究之一是，2020 年 7 月 24 日出版的《信息和通信安全指南》。该指南是该领域出版的主要国家参考文件。它在加强公共机构和关键基础设施服务提供商的网络防御能力方面发挥着重要作用。

公共机构和关键基础设施服务提供商应在指南规定的期限内完成合规活动，并应至少每年进行一次审计。各机构在这方面必须执行的审计政策和程序均记录在数字转型办公室发布的信息和通信安全审计指南中。

此外，在土耳其有关方面的合作下，启动了关键基础设施国家试验台中心，该中心开展研究，以确保电力分配和水管理基础设施的安全。该中心是能源和水管理系统的模拟中心，旨在提供一个工作环境，以便寻找和开发与关键基础设施安全有关的保护性和预防性解决方案，并为网络安全生态系统做出贡献。

制定改善信息安全和网络安全项目，是数字转型办公室的主要职责之一，这是根据 2019 年 10 月 24 日第 30928 号政府公报发布的第 48 号总统令，纳入 2018 年 7 月 10 日第 30474 号政府公报发布的关于第 1 号总统组织的总统令的条款规定的。

在这方面，开展了各种与信息和网络安全有关的项目，包括网络情报竞赛和 HackZeugma 夺旗竞赛。

- 网络情报竞赛是培训和意识活动的一部分，旨在让更多人具有网络安全意识；事实证明，这方面非常有效。数字转型办公室组织了第二届网络情报竞赛，作为 2021 年网络意识月活动的一部分

- HackZeugma 夺旗竞赛由数字转型办公室组织，是 2020 年 Teknofest 航空航天和科技节的一部分。HackZeugma 是一项向世界各地成千上万黑客敞开大门的比赛，让他们展示自己的才华。竞赛的筹备工作特别关注操作技术系统的安全。

此外，启动了 100 万就业项目，以培养信息技术领域的合格劳动力，给训练有素的劳动力和雇主塔桥，增加就业。该项目的新特点是，雇主可以通过免费和无条件的注册来扫描简历。该项目由财政和金融部所有，力求到 2023 年使 100 万人做好在信息技术领域就业的准备，并在"国家技术行动"目标范围内实施，以实现我国的数字转型。

土耳其网络安全群组是一个得到数字转型办公室密切关注和支持的平台，其主要目标是，根据建立国家网络安全生态系统、开发地方和国家网络安全产品并推广其使用的使命，使土耳其在网络安全领域产生技术并能够在世界上开展竞争。该群组开展的活动包括：

- 建立测试和分析实验室，为部门的测试和开发提供基础设施
- 建立认证实验室
- 建立网络安全学院
- 组织国内和国际活动，如会议、培训、研讨会、小组讨论和交易会，并协调实习活动的需求和供应
- 支持开设副学士学位、本科和研究生教育课程。

除上述努力外，土耳其标准研究所和数字转型办公室还制定了行业标准，作为改善关键基础设施所有者和运营商网络安全的一种方法。与国际标准化组织/国际电工委员会第 27701、27011、27017、27018、27019、27031、27799、31000 和 62443 号标准相关的研究已经完成，土耳其标准研究所发布了关于关键基础设施的标准。

鉴于网络安全的性质，开展国家活动，发展国际合作非常重要。随着信息和通信技术的广泛使用，这些技术与国际和平、稳定和安全以及基本权利和自由等主题之间的关系正在不断发展。这种情况要求努力将信通技术用于和平目的，并确保各国不断处理国际稳定与安全问题。显然，政府专家组和工作组的报告以及相关研究中阐述的国际法、规范和规则有助于在国际和平与安全背景下使用信息和通信技术方面负责任的国家行为的共同框架。如上述报告所述，发展国际合作、尊重基本权利和自由、保护关键基础设施和防止恶意使用信息和通信技术等概念，将在未来一段时期，在国际稳定和安全努力中继续占有重要地位。

与此同时，还应考虑在网络空间保护国家主权的重要性，以及在现有规范之外制定新规范的必要性。改善合作和支持信息和经验共享机制对于打击网络威胁至关重要，需要给予适当考虑。

土耳其意识到实施国际法、网络空间负责任的国家行为规范和建立信任措施的重要性，以及开展有效国际合作的必要性，坚决采取必要步骤实现这些目标。

## 乌克兰

[原件：英文]
[2022 年 5 月 31 日]

乌克兰长期以来一直遭受俄罗斯持续武装侵略，还是其框架内网络攻击的目标，包括对乌克兰关键基础设施的攻击。因此，乌克兰完全赞同大会第 76/19 号决议序言部分第五段表达的合理关切，条件是：信息技术和手段不仅可能被使用，而且已经是侵略国在实践中积极使用的工具，而且不仅仅是针对乌克兰。

俄罗斯一再证实其无法遵守国际义务，令人怀疑其是否愿意遵守第 76/19 号决议执行部分第 3 和第 6 段的规定。

这同样适用于莫斯科提议制定的设想中的关于打击为犯罪目的使用信息和通信技术行为的全面国际公约。因为，如果俄罗斯为其草案设计的条款严重限制公民权利和自由的风险，因而不能写入公约的最终版本，那么莫斯科将不会对公约感兴趣。

俄罗斯公约草案中提出的这种限制，是乌克兰和 2001 年《欧洲委员会网络犯罪公约》缔约国中其他民主国家所不能接受的，但它适合未加入该公约的独裁政权，包括俄罗斯和白俄罗斯的独裁政权。

尽管俄罗斯进行了军事和网络侵略，但乌克兰正在西方伙伴的物质和咨询援助下，进一步加强其网络安全系统。

乌克兰网络安全战略建立的国家网络安全系统以国防部、国家特别通信和信息保护局、安全局、国家警察和国家银行为基础。它确保处理电子通信和信息安全或拥有重要信息基础设施的所有政府机构、地方当局、军事单位、执法机构、研究和教育机构、民间团体、工商业和组织之间的协作，无论其所有权形式如何。

确保国家网络安全系统的主题符合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的报告中所载的评估和建议。

乌克兰国家安全和国防委员会协调管控安全和国防部门各实体的活动，通过其工作机构、国家网络安全协调中心确保乌克兰的网络安全。

该中心具有监督职能，承担与分析国家网络安全状况和应对网络威胁的防备工作，以及预测和检测相关的潜在和实际威胁的相关任务。

在实施了先前的 2016-2020 年乌克兰网络安全战略后，国家能够组建国家网络安全系统的核心。乌克兰增强了潜力，可在威慑、网络复原力和互动的基础上进一步发展该系统。

乌克兰目前的网络安全战略是为 2021-2025 年期间制定的，其目的是为网络空间的安全运作及其本着个人、社会和国家利益为使用创造条件。该文件是基于威慑、网络复原力和互动的原则。

上述努力使乌克兰得以确定俄罗斯准备对乌克兰基础设施进行恶意网络攻击，这与实际侵略同时发生。从 2021 年秋季开始，我们看到越来越多的俄罗斯附属黑客团伙攻击乌克兰重要的数字和电信服务供应商。这些攻击的质量也有所提高，变得更有针对性，并使用更复杂的工具。

然而，应该指出，这些网络攻击大多没有成功。在国际伙伴的支持下，我们的利益攸关方发现并排解了这些问题。

乌克兰正在积极发展网络领域的合作，主要是与美国、联合王国、爱沙尼亚和其他西方伙伴国家、欧洲联盟和北大西洋公约组织(北约)的合作。它通过在国外和乌克兰的双边和多国培训课程、研讨会和会议获得财政援助和咨询建议，以及援助、现代硬件和软件，以满足网络安全需求，进行专业的计算机取证和调查网络犯罪。

乌克兰感谢美国、联合王国、欧洲联盟和其他国家和机构最近发表声明，谴责俄罗斯在网络空间对乌克兰和其他国家的侵略行为。

自 2016 年以来，乌克兰外交部与 13 个国家(日本、新加坡、马来西亚、芬兰、美国、德国、联合王国、爱沙尼亚、荷兰、斯洛文尼亚、西班牙、巴西和以色列)组织了 22 轮双边网络磋商。计划在 2022 年与一些国家进行此类磋商，但由于俄罗斯的军事入侵而推迟。

在网络防御领域，乌克兰一直与北约网络防御信托基金密切合作，以提高乌克兰应对网络威胁的技术能力，并期待作为北约合作网络防御卓越中心的一个贡献国，与北约开展有效合作。

乌克兰将感谢所有可能协助执行以下项目的联合国会员国，这些项目是根据乌克兰目前的网络安全战略实施的，目的是加强网络安全和网络防御领域的能力，并发展信息技术基础设施和国家情况中心网络的服务：

- 建立网络范围并进行全国网络演习
- 技术平台的网络威胁情报工具
- 关键国家信息资源的国家备份中心
- 国家网络威胁监控系统
- 国家云网络安全服务平台。

外交部愿意提供关于这些项目的详细信息，协助与项目执行者建立联系。

乌克兰的经验表明，为了应对严重和持续的网络威胁和网络攻击，有必要加强国家当局之间、私营部门和国际伙伴之间的多层面合作，以建设必要的能力并有效应对这种威胁。

# 三. 从政府间组织收到的答复

## 欧洲联盟

[原件：英文]
[2022 年 5 月 31 日]

网络空间，特别是全球、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。欧洲联盟及其成员国支持基于法治、人权、基本自由和民主价值观的开放、自由、全球性、稳定和安全的网络空间，从而实现全球社会、经济和政治发展。

随着互联网和信息通信技术(信通技术)越来越深入我们的生活，我们对这些技术的依赖使我们越来越容易被滥用。网络空间正越来越多地被恶意利用，国际层面日益加剧的两极分化正在阻碍有效的多边主义。俄罗斯在网络空间的不负责任行为是其非法和无理入侵乌克兰的一个组成部分，违背了包括俄罗斯联邦在内的联合国所有会员国对商定的联合国负责任国家行为规范的期望。同样，恶意攻击关键基础设施是重大的全球风险。对互联网的限制和互联网上的限制，及恶意网络活动的增加，包括影响信通技术产品和服务的安全和完整性的活动的增加，威胁到开放、自由、全球性、稳定和安全的网络空间，以及民主、法治、人权和基本自由。

欧洲联盟及其成员国经常对此类恶意活动表示关切，这些活动破坏了基于规则的国际秩序，增加了冲突的风险。恶意使用信通技术破坏了互联网和信通技术给整个社会带来的好处，并表明一些行为者准备威胁国际和平、安全和稳定。所有行为者都应避免在网络空间开展不负责任和破坏稳定的活动。

### 在国家一级为加强信息安全和促进该领域的国际合作所做的努力

加强全球网络复原力是维护国际和平与稳定的一个关键因素，因其减少冲突风险，也是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。欧洲联盟及其成员国大力支持上述开放、自由、全球性、稳定和安全的网络空间愿景，为此推动和实施一个包容性和多层面的网络空间预防冲突和稳定战略框架，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，欧洲联盟努力加强全球复原力，推进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，包括区域建立信任措施。

题为“开放、安全和有保障的网络空间”[5] 的 2013 年网络安全战略以及下文引用的后续政策文件、文书和战略，代表了欧洲联盟关于如何最好地预防和应对网络扰乱和网络攻击的全面愿景。它们旨在推广欧盟价值观，确保数字经济增长

[5] 见提交给欧洲议会、欧洲理事会、欧洲经济和社会委员会以及地区委员会的联合公报，题为“欧洲联盟的网络安全战略：一个开放、安全和有保障的网络空间”。

的条件到位。某些具体行动旨在提高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结论中强调，[6] 必须进一步制定和实施欧洲联盟共同和全面的网络外交方法，以促进人权和欧洲联盟的基本价值观，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，并为国际关系提供稳定。欧洲联盟还呼吁加强互联网治理的多方利益攸关方模式，加强第三国的能力建设努力。此外，欧洲联盟确认与关键伙伴和国际组织接触的重要性。欧洲联盟还强调现行国际法在网络空间和国际安全领域的适用和行为规范的相关性，以及互联网治理作为欧洲联盟共同和全面网络外交方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，欧洲联盟在成员国和欧洲联盟各有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，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[7] 阐述了挑战的规模和在欧洲联盟一级设想的一系列措施，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。

对日益增加的网络安全挑战的关切推动制定了关于欧洲联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。[8] 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。这种活动可能构成国际法规定的不法行为，可能导致不稳定和连带影响，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，欧洲联盟联合外交对应框架是欧洲联盟网络外交方法的一部分，有助于预防冲突、减轻网络安全威胁和增进国际关系的稳定。该框架鼓励合作，促进减轻当前和长期威胁，并从长期来影响恶意行为者的行为。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呼吁国际社会加强国际合作，支持一个开放、自由、全球性、稳定和安全的网络空间，其中充分适用人权、基本自由和法治。他们决心继续努力防止、阻止、威慑和应对恶意活动，寻求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下的网络安全数字转型战略。[9] 欧洲联盟的数字十年网络安全战略旨在促进和保护基于人权、基本自由、民主和法治的开放、自由、全球性、稳定和安全的网络空间。该战略载有具体建议，以应对复原力、预防、威慑和应对网络威胁，推进全球开放的网络空

[6] 《欧盟理事会关于网络外交问题的第 6122/15 号结论》。

[7] 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。

[8] 《欧盟理事会关于欧洲联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 9916/17 号结论草案》。

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

间。防止技术滥用、保护关键基础设施和确保供应链完整，也使欧洲联盟能够遵守联合国负责任的国家行为规范、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，界定负责任行为的规范，倡导在网络空间适用现行国际法，同时协助欧洲联盟以外的国家进行网络安全能力建设，并促进网络问题上的国际合作。欧洲联盟继续与国际伙伴合作，推进和促进一个开放、自由、全球性、稳定和安全的网络空间，在这个空间，国际法，特别是《联合国宪章》得到尊重，负责任的国家行为自愿、非约束性规范、规则和原则得到遵守。为推进网络空间的和平与安全，显然需要执行前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商定、经大会认可的联合国网络空间负责任国家行为框架。欧洲联盟与 60 个联合国会员国一道，提议制定一项行动纲领，以促进网络空间中负责任的国家行为。

行动纲领以大会一致认可的现有成果为基础，在联合国提供了一个常设、包容和注重行动的机制，以推进执行共识报告，支持各国的国家网络安全政策，特别是通过针对受益国确定的需求的能力建设方案提供支持。它还在联合国内部提供了一个体制机制，以改善与私营部门、学术界和民间社会等其他利益攸关方的合作，履行各自的责任，维护一个开放、自由、安全、稳定、无障碍及和平的信通技术环境。行动纲领将以互补和协调的方式与其他相关进程一起运作，如 2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组。

为加强其预测、遏制和应对当前和快速出现的威胁和挑战的能力，维护欧洲联盟的安全利益，欧洲联盟于 2022 年 3 月 21 日正式批准了战略指南。[10] 该指南为欧洲联盟提供了一个雄大的行动计划，以便到 2030 年加强其安全和防御政策，包括加强欧洲联盟网络外交工具箱，进一步发展欧洲联盟网络防御政策，以更好地防备和应对网络攻击。

欧洲联盟及其成员国回顾，欧洲联盟理事会于 2022 年 5 月 23 日通过了关于发展欧盟网络态势的结论。这一态势旨在表明，欧洲联盟决心对试图阻止欧洲联盟安全和公开进入网络空间的威胁行为者做出立即和长期的回应。

### 工作组报告和政府专家组报告中提到的概念的内容

#### *现有威胁和新出现的威胁*

欧洲联盟及其成员国确认，网络空间为经济增长以及可持续和包容性发展提供了重大机遇。尽管如此，政府专家组前几份报告和工作组报告中[11] 指出的信息和通信技术的严重威胁依然存在，并带来不断变化的挑战。

欧洲联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通技术，对通过网络盗窃知识产权的增加感到关切。

[10] 第 7371/22 号，“安全与防务战略指南-建立一个保护其公民、价值观和利益并为国际和平与安全作出贡献的欧洲联盟”。

[11] A/75/816。

这种行为破坏和威胁经济增长以及国际社会的完整、安全和稳定，会导致不稳定和连锁反应，增加冲突风险。

2019 冠状病毒病(COVID-19)大流行疫情证明了恶意信通技术活动的风险和后果。欧洲联盟及其成员国观察到针对重要运营商的网络威胁和恶意网络活动，承认成员国及其合作伙伴的关键信息基础设施、向公众提供基本服务的基础设施、对互联网普遍可用性或完整性至关重要的技术基础设施、以及卫生和其他关键部门实体的脆弱性。欧洲联盟及其成员国特别感到震惊的是，影响信息和通信技术产品和服务的安全和完整性的活动有所增加，这可能会产生系统性影响。此外，俄罗斯在网络空间的不负责任行为也是其非法和无理入侵乌克兰的一个组成部分，在这种情况下，欧洲联盟及其成员国看到了使用破坏性工具(如“wipers”)进行的网络攻击造成系统故障，以及针对乌克兰的服务中断、入侵企图、破坏和分布式拒绝服务攻击，这有可能蔓延到其他国家，特别是乌克兰的邻国。

欧洲联盟及其成员国谴责这种网络空间的恶意行为，包括旨在利用漏洞的恶意信通技术活动，并强调继续支持提高全球网络复原力。任何阻碍重要基础设施的企图都是不可接受的，会危及人们的生命。

欧洲联盟及其成员国呼吁每个国家不要在知情的情况下让其领土被用于利用信通技术在网络空间实施国际不法行为，并根据国际法以及政府专家组 2010 年、2013 年、2015 年和 2021 年共识报告和和工作组 2021 年共识报告，对从其领土开展此类活动的行为者采取适当行动。欧洲联盟及其成员国再次强调，各国应采取一切适当措施和合理可行的步骤来查明、调查和处理这一情况。

此外，正如政府专家组和工作组以前报告所承认，鉴于信通技术的独特性，欧洲联盟在国际安全背景下处理网络问题的方法仍然适应于新的技术发展，同时也指出，网络空间负责任的国家行为规范在技术上是中性的。这符合这一概念，也符合联合国对现行国际法适用于新领域的承认。

欧洲联盟及其成员国只能支持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法的信息和通信技术、系统或服务的开发和使用。

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一个依据基于规则的国际秩序的有效多边体系，其在应对网络空间当前和未来全球挑战方面取得成果。

一个真正普遍的网络安全框架只能基于现行国际法，包括整部《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，正如政府专家组 2010 年、2013 年、2015 年和 2021 年报告以及 2021 年报告第 71(b)至(g)段和工作组所确立的原则所确认，现行国际法适用于网络空间的国家行为。

国际人道法等国际法纳入了人道、区分、谨慎、军事必要和相称性原则，适用于网络空间的国家行为，并通过为其合法性设定明确的界限而提供全面保护，即使在冲突背景下也是如此。欧洲联盟强调，国际人道法不是冲突的促成因素；相反，国际人道法界定了有关军事行动的规则，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。欧洲联盟及其成员国欣见人权理事会[12] 和大会以及政府专家组和工作组也确认了这些原则。

出于这些原因，欧洲联盟及其成员国不呼吁在现阶段为网络问题制定新的国际法律文书，强调需要开展更多工作，以澄清国际法如何适用于网络空间。

欧洲联盟及其成员国重申，它们支持继续对话与合作，以促进对各国利用信息和通信技术适用现行国际法的共同理解，并支持努力在法律上澄清如何适用现行国际法，因为这将有助于维护和平、预防冲突和确保全球稳定。

我们继续支持正在进行的努力，以促进现行国际法在网络空间的应用，包括就现行国际法在网络空间的应用交流信息和最佳做法。我们致力于继续报告各国关于国际法如何适用于各国使用信息和通信技术的立场，因为这有助于提高透明度，促进全球对国家做法的理解，这对于维护长期和平与稳定至关重要，并减少了通过网络空间行为发生冲突的风险。应进一步重视提高对现行国际法适用性的认识和能力建设，以此作为促进网络空间稳定和防止冲突的手段。

负责任的国家行为规范、规则和原则

欧洲联盟及其成员国鼓励所有国家继续开展并推进大会、特别是第 76/19 号决议一再认可的工作，并推动执行这些商定规范和建立信任措施，这些规范和措施在预防冲突方面发挥着重要作用。

正如政府专家组在 2010 年、2013 年、2015 年和 2021 年连续几份报告中所阐述，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，遵守负责任的国家行为的自愿、不具约束力的规范、规则和原则及其在网络空间的实施。欢迎在工作组内继续开展包容性和建设性的对话，以进一步深化关于这一框架以及与使用信通技术相关的安全挑战的讨论。我们认为，切实可行的前进道路应该鼓励加强合作和透明度，以分享最佳做法，包括探讨如何通过相关倡议和框架，如区域组织和机构，适用政府专家组的现行规范，以促进提高认识，有效执行商定的负责任的国家行为规范。

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平台，为具有共同关切和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、东南亚国家联盟区域论坛、美洲国家组织和其他区域环境中制定和实施网络信任建设措施，包括合作和透明度措施，将提高国家行为的可预测性，减少信通技术事件可能引发的误解、升级和冲突的风险，从而促进网络空间的长期稳定。

[12] 见人权理事会第 20/8 号决议。

信息和通信技术安全和能力建设方面的国际合作与援助

为了防止冲突和减少滥用信通技术造成的紧张局势，欧洲联盟及其成员国力求加强全球复原力，特别强调发展中国家，以此作为应对经济和社会数字化相关挑战的手段，并降低潜在犯罪者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，并支持促进交流最佳做法的举措，无论是通过直接接触、双边接触，还是通过区域和多边机构进行接触。

欧洲联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、更可信的网络空间。我们认识到，所有相关行为体都有责任参与这方面的能力发展，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和稳定，为此鼓励和促进就网络空间负责任的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的支持下，促进专门针对受益国确定的需求的能力建设方案，如行动纲领，并确定促进所有利益攸关方参与执行负责任行为框架的机制。