联合国 A/74/120

大 会

Distr.: General
24 June 2019
Chinese
Original: English/French/Spanish

第七十四届会议

暂定项目表* 项目 95

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/74/50。

19-10580 (C) 260719 010819

一. 导言

1. 大会第七十三届会议在议程项目 96 下通过了从国际安全角度看信息和电信领域的发展的两项决议。

2. 大会于 2018 年 12 月 5 日通过了从国际安全角度看信息和电信领域的发展的第 73/27 号决议，并于 12 月 22 日通过了从国际安全角度促进网络空间国家负责任行为的第 73/266 号决议。

3. 在第 73/27 号决议第 4 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政府专家组报告所载评估和建议，继续向秘书长通报它们对下列问题的看法和评估：

(a) 对信息安全问题的一般看法；

(b) 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；

(c) 决议第 3 段所述概念的内容；

(d) 国际社会为加强全球一级的信息安全可能采取的措施。

4. 大会在第 73/266 号决议第 2 段中请所有会员国考虑到政府专家组报告所载的评估和建议，继续向秘书长通报它们对下列问题的看法和评估：

(a) 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；

(b) 政府专家组各项报告所述概念的内容。

5. 根据这一请求，2019 年 2 月 6 日向所有会员国发出了一份普通照会，请各国提供有关该主题的信息。截至本报告编写之时收到的回复载于第二节。2019 年 5 月 15 日之后收到的其他答复将以来件原文张贴在裁军事务厅网站(www.un.org/disarmament/ict-security)。

二. 从各国政府收到的答复

阿根廷

[原件：西班牙文]
[2019 年 5 月 15 日]

对信息安全问题的一般看法

信息和通信技术(信通技术)为经济、社会、文化、科学和政治进步提供了前所未有的机会，这种技术的发展与更高水平的发展和福祉密不可分。网络空间已经成为个人和组织生活的基本组成部分，基本服务越来越依赖于计算机网络。

然而，尽管网络空间使互动和进步达到了前所未有的水平，但它也受到多种不同威胁和行为者的影响，这些行为者危及人民、公司、机构和国家的安全以及国际和平与安全。

经济发展、基本服务的提供、公民的福祉和国家机构的正常运作在很大程度上依赖于网络安全。

广泛使用相对低成本的智能设备增加了新的风险。使用这些设备可以在没有最低安全级别的情况下访问互联网，潜在网络攻击的范围因而扩大。

这一新增的风险需要国家政策和企业责任战略加以配合和应对。

同样，一些国家在开发解密设备/应用程序和/或后门机制上的计划也产生额外风险。

国家一级为加强信息安全所作的努力

2017 年，阿根廷政府通过第 577/2017 号法令设立了网络安全委员会，由内阁执行办公室现代化政府秘书处担任主席，成员如下：内阁执行办公室战略事务秘书处、国防部、安全部、外交和宗教事务部以及司法和人权部。该委员会的部分作用是制定一项国家网络安全战略以及实施该战略的行动计划。

设立网络安全委员会为建立事件信息交流论坛提供了便利，使应对得以更好地协调；2018 年在阿根廷举行的二十国集团会议便证明了其有效性。

阿根廷根据内阁执行办公室第 580/2011 号决议，制定了国家关键信息和网络安全基础设施方案。该方案的目标是，界定和保护公共和私营部门以及国际组织的战略和关键基础设施，管理关于安全事件报告的所有信息，并有组织、综合性地为潜在的解决方案提供指导等。

在这一背景下，就公共机构极易受到数字安全风险影响的情况制定了一项规程，订定了与私营部门的联系。

目前正在制定一项规范，将确立“关键信息基础设施”的定义，这是确定基础设施是否关键的标准，并对各个部门的基础设施进行分类。

在国家关键信息和网络安全基础设施方案的框架内，根据第 2/2013 号令成立了计算机安全事件响应小组。

在立法方面，2008 年通过第 26.388 号法案将网络犯罪纳入《刑法》。2013 年，国会通过第 26.904 号法案，将诱骗儿童定为犯罪，并加大了对互联网上儿童色情相关犯罪的处罚力度。2017 年，通过国会通过的第 27.411 号法案，阿根廷加入了《网络犯罪公约》。2019 年 1 月，国会通过第 27.482 号法案，修订了《联邦刑事诉讼法》，获取数字证据的工具(数字通信截取、数据记录和保留以及计算机系统)现已涵盖在内。

目前正在进行修订《刑法》的法律草案工作，这将把一些与信息技术有关、特别是破坏关键基础设施的犯罪定为犯罪。

为了提高打击网络犯罪的能力，司法和人权部在美洲国家组织(美洲组织)和欧洲委员会等国际机构的支持下，为刑事司法系统行为者举办了多个关于网络犯罪、数字证据处理和现代调查方法的培训讲习班。讲习班在全国不同地区举行，

对象是法官、检察官以及联邦和省安全部队成员。2016 年至今，全国近 500 名法官和检察官参加了这些培训方案。

第 996/2018 号法令通过的《阿根廷数字议程》的一个目标是，发展网络安全能力以便在数字环境中建立信任。在这方面，为了加强提高对使用社交媒体和互联网风险的认识的能力，并注重普通民众，特别是被认为处于风险中的群体，与 Punto Digital 方案协作制定了培训培训员的方案。网络欺凌、诱骗儿童、网络钓鱼、网络安全等议题，以及照顾和收容受害者、预防和发现计算机相关犯罪的战略等也已着手进行，青年、青少年和老年人是工作的重点。

关于保护个人数据，阿根廷通过了第 25.326 号法案，阿根廷是本区域第一批建立保护个人数据监管框架的国家之一。阿根廷还加入了欧洲委员会《关于在自动处理个人数据方面保护个人的公约》。

2019 年 6 月 1 日，《关于在自动处理个人数据方面保护个人的公约》及其附加议定书在阿根廷共和国生效。

为促进信息安全领域的国际合作而采取的措施

阿根廷推动在双边、区域和多边各级建立旨在促进网络空间和平与安全的协定，努力参与国际机构在网络安全领域的全部工作，积极参与所有涉及网络安全的国际学术和技术领域。

在这方面，阿根廷积极参与网络犯罪公约委员会的活动，并支持尚未加入但希望加入该公约的国家。该条约为其成员提供的具体优势包括加入 24/7 网络，该网络为缔约国之间的援助提供了一个渠道，并为它们之间的刑事调查提供了便利。

然而，考虑到网络犯罪的跨国性质和建立全球应对机制的必要性，阿根廷支持《网络犯罪公约》下的进程和有关寻求在联合国框架内推动就这一领域的普遍法律框架进行谈判的论坛(维也纳进程)。

2013 年和 2014 年，阿根廷参加了从国际安全角度看信息和电信领域的发展政府专家组，并寻求为大会就这一主题的讨论作出贡献。

阿根廷意识到能力建设至关重要。阿根廷是全球网络专门知识论坛的成员，并与美洲组织、智利、墨西哥、爱沙尼亚和西班牙一道参加了美洲组织网络安全倡议。

2018 年 11 月，阿根廷加入了“网络空间信任与安全巴黎呼吁”。

在区域一级，阿根廷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的会议，并为拉丁美洲和加勒比网络安全观察站的活动作出了贡献，为美洲组织-美洲开发银行题为《网络安全：我们拉丁美洲和加勒比准备好了吗？》的联合研究报告第二版提供了信息。

阿根廷于 2018 年 5 月 29 日和 30 日主办了第二届性别与网络安全国际论坛，该论坛是与美洲组织共同组织的。

在南方共同市场(南共市)的范围内，阿根廷推动订立了《南共市数字议程》，该议程也涉及网络安全。

在双边一级，2017 年，阿根廷与西班牙签署了一项关于网络安全的机构间谅解备忘录。同年，阿根廷与美国商定成立政府间双边网络政策工作组，重点关注网络安全问题，并于 2018 年与智利签署了网络安全、网络犯罪和网络防御合作协定。阿根廷认为，有必要与所有国家和区域保持开放的网络安全对话渠道。

关于政府专家组报告内容的评论意见、大会第 73/27 号决议以及国际社会为加强全球一级的信息安全可能采取的措施。

阿根廷支持并同意政府专家组报告中提到的概念的内容。

各国有责任确保网络空间的和平与安全；各国因此必须负责行事，根据专门讨论这一问题的联合国大会第 69/28、70/237、71/28、73/187、73/266 号决议，采用现有国际法并制定新的自愿标准、国际合作和建立信任措施。

双边、区域和多边合作对于建设各国所需的国家能力至关重要，用于加强各国的网络空间威胁的预防、检测、预警和应对系统。

有效打击网络犯罪对于确保网络空间的和平与安全至关重要，因此这是国家间合作处理的最高优先事项。

阿根廷同意大会第 72/27 号决议的重要性，特别是该决议第 1 段所载的国家负责任行为的一套国际规则、规范和原则。然而，应当指出，由于网络空间威胁的性质及其演变速度，各国应尽最大努力防止非国家行为者利用其领土使用信通技术进行国际不法行为。然而，无法保证各国能够做到这一点。

此外，鉴于网络空间威胁的全球性和跨国性，国际社会应更加重视所有国家的能力建设，尤其应支持发展中国家加强网络空间威胁的预防、检测、预警和应对系统。

阿根廷认为，有必要继续在联合国进程框架内开展工作。这些进程包括，大会第 73/27 号决议设立的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。必须就国际法如何适用于网络空间达成共识，这需要就每个国家的愿景进行对话和提高透明度。还需要至制定机制和工具，以便能够快速适应技术迅猛进步不断带来的变化和新挑战。

哥伦比亚

[原件：西班牙文]
[2019 年 5 月 15 日]

一般看法

哥伦比亚政府赞同，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；国际法对各国使用信息和通信技术的适用；以及国家负责任行为的规则、规范和原则。

各国负责任地使用信通技术，以及将信通技术作为经济和社会发展的工具加以推广，对于国际稳定至关重要。

哥伦比亚赞成互联网应自由、开放和安全，各国必须拥有有效合作打击网络犯罪所需的工具，加强其国家能力，加强国家间的建立信任措施。

必须认识到与以下事项有关的挑战并加以应对，这些挑战包括：数字身份；与互联网服务提供商的合作；数字证据及其收集、存储、监管链、认证和有效性技术；以及数据保护、隐私和对个人权利和自由的尊重。

然而，我们认为，网络犯罪问题应由联合国预防犯罪和刑事司法委员会继续从技术和政治角度进行讨论。网络犯罪问题政府间专家组应作为主要论坛，而不应新设限制各国参与的其他小组，如从国际安全角度看信息和电信领域发展政府专家组。

哥伦比亚有兴趣参加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政府专家组的国际讨论。哥伦比亚已向后者提名一名候选人。如果无法参加政府专家组，哥伦比亚将通过美洲国家组织(美洲组织)为此目的设立的区域协商论坛作出贡献。

与大会关于从国际安全角度促进网络空间国家负责任行为的第 73/266 号决议、从国际安全角度看信息和电信领域的发展的第 73/27 号决议有关的意见

哥伦比亚政府赞同必须改善国家间的协调与合作，以促进各国负责任地使用信通技术；这对于国际稳定以及信通技术在社会和经济发展中发挥真正作用都极为重要。

哥伦比亚在 2014 年至 2015 年积极参加了政府专家组，在此期间获得了最新的背景文件，哥伦比亚完全同意其中所载的概念、考量、解释和建议。

哥伦比亚政府认为，国际法应适用于虚拟世界和物理世界。这一立场或愿景不仅由联合国政府专家组进行了审议并就国际法的基本适用方式达成了共识：还反映在欧洲安全与合作组织和东南亚国家联盟的建立信任的措施中，以及七国集团关于网络空间国家负责任行为的《卢卡宣言》中。编写塔林手册 2.0 的专家组也一致支持这一立场或愿景。在任何情况下，国际法对网络行动的适用性均需作进一步研究，以确保在适用性解释方面没有灰色地带或差异。

对于技术不太先进的国家，最重要的是订立协议，以确保网络空间不会因对这些国家的潜在影响而成为冲突日益加剧的舞台，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。

在技术不太先进的国家，对关键网络基础设施的任何损害都会产生巨大影响。这不仅是因为对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。

我们认为，必须就《联合国宪章》的影响及其对维护和平与稳定的适用性发起最高级别的讨论，以便营造一个开放、安全、稳定、无障碍与和平的信通技术环境。

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以及国内挑战

为应对不确定性、风险、威胁、脆弱性和数字事件，2011 年，政府发布了国家经济和社会政策委员会第 3701 号文件“网络安全和网络防御政策指南”。这项政策侧重于国家在以下方面的努力：应对数字威胁的增加，这一威胁已对哥伦比亚产生重大影响；制定一个应对网络安全挑战的监管和体制框架。下文概述了在执行政策指南以及 2014 年和 2015 年在修订指南上取得的进展。

第 3701 号文件的总体目标是，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。为实现这一总体目标，制定了三个具体目标：(a) 建立适当的机构，负责对网络事件和紧急情况的预防、协调、应对、监测和控制，并制定建议，以应对国家网络安全和网络防御面临的威胁或风险；(b) 提供关于信息安全的专门培训，并扩大网络防御和网络安全研究的范围；(c) 加强网络安全和网络防御立法，强化国际合作；并加快哥伦比亚加入这一领域的各项国际文书。

为制定这一政策，并根据国际最佳做法，特别是北大西洋公约组织(北约)、经济合作与发展组织、国际电信联盟和美洲组织等多边组织，以及分析了如何在当前数字环境中解决数字安全问题的全球私营部门组织提出的原则和建议，国家政府展现了新愿景，并于 2016 年发布了国家经济和社会政策委员会第 3854 号文件“国家数字安全政策”，其有效期至 2019 年 12 月，其中确定了以下目标：在合作、协作和援助框架内，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。这将有助于国家数字经济的增长，从而促进国家的经济和社会繁荣。

为制定这一公共政策的总体目标，制定了以下具体目标：

(a) 建立与强调风险管理相一致的数字安全体制框架；

(b) 创造条件，使各利益攸关方能够管理其社会经济活动中的数字安全风险，并建立对使用数字环境的信心；

(c) 在国家和跨国两极加强数字环境中个人和国家的安全，重点是风险管理；

(d) 加强数字环境中的国防和主权，重点是风险管理；以及

(e) 建立永久性战略机制，促进国家和国际两级在数字安全事项上的合作、协作和援助。

自国家经济和社会政策委员会于 2016 年 4 月通过国家数字安全政策行动和监测计划以来，主管公共实体一直在开展该计划设想的活动，以期实现该政策的总体目标和具体目标。

总结所采取的一系列行动，以下成就值得强调：

- 我们已着手建立一个经过协调的体制框架，其中涉及执行国家数字安全政策的各利益攸关方；特别是，我们在共和国总统办公室内设立了国家数字安全协调员的职位，并确保哥伦比亚网络应急小组的工作将继续。
- 我们已着手设计并在国家政府中付诸实施数字安全风险管理模型的进程，该模型考虑到这一政策的概念框架、国际安全标准和全面的国家风险管理框架。
- 我们已着手创造条件，使各利益攸关方能够管理其社会经济活动的数字安全风险，并建立对使用数字环境的信心；特别是，我们正在对哥伦比亚数字犯罪和违法行为的影响进行研究，并正在调整信通技术部门的监管框架，以加强数字安全。
- 我们已起草计划，以加强业务、行政、人力和科学能力以及组成现有国家政府机制的机构的物质和技术基础设施。
- 我们与伙伴国家和重要行业代表签署了国际合作协定，旨在加强能力和交流威胁方面的信息。2017 年，北约一致批准与哥伦比亚签署一项单独的协作与合作方案，使我国成为拉丁美洲第一个获得这一地位并成为全球伙伴的国家。这项法律文书包含的一个要点是提高网络技能。哥伦比亚认为，加强在联合国系统内不同环境下运作的现有举措十分重要。

关于建立与强调风险管理相一致的数字安全体制框架的目标，我们取得了以下进展：设立国家数字安全协调员职位(配备技术和法律工具)，并设立数字安全委员会，该委员会将向公务员提供管理和绩效指导，并作为国家政府中最高级别的机构间和部门间实体，就数字安全问题提供高级别指导。我们还设计了关键工具，如数字安全风险管理模型，国家行政部门实体必须采用和实施该模型。2018 年 8 月，公务行政部门还将该模型纳入了《公共实体处理有关管理、腐败和数字安全风险和设计审计的指南》。

查明的挑战包括，需要在负责确定体制框架内网络安全和网络防御事务的机构中实施和加强数字安全风险管理。还有必要加强部门能力，为推动建立部门计算机安全事件响应小组制定更有效的方法，有必要为数字安全委员会的有效发展制定路线图，为部门和地方联络设施与国家数字安全协调设施之间的联系制定有效规程，并使所有利益攸关方能够识别、评估和有效管理风险。

关于第二个目标，即创造条件，使各利益攸关方能够管理其社会经济活动中的数字安全风险，并建立对使用数字环境的信心，在制定国家数字安全议程草案方面取得了一些进展。然而，有必要继续加强所有不同利益攸关方讨论之间的联系，就这一主题作出更多学术贡献(研究)，并支持公共实体采用数字安全风险管理模式。开展了若干提高认识运动，如“我信任信通技术”方案，并在美洲组织的支持下，编写了《2017 年哥伦比亚网络事件、威胁和攻击的经济影响研究》，2018 年也进行了同样研究。

作为挑战，我们认识到，有必要确定应继续和加强研究的数字安全相关领域，确定一个明确和有效的协调和沟通模式，以促进建立必要的数字安全法律框架，支持各利益攸关方的数字转型，高效传达政府高层的战略研究的结果，以指导决策，并重新确定发展教育内容的战略，以便纳入教育系统各级使用的教学课程。

关于第三个目标，即在国家和跨国两级加强数字环境中个人和国家的安全，重点是风险管理，我们在建设关键行为者能力的计划、网络犯罪统计报告和加强国家网络安全负责人的风险管理能力方面取得了进展。

面临的挑战是，迫切需要执行计划，以加强负责网络安全的机构和实体的业务、行政、人力和科学能力以及物质和技术基础设施，并制定准则，调整现有法律和监管框架以满足下列方面的需求：(a) 分析、预测、预防、侦查、应对和调查数字环境中的网络不法行为、网络犯罪和现象，以及涉及使用数字环境的不法行为和犯罪；(b) 起诉和定罪新形式的犯罪，包括协助洗钱的网络不法行为；(c) 根据国家数字安全政策的基本原则，实现负责数字环境中的安全、国防和情报机构的现代化。

关于第四个目标，即加强数字环境中的国防和主权，重点是风险管理，在以下方面取得了进展：制定提高关键行为者能力的计划，定期更新国家关键网络基础设施的目录，制作关键网络基础设施保护计划的部分内容，建立一系列部门计算机安全事件响应小组，协助对影响国家关键网络基础设施(如政府、金融部门和电力部门基础设施)的数字事件进行适当管理，帮助某些利益攸关方参与国家和国际层级的模拟和培训活动，以期发展负责国家关键网络基础设施和数字环境中国防的各利益攸关方的技能和能力。

实现这一目标的挑战是，需要顾及新形势，从最高级重新制定保护和防卫国家关键网络基础设施的准则，还需要发布一份正式协议，用于管理和应对影响此类基础设施的数字安全事件。还需要制定一项国家政府战略，用于集中开展与国防有关的数字安全的提高认识和培训工作。

最后，关于第五个目标，即建立永久性战略机制，促进国家和国际两级在数字安全事项上的合作、协作和援助。我们在坚持促进国际一级的数字安全合作、协作和援助的机制上取得了进展。突出例子包括，加入《网络犯罪公约》的进程，以及在制定国际合作、协作和援助战略议程草案上的进展。

关于挑战，有必要确定在数字安全事项方面哥伦比亚应当参与的机构并确定其优先次序，同时确定利益攸关方之间协调和沟通的明确有效模式，以便能够起草和执行关于促进国家和国际两级在数字安全事项上的合作、协作和援助的战略文件。

鉴于上述所有情况，并且由于国家经济和社会政策委员会 2016 年第 3854 号文件确立的国家数字安全政策所含的一项行动计划将于 2019 年到期，在美洲组织的支持下，国家政府正在起草一项应对上述挑战的新政策。

古巴

[原件：西班牙文]
[2019 年 4 月 29 日]

应当为人类的共同利益和平利用新的信通技术，促进所有国家的可持续发展，无论其科学和技术发展水平如何。

此类科学和技术发展可能具有民用和军事用途，有必要防止这种进步危及各国的国际安全。

只有通过所有国家之间的通力合作，才能防止网络空间成为军事行动的战场。

在这方面，我们支持根据大会第 73/27 号决议设立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，以期使联合国关于信通技术使用安全问题的谈判进程更加民主、包容和透明。

我们认为，有必要确立具有法律约束力的国际监管框架，该框架应对现行国际法形成补充，但要适用于信通技术。

所有国家都必须尊重这一领域现有的国际标准。在接入另一国的信息或电信系统时，应遵守所缔结的国际合作协定，并以征得相关国家同意的原则为前提。交互的性质和范围必须尊重准予接入国的法律。

出于破坏各国法律和政治秩序的公开或秘密目的，将电信用于敌对用途的做法，违反了这一领域的国际商定规范，是对这种媒介非法和不负责任的使用。

美国不断通过非法电台和电视广播攻击古巴的空中电波，传播专门用于煽动人心、推翻古巴人民所建立的宪法秩序的节目。

2018 年，平均每周有 1 653 小时的反古巴节目使用 20 个频率从美国境内传输，这违反了《联合国宪章》的宗旨和原则、国际法以及国际电信联盟的规则。

古巴再次要求立即终止上述侵略性政策，这些政策侵犯了古巴主权，也不符合各国在相互尊重和合作基础上发展关系的原则。

美国政府近 60 年来对古巴实施的经济、商业和金融封锁给古巴人民造成严重损失，包括在使用和享受信通技术方面。

拉丁美洲和加勒比各国的国家元首和政府首脑在拉丁美洲和加勒比国家共同体(拉共体)第二次国家元首和政府首脑会议上宣布该区域为和平区，以便除实现其他目标外，促进区域内各国之间以及与其他国家的合作和友好关系，无论各国在政治、经济和社会制度或发展水平上有何差异，同时实现宽容及睦邻和平共处。

2017 年 1 月在蓬塔卡纳(多米尼加共和国)举行的拉共体第五次首脑会议再次强调，必须将包括互联网在内的信通技术作为促进和平、人类福祉、发展、知识、社会包容和经济增长的手段。

埃及

[原件：英文]
[2019 年 5 月 9 日]

导言

过去 30 年来，互联网、智能手机以及现代信息和通信技术(信通技术)设备的使用在世界范围内急剧增加，同时信通技术在商业、商贸、政府服务、教育、知识、娱乐、旅游、保健以及其他经济、社会和文化活动中的使用量也极为庞大。在认识到电信和互联网使用量持续增长以及电子交易和电子服务激增所带来机遇的同时，还必须认识到信通技术基础设施和电子交易总体面临的威胁和挑战，并采取应对措施，因为这些威胁和挑战尤其会削弱对电子服务和电子商务的信心和信任。

因此，埃及对发展和应用最新信息技术和电信手段的重要作用非常重视，以便在国家和国际两级实现经济和社会进步。埃及还积极支持为人类的共同利益利用信通技术，促进所有国家的可持续发展，无论其科学和技术发展水平如何。此外，埃及还认为，联合国应发挥核心作用，牵头开展相关国际工作，促进会员国之间的对话，就国际法及规范、规则和原则适用于信息领域负责任的国家行为问题、包括执行具有法律约束力的文书问题达成共识。

最重大的网络挑战和威胁

1. 渗透和破坏信通技术基础设施的威胁

最近出现了极为严重的新型网络攻击，这些攻击的目标是干扰关键服务，植入恶意软件和病毒，破坏或扰乱信通技术基础设施和关键工业控制系统，特别是核电、石油、天然气、电力、航空、各类运输、国家重要数据库、政府服务、保健、紧急援助服务等实体的重要设施。此类网络攻击会利用包括无线网络和移动存储在内的几种渠道，以及电子邮件、网站、社交媒体、电信网络等其他常见渠道，可严重影响关键基础设施以及相关服务和业务的使用。在实际中，关键设施即使没有直接接入互联网，也可能遭到高级网络攻击。

2. 网络恐怖主义和网络战的威胁

最近，各种使用先进技术的危险网络攻击和网络犯罪蔓延，这些技术包括云计算、窃听和网络入侵设备、高级加密、针对计算机系统和数据库的自动化黑客工具等。此外，高级恶意软件可破坏网络安全系统，危害计算机系统，形成僵尸网络，而僵尸网络随后又可用于实施各种犯罪和非法活动。自动化僵尸网络可能由数万、数十万或数百万台受损计算机组成，这些计算机可用于发起严重的网络攻击，例如针对目标网络和网站进行分布式拒绝服务攻击，以达到实施破坏、开展恐怖主义活动和(或)敲诈勒索的目的。

要制作复杂精密的计算机病毒，往往需要将只有在技术先进国家才能获得的高级知识和非常规专业技能用于战术、战略和战争目的，配合或在某些情况下取代常规军事攻击，发动所谓的网络战。但恐怖主义组织正在转让、复制或仿造此

类恶意技术，用于实施恐怖主义行动和有组织犯罪，威胁和干扰信通技术基础设施，以达到敲诈勒索和(或)从事工业间谍活动的目的。埃及重申主要网络安全专家的立场，他们预计猛烈和复杂的网络攻击将会在今后一段时期内激增。

3. 窃取数字身份和私人数据的威胁

窃取数字身份是威胁互联网用户和电子服务未来的最严重犯罪之一。被窃取的凭证和个人数据可用于在网络空间冒充他人，可能导致金钱和财产损失，也可能会使受害者的姓名卷入可疑或非法活动。窃取身份者通常使用互联网上已有的信息，特别是来自以下来源的信息：开放的社交媒体和专业网络；国家数据库；政府服务、社会保障服务和保健网络；电子商务网站；虚拟市场；电子支付网络；自动柜员机；证券交易所。此外，用于进行电子交易的工具和系统可以被入侵、盗用或损坏，从而严重危及用户的利益和电子服务的未来。广泛的大规模攻击可能会影响国家金融部门。公共机构和公司的数据也可以被窃取，造成巨大的物质和信誉损失，导致声誉受损，客户流失，无形资产价值下降，可能损害整个国民经济。

新兴网络威胁严重性的主要方面

由于以下三个主要方面，新兴网络威胁可达到极为严重的程度：

1. 新兴网络威胁经常使用先进和精密技术，而这些技术往往由高度发达国家和大公司垄断。其中许多技术是最高机密，不得出口。此外，某些技术的可出口版本还可能包含后门或漏洞，或许会造成额外的威胁。

2. 新兴网络威胁易于传播。攻击者可以非常轻易和迅速地散播恶意病毒，发起分布式拒绝服务攻击和其他高级网络攻击，因为信通技术使用广泛，攻击者从任何地点都能以较低的成本轻易发起远程攻击，跨界传输病毒。此外，这些威胁和风险的主要来源难以追踪，往往无迹可寻，因此无法加以解决和消除。

3. 新兴网络威胁可产生广泛影响，网络攻击可以对基础设施造成大规模的直接和间接影响，导致严重破坏和损失。此外，此类攻击还可远程实施并以不可预测的方式急速扩散，有可能影响关键实体和大量公民(成千上万人或成百上千万人)。

今后的方向：应对网络挑战

网络攻击和网络犯罪可超越国家的地理边界，通常依赖传统和技术性的有组织犯罪网络。因此，在对付此类攻击和犯罪时，必须采用打击犯罪和应对网络威胁的传统国际合作机制，同时建立设有特殊机制、可处理新兴技术发展情况的立法和监管框架。要有效应对网络攻击和网络犯罪，就需要在国家一级、提供和运营关键部门基础设施的合作伙伴以及提供服务的合作伙伴(包括政府部门、机构和公司)之间开展合作与协调。此外，国际和区域合作与协调非常必要，需要将关键的国际组织、区域会议以及专业和专门的国际论坛纳入其中。

埃及的贡献

埃及认识到国际合作在应对网络安全挑战方面的重要意义。埃及专家为一些相关的政府专家组作出贡献，这些专家组获得大会授权，从国际安全的视角就网络安全问题提出商定建议。此外，埃及作为国际电信联盟(国际电联)成员，参与了国际电联网络安全问题高级别专家组及其全球网络安全问题议程活动。另外，埃及还提议设立国际电联理事会儿童在线保护问题工作组，并于 2010 年至 2017 年担任该工作组主席。埃及还参加并主办由国际电联、伊斯兰合作组织、欧洲安全与合作组织、经济合作与发展组织、事件应对和安全小组论坛等国际组织举办的区域网络演习以及网络安全会议和讲习班，并与全球移动通信系统协会等专业组织共同参与国际和区域网络安全研究。此外，埃及还积极参与非洲和阿拉伯区域的工作，促进有助于建立信任和建设能力的透明化措施，传播最佳做法。埃及也与一些国家、国际组织和合作伙伴开展了双边磋商和谈判，在这一战略领域缔结双边合作协定。

在国家层面，根据《埃及宪法》第 31 条，埃及于 2014 年底在内阁一级设立了关键信息基础设施保护和网络安全最高理事会(即埃及网络安全最高理事会)。该理事会由通信和信息技术部长担任主席，成员来自关键部门和主要安全机构。在业务层面，国家计算机应急准备小组充当该理事会的技术部门。2017 年，理事会制定了埃及第一项国家网络安全战略。该战略的范围、结构和目标符合国家需要，遵循国际规范、规则和原则。同样，该战略的执行工作也遵照同样的精神。

结论

埃及重申亟需加强发展中国家在信通技术安全领域获得的能力建设和技术援助，特别是考虑到在许多情况下，网络空间的安全可能取决于最薄弱的环节。

此外，从国际安全角度看信息和电信领域的发展政府专家组开展的有效工作以及秘书长向大会转递的相关成果报告代表了朝着正确方向采取的重要步骤。其中的主要内容是强调各国必须承诺遵守《联合国宪章》的原则和其他国际法原则，包括：主权平等；以和平方式解决国际争端；在国际关系中不对任何国家的领土完整或政治独立使用武力或以武力相威胁，或采用不符合联合国宗旨的任何其他方式；尊重人权和基本自由；不干涉他国内政。最终目标是实现可靠、安全的信息和通信技术环境，但须顾及维护信息自由流通的需要。

鉴于新兴网络威胁的严重性，埃及高度重视和支持第 73/27 号决议中的建议，即设立不限成员名额工作组，在协商一致的基础上采取行动，作为优先事项，继续进一步制定国家负责任行为的规则、规范和原则，以期使联合国关于信息和通信技术使用安全问题的谈判进程更加民主、包容和透明。此外，埃及还期待加入和支持不限成员名额工作组的工作，制定实施这些规则、规范和建立信任措施的方式。

埃及也期待参与第 73/266 号决议所设政府专家组的活动，包括通过一系列磋商与相关区域组织协作的活动。

法国

[原件：法文]
[2019 年 5 月 14 日]

1. 对信息安全问题的一般看法

法国首先希望重申其不使用“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。法国作为在线言论自由的积极倡导者(法国是人权理事会 2018 年第 38/7 号决议的共同提案国，即证明了这一点)，认为信息本身并非潜在的漏洞来源，无需针对其制定保护措施。这一观点并不妨碍根据《公民权利和政治权利国际公约》第十九条，在法律严格规定的条件下，以适当和透明的方式采取措施。

因此，“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。网络安全利用技术保障信息系统的安全，加强打击网络犯罪和实施网络防御。

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，支持我们社会的繁荣和进步。正如之前在 2015 年国家数字安全战略[1] 中强调的那样，法国认为，数字技术通过新的用途和服务推动创新。数字技术正在为大多数专业领域带来改变，促进行业和企业转型，使其更具灵活性和竞争力。竞争增加和共享经济使得数字技术能够通过在线通信、贸易和信息服务改善日常生活，带来经济机会，从而为社会成员提供机遇。

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，但如今却因新型破坏性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、操作简单以及漏洞扩散)使一些行为体能够开发用于间谍活动、非法贩运、扰乱稳定和破坏活动的数字武器库。虽然一些低级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、关键基础设施或主要企业使用网络武器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。正如 2017 年国防和国家安全战略审查[2] 所强调的那样，我们的社会在过去 10 年经历的大规模数字化现象以及全球范围内的信息和通信系统网络正在产生新的威胁和机遇。这些现象使得人人都能获得强大的表达、影响、宣传和信息工具以及大量数据，同时也能获得威力强大的攻击手段。新的私人行为体因此而势力增强，在国际舞台上站稳脚跟，

[1] 可查阅 www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf。

[2] 可查阅 www.defense.gouv.fr/dgris/presentation/evenements-archives/revue-strategique-de-defense-et-de-securite-nationale-2017。

有时挑战各国主权，有时又是必要的合作伙伴。上述现象实际上转变了国家行为体、非国家行为体和私营部门之间的权力关系。

我们都有责任维护、发展和推动开放、安全、稳定、可访问、和平的网络空间。多年来，法国一直针对影响国际稳定和安全的共同威胁，采取积极的政策和外交手段，以期加强网络空间中的安全、信任和稳定。

2. 国家一级为加强网络安全和促进这一领域的国际合作所作的努力

(a) 提升法国网络安全

法国政府最高层在近年来的战略方向中，继续坚持将网络安全作为当局采取行动的优先领域。

法国继续扩大和制定国家战略。过去 10 年来，法国采取的措施包括：自 2009 年以来设立并扩大国家信息系统安全局；在 2011 年 2 月制定法国第一项国防和信息系统安全战略；强化法律手段，通过最新的军事规划法，大幅增加对网络安全的资源分配；军队部于 2014 年 2 月公布网络防御契约；发展网络安全卓越中心，以推动发展与网络安全有关的培训、学术研究以及工业和技术基础。为了落实上述措施，法国还在其战略范围内执行兼具国内和国际性质的透明化政策。

自 2015 年以来，法国一直拥有旨在支持法国社会数字化转型的国家数字安全战略。在安全方面，该战略规定应对恶意网络活动作出强有力的回应，并寻求通过数字安全为法国企业提供竞争优势。

2017 年 12 月，法国的国际数字战略[3] 对该文件作出补充，阐述了法国在国际一级的数字领域内追求的原则和目标。该战略围绕三大支柱(治理、经济和安全)，力求实现以下目标：

- 在全球一级推动开放、多元、可信的数字世界；
- 提出经济增长、基本权利与自由和安全之间相互平衡的欧洲模式；
- 加强法国和法国行为体在数字世界中的影响力、吸引力、安全和贸易地位。

2018 年 2 月提出的网络防御战略审查[4] 确立了网络危机管理的原则，明确了国家网络防御战略目标。这项审查表明了法国模式的现实意义和国家对网络安全负有的主要责任，围绕七项主要原则拟定：

- 完善我国信息系统保护；
- 通过一套防御措施抵御攻击，增强抵御能力以及反应和应对能力；
- 确认和行使法国的数字主权；
- 对网络犯罪采取更加有效的刑事司法对策；

[3] 可查阅 www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf。

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

- 推动共同的信息安全文化；
- 参与发展安全可信的数字欧洲；
- 采取国际行动，促进网络空间的集体治理和控制。

2019-2025 年军事规划法[5] 规定，应在与以往法律保持连续性的情况下，大幅增加对网络防御的资源分配，特别是人员分配。这项法律包含新增 1 500 名人员的征聘目标，力求在 2025 年之前将军队部负责应对此类问题的人员数目增至 4 000 人。

以下行为体为法国技术和业务战略的成效作出了贡献：

- 国家信息系统安全局负责通过规范行动等方式，预防针对政府和主要运营方的信息技术事件，并对此类事件作出反应。该机构现有 600 名员工，还在继续发展壮大，已成为界定相关网络安全标准的协调中心。
- 军队部的双重任务是切实保护用于保障其活动的网络，并将网络空间内的行动纳入军事行动。为了巩固其在这一领域所作的努力，军队部于 2017 年 9 月任命了一名在军队参谋长指挥下负责网络防御工作的总指挥官。在这方面，军队部于 2019 年初发布了打击网络犯罪的防御政策；与此同时，军队参谋长首次就主动打击网络犯罪、促进军事行动的原则发表公开声明。
- 内政部和司法部的任务是打击针对机构和国家利益、经济行为体、公共当局以及个人的各类网络犯罪。

(b) 推动国际合作，促进网络空间的稳定和安全

加强网络空间的战略稳定和国际安全是法国的优先目标。正如网络防御情况战略审查所述，“国际社会在网络空间内开展的合作可增进利益攸关方之间的相互了解甚至是信任，并为联合开展危机管理、沟通和缓和工作设立机制，从而有效促进稳定”。法国在欧洲和国际两级努力推动与网络安全问题有关的国际合作。

通过加强合作和能力发展预防危机

法国认为，预防危机是其在数字空间内开展工作的主要目标。因此，正如网络防御战略审查所强调的那样，“加强网络空间内所有行为体的保护、抵御力和合作直接有助于巩固我们的国家安全”。要实现这一目标，就必须加强与国家合作伙伴和国际组织的技术、业务和架构性合作，发展上述不同行为体各自的能力和全世界网络空间的抵御力。

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，法国正在通过双边或多边倡议，对网络安全合作伙伴的能力建设进行投资。此类合作投

[5] 可查阅 www.legifrance.gouv.fr/eli/loi/2018/7/13/ARMX1800503L/jo/texte。

资有益于各方，能够使我们通过与同行接触和向他们学习做到与时俱进，促进有关行为体彼此增进知识和专业技能并建立信任。

在技术层面，国家信息系统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，例如与产品和服务的薄弱环节或故障有关的信息。此外，国家信息系统安全局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、欧洲计算机安全和事件应对小组工作队、欧洲政府计算机应急小组集团、欧洲联盟计算机安全事件响应小组网络)，与世界各地的其他计算机应急小组保持联系。

法国正在实施积极的业务和架构性合作政策。近年来，法国向伙伴国的国内安全部队派遣了网络安全方面的国际技术专家。法国还在与塞内加尔合作，启动达喀尔国家网络安全学校的各项活动。这所学校是2018年末成立的区域性机构，旨在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。

为了加强欧洲联盟一级的网络抵御力，法国正在推动制定用于预防和解决事件的自愿合作框架。该框架尤其以制定伙伴合作的共同业务标准和程序为基础，这些标准和程序会在泛欧演练活动中接受检验。法国还参与开发了“网络工具箱”，该工具箱通过运用预防、合作和稳定措施，为联合采取外交手段应对网络攻击提供了欧洲框架。

法国还支持通过相关欧洲法规，在考虑到竞争力需求和数字技术潜力的同时，继续保护公民、企业和成员国(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)。以下法规表明了法国在这方面所作的努力：2016 年 4 月 27 日欧洲议会和欧盟理事会关于在处理个人数据和此类数据的自由流通方面保护自然人的(EU)2016/679 号条例，以及 2016 年 7 月 6 日欧洲议会和欧盟理事会关于采取措施使全欧盟网络和信息系统共同达到较高安全水平的(EU)2016/1148 号指令获得通过，2019 年 4 月 17 日欧洲议会和欧盟理事会关于欧洲联盟网络安全局以及信息和通信技术网络安全认证的(EU)2019/881 号条例(废除(EU)526/2013 号条例(网络安全法))即将生效。法国还积极支持通过欧洲联盟条例，防止在线传播恐怖主义内容，要求互联网提供方履行统一义务。

最后，法国正在努力确保欧洲联盟的产业政策能够支持先进研发能力，以加强部署安全水平可靠且经过评估的数字技术和服务。

在法国的倡议下，北大西洋公约组织(北约)各盟国在 2016 年 6 月的华沙首脑会议上通过了与网络防御有关的承诺，即“网络防御承诺”。这项承诺确保北约所有成员国均将适当份额的资源用于加强网络防御能力，从而提升所有国家的整体安全水平。2018 年 5 月，法国主办了有史以来第一次关于该承诺的会议。各盟国承认网络空间是战区，从而要求北约必须像在陆域、空域和海域中那样，在该领域内进行自我防卫。

通过制定规范网络空间内行为体行为的标准预防危机

法国认为，集体网络安全框架的出现只能建立在国际法界定的平衡关系之上。法国的数字安全国际战略还强调，法国必须与所有相关的公共和私人利益攸关方以及所有有意愿的国际合作伙伴开展双边和多边合作对话。

法国在联合国内部的谈判中发挥了积极作用，这些谈判是在从国际安全角度看信息和电信领域的发展政府专家组以往五次会议的框架内进行的。法国将继续致力于恢复政府专家组和不限成员名额工作组的讨论，推动实现其愿景，即建立自由、交流和增长的数字空间，确保我们社会的繁荣和进步。法国还参与其他探讨数字空间安全问题的国际论坛。

2006 年，法国批准了《布达佩斯公约》，该公约为确定与打击网络犯罪有关的各种罪行提供了法律依据，为在这一领域内开展国际合作规定了灵活和现代化的途径，例如设立昼夜运行的网络，以加快缔约国之间的援助程序。法国目前正在呼吁各国普遍加入《布达佩斯公约》，该公约现有 63 个来自各大洲的缔约国。法国正在积极参与该公约第二项附加议定书的谈判，该议定书旨在进一步加强这一领域的国际合作，发展警务合作和刑事互助，特别是在获取电子证据方面。此外，法国还支持负责深入研究网络犯罪问题的不限成员名额政府间小组开展工作，认可联合国毒品和犯罪问题办公室在该领域的核心作用。

2018 年 11 月 12 日，法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《网络空间信任和安全巴黎呼吁》，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。[6] 该文件现已获得 66 个国家和近 500 个非国家实体的支持，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、国家负责任行为、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。

法国还在经济合作与发展组织(经合组织)内部参与相关工作。2018 年 12 月，法国举办了经合组织数字安全促进繁荣全球论坛第一次会议，会议的主题是私营部门行为体在数字安全方面的责任。

2016 年设立的七国集团伊势志摩网络小组推动《卢卡宣言》于 2017 年获得通过，这份雄心勃勃的宣言涉及网络空间内负责任行为的标准。法国在 2019 年 3 月担任主席期间，提议启动后续机制，执行联合国一级经核准的标准和建议，该机制在关于网络规范倡议的《迪纳尔宣言》中得到确认。[7]

法国正在努力确保二十国集团的工作按照《网络空间信任和安全巴黎呼吁》，解决数字经济中的竞争、新监管方法、治理和数字安全等基本问题。

[6] 可查阅 www.diplomatie.gouv.fr/IMG/pdf/texte_appel_de_paris_-_fr_cle0d3c69.pdf。

[7] 可查阅 www.diplomatie.gouv.fr/IMG/pdf/g7_declaration_de_dinard_sur_l_initative_pour_des_normes_dans_le_cyberespace_cle8a8313.pdf。

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就网络问题制定的 16 项建立信任措施。其中包括试行关于保护关键基础设施的建立信任措施。

为了加强打击扩散恶意工具和技术的行为，法国支持将入侵软件列入《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。法国认为，必须以这种方式进行监管，根据所致影响的严重程度，将某些网络工具列入战争物资清单。

法国认为，与网络安全有关的许多挑战应通过多行为体或多利益攸关方共同参与的办法解决，以便考虑到非国家行为体的作用和具体责任。在这方面，法国支持全球网络空间稳定委员会的工作。委员会制定标准和政策建议，以加强国际安全和稳定，指导网络空间内的负责任国家行为。

3. 旨在加强全球网络安全的相关国际概念

(a) 与维护国际和平与安全有关的概念

为确保开放、安全、稳定、无障碍及和平的网络空间，法国重申其对国际法，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各国使用信息和通信技术的承诺。

国际公法

从国际安全角度看信息和电信领域的发展政府专家组在其 2013 年报告中阐述了指导各国在网络空间行动的国际法原则和规则。即使考虑到网络空间的具体特征，如匿名和私人行为者的作用，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。因此，不加归属，不应对现行国际法的实施构成不可逾越的障碍。

主权原则适用于网络空间。在这方面，法国根据其国际法义务，重申对其领土上信息系统、个人和网络空间相关活动的主权。国家实体或在国家指挥或控制下行事的非国家行为者使用网络空间未经授权渗透法国系统或在法国领土上产生影响，可构成对主权的侵犯。

各国为应对可能的网络攻击可以采取的措施的范围，取决于攻击的严重性：网络攻击越严重，措施的范围就越广。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。是否跨过这个门槛，与网络攻击手段无关，而与其影响有关。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，如果一国或在一国监督或指示下行事的非国家行为者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、关键基础设施不足但具有重大后果)，并可归咎于一国，这可构成《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。如有必要和相称，自卫权可以通过传统或电子手段行使。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。

法国认为，在现阶段没有必要制定一项新的具有法律约束力的国际文书，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。

国际人道主义法

法国支持将国际人道主义法适用于在武装冲突背景下和与武装冲突有关的网络行动。

虽然进攻性网络行动目前是与常规军事行动同时进行的，但原则上不能排除完全由数字活动构成的武装冲突的可能性，因为其依据是，网络行动有可能达到构成国际或非国际武装冲突所订的暴力门槛。

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，其影响限于国际武装冲突参与国领土，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进行网络攻击。某些数据虽然是无形的，但可能构成受国际人道主义法保护的平民资产。

- **人道原则**。除非平民直接参与敌对行动，除非在参与敌对行动期间，一般平民和单个平民不得成为目标。在武装冲突中，任何身为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任何有组织武装团体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**。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，无论这些影响是直接的(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)，只要这些影响与攻击有充分的因果联系。这项原则还禁止使用无法控制的网络武器(在时间或空间上)，因此可能对民用基础设施、系统或数据造成不可逆转的损害。

上述原则包含在 2019 年初公布的法国进攻性计算机战争军事理论的公开内容中。

人权

法国支持人在网下享有的权利，也必须在网上得到保护，以及国际人权法适用于网络空间的原则。这些价值观尤其受到非法材料在线传播的挑战，例如那些宣扬恐怖主义、仇恨和反犹太主义的材料。特别重要的是，让私人数字行为者参

与打击非法内容的斗争，澄清他们在国际一级打击非法内容和保护在线人权和基本自由的作用和责任。

尽职原则

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。目的是澄清尽职原则的适用；该原则规定，每个国家都有义务“不在知情的情况下将领土用于违反其他国家权利的行为”，[8] 因此，各国不应明知故犯地允许其领土被用于通过国际法禁止的电子手段实施的行为，也不应允许非国家中介(代理)利用这一领土违反国际法。更好地理解该原则如何适用于电子挑战，将加强各国在保护某些关键基础设施，消除经由第三国过境的重大网络攻击方面的合作。

(b) 加强各国合作和信任的概念

行为规范

在政府专家组框架内进行的各轮谈判导致了网络空间国际监管方面的切实进展。在其 2015 年报告中，概述了网络空间国家负责任行为 11 项准则。法国认为，每个国家都必须尊重这些规范，建立实施这些规范的机制。今后还可以制定适用于国家行为或网络空间其他行为者的其他规范。

建立信任措施

需要加强各种论坛和区域组织制定网络安全建立信任措施的努力。法国将继续鼓励其伙伴采取部际程序，确保危机时期各国之间的有效沟通。基于透明度和沟通的程序和机制的发展对于预防网络空间冲突至关重要。

能力建设

法国支持加强国际网络安全能力，这直接增强了所有人的安全和网络空间的稳定。法国将通过在双边、区域和多边各级采取的能力建设举措，充分参与这些努力。

(c) 非国家行为者的作用和责任

多方利益攸关方方法

在《巴黎网络空间信任与安全呼吁》中，法国强调“必须加强多方利益攸关方方法”。法国认为，民间社会、学术界、私营部门和信通技术界拥有协助制定相关网络安全政策的专门知识和资源。

数字产品设计和维护中私人行为者的安全责任

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，包括一些系统行为者，带来了维护国际和平与安全的关键作用和前所未有的责任。《巴黎呼吁》

[8] “科孚海峡”案，1949 年 4 月 9 日判决书，《国际法院案例汇编》(1949)，第 4 页。

确认“关键私营部门行为者在网络空间建立信任、安全和稳定的责任”，鼓励“加强数字流程、产品和服务安全的举措”。

法国认为，应在国际一级制定一项原则，规定私营系统行为者在开发、整合、使用和维护其数字产品、流程和服务整个生命周期和整个供应链中的问责。

数字平台在反恐斗争中的责任

法国还促进私营数字行为者的问责，打击出于恐怖主义目的滥用其服务现象。法国已向七国集团和欧洲联盟提出这一问题，积极支持通过一项欧洲条例草案，规范互联网提供商打击网上恐怖主义内容的活动。该草案规定，应一个会员国的请求，必须立即删除恐怖主义内容，可能接触恐怖主义内容的平台应采取积极措施，建立 24 小时联络点，受理报告和删除请求，处罚有系统的不合作行为。

防止私人行为者的攻击性活动

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。因此，法国支持禁止包括私营部门在内的非国家行为者代表自己或代表其他非国家行为者在网络空间开展攻击性活动。这种基于合法自卫原则(“反击”)的做法有可能扰乱第三方，造成负面影响，并可能加剧国家间的升级。因此，法国认为，应阐明私人行为者应对事件的维度。

4. 国际社会为加强全球网络安全可能采取的措施

面对数字革命带来的新威胁，法国认为，合作和法律是防止网络空间成为永久冲突区的必要条件。如同在其他领域一样，各国有义务尊重数字空间的国际法。此外，应巩固近年来出现的关于网络空间国家负责任行为的规范框架。法国认为，以下步骤可以加强全球网络安全：

- **在政府专家组前几次会议所做工作的基础上继续努力**。在不影响前几轮谈判中协商一致商定的规范和建议的情况下，不妨澄清如何落实这些规范和建议，以及如何在国际上更好地理解相关良好做法。
- **在即将举行的联合国关于网络安全挑战的讨论中借鉴巴黎呼吁**。迄今为止，呼吁汇集了三分之一以上的联合国会员国和数百名著名的非国家行为者，就规范各行为者在线行为的原则达成共同愿景。
- **普及《网络犯罪公约》**。《公约》于 2001 年 11 月通过，旨在加强国际合作，迄今已获 63 个国家批准，并影响了三分之二以上联合国会员国的国家立法。
- **鼓励各国展示透明度，**特别是在网络安全战略、危机管理和网络攻击应对理论，以及解释国际法在网络空间的应用方面。
- **在相关区域或国际框架内，实施针对信通技术问题的建立信任措施**。
- **加强交流良好做法和能力建设的举措和机制**。此类机制应确保所有国家都设有有效的网络安全系统，特别是通过：

- 制定网络安全战略；
- 发展促进网络安全和打击网络犯罪的立法框架；
- 组建计算机应急小组；
- 制订与私营部门，特别是主要数字技术公司合作的程序；
- 制订保护网络空间关键基础设施的框架。

- **在国际一级确认私营系统行为者对安全的问责**。这种问责延伸到其数字产品、流程和服务的设计、集成、使用和维护的整个生命周期和整个供应链。

希腊

[原件：英文]
[2019 年 5 月 15 日]

2018 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国家负责任行为的决议。决议请秘书长就以下方面征求会员国的意见和评估：(a) 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；(b) 政府专家组各项报告所述概念的内容。

希腊支持政府专家组的共识，即国际法，特别是《联合国宪章》，也适用于网络空间，对于维护和平与稳定以及促进开放、安全、和平和无障碍的信息和通信技术环境至关重要。希腊还支持在联合国第一委员会继续讨论国家负责任行为规范、建立信任措施和国际法的进程，支持新设一个政府专家组。

我们认识到，网络空间的相互关联和复杂性质要求各国政府、私营部门、民间社会、技术界、用户和学术界共同努力应对所面临的挑战，并呼吁所有利益攸关方认识到并承担起维护一个开放、自由、安全和稳定的网络空间的具体责任。

我们还认识到联合国在进一步制定网络空间国家负责任行为规范方面的作用，并回顾政府专家组讨论的结果阐明了一套协商一致的规范和建议，对此大会一再认可，各国也应将其作为网络空间国家负责任行为的基础。

通过参加联合国、欧洲联盟、北大西洋公约组织和欧洲安全与合作组织等国际组织，我们寻求建立在使用网络空间方面负责任的国家行为的普遍规则和原则，开展合作，交流经验和最佳做法，并共同制定适当的手段来应对与网络安全有关的威胁和挑战。我国尽最大可能帮助制定和执行在国际组织框架内通过的相关决定，力求加强合作和透明度，减少冲突风险。

希腊认识到网络犯罪是一个全球性问题，签署并批准了欧洲委员会《网络犯罪公约》，又称《布达佩斯条约》。该条约为通过我国立法和打击网络犯罪的国际合作提供了一个重要框架。第 4411/2016 号法律批准了该条约。此外，在参加欧洲安全与合作组织的框架内，我国还签署了《建立信任措施协定》，旨在会员国在网络安全问题、透明度、稳定和减少网络空间对抗风险方面的合作。

在欧盟承诺的框架内，希腊已将关于网络和信息系统安全的第 1148 号指令(又称“NIS 指令”)纳入国家立法，指令包括在整个欧盟范围内实现高级共同安全的措施、实施网络安全措施、制定国家战略和加强成员国之间的合作。因此，加强了对我国所有重要基础设施的保护，同时保障了开放社会、宪法自由和个人权利的原则。在数字政策部主持下运作的国家网络安全局全面负责实施国家网络安全战略。

我们国家网络安全战略的主要目标是：

- 在国家、欧洲和国际标准和做法的基础上发展巩固安全和有复原力的网络空间
- 不断提高我们抵御网络攻击的能力，重点是关键基础设施
- 发展强大的公共和私人安全文化，发挥学术界以及公共和私人行为者的潜力
- 提升对信息系统和基础设施安全威胁的评估、分析和预防水平
- 建立公共和私人利益攸关方之间协调与合作的有效框架
- 国家积极参与国际组织的国际倡议和网络安全行动
- 提高所有社会利益攸关方的认识，让用户安全使用网络空间
- 国家体制框架不断适应新的技术要求和欧洲准则
- 促进安全问题的创新、研究和发展。

日本

[原件：英文]
[2019 年 5 月 14 日]

1. 对信息安全问题的一般看法

网络空间中的知识、技术和服务，如人工智能、物联网、金融技术、大数据和 5G，正在社会中建立起来，促成创新，改变了我们社会经济活动的现有结构和人们的日常生活；这些变革正在网络空间和真实空间的统一方面带来进展。为享受网络空间的知识、技术和服务带来的好处，必须控制其中潜在的不确定性。在无法进行这种控制时，与网络安全相关的威胁有可能迅速增加。

网络空间的好处

世界上互联网用户数量正在增加，互联网本身的传播也在增加。此外，就设备而言，个人智能手机拥有率大幅上升，互联网使用率也在上升。社交媒体用户的比例也在上升，因此现在有了一个在网络空间轻松交流的环境。社会越来越多地在网络空间采用服务，这不仅促进了信息的自由流动，还促进了不同社区的形成和信息共享。金融活动领域也取得了进展，包括网上购物、股票交易和网上银行，而金融技术和共享经济领域的新服务正在时常出现，引领创新。信息和通信

技术在医疗和护理、福利、教育和其他与社会问题有关的领域，如工作年龄人口下降和地方社区老龄化方面也取得了进展。

网络空间面临更多威胁

虽然人工智能、物联网和其他技术和服务有可能给人们带来许多好处，但这些技术和服务的提供者总有失去控制能力的潜在风险，在这种情况下，它们可能造成不可估量的经济和社会损失或损害。随着网络空间和真实空间逐渐统一，这种可能性呈指数级增长。此外，网络空间是一个不受空间或时间限制的地方，任何人，包括恶意行为者，都可以轻易地乱用和滥用新的信息和通信技术。数字技术的本质使恶意行为者能够轻易复制散发敏感数据和信息，启动攻击程序，灵活地整合和随意利用人工智能和区块链等新兴技术。因此，攻击者相对于防御者具有不对称优势，尤其是当防御者的防线依赖于现行政策和技术系统时，这种优势更会增加。有鉴于此，针对物联网、金融技术(包括加密货币)、关键基础设施和供应链的攻击已经发生，除了通常的数据泄露，威胁社会经济活动可持续发展和人民生活的安全保障，还造成直接的财务损失以及业务和服务中断。还发生了被怀疑是国家资助的大规模事件。人们还担心，如果网络空间由一些条件优越国家的政府控制和管理，信息基础设施的可信度可能会受到动摇。人们相信，随着网络空间与真实空间进一步统一，人们将越来越担心可能攻击物联网、供应链和开放创新中薄弱环节的企图，而且这些系统中会出现意想不到的行为。这不仅会严重影响政府机构和关键基础设施运营商，还会影响其他工商业，甚至个人。

坚持网络空间的基本立场

为继续遏制恶意行为者活动，保障人民的安全和权利，日本保留政治、经济、技术、法律、外交和所有其他可行有效的手段作为其选择手段。日本坚持发展实施网络安全措施的五项原则：㈠ 保证信息自由流动；㈡ 法治；㈢ 开放；㈣ 自治；㈤ 多方利益攸关方之间合作。

㈠ 保证信息自由流动

为将网络空间作为创造和创新场所进行可持续发展，必须建设维护一个传发信息能够到达预期接收方、不会在途中受到不公平审查或非法修改的世界。还必须确保隐私考虑。道德和常识是网络空间信息自由流动的基本条件，其要求不得侵犯他人的权益。

㈡ 法治

随着网络空间和现实空间的统一，网络空间的法治也应该像现实空间一样得到维护。网络空间适用各种国内规则和规范，包括国内法律和条例。同样，现行国际法也适用于网络空间。适用现行国际法和制定规范对于作为安全可靠空间的网络空间的可持续发展仍然至关重要。

㈢ 开放

为实现网络空间作为产生新价值空间的可持续发展，网络空间必须向所有行为者开放，不限制不同想法和知识联系起来。日本坚持这样立场，即网络空间绝不能完全被其中的一小部分行为者所主宰。

㈣ 自治

网络空间是通过多方利益攸关方的自主倡议发展起来的。一个国家不应该，也不可能全面负责维护网络空间秩序，可持续地发展一个秩序和创造力并存的空间。维持秩序、阻止和处理恶意行为者行为的唯一方法是，社会各个系统自主运作。日本将推广这种方法。

㈤ 多利益攸关方之间的合作

网络空间是一个多层面世界，通过多个利益攸关方的活动建立起来，包括国家、地方政府、关键基础设施运营商、网络相关企业和其他企业、教育和研究机构以及个人。为了网络空间的可持续发展，要求所有行为者自觉履行各自的作用和责任。除个人努力之外，还需要协调与合作。各国在促进这种协调与合作方面发挥主导作用，将促进有助于发挥这种作用的措施。

2. 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

国家一级为加强信息安全所作的努力

在日本，为利用数据奠定了法律基础，包括《促进公共和私营部门数据利用基本法》和《个人信息保护法修正案》等。政府还采取了实现以人为中心的社会的政策，通过网络空间与真实空间的高度融合，实现经济发展，解决社会问题。在这种情况下，现实空间中传感器和设备产生的大量数据目前正在网络空间中积累和分析。此外，通过使用数据增加价值的新产品和服务在现实空间中提供，可在许多领域中循环出现，往复发展。网络空间和真实空间已不再分门独立，而是作为相互作用的实体存在，也即不再被认为是相互分离的。因此，这两个空间应该被视为一个单一的持续进化的有机实体。

网络空间和真实空间的统一极大地增加了令社会富足的潜力，但同时也增加了恶意行为者滥用网络空间的机会。预计，真实空间中遭受经济和社会损失或损害的风险会成倍扩大和加速。在这种情况下，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，有一种趋势是，某些国家通过强调国家从主导地位进行管理和控制来应对网络威胁。然而，由国家加强对网络空间的管理和控制会阻碍自治和可持续发展。因此，必须尊重通过所有利益攸关方自主发展起来的当今网络空间，必须与这些利益攸关方开展协作合作，确保网络安全。基于这一理解，考虑到 2020 年及其后的事态发展，并考虑到主办第三十二届奥运会和 2020 年东京残奥会(以下简称“东京 2020 年奥运会”)等国际活动，日本将不遗余力地采取网络安全措施，明确网络安全的基本愿景，确定需要解决的新问题，并迅速采取措施。

国家一级为促进国际合作所作的努力

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合作，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，政府将积极促进各种国际讨论和工作，以分享信息并就网络相关问题达成共同理解。政府还将与外国分享专门知识，推动开展具体合作并采取行动。

关于分享专门知识和协调政策，政府将利用关于网络安全的双边对话和国际会议，交流关于应对网络安全的政策、战略和系统的信息，并利用这些知识规划日本的网络安全政策。我们还将在网络安全政策方面，加强同与我们秉持相同网络安全基本原则的战略伙伴的合作。

关于应对事件的国际合作，政府将分享关于网络攻击和威胁的信息，加强计算机应急小组间的合作，以便在事件发生时协调一致地进行应对。政府还将通过联合培训以及参加国际网络演习和联合培训，努力提高协调应对能力。此外，政府将通过适当的国际合作，在发生事件时采取恰当的对策。

关于网络相关国际合作的外交方面，我们的承诺包括三大支柱：网络空间的法治、建立信任措施和能力建设。

- 促进法治对于国际和平与稳定以及日本的国家安全具有重要意义。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。

- 日本将努力建设国家间信任，以防止因网络攻击发生意外情况和造成局势恶化。由于网络攻击具有匿名性和保密性，网络攻击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开展合作，考虑建立协调网络空间相关问题的机制。在这方面，日本积极推动建立信任措施，包括发起设立并共同主持东南亚国家联盟(东盟)地区论坛网络安全领域闭会期间会议，同时主要在亚太区域稳步实施能力建设援助。

- 关于能力建设，随着跨境相互依存加深，日本不可能独善其身，确保和平与稳定。通过全球协调，减少并消除网络安全脆弱性，这对确保日本的国家安全至关重要。从这一角度来看，协助其他国家开展能力建设可以确保日本居民的稳定生活，确保日本公司在其他国家稳定开展业务活动，这些活动要依赖这些国家的关键基础设施以及网络空间使用的健康发展。同时，它也与确保所有网络空间的安全直接相关，并有助于改善

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《网络犯罪公约》为数不多的非欧洲缔约国之一，并通过在亚洲区域开展能力建设援助，在促进《公约》方面发挥积极作用，《公约》是打击网络犯罪的一个重要法律框架。

3. 旨在加强全球信息和电信系统安全的有关国际概念

日本支持前几届政府专家组达成的共识协定，即现行国际法在网络空间适用。我们已看到讨论把制定规范行为、落实建立信任措施和能力建设作为塑造网络空间国家负责任行为的关键办法。特别是，日本认识到，执行 2015 年关于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述不具约束力、自愿的网络空间国家负责任行为规范必须成为确保国际稳定和可预测性的基础，成为今后有关这一问题的讨论的基础。在这方面，我们认为，目前，缔结新的全面条约或类似文书的尝试不会积极地加强网络安全。

4. 国际社会为加强全球一级的信息安全可能采取的措施

日本作为一个负责任的国家，促进国际社会根据现行国际法与相关区域框架进行协调以及通过政府专家组确定的所有概念，同时，日本认为，就自愿、不具约束力的国家负责任行为规范达成共同理解以及执行这些规范，将有助于加强国际安全。

5. 政府专家组各项报告所述概念的内容

日本认为，各国考虑政府专家组确定的下列概念是有效和有意义的：

恶意网络行为对国际社会的影响

为了灵活地将信息和通信技术的快速发展纳入我们的生活，防止恶意网络行为造成的损害，我们应承认预见网络空间现有和潜在威胁以及国际社会可能如何受其影响的重要性。

执行自愿、不具约束力的国家负责任行为规范

为了最大限度地减少恶意网络行为的影响，威慑有意实施此类行为的人，我们应回顾，政府专家组共识报告，包括其中提到的自愿、不具约束力的国家负责任行为规范，具有重要意义。我们应与相关区域组织合作，深化讨论，以切实有效地利用这些有价值的工作。

促进执行自愿、不具约束力的国家负责任行为规范以及合作开展相关建立信任措施和能力建设

为了在国际安全方面进一步加强各国发展并维护自由、公正和安全网络空间的努力，我们应重申，所有国有强烈意愿来消除网络空间的安全漏洞并防止网络犯罪和其他恶意行为。在这方面，专家组成员应始终致力于鼓励所有国家稳步执行自愿、不具约束力的国家负责任行为规范，包括实施建立信任措施并开展合作以帮助建设国家执行上述自愿、不具约束力的规范和建议的能力，包括通过下一届政府专家组和不限成员名额工作组进程这样做。

新加坡

[原件：英文]
[2019 年 5 月 13 日]

新加坡认识到，开放、安全与和平的网络空间受到的威胁越来越具有复杂性、跨界性和不对称性。新加坡是一个高度互联的小国，曾数次遭受网络攻击，新加坡坚定致力于在网络空间建立基于规则的国际秩序。这将成为会员国之间建立信任和信心的基础并促进经济和社会进步。为了充分受益于数字技术，国际社会必须发展安全、可信和开放的网络空间，其基础是适用于网络空间的国际法、明确界定的国家负责任行为规范、强有力的建立信任措施和协调一致的能力建设。三者共同形成相辅相成的三角环，从而能够建立安全和应对能力强的网络空间。讨论此类法律、规则和规范的努力必须继续在联合国进行，因为，联合国是唯一具有普遍性、包容性的多边论坛，在这里，所有国家，无论大小，都有发言权。新加坡致力于这一进程。

新加坡欢迎设立从国际安全角度看信息和电信领域的发展政府专家组以及决定召集不限成员名额工作组。新加坡认为，政府专家组和工作组的工作可以而且应该是相辅相成的。主要参与者必须本着共识、相互尊重和相互信任的精神共同努力。新加坡乐观地认为这两个平台能够积极互补，并致力于为两个进程做出建设性贡献。

在区域一级，新加坡与东南亚国家联盟(东盟)其他成员国合作，在 2018 年 4 月举行的第三十二届东盟峰会期间发表了第一份东盟领导人关于网络安全合作的声明。东盟领导人在声明中重申，需要在网络空间建立基于规则的国际秩序。他们还责成相关部长确定适当的机制或平台，以协调东盟的网络安全政策、外交、合作以及技术和能力建设努力，并拟订一份可供东盟通过的自愿、实用的网络空间国家行为规范具体清单。根据领导人的声明，2018 年 9 月，在新加坡举行的第三届东盟网络安全部长级会议的与会者商定，原则上赞同 2015 年政府专家组报告(A/70/174)中的 11 项规范，并重点关注实施这些规范的区域能力建设。

能力建设对确保各国发展成功执行行为规则和规范的能力至关重要。新加坡有一个 1 000 万新元的东盟网络能力方案，这是一个模块化、多学科和多利益攸关方方案，重点关注东盟国家在网络政策、战略和技术问题上的能力建设。自 2016 年启动以来，已有 160 名东盟官员在该方案下接受了培训。新加坡还与裁军事务厅合作编制了在线培训旗舰课程，以推动理解并执行政府专家组达成的共识。新加坡还将与裁军厅合作开展联合国-新加坡网络方案，以提高东盟成员国对网络规范和网络情景政策规划的认识。作为东盟网络能力方案的延伸，新加坡将于 2019 年启动耗资 3 000 万新元的东盟-新加坡网络安全卓越中心，以进一步建设东盟国家的网络安全决策、战略制订以及技术和业务能力。该中心将保持开放包容，东盟成员国可以利用中心与国际伙伴更密切地接触。

在国家一级，新加坡在加强系统和网络的网络安全方面取得了重大进展，主要在以下三个方面，即建设具备抵御灾害能力的基础设施、创建更安全的网络空间、发展充满活力的网络安全生态系统：

(a) *建设具备抵御灾害能力的基础设施*。越境网络威胁正日益危及各国的关键基础设施置。超国家信息基础设施，如金融、海事、电信和航空部门的基础设施尤为如此，在这些领域，成功网络攻击的后果可能蔓延到国界外，影响全球相互关联的中心。2018 年一项主要事态进展是通过并实施了《网络安全法》，该法为监督和维护新加坡的国家网络安全建立了法律框架。在该法中，强调积极防范对关键信息基础设施(意即支持提供基本服务的计算机或计算机系统)的网络攻击。实现这种保护的途径是规定此类基础设施的所有者在法律上有义务除其他外，采取以下措施：㈠ 建立检测网络安全威胁和事件并报告此类事件的机制；㈡ 定期对关键信息基础设施进行风险评估和审查；㈢ 参加国家网络安全局举办的网络安全演习。除加强对此类基础设施的保护外，该法还授权国家网络安全局预防、应对并调查网络安全威胁和事件；

(b) *创建更安全的网络空间*。2019 年 1 月，新加坡获得了共同标准互认安排证书授权国地位，这是一项在 30 个国家相互承认共同标准证书的国际安排。共同标准是用于评价和认证信息技术安全产品的技术标准，被政府和业界广泛采用。新加坡现在是该安排下 30 个成员中 18 个证书授权国之一。因此，新加坡获准在当地认证信息技术安全产品，从而可以帮助改进新加坡中小企业网络安全产品的质量，使其参照国际安全标准；

(c) *发展充满活力的网络安全生态系统*。新加坡认识到，加强网络安全需要建设网络生态系统和鼓励业内创新。为此，新加坡于 2018 年 3 月推出了首个网络安全综合创业中心，被称为“网络安全创新生态 71 区”，目的是加强新加坡不断增长的网络安全生态系统，吸引并发展各种能力和深度技术，以帮助减轻迅速增加的网络安全风险。该中心还帮助发展世界各地的网络安全创业企业，提供各种旨在支持创业者的方案，包括从提出创意到实现网络安全创业企业的加速发展和规模化以走向全球市场。

土耳其

[原件：英文]
[2019 年 5 月 10 日]

信息和通信技术(信通技术)已成为社会和经济的重要组成部分。信通技术被用于包括公共部门、私营部门、关键基础设施和个人在内的广泛网络，已在土耳其和世界上广泛使用。因此，信通技术对可持续增长和发展起着重要作用。然而，我们越是使用技术，对技术的依赖性就变得更强，也更加容易受到技术带来的风险的影响。个人、企业、关键基础设施和国家因网络威胁而面临严重问题。

技术渗透于我们生活的方方面面，使我们在网络安全方面进入了相关风险的新阶段。确保网络安全对应对技术密集型领域的威胁是必要的，不仅如此，由于

对社会经济生活进程带来的风险，确保网络安全也是影响国家繁荣与国家安全的突出因素。

信通技术的安全缺陷可能导致信通技术系统停用或被利用，或者可能最终导致人员伤亡、大规模经济损失、公共秩序动荡或国家安全受到损害。

土耳其注重采取必要措施，改善国家网络安全，一直在执行国家网络安全战略和行动计划(涵盖 2016 年至 2019 年期间)，旨在建立国家网络安全，拟订和协调高效、可持续的政策并落实这些政策。交通和基础设施部负责制定土耳其国家网络安全的政策、战略和行动计划。在此背景下，在交通和基础设施部协调下，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。

战略和行动计划有两个主要目标：首先，让所有利益攸关方认识到，网络安全是国家安全的必要组成部分；其次，获得能力，以便采取行政和技术预防措施，维护国家网络空间中所有系统和利益攸关方的绝对安全。

战略和行动计划中的每一项行动都已由交通和基础设施部及相关机构实施，该部还监测各项行动的一切进展。

此外，信息和通信技术管理局自 2013 年以来一直是土耳其国家计算机应急小组。它负责土耳其电子通信和邮政服务的所有监管职能。此外，它还有权采取必要措施打击网络攻击，以确保国家网络安全。该小组是国家一级的协调中心，以查明对国家网络安全的威胁，采取措施减少或消除潜在网络攻击的影响，并与特定行为体共享信息。该小组与公共或私营机构和个人等所有利益攸关方协调，以发现并消除网络威胁。它在网络安全方面的重点领域是：

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

能力建设方面的活动包括人力资源、培训和准备。在这些活动方面，我们组织了关于网络安全的“夺旗”竞赛。我们认为，人力资源是网络安全最重要的因素之一。我们在国家计算机应急小组框架内开展能力建设重点项目。在这方面，我们为能源、卫生和公共机构等各关键部门的机构计算机应急小组举办网络安全培训。我们还为在校学生和毕业生举办实操培训和竞赛。过去两年，超过 2 500 名学员参加了我们的网络安全培训课程。

我们还建立了网络靶场实验室，以改进我们的培训课程，提供更多实操活动机会。实验室也有助于衡量专门知识水平，并为参与者提供认证方案。

我们在技术措施方面的研究涉及早期检测、警报和警告活动。为此，我们开发了一些检测和预防系统。这些系统通过提供可视性并检测僵尸网络和恶意软件的指挥和控制中心，在提高国家网络安全水平方面发挥了巨大作用。

在土耳其加强网络安全的办法方面，要强调的另一个重点领域是网络威胁情报。在这方面，我们与互联网行为体、国际组织、司法当局、研究中心和私营公司等若干方协作。此外，在公共和私营机构下设立了关键基础设施部门计算机应急小组和 1 000 多个机构计算机应急小组。

除此之外，由于网络空间是一个无国界的领域，任何一方难以独自确保其网络安全。这是一个涉及多利益攸关方的跨学科问题。我们与用户、私营部门、非政府组织、学术界和国际同行开展合作，以打击网络威胁。例如，土耳其计算机应急小组接收各国计算机应急小组发送的网络通知，并通知相关方采取必要措施。它也发送网络威胁信息并与其他国家的计算机应急小组和国际组织分享情报。

从确保互联网安全角度出发，2017 年在信息和通信技术管理局内设立了安全互联网中心，以提高对正确安全使用互联网的认识。

我们启动了互联网求助线和一个网页安全网站，人们可以借此获得高效使用互联网的建议。此外，为接触信通技术机会有限的儿童和年轻人提供了配备信通技术工具的“互联网安全卡车”。卡车为人们提供了一个可以直接体验技术的平台，并对更多接触互联网和技术的儿童帮助提高对安全、负责任地使用互联网的认识。

管理局每年组织一次“互联网安全日”活动。2018 年的主题是“创造、连接和分享尊重：更美好的互联网从你开始”。管理局和花园城市大学发起了一项桌游竞赛，鼓励 12 至 18 岁的年轻人根据国际主题设计游戏。在整个竞赛过程中提交了许多游戏设计，竞赛获胜者获得了奖励。在这次活动期间，脸书和谷歌为学生举办了关于数字游戏和提高互联网安全的讲习班。

此外，管理局就负责任和安全地使用信通技术和互联网的提高认识活动和培训员培训，与家庭和社会政策部、互联网接入服务运营商协会和教育部签署了协议。培训内容被纳入远程教育模块，向教育部系统内任职的所有教师提供。迄今为止，教师和数千名学生已通过这项远程教育服务接受了培训。

此外，在提供和维护网络空间安全方面，不仅国家协调，国际合作、信息交流和建立信任也发挥至关重要的作用。

下文概述土耳其就 2015 年关于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(A/70/174)所述建立信任措施的范围以及报告中界定的国家负责任行为的概念开展的相关工作和研究。

随着个人越来越多地使用信通技术，个人信息或数据已成为网络攻击者觊觎的目标。在人的基本权利和自由方面，保护个人信息和数据也成为一个令人关切的主要问题。

除网络环境的透明度、问责制和道德价值观外，土耳其所有利益攸关方在努力确保网络空间安全时，也关注法治原则、基本人权和自由以及隐私保护。

在这方面，关于保护个人数据的第 6698 号法于 2016 年 4 月 7 日在《政府公报》(29681 号)上公布并生效。该法旨在保护在处理个人数据方面人们的基本权利和自由，特别是隐私权，并规定对处理个人数据的自然人或法人具有约束力的义务、原则和程序。

土耳其在许多组织中发挥了重要作用，要么是作为创始成员，要么是为关于网络安全和信息安全问题的合作做出贡献。因此，土耳其力求通过与不同国家和组织就决策、能力建设和信息共享交流各领域的信息和想法来确保网络安全。

网络空间是一个无国界领域，国际合作是应对网络威胁的必由之路。因此，土耳其定期关注并参与联合国、北大西洋公约组织(北约)、欧洲联盟、欧洲安全与合作组织(欧安组织)和其他国际组织与机构内的国际网络安全研究。

此外，还与各国签订双边协议以确保网络安全。土耳其交通和基础设施部、信息和通信技术管理局以及计算机应急小组已与格鲁吉亚、俄罗斯、吉尔吉斯斯坦、塞尔维亚、波斯尼亚和黑塞哥维那、克罗地亚和希腊等一些国家签署了网络安全谅解备忘录。

北约网络防务委员会核准了说明北约与其盟国之间合作的谅解备忘录，委员会考虑了我国的意见，备忘录已由北约和土耳其共和国国防部签署。已设立了联络人，正在开展谅解备忘录范围内的相关工作。

土耳其也关注北约民事应急规划委员会以及工业资源和通信服务小组的工作。此外，自 2015 年以来，土耳其作为赞助国，一直是北约认可的知识中心、智库和培训设施——卓越合作网络防御中心——的成员。

土耳其参加并促进经济合作与发展组织关于安全和隐私问题的会议以及欧安组织网络安全问题非正式工作组。

土耳其参与区域军备控制核查和执行援助中心的各次会议，正在稳步发展就各类事项开展的合作。该中心的战略目标是加强国家安全战略的制定，为此鼓励开展区域安全合作和有效互动，以可持续地应对新出现的安全挑战，例如网络安全和其他形式的跨国威胁，包括恐怖主义、大规模毁灭性武器扩散、贩运、有组织犯罪、边境安全和管理以及气候变化，同时将特别关注由此产生的所有新安全威胁。

土耳其参与努力推动国际合作。土耳其计算机应急小组是事件应对和安全小组论坛、可信介绍者服务、国际电信联盟(国际电联)国际打击网络威胁多边伙伴关系、北约恶意软件信息共享平台和网络安全共同进步联盟的成员，力求在国际一级开展尽可能多的合作，以加强网络安全信息并分享专门知识和威胁情报。

网络安全演习是合作和准备的另一项重要活动。在国家和国际两级开展的这类演习有助于加强网络空间并测试拟对潜在网络威胁采取的措施。在这方面，2011 年、2012 年、2013 年和 2017 年与交通和基础设施部协调举行了国家网络安全演习。2014 年 5 月 15 日和 16 日，与国际电联及其国际打击网络威胁多边伙伴关系合作，在伊斯坦布尔成功完成了国际网盾演习，19 个国家参加了这次演习。

土耳其定期参与并促进与网络安全有关的国际演习，即北约网络联盟、北约锁盾和北约危机管理演习。

由于网络空间没有国界，网络攻击的来源和目标可能在不同国家，包括盟国。指挥和控制中心可能在一个国家，而目标在另一个国家。因此，共享关于网络攻击和网络犯罪分子的信息在全球打击网络威胁方面发挥着至关重要的作用。

欧洲委员会起草的《网络犯罪公约》是唯一具有约束力的公约，该公约于 2001 年在布达佩斯开放供签署，于 2004 年生效。土耳其于 2010 年在斯特拉斯堡签署了该公约。该公约涵盖各种罪行，例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、儿童色情和侵犯网络安全，这些罪行现已纳入土耳其国家法律。此外，土耳其刑法还对未经授权访问信息技术系统以及未经授权干扰或截取、修改或破坏此类系统做出规定。被判犯有这些罪行的人可被判最高三年的监禁或罚款。此后，通过《核准批准<网络犯罪公约>法》，该公约得到批准，在 2016 年底前完成了将公约纳入国内法律的工作。