联合国 S/2021/621

安全理事会

Distr.: General
1 July 2021
Chinese
Original: English

2021 年 7 月 1 日安全理事会主席给秘书长和安全理事会成员国常驻代表的信

谨随函附上裁军事务高级代表中满泉的情况通报副本以及爱沙尼亚总理卡娅·卡拉斯、尼日尔总理马哈马杜·乌胡穆杜、爱尔兰外交和国防部长西蒙·科文尼、越南外交部长裴青山、肯尼亚信息通讯、技术、青年和创新部长乔·穆切鲁、美国常驻联合国代表兼拜登总统内阁成员琳达·托马斯-格林菲尔德、印度外交秘书哈什·瓦尔登·什林拉、圣文森特和格林纳丁斯负责外交事务和对外贸易的国务部长凯萨尔·彼得斯、挪威副外交大臣奥登·哈尔沃森、大不列颠及北爱尔兰联合王国英联邦、联合国和南亚事务部国务大臣温布尔登勋爵塔里克·艾哈迈德、法国欧洲事务和外交部长下属外贸和经济吸引力部长级代表弗兰克·里斯特以及中国、墨西哥、俄罗斯联邦和突尼斯的代表在 2021 年 6 月 29 日星期二举行的主题为“维护国际和平与安全：网络安全”的视频会议上所作的发言。

根据安理会成员就本次视频会议达成的谅解，下列代表团提交了书面发言(在此附上发言副本)：阿根廷、澳大利亚、奥地利、巴林、比利时、巴西、加拿大、智利、捷克、丹麦、厄瓜多尔、埃及、萨尔瓦多、欧洲联盟、格鲁吉亚、德国、希腊、危地马拉、印度尼西亚、红十字国际委员会、国际刑事警察组织、伊朗伊斯兰共和国、意大利、日本、哈萨克斯坦、拉脱维亚、列支敦士登、马耳他、摩洛哥、荷兰、新西兰、巴基斯坦、秘鲁、波兰、卡塔尔、大韩民国、罗马尼亚、塞内加尔、新加坡、斯洛伐克、斯洛文尼亚、南非、瑞士、泰国、土耳其、乌克兰和阿拉伯联合酋长国。

根据 2020 年 5 月 7 日安全理事会主席给安全理事会成员常驻代表的信(S/2020/372)中提出的成员们鉴于冠状病毒病(COVID-19)大流行造成的特殊情况而商定的程序，这些情况通报和发言将作为安全理事会的文件印发。

安全理事会主席

尼古拉·**德里维埃**(签名)

21-09125 (C) 010921 290921

附件一

裁军事务高级代表中满泉的发言

我谨感谢爱沙尼亚组织本次会议并邀请我在本次关于维护网络空间国际和平与安全的公开辩论会上作情况通报。

截至今年 1 月，全球互联网活跃用户已超过 46 亿。估计到 2022 年，将有 285 亿台联网设备连接到互联网，比 2017 年的 180 亿大幅增加。

随着数字技术的进步继续给人类生活带来革命性变化，我们必须对恶意使用这种技术可能危及子孙后代安全的情况保持警惕。

数字技术对现有的法律、人道和道德规范、防扩散、国际稳定以及和平与安全造成越来越大的压力。

这些技术还降低了进入门槛，并打开了新的冲突以及国家和非国家行为体实施攻击、包括跨国界攻击能力的潜在范围。

特别是在信息和通信技术(信通技术)方面，我们看到近年来恶意事件的发生频率急剧上升。这些事件形式多样，从虚假信息到中断计算机网络。这种行为正在削弱各国之间的信任和信心。

这些动态还对信通技术带来的关键基础设施构成特定风险，如金融部门、电力网和核设施等。秘书长提请各方注意大流行病期间对卫生保健设施的网络攻击，呼吁国际社会采取更多措施防止和制止这些可能对平民造成进一步严重伤害的新形式的侵害行为。[1]

这种信通技术威胁也造成对不同性别的影响，必须从这一视角加以审视。网络暴力极端主义和贩运活动对妇女、男子和儿童的不同影响往往被忽视，其他与信通技术有关的威胁也是如此，如网络盯梢、亲密伴侣暴力以及未经同意传播私密信息和图像。因此，我们需要尽一切努力确保男女平等、充分和有效地参与数字领域的决策。

信通技术的威胁正在增加，但应对这些威胁的工作也在进行中。在过去的 15 年里，先后五个政府专家组在联合国研究了信通技术对国际安全的现有和新出现的威胁，并提出了应对这些威胁的建议措施。成立于 2018 年的联合国另外两个进程即不限成员名额工作组和第六届政府专家组最近圆满结束了各自的工作，通过采用具体、务实的建议，在这一专题上迈出了重要步骤。

这两个小组确认了一套自愿的、不具约束力的负责任国家行为规范，承认可以随着时间可制定更多的规范。它们还重申，国际法、特别是《联合国宪章》，对于维护信通技术环境中的和平、安全和稳定是适用的，也是必不可少的。这些小组建议在以往工作进程的基础上采取建立信任、能力建设与合作措施。此外，不

[1] 见 www.un.org/sg/en/content/sg/statement/2020-05-27/secretary-generals-remarks-the-security-council-open-debate-the-protection-of-civilians-armed-conflict-delivered。

限成员名额工作组还根据其任务规定，就建立关于信通技术问题的定期机构对话作出结论和提出建议。

正如最新政府专家组在其报告中指出的那样，之前的政府专家组和不限成员名额工作组建议的措施共同构成了负责任国家使用信通技术行为的初步框架。[2]

新的第二个不限成员名额工作组也刚刚举行了组织会议，并将于今年晚些时候开始实质性工作。

在区域一级，各区域组织正就信通技术问题作出重大努力。根据不同的优先事项和需要，区域方法采用了各种形式。一些区域更加重视通过能力建设工作而实施自愿的、不具约束力的负责任国家行为准则，而另一些区域则开创了自己的区域建立信任措施，以减少信通技术活动引起的冲突风险，或采用其他区域性工具来应对信通技术威胁。另外，还制定了应对信通技术各具体方面的各种区域文书。

虽然各国对维护国际安全负有主要责任，但信通技术是各个社会不可分割的一部分，其他利益攸关方在保障网络空间安全方面可发挥关键作用并享有利益，也负有责任。

许多优秀的私营部门主导的网络举措已经落实，如微软主导的《网络安全技术协议》、西门子和慕尼黑安全会议主导的《信任章程》、Kaspersky 实验室的“全球透明度倡议”。

2018 年“网络空间信任与安全巴黎呼吁”将产业界、国家、公民社会和学术界聚集在一起，承诺实行网络安全九项原则。这些原则涵盖一系列问题，从制定防止恶意信通技术工具和做法扩散的方法，到促进负责任行为国际准则的广泛接受和实施，以及采取网络空间信任措施。

私营部门、民间社会和学术界的观点为国际社会正在寻求的网络安全集体解决方案做出了独特而重要的贡献。

联合国随时准备支持各国与其他利益攸关方一道促进和平的信通技术环境。秘书长召集了一个数字合作高级别小组，它于 2019 年发布了报告。通过随后与各国和其他主要利益攸关方的一系列圆桌讨论，制定了一份路线图，其中建议采取进一步行动，推进数字空间关键领域的合作。

在和平与安全方面，秘书长还提出一项裁军议程，强调需了解和应对可能对现有法律、人道主义和道德规范、不扩散及和平与安全构成挑战的新一代技术。

秘书长在其议程中承诺与科学家、工程师和业界合作，鼓励负责任的科技创新，并确保将其应用于和平目的。

他还第二次承诺与会员国合作，帮助培养一种问责并遵守网络空间负责任行为的新规范、新规则和新原则的文化。

[2] 见政府专家组报告第 21 段。预览版可查阅 https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf。

虽然数字空间已成为支撑几乎日常生活方方面面的基础，但信通技术“不安全”的范围和普遍存在，现在也被认为是人们的一个主要担忧。确定信通技术攻击的责任方面的政治和技术困难，可能带来重大后果，包括意外的武装反应措施和升级。

这些动态因素可能会鼓励刺激各国采取攻击姿态带有敌意地使用这些技术。它还会使寻求发展或获得可能具有破坏稳定能力的非国家武装和犯罪团体和个人逍遥法外。鉴于信通技术威胁对维护国际和平与安全造成的这些影响，安全理事会的当务之急是参与应对这一问题。

因此，我欢迎有此机会向安理会通报情况，我期待着随后将进行的讨论。

附件二

爱沙尼亚总理卡娅·卡拉斯的发言

联合国创建之时已考虑到了未来。即使我们面临一些新的挑战，但 76 年前在《联合国宪章》中商定的价值观和原则在今天依然有效。在日益数字化的未来坚持这些价值观和原则，已经成为最紧迫的全球任务之一。今天，我想谈谈机遇、威胁以及我们已有的应对机制。

第一，机遇：过去一年半的远程工作、学习和生活清楚地表明，我们对数字和通信技术的依赖只会随着时间的推移而增长。我们有责任构建一个所有行为者在网络空间的行为中都遵守一定义务的未来。

所以，今天的辩论不是关于技术的辩论，而是关于如何利用网络空间的辩论。史蒂夫·乔布斯对此说得很好：“技术并不重要。重要的是你要对人有信心，他们基本上都是善良和聪明的，如果你给他们工具，他们会用来做了不起的事”。

作为一个蓬勃发展的数字社会，爱沙尼亚亲身经历了这一点。自由、开放、稳定、安全的网络空间是我们命脉的一部分。由于将大多数政府服务搬到网上，我们每年多节省了 2%至 3%的国内生产总值。我们实行无纸张公共行政管理已经超过 15 年。爱沙尼亚也是人均科技独角兽公司数量最多的国家。

第二，威胁：我们必须认识到，快速的数字化也有其黑暗的一面。

恶意行为者可将网络空间作为另一个制造严重破坏的地域。例如，想象一下如果在干旱期间，一个国家的水供应链停止运行；或者在寒冷的冬季，一个国家的电网中断，会发生什么情况。

在过去的一年里，我们已经看到，针对医疗保健部门的有害网络活动可以构成真实而切实的威胁。干扰关键基础设施造成的人道主义影响可能是毁灭性的。

虽然我们可以在发电厂和其他关键基础设施周围设置高高的栅栏和布置警卫，但这永远不能成为网络空间解决方案的一部分。相反，我们必须共同承担起守护者的角色。

最后，如何应对这些威胁：正如尊敬的情况通报人中满泉女士也概述的那样，幸运的是我们有开展此项工作的坚实基础。

在过去十年中，会员国就网络稳定和预防冲突的有效规范框架达成了一致。这包括现行国际法、11 项关于负责任国家行为的非约束性自愿准则、建立信任措施和能力建设。

爱沙尼亚坚定认为，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，都适用于网络空间。

我要强调，各国对违反其国际法义务的任何行为都负有责任。

特别是为了在武装冲突局势中确保保护平民和民用物体，至关重要的是，在这方面使用网络能力时必须遵守国际人道法规定的义务，安全理事会也定期讨论这一问题。

我们商定的 11 项负责任国家行为准则反映了国际社会的期望，并为国家在网络空间的活动确定了重要的补充准则。

今年春天，国际社会掷地有声地重申了这一规范框架。我们对最新的政府专家组和不限成员名额工作组成功取得协商一致成果感到鼓舞并以其为指导。落实这一框架是国际社会的一大目标。

在全球努力的同时还需要开展区域活动和能力建设。在这方面，我们着重强调区域组织为增进信任、推进合作所做的重要工作。爱沙尼亚还优先开展消除数字鸿沟的工作，这必须与网络复原力能力建设和网上人权保护齐头并进。

我们还必须认识到，我们与私营部门、民间社会和学术界一起应对网络威胁。公司尤其可以通过投资于网络安全和帮助消除漏洞来发挥重要作用。

我相信，今天的讨论将在安全理事会的历史上留下印记，因为我们讨论的问题将对在今后的岁月中维持国际和平与稳定更加重要。

只有我们遵循共同的前进规则，我们的数字未来才会得到保障。

附件三

[原件：法文]

尼日尔共和国总理马哈马杜·乌胡穆杜的发言

首先，我谨赞扬爱沙尼亚致力于将与网络空间有关的安全风险问题列入安理会议程。我还要感谢中满泉女士的通报以及她对解决这一问题的坚定承诺。

在过去二十年里，互联网的普及和信息通信技术(信通技术)的使用以闪电般的速度增长。今天，网络空间已经成为一个地缘政治因素，使各国能够在经济、政治和文化层面扩大自己的势力范围。

数字革命使边界消失，使我们紧密地联系在一起。但由于与数字革命相关的法律具有域外性质，它也给主权带来了新的挑战。同样，这个空间可以通过为所有声音提供一个平台和手段来聆听即使是持不同政见者的声音而加强各国的民主制，它也可证明是犯罪行为者和团体的避风港，他们的唯一目的就是破坏我们各国的稳定。

冠状病毒病(COVID-19)大流行向我们展示了网络空间的两个方面：一方面，我们日益依赖数字技术，而这次虚拟会议就是一个例子；另一方面，我们的系统在面对可能的网络犯罪和网络间谍活动时十分脆弱，其表现为对医疗保健系统的勒索软件攻击和旨在破坏各国公民对疫苗接种工作的信心的散布虚假信息活动。

此外，社交网络和其他讨论平台的蓬勃发展导致某些类型的言论激增，煽动叛乱、恐怖主义、攻击道德价值观和我们民主社会基础的行为。

鉴于上述情况，我谨提出一些建议，我认为这些建议可能会加强对国际法的尊重以及关于国家参与网络空间的负责任规则的执行。

首先，必须弥合国家之间的数字鸿沟、主要是与非洲大陆的数字鸿沟，那里四分之三的人口没有足够的互联网接入，或者根本没有接入。

正如专家们所言，这种情况是加深贫困的一个因素，其影响波及到每个人和社会的每个组成部分，从医疗保健到经济繁荣再到教育；这使得这些领域更容易受到散布虚假信息运动和其他数字威胁的影响。如果不确保数字公平，我们就不能指望网络空间是健康和安全的。

根据这一点，我的第二个建议是通过综合协调的办法建立一个全球架构，使适用于网络空间的国际法规则在医疗保健、国际人道法、选举进程和经济活动等广泛领域得到明确界定。

但在这样做的同时，我们还必须认识到，这一架构在落实和利用其好处方面都必须是公平的，以避免建立采用双重标准的新机制，这只会迫使各国应对其他负面影响，从而加深各国之间的不平等。

按照这一思路，全球一级任何新的监管架构都应该受到区域一级已确立的架构的启发，协调国家一级的适用法规需要这种架构。因此，我们应该提到西非国家经济共同体(西非经共体)关于打击网络犯罪的指令，该指令规定了成员国在这方面的义务，包括对某些行为的惩罚，并为促进网络安全方面的区域合作建立了一个框架。

我的最后建议是，安全理事会着力于对《联合国宪章》作出更具包容性、更少歧视性的解释，而且要以这种方式解释其任务规定，这样我们的审议才能反映当今世界的现实，从而应对网络安全、气候变化和大流行病等议题，因为这些都是真实的威胁，它们就像 COVID-19 一样不受边界约束。

附件四

爱尔兰外交和国防部长西蒙·科文尼的发言

我祝贺爱沙尼亚圆满担任安理会主席。

我还感谢高级代表的宝贵见解。

我欢迎这次及时的讨论，这是安全理事会的第一次此类讨论。

秘书长在去年的讲话中呼吁各国为他所说的“网络空间的荒蛮西部”建立秩序。

尽管联合国近几个月来取得可喜的进展，但各国面临的网络安全挑战继续扩大，危及国际和平与安全。

我今天的发言主要集中在三个方面：

- 挑战与机遇
- 各国需要实施在联合国商定的措施
- 基于价值观的方法对解决该问题至关重要

首先，挑战与机遇并存。

数字和通信技术继续推动经济增长，改变我们的生活、通信和工作方式。

创新是应对当今一些重要全球挑战的关键，包括气候变化。它还促进了医学研究的重要发展，改善了接受教育的机会，并提高了我们维和人员的能力，帮助他们保持安全。

在过去的一年里，大流行病突显出我们对信息和通信技术的日益依赖，在人们不得不相互隔开的时候将他们相互接触，同时暴露了我们的脆弱性。

我是根据最近的经验述及最后一点的。爱尔兰的公共医疗保健系统上个月遭受了一次极具破坏性的勒索软件攻击，影响到关键的医疗服务。

在全球大流行病期间发生这种袭击是令人震惊的。不幸的是，爱尔兰的经历在国际上并不是孤立的。

近年来，恶意网络活动激增，包括严重的勒索软件攻击、网络犯罪、知识产权盗用以及虚假信息和仇恨的传播。

关键基础设施正日益成为攻击目标。

爱尔兰极为关切这一活动对国际和平与安全构成的威胁。

现有的安全挑战正因为网络威胁而更加复杂，例如核武器指挥和控制系统易受网络攻击。这增加了需要在核裁军方面取得进展的新紧迫感。

我们不能让网络空间不受规则或法律的约束，恶意行为者在这一空间随意行动。

网络空间的国际争端必须通过和平方式解决。

安理会必须发出明确信息，支持建立在共识和互信基础上的和平与安全的全球网络空间。

关于我的第二点，爱尔兰欢迎联合国最近在商定网络空间负责任国家行为框架方面取得的进展。

各国现已重申，现行国际法、特别是《联合国宪章》为所有网络安全方法提供了牢固和立于规则之上的基础。

爱尔兰支持旨在促进各国对将国际法适用于网络空间的更深层理解的工作。

我们很快就会公布我们的国家立场，并鼓励其他国家也这样做。

当然，负责任的国家行为也至关重要。

所有会员国都同意以 11 项自愿的国家网络空间行为准则为指导。

我们现在需要在国际法的基础上，努力促进对这些准则的理解和执行，以加强全球网络安全。这将减少冲突的可能性，改善国际关系。

包括对话在内的建立信任措施可建立信任并缓解国家间的紧张局势。我知道这是在说不言自明的话，但它确实需要说出来。

我们欢迎包括欧洲安全与合作组织在内的区域组织在这方面发挥的主导作用。爱尔兰和我们的欧洲联盟伙伴致力于支持能力建设举措。

在高度互联互通的网络空间里，只有所有国家都安全，任何一个国家才会安全。诚然，冠状病毒病(COVID-19)大流行告诉了我们这一点。

我们还继续致力于消除全球数字鸿沟。在下一个十年中，所有人都能上网将是实现可持续发展目标的一项关键内容。

我的第三点是，维护网络空间的国际和平与安全必须以人为本、以价值观为基础。

爱尔兰支持一个安全、可靠和易使用的网络空间，人权和基本自由在这里无论是线上还是线下均适用。

我们坚定地重申，国际人权法适用于各国在网络空间的行动。

保护平民仍然是我们工作所有方面的首要优先事项。在这方面，爱尔兰致力于确保在网络空间尊重国际人道法。

不幸的事实是，太多妇女和女童所经历的性别暴力也伴随着网络暴力和网络威胁，并因此而加重。

这使得作为领导人的我们及所有领导人更需要自觉地促进妇女参与联合国关于网络的进程、决定和政策。

我们需要更加努力，克服性别数字鸿沟。

爱尔兰一贯主张在联合国关于网络安全和能力建设的讨论中纳入更广泛的专门知识。

各国政府以及那些推动和引领技术创新的人有责任维护安全自由的网络空间。

民间社会、技术专家、学者和私营部门的贡献丰富了联合国过去关于网络的讨论。我们认为，迄今他们在网络安全问题上的参与非常有限。

我们还支持包括“网络空间信任与安全巴黎呼吁”在内的倡议，这些倡议将国家和非国家利益攸关方聚集在一起，以实现促进和平与安全的共同目标。

我们必须共同努力，取得更好的共同解决方法。

最后，爱尔兰将继续支持建立在共识基础上的建设性、多边和多方利益攸关方的做法，以加强全球的网络复原力。

我们呼吁所有国家负责任地行事，充分遵守国际法，并实施规范框架。

我们重视安全理事会在预防冲突、促进包括网络空间在内的和平与安全方面发挥的作用。

我们敦促所有国家在联合国近几个月取得的成就基础上再接再厉。

通过这种方式，我们可以确保一个更安全、更和平的全球网络空间，让每个人都从中受益。

附件五

越南外交部长裴青山的发言

我感谢主席和主席国爱沙尼亚就一个非常相关的议题召开本次会议。我感谢中满泉副秘书长富有洞察力的发言。

信息和通信技术(信通技术)的爆炸性发展极大地改变了人们的生活、工作和互动方式。它促进了全球沟通、知识共享和文化交流，帮助人民和国家更加接近，也使生产朝着更高效、可持续和包容的模式发展。

另一方面，这些先进技术如果落入不良之徒手中并被恶意使用，可能会对国家的主权、安全和繁荣构成严重威胁。恐怖分子或跨国犯罪分子使用这种技术，能够破坏经济体系，破坏社会稳定，侵蚀文化和人类价值。

让我们以网络攻击造成的经济损失为例。2020 年，全球年度网络安全支出达到 1 万亿美元，与 2018 年相比增长了 50%，自 2013 年以来增幅达 3 倍。大部分支出用于对损坏的修复和恢复。

更令人担忧的是，有报道称跨国网络攻击破坏了全球和国家安全，甚至可能引发网络战。

因此，网络安全对国家和全球的和平、安全、发展与繁荣都非常紧迫和关键。在此背景下，我想谈一谈以下几点想法。

首先，每个国家对网络空间都有自己的主权和利益，需要得到充分尊重。每个会员国对在其领土内建立适用于其公民的监管网络空间行为的法律框架方面负有首要责任。此外，依法规范行为、防止非法恶意行为、促进积极活动，是为和平、发展和人类创造安全、稳定的网络空间的指导原则。

越南是一个互联网覆盖率很高的国家，我国近 70%的人口活跃在互联网和社交网络上。我们的成功在于建立了促进信通技术发展和防止信通技术被滥用的全面法律框架。越南还优先重视加强自我保护、自力更生和复原力，并结合有效的国际合作。

第二，网络攻击是跨国性的，全球互联网网络成为犯罪者不断利用的目标。与此相应的是，它需要全球和跨国家的网络安全解决方案。越南支持在协商一致和各国最广泛参与的基础上，包括在联合国目前进程的基础上建立网络空间负责任行为规则和规范的国际框架。我们关注并反对以恶意、有害的方式使用信通技术，特别是对人们如此需要的医疗、电力、水和食品设施的网络攻击。网络空间的活动必须遵守《联合国宪章》和国际法的原则，特别是尊重主权、不干涉内政、不使用武力及和平解决争端的原则。

第三，加强网络安全离不开加强国际合作、建立信任和问责。所有国家不分大小和发展水平，都受益于安全和有保障的全球网络空间。因此，它们需要积极参与，为确保全球网络空间的安全和保障、为各国的和平、稳定和可持续发展做出更加务实和负责任的贡献。

信通技术的发展是我们共同追求繁荣的重要起点。越南积极实施国家数字转型战略。我们的目标是到 2030 年数字经济占国内生产总值的比例达到 30%。在东南亚，越南积极参与区域网络安全机制，包括东南亚国家联盟的网络安全合作战略。我们还与许多国家和国际伙伴在这一领域开展卓有成效的双边合作。越南愿进一步推动加强国际合作，建设和平、稳定、安全、有保障的网络空间，实现共同繁荣和可持续发展。

附件六

肯尼亚信息通讯、技术、青年和创新部长乔·穆切鲁的发言

我祝贺主席首次在安全理事会单独召开关于网络安全的讨论会。我感谢裁军事务高级代表中满泉女士所作的内容翔实的通报。

我们对信息和通信技术(信通技术)的依赖与日俱增，既有好处，也有弱点。

那些为和平目的开发和使用信通技术及新兴技术者的努力与站在其对立面者的行为紧密对峙，后者利用这些技术进行控制、非法监视、欺诈、激进化和破坏稳定。

肯尼亚致力于维持和保护一个自由、开放的互联网域。我们把它视为国家发展的关键驱动力，并力求使我们的年轻人在其使用方面获得权能和竞争力。

我们是数字货币领域的世界领先者，率先推出了 M-Pesa 这一首个广泛使用的手机货币平台。我国政府还通过分布在全国各地的称为胡杜马中心的一站式服务设施，采用数字化公共服务交付平台。

肯尼亚的青年人正在开创和建立变革性公司。这一点已得到全球投资者的认可，我们的“硅草原”在我们所处区域吸引了最多的投资。我们相信，我们许多未来的体面工作都将来自这些公司。

由于对数字领域的广泛接触，肯尼亚将其视为确保信通技术安全的重大国家安全目标。

为此，我们建立了健全的监管制度。我们应对威胁的能力也在不断增强。我们的计算机紧急事件应对团队与其他的国家计算机事件应对团队合作，并通过全球事件应对和安全小组论坛在国际上进行合作。

我们今天的任务是就安全理事会如何更好地确保国际和平与安全免遭通过网络空间或利用网络空间带来的威胁提出建议。

我要着重指出我们认为将受益于更好的国际合作和协作的三个领域。

第一个领域涉及信通技术和新兴经济体。网络犯罪越来越多地集中在新兴经济体。在加强现有区域和国际经济冲突解决机制方面需要加强合作，包括共同努力查明和减轻与信通技术相关活动有关的风险，如数字化欺诈、加密货币对国家中央银行系统的影响以及对关键基础设施的网络攻击。

随着工业自动化的加速，失去的工作必须被其他体面的工作所取代，否则和平与安全将受到影响。在投资于数字技能方面需要做更多的事，使工业不发达的国家能够吸引可提供数百万新就业机会的投资。

第二个领域涉及信通技术和暴力极端主义。新兴技术的无处不在、可编程和数据驱动的性质虽然有益，但也为武装组织和恐怖分子的滥用打开了一扇门。这

些组织利用不透明的控制机制、算法、3D 打印、密码学应用和简化的用户界面来招募、策划和实施恐怖行为。这种情况加强了激进化和军事化。

肯尼亚呼吁加强安全理事会和反恐办公室之间的合作，以建立强有力和顺应会员国能力建设需要的网络空间安全能力。

联合国的和平行动任务还需要考虑到敌对的军事化行为体利用网络空间的情况。

我的第三个重点领域是信通技术和社交媒体。假新闻、深度造假、错误信息和虚假信息对和平与安全的影响越来越大，怎么强调都不为过。最近，我们看到假新闻通过推动对疫苗的迟疑态度来削弱对冠状病毒病(COVID-19)大流行威胁的应对措施。

对于社交媒体公司将要追究其责任，并要求其确保假新闻、特别是包括一些得到国家支持的老练的行为者提供的假新闻，不会在他们的平台上扩散。这样的监管工作将需要建立在一个多边平台上，以确保效果的一致性。

最后，我要申明，肯尼亚愿意为加强全球努力、体制框架和规范作出贡献，以扩大自由、和平与稳定的网络领域的潜力，同时减轻威胁。

附件七

美利坚合众国常驻联合国代表琳达·托马斯-格林菲尔德的发言

我感谢主席及爱沙尼亚组织今天的这次重要讨论。我们非常感谢爱沙尼亚提请安理会注意这一问题。我也感谢中满泉高级代表见解深刻的通报。

这场辩论举行得正是时候。特别是随着冠状病毒病(COVID-19)的大流行，我们从未像现在这样依赖科技，我们今天也看到了这一点。但是，国家行为体和非国家行为体都在利用这种日益增加的依赖。在美国，多起备受瞩目的勒索软件事件扰乱了大型食品加工公司 JBS 和为我国东海岸大部分地区提供燃料的公司 Colonial Pipeline。这些事件表明了网络犯罪对关键基础设施构成的严重和无法接受的风险。这些恶意活动的影响通常也是跨国界的。例如恶意网络活动针对的是软件公司 SolarWinds 和微软的 Exchange Server 软件。

风险是显而易见的。我们无论是线上还是线下的基础设施都岌岌可危。我们从吃的食物到喝的水、再到我们在大流行病期间都依赖的卫生保健服务等最基本和最关键的服务，都成了被攻击的目标。因此，在当今世界中，当我们谈论全球安全时，不得不谈到网络安全。幸运的是，尽管我们在意识形态上存在分歧，但会员国在过去十年里一再携起手来，力图防止因网络能力而引发的冲突。我们通过政府专家组的进程共同阐明了网络空间负责任国家行为的框架。该框架明确指出，国际法适用于网络空间。它还概述了各国应采取的自愿规范和实际合作措施。

近几个月来，由所有会员国组成的不限成员名额工作组就一份明确赞同网络空间负责任国家行为框架的新报告达成了共识。就在上个月，第六届联合国政府专家组工作也圆满结束，就该框架提出了一系列强有力的建议和新的指导方针。这就是进展。这些报告提供了从国家使用网络能力到处理网络事件起因归属这一复杂问题的实际指导。该框架还考虑到各国应如何合作，以减轻源自某一特定国家领土的重大恶意网络活动的影响，包括犯罪分子从事的活动。

我们共同担这一责任。正如拜登总统最近指出的那样，我在此引用他的话：“各国需要对在其领土上进行勒索软件活动的罪犯采取行动”。因此，我要明确指出：当一个国家得知来自其领土的有害活动时，它必须采取合理步骤加以应对。鉴于网络空间的跨国性质，这种合作至关重要。

会员国如此努力地制定的框架现在提供了前进规则。我们都承诺实施这一框架。现在，是时候把承诺付诸实践了。我们有大量工作要做，以确保所有希望在网络空间负责任地行事的国家都拥有开展这种工作所需的政策知识和技术能力。在完成这项工作的同时，我们还需要继续保护互联网自由。人们在线下享有的权利，包括表达自由、结社及和平集会的权利，也必须在线上得到保护。

会员国表现出弥合分歧并就这些问题达成共识的非凡意愿。让我们继续表现出这种诚意，为全世界建立网络安全方面的联合战线。我们将共同建设开放、安全、稳定、惠及所有人的网络空间。

附件八

印度外交秘书哈什·瓦尔登·什林拉的发言

我感谢主席，并欢迎爱沙尼亚主动组织本次公开辩论会，以着重指出网络安全的一个重要新兴领域。我也感谢中满泉副秘书长的通报。

虽然自安全理事会成立以来，和平的意义一直未变，但几十年来，冲突的性质及其基本的使用工具发生了巨大变化。今天，我们看到了来自网络空间的对会员国的安全威胁与日俱增，这一威胁再也不能被忽视。因此，公开辩论举行得正是时候。

越来越多地使用网络技术及信息和通信技术加快了经济发展，改善了向公民提供服务的方式，提高了社会意识，并让信息和知识掌握在每个人手中。如今网络时代的政治、社会、经济、人道主义和发展等大多数活动(包括安全理事会本次高级别会议)，现在都是在网络空间进行或与网络空间相连。冠状病毒病(COVID-19)大流行只是加速和扩大了这些活动的数字化。

网络空间的动态和不断演变的特点也将网络安全带入了关于和平与安全的讨论。网络空间的无国界性质，以及更重要的是行动实施者的匿名性质，挑战了传统上被接受的主权、管辖权和隐私概念。网络空间的这些独特性质给会员国带来了一系列挑战。我将在发言中重点谈到三个关键挑战：

第一，一些国家正在利用其在网络空间的专门知识来实现其政治和安全相关目标，并沉迷于当代形式的越界恐怖主义。世界已看到利用网络工具危害国家安全的情况，手法包括攻击关键的国家基础设施，其中有卫生和能源设施，甚至通过激进化破坏社会和谐。开放的社会尤其易受网络攻击和虚假信息运动的影响。

第二，我们看到了世界各地的恐怖分子老练地利用网络空间扩大他们的诉求，散布恶毒的宣传，煽动仇恨和暴力，招募青年和筹集资金。恐怖分子还利用社交媒体策划和实施恐怖袭击并造成严重破坏。印度作为恐怖主义的受害者，始终强调会员国需要更战略性地应对和处理恐怖主义利用网域的影响。

第三，构成网络空间基石的信通技术产品的完整性和安全性正在受到损害。人们普遍担心，国家和非国家行为体正把脆弱性和有害的隐藏功能、包括利用后门渠道加入信通技术网络和产品。这种邪恶的行为破坏了对全球信通技术供应链的信任和信心，损害了安全并可能成为国家之间的导火索。确保所有行为体遵守其国际义务和承诺、不沉迷于可能对通信技术产品全球供应链和贸易产生破坏性影响的做法，符合国际社会的利益。

网络领域的互联性要求不能孤立地解决网络空间产生的复杂问题和威胁。作为会员国，我们需要在网络空间采取基于规则的协作方式，努力确保网络空间的开放、稳定和安全。从国际安全角度促进网络空间负责任国家行为政府专家组和信通技术发展问题不限成员名额工作组取得的积极成果所产生的势头应得到利用，以进一步寻找共同点并改进已经商定的网络规范和规则。这些规则必须着力于通过国际合作确保集体网络安全。多方利益攸关方的参与将是实现这一目标的关键。

促进公平使用网络空间及获得其利益，也应成为这一国际合作的重要组成部分。各国之间不断扩大的“数字鸿沟”和“数字知识鸿沟”在网络领域造成了一个不可持续的环境。后冠状病毒(COVID-19)时代对数字的日益依赖加重了风险，并暴露出这些数字不平等的裂痕。必须通过能力建设来弥合这些裂痕。网络空间的无处不在和无边界的性质，意味着我们的强大只能取决于全球网络中最薄弱的一环。我们“唯有团结”才能实现全球安全、具复原力的网络空间的目标，我们必须确保在这一集体努力中不让任何国家掉队。

印度致力于营造开放、安全、自由、易使用和稳定的网络空间环境，这将成为创新、经济增长、可持续发展的引擎，确保信息自由流动，尊重文化和语文多样性。近年来，通过 IndiaStack、Aadhar 和 UPI 等变革性技术举措，我们成功地利用了网络技术的巨大潜力来落实《2030 年可持续发展议程》并改善治理。作为其 COVID-19 疫苗接种活动(世界上最大的此类活动之一)的一部分，印度开发了 Co-WIN 这一可扩缩、包容和开放的技术平台。Co-WIN 平台可以为全球卫生干预措施而定制和扩大规模。我们正在努力与伙伴国共享这一平台。

我们的首要目标是利用网络空间促进人民的增长和赋权，不仅是为了我们自己的国家，而且是为了全人类。印度随时准备在这一努力中提供其专门知识和分享其经验。

附件九

圣文森特和格林纳丁斯负责外交事务和对外贸易的国务部长凯萨尔·彼得斯的发言

我们表示赞赏主席国爱沙尼亚率先就一个极其重要的议题举行今天的高级别公开辩论会，评估安全理事会在维护国际和平与安全任务中的表现。我还要感谢今天所有情况介绍者所作的见解深刻的介绍。

在当今世界中，网络空间几乎触及到我们日常生活的方方面面。信息和通信技术(信通技术)在促进经济和社会福利方面的作用是显而易见的。然而，尽管有这些好处，全世界仍必须认识到存在的严重信通技术问题。全球信通技术环境正面对国家和非国家行为体恶意使用信通技术的急剧增加。可以肯定，信通技术的滥用给所有国家带来风险，并有可能对国际和平与安全产生负面影响。因此，当务之急是我们必须在早先承诺的基础上制定建立信任措施，以加强国际和平与安全，并增强会员国在这一领域的合作、透明度、可预测性和稳定性。

一个开放、安全、稳定、易使用、和平的信通技术环境对所有国家都至关重要，需要各国开展有效合作，以降低对国际和平与安全的风险。此外，来自全球信通技术链各级不同部门的其他行为体具有不同的能量和能力，在确保网络安全方面发挥着关键作用。我们必须探索进一步开发能力建设和提供技术援助资源的可能性。联合国需要加强对会员国的援助，并进一步帮助确保参与网络空间的各种联合国实体之间的一致努力。这些努力应该与本组织更广泛的目标挂钩。

圣文森特和格林纳丁斯尽管作为一个小岛屿发展中国家面临许多挑战，但已采取具体步骤提高其应对网络犯罪祸害的能力。《电子证据法》(2004 年)和《电子交易法》(2007 年)这两部法律为我国网络安全的基本立法框架奠定了基础。2016 年 8 月，立法者通过了 2016 年《网络犯罪法案》，从而为国家提供了实体和程序法，以便能够更有效地应对网络犯罪。我们还承诺遵守美洲国家组织和加共体内的区域网络安全协议。

由于冠状病毒病(COVID-19)大流行以及最近火山喷发造成的进一步破坏，我国的学校已经转为远程教育，世界各地都是如此。随着数以千计的儿童收到政府提供的平板电脑来协助这一过渡，互联网使用量和网屏时间都有所增加。考虑到这一点，教育与民族和解部发起了一项#GoCyberSmart 运动，以促进网络安全。这项活动是一项提高认识的举措，旨在增强学生做出正确数字决策的能力。三个重点领域是信息安全、硬件安全和安全上网浏览。

会员国以及区域和国际组织之间交流信息意义重大，对于确保稳定和防止网络安全事件升级必不可少。此外，我们呼吁会员国继续致力于遵守国际法和网络空间负责任国家行为框架。

在我们努力在国际和平与安全的背景下推动网络空间负责任国家行为时，必须以 2010 年、2013 年、2015 年和最近 2021 年政府专家组的共识报告中所载的评估和建议以及联合国不限成员名额工作组最后报告的结论和建议为指导。

最后，如果不能就和平的信通技术环境接触规则、政策规范和国际合作机制达成一致，只会产生新的不稳定和冲突根源。在网络空间中，我们鼓励国际社会所有行为体遵守其国际法律义务，包括尊重《联合国宪章》规定的主权和政治独立以及以与现实世界相同的方式和平解决争端的原则。维护网络空间国际和平与安全的紧迫努力绝不能停止。

附件十

挪威副外交大臣奥登·哈尔沃森的发言

一个全球易使用、自由、开放、安全的网络空间对于维护国际和平与安全至关重要。我们欢迎爱沙尼亚提请安全理事会注意这一议题，安理会是根据《联合国宪章》负责维护国际和平与安全的联合国主要机构。

信息和通信技术(信通技术)是全球基础设施的基本组成部分。它们是所有国家发展、稳定和安全的核心。然而，网络空间也越来越多地成为国家之间竞争和潜在冲突的舞台。

在过去十年中，我们目睹了国家和非国家行为体的恶意网络行动在范围、规模、严重程度和复杂性方面都有所增加。我们发现自己正处于一场全球大流行病之中，即使是关键的卫生基础设施也成为此类恶意活动的目标，危及公民的安全和我们管控 COVID 危机的全球努力。

然而，也有使人乐观的理由。过去的一年表明，国际社会准备迎头而上，共同努力推动负责任国家网络空间行为。不限成员名额工作组和政府专家组的共识报告表明，所有会员国都致力于维护基于规则的网络空间国际秩序。这是多边主义的胜利。

确认国际法对网络空间的适用性，是政府专家组和不限成员名额工作组共识报告的基础。国际法是各国共同致力于预防冲突和维护国际和平与安全的基石。它是增强各国间信任的关键。这两份报告都重申，国际法、特别是《联合国宪章》，对于维护和平与稳定、促进开放、安全、稳定、易使用与和平的信通技术环境是适用的和必不可少的。

我们认为，政府专家组的报告承认国际人道法适用于所有武装冲突、也适用于网络冲突，这是迈出的重要一步。

国际人道法旨在尽量减少武装冲突造成的人类痛苦。它规范和限制武装冲突期间的网络行动，就像它规范和限制任何其他战争手段和方法一样。因此，禁止袭击平民或民用物体，医疗服务部门必须得到保护和尊重。因此，禁止攻击关键基础设施，如电力供应、食品生产、饮用水设施或其他对民众生存不可或缺的物体。

承认国际人道法在网络空间的适用性并不能使网络战合法化。各国的武力使用仍受《联合国宪章》和习惯国际法规则的管辖。国际争端必须以和平方式解决，在网络空间和所有其他领域都是如此。

所有会员国都支持网络空间负责任国家行为框架。这一框架的基础是：国际法的适用性、遵守商定的自愿规范、切实的建立信任措施和能力建设工作，以增强所有人的复原力和安全。这是一项重大成就；但其价值只能通过所有国家的执行和遵守才能实现。

今天的会议是对网络空间恶意活动可能严重影响国际和平与安全的认识。今天的会议也是向所有国家发出的明确信号，即指望我们遵循我们商定的网络空间负责任国家行为框架：我们必须履行国际法规定的义务，遵守我们商定的准则。

附件十一

大不列颠及北爱尔兰联合王国英联邦和南亚事务部国务大臣温布尔登勋爵艾哈迈德的发言

今天，几乎世间一切都具有数字维度。

国际社会需要抓住互联网提供的巨大机会，无论是学习、商业、交流甚至是娱乐的机会。

但我们也需要以应有的严肃态度对待随之而来的威胁。

现在，网络空间恶意和危险活动带来的威胁比以往任何时候都更加明显。

事实上，就在上个月，一个犯罪团伙以 Colonial Pipeline 为目标，将美国最大的燃料管道作为勒索对象，并威胁要造成严重的经济混乱。

其中一些活动的目的是盗窃或敲诈勒索。通常，这只是一种造成破坏和混乱的行为。

但我们作为国际社会，肩负创造一个惠及所有国家、实际上惠及所有人的网络空间的集体责任。我们应该共同制定促进公同利益的规则。

在这方面，我们当然不是从零开始。

十年前，联合王国在伦敦聚集了 60 多个国家，以确立普及互联网、保护个人在线权利等基本原则。

十年之后，我们已自此走过了很长一段路。

就在今年，联合国大会一致重申了国际法在网络空间的适用性，并商定了一套自愿原则，包括需要保护卫生基础设施。

一个政府专家组增强了我们对网络空间规范、规则和原则的理解，并对如何适用国际法提出了明确的解释。

但我们想更进一步。各国正在开展网络行动以支持其军事和国家安全能力，这已不是什么秘密。事实上，联合王国就是其中之一。

我要表明：我们将利用这些能力保护自己不受那些试图伤害我们的人之害。我们承诺在必要的情况下，以比例对等的方式并依照国际法使用这些能力。

我们在这方面的共同挑战是澄清国际法规则如何适用于国家在网络空间的活动，防范恶意行为者违反规则，并迫使那些实施恶意网络活动者承担后果。

联合王国致力于同所有国家及其众多利益攸关方合作，确保网络空间遵循加强我们集体安全的规则和规范。

这些促进民主价值观的规则和规范，是支持全球经济增长的规则和规范，并遏制数字威权主义的蔓延。

我们必须维护网络空间的法治：体现负责任的国家行为，鼓励遵守合规，威慑攻击，并追究其他人对不负责任国家行为的责任。

我们还必须绝对优先考虑并确保在网络上保护人权，如同在离线时一样，以保证我们建立一个人人可用的自由、开放、和平和安全的网络空间。

联合国网络空间负责任国家行为框架是我们的出发点。我们必须支持所有国家现在就执行这一框架。

联合王国上个月高兴地宣布，我们将投资 3 000 多万美元，支持脆弱国家的网络相关能力建设，特别是在整个非洲和印度洋-太平洋地区。

我们与国际刑警组织的合作将帮助包括埃塞俄比亚、加纳、尼日利亚、卢旺达和肯尼亚在内的国家支持打击网络罪犯的联合行动。

在其他地方，联合王国的资金将帮助建立国家应急小组保护各国免受这些威胁。

当然，如果没有私营部门的伙伴以及学术界和民间社会的伙伴，我们无法做到这一切。

但总而言之，当我们今天聚集在此时，安全理事会也要发挥关键和重要的作用。

当恶意活动对国际和平与安全构成威胁，导致加剧冲突或造成人道主义痛苦，安全理事会就必须随时准备作出反应。

安理会应该像应对常规手段构成的威胁一样作出反应。

我们有机会抓住网络空间带来的机遇，确保网络空间继续成为促进所有人繁荣和进步的力量。

为此，当务之急是我们必须共同努力，对抗那些危及我们集体安全的人。

我要向你们保证：联合王国完全致力于为子孙后代保护一个自由、开放、和平与安全的网络空间。

附件十二

法国欧洲事务和外交部长下属部长级代表弗兰克·里斯特的发言

[原件：法文]

我谨感谢爱沙尼亚总理为这次会议所做的努力。安全理事会负责维护国际和平与安全，也应该能够在网络空间做到这一点。

网络空间既是充满机会的地方，也是新的威胁之地。它已经成为大国之间战略竞争的领域。无论是国家行为体还是非国家行为体，恶意使用信息和通信技术(信通技术)的行为都在激增。

在过去几个月里，特别是在冠状病毒病(COVID-19)大流行的背景下，我们看到对这些技术的依赖有所增加。我首先想到的是使用勒索软件对医院和其他关键基础设施发动的令人发指的网络攻击。我谨表示法国完全声援这些袭击的受害者。我还想到了通过传播“信息疫情”或互联网日益碎片化来操纵信息的活动，这些做法与民主价值观背道而驰。网络空间的行动产生非常真实的后果，这些后果可能证明对我们的生活和社会而言是严重的。

下个世纪的挑战将是建立网络空间的集体治理和监管。我们既不想要一个“数字荒蛮西部”，也不想要一个与世隔绝的网络空间。我们在“网络空间信任与安全巴黎呼吁”以及在七国集团关于网络规范倡议的《迪纳尔宣言》的框架内确认了这一点。法国决心与伙伴们共同建设开放、安全、稳定、不碎片化、易使用、和平的网络空间。

包括《联合国宪章》在内的国际法完全适用于网络空间。这也意味着在武装冲突期间进行的网络行动须遵守国际人道法。

面对日益增多的网络空间威胁和网络攻击，各国政府应该通过合作和法律来应对。十多年来，法国在各项多边努力中发挥了先锋作用。这些努力促成了各国在使用信通技术方面负责任行为框架的出现。这一框架以国际法、一套连贯的非约束性行为准则以及透明和信任措施为基础。它使各国在网络空间的相互合作与了解方面取得了进展。我谨赞扬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问题第六届政府专家组最近取得的成功，它们通过了两份平衡和有用的共识报告。法国愿继续以建设性方式参加联合国内部，包括在大会第 75/240 号决议设立的新的信息和通信技术安全和使用问题不限成员名额工作组框架内的多边讨论。

展望未来，必须首先有效地付诸实施已商定的准则和原则。法国与 52 个合作伙伴提议由联合国制定关于网络安全的《行动纲领》。这一新工具是对新的不限成员名额工作组的补充，将促成建立一个持久的架构。其目的将是支持能力建设并创造与民间社会、研究人员和私营行为体进行对话的空间。法国愿意与所有有意于完善这一注重行动的提议并在此基础上再接再厉的国家和利益攸关方进行对话。

至关重要的是要有多个行为体做出这种集体承诺。在网络空间，国家当然肩负着其他行为体无法承担的责任，但它们无法单独行动。我们必须全面参与这种新形式的外交工作。

附件十三

中国常驻代表张军的发言

[原件：中文]

我感谢中满泉副秘书长所作的通报。

当今世界，新一轮科技革命和产业变革方兴未艾，数字和网络技术发展迅速，极大改变了人类生产生活方式，促进了各国经济社会发展。与此同时，网络监听、网络攻击、网络犯罪和网络恐怖主义成为全球公害，网络空间军事化、政治化、泛安全化和意识形态化愈演愈烈。各国在网络世界既享有共同机遇、拥有共同利益，也面临共同挑战、承担共同责任，正日益成为休戚与共的命运共同体。

中国国家主席习近平指出，各国虽然国情不同、互联网发展阶段不同、面临的现实挑战不同，但推动数字经济发展的愿望相同、应对网络安全挑战的利益相同、加强网络空间治理的需求相同。中方始终主张国际社会应携手合作，共同保障网络安全，维护国际和平。

- 我们应以维护和平促安全，防止网络空间成为新的战场。国际社会应遵守《联合国宪章》宗旨和原则，特别是主权平等、禁止使用武力、不干涉内政、和平解决争端等原则。应尊重各国自主选择网络发展道路、网络管理模式、平等参与网络空间治理的权利，不从事危害他国安全的网络活动。应审慎对待武装冲突法等适用于网络空间问题，防范网络空间军备竞赛。

- 我们应以交流合作促安全，营造网络空间良好环境。维护网络安全是全球性课题，没有哪个国家能够置身事外、独力应对。网络空间霸权主义、单边主义、保护主义只会加剧紧张对抗，毒化合作氛围，应当受到国际社会共同抵制和反对。各国应携手努力，深化在技术研发、规则制定、信息共享等方面的交流合作，共同遏制信息技术滥用。应共同反对网络监听和网络攻击，打击网络恐怖主义和网络犯罪，提升网络安全保障能力。应为企业提供开放、公平、非歧视的营商环境，保障全球信息通信产业链供应链开放、稳定、安全，推动全球经济健康发展，反对以各种理由人为干扰企业正常经营行为。

- 我们应以加强治理促安全，推进网络空间公平正义。各国应践行真正的多边主义，在联合国框架下建立各方平等参与、开放包容、可持续的网络安全治理进程，制定各国普遍接受的网络空间国际规则，反对搞小圈子和集团政治。中方高度赞赏联合国网络安全问题开放式工作组和政府专家组顺利达成报告，期待新一届开放式工作组为维护网络安全作出新贡献，愿与各方一道推动在联合国框架下制订打击网络犯罪国际公约。我们应本着共商、共建、共享精神，充分发挥政府、互联网企业、技术社群、民间机构、公民个人等多利益攸关方作用。

- 我们应以普惠发展促安全，实现网络空间共同繁荣。当前世界经济发展艰难乏力，数字和网络技术可以成为各国疫后复苏与恢复经济社会发展的重要引擎。各国应采取更加积极、包容、协调、普惠的政策，促进信息通讯技术在全球范围内均衡发展，大力发展数字经济等新模式新业态，反对搞科技霸权。应加强数字基础设施建设和互联互通，打破信息壁垒，弥合数字鸿沟，帮助发展中国家提高数字化、网络化、智能化水平，落实《2030 年可持续发展议程》。应加大对发展中国家的网络安全合作与援助，提升其网络安全事件预警防范和应急响应能力。

中国高度重视网络安全和信息化建设，致力于建设数字经济、数字社会、数字政府，以数字化转型整体驱动生产方式、生活方式和治理方式变革。中国将在《网络安全法》和《数据安全法》基础上，继续健全国家网络安全法律法规和制度标准。

中方去年提出《全球数据安全倡议》，聚焦关键基础设施和个人信息保护、企业境外数据存储和调取、供应链安全等重大问题，为维护全球数据和网络安全提出建设性解决方案。不久前，中方同阿拉伯国家联盟发表《中阿数据安全合作倡议》，体现了双方维护网络和数据安全的共同呼声。我们欢迎各方积极响应，共同参与，携手打造全球数字治理规则。中方还积极推进“数字丝绸之路”建设，同各国共同构建面向未来的智能化互联互通新格局。

网络空间承载人类梦想，关乎民众福祉与和平安全。中方愿同世界各国一道，把握信息革命机遇，培育创新发展新动能，开创数字合作新局面，打造网络安全新格局，构建网络空间命运共同体，携手创造人类更加美好的未来。

附件十四

墨西哥常驻联合国代表团的发言

[原件：西班牙文]

墨西哥欢迎召开本次公开辩论会，并欢迎副秘书长兼裁军事务高级代表中满泉通报情况。

正如我们在这里以及在许多其他论坛上听到的那样，网络空间日益重要，这是不可否认的。世界变得越来越依赖信息和电信技术，在大流行病的背景下更是如此。国际关系也迅速进入虚拟世界，安全理事会不能也不应该意识不到它对国际和平与安全的影响。

尽管全球近一半的人口没有互联网接入，但这并不能使其免于成为每天针对政府网络、银行业和金融机构以及研究和卫生机构的数千起网络攻击的受害者。

这些潜在风险导致联合国系统各机构对威胁作出反应，并力求各国之间达成协议，以确保网络空间不被用于犯罪、敌对甚至恐怖主义目的，同时又不忽视其与和平利用之间的平衡及其为可持续发展提供的巨大机遇。

墨西哥认为，防止网络空间风险升级至关重要。与任何其他自然环境一样，网络空间的使用应该按照非常明确的准则和参数进行监管，同时需要帮助促进构建开放、自由、安全、稳定、易使用和具韧性的网络空间。

因此，墨西哥赞扬政府专家组和不限成员名额工作组圆满完成工作，促成以协商一致方式通过实务报告，这是多边努力的根本先例。我国认为，这一事实再次证实了人们对多边主义的普遍信心，以及联合国在实现综合、合法和长期应对网络空间及信息和通信技术的挑战方面可发挥的建设性作用。

然而，这还不够。必须在网络空间全面适用国际法，包括《联合国宪章》、国际人权法、国际人道法并发展这些领域的判例法方面取得进展。

我们坚信，应提高网络空间活动的透明度和问责制，呼吁制定由大会通过的负责任国家行为准则，并辅之以促进国际合作建设和加强各国网络能力的措施。

墨西哥希望，在安全理事会今后的审议和工作中，能够听到民间社会、学术界和私营部门越来越多的声音。它们理所当然拥有一个共同目标：确保和平利用网络空间以开发和使用数字技术。

附件十五

俄罗斯联邦常驻联合国代表瓦西里·涅边贾的发言

[原件：俄文]

2019 冠状病毒病(COVID-19)大流行暴发后的一年对全世界来说是一场重大的磨难。它首先被铭记为充满挑战和损失的一年。许多外交努力受挫，谈判在多个方面停滞不前。

联合国关于国际信息安全的多边讨论在这方面表现突出，因为它不仅保持了势头，而且取得了我敢说是历史性的成果。联合国大会指定的两个专家论坛——政府专家组和不限成员名额工作组——都能够以协商一致方式通过其最后报告。

这两个小组的谈判并不容易，使来之不易的成果更加珍贵。这些成果清楚地表明，只要对话是务实、非政治化和建设性的，国际社会就能够在关键问题上达成一致。由于这些努力，我们现正进入一个重要的新阶段。这一阶段始于新的 2021-2025 年不限成员名额工作组 2021 年 6 月举行的组织会议。

这一成果是国际社会的共同成就。几十年来，我们一直致力于为建立确保国际信息安全的全球体系作出贡献。1998 年，俄罗斯首次在联合国提出需要应对国际信息安全的威胁，并为此提出了一项大会决议。21 世纪初，我们提议成立政府专家组，作为讨论国际信息安全的专家论坛。2019 年，当这一议题显然超出了专家组关注的狭隘范围时，我们与志同道合的代表团一起，响应国际社会的需求，发起了国际信息安全的公开民主谈判进程。这一进程由所有会员国参与并采用不限成员名额工作组的形式。

这是一个非常重要的里程碑。这是有关数字安全的讨论第一次向联合国大多数会员国开放。我们的理由非常直截了当：我们相信公平和相互尊重的对话。如果我们在面临国际信息安全的威胁时都是平等的，那么，这种威胁不应由技术先进的国家组成的小圈子来讨论，而应由联合国所有会员国来讨论。自认为更“先进”的国家不应将自己的意志强加于人。

我们关于设立政府专家组以及后来的不限成员名额工作组的提议，起初并非人人喜欢。一些国家，包括参加今天会议的国家，投票反对成立上述机构。然而，他们逐渐开始加入对话，并最终成为积极和建设性的参与者。

联合国在国际信息安全领域的有效多边外交补充了各国在这一议题上的双边合作。这是一个很好的例子，说明应如何处理这些问题，克服互不信任和化解担忧。它与臭名昭著的“扩音器外交”形成鲜明对比。然而，不幸的是，我们的一些伙伴有时会诉诸后一种方式。

与此同时，我们不幸地看到一种危险趋势，即联合国安全理事会试图对政府专家组和不限成员名额工作组内达成的协议进行单方面解释。这实际上是要求支持，或更糟糕的是修改这些指定的大会论坛的讨论结果。我们认为这种企图是破坏性的。它们正在把国际社会推向不可测、不可取的对抗。

具体而言，一些国家正在试图通过歪曲协议，其中包括关于使用信息和通信技术(信通技术)的国际法律方面的协议，为其行为进行辩护。这些行为有，对其他会员国施加单边压力和制裁，并可能对其使用武力。令人严重关切的是，一些技术先进的国家正在积极追求信息空间的军事化，宣扬“预防性军事网络打击”、包括针对关键基础设施进行打击的概念。这些对抗性理论违背了他们(包括今天)宣布的防止使用信通技术引起的冲突的承诺。这些国家是在试图利用其实力地位，在信息领域强加自己的“游戏规则”。

我想强调的是，尽管数字领域并非不受监管，但关于如何准确地将国际法适用于数字领域的辩论远未结束。这些问题将在指定的大会论坛——新的不限成员名额工作组内至少再讨论五年。

在这方面，政府专家组和不限成员名额工作组的最后报告代表了一套微调、平衡的协议，其中包括需要就信息空间负责任国家行为制定新的规范，同时考虑到信息空间的特殊性。在俄罗斯联邦的倡议下，大会于 2018 年通过了关于国际信息安全的决议，其中载有此类规则的初步清单。然而，不幸的是，我们的西方同事现正试图从这份清单中挑出对他们最有利的条款，同时将国际法在数字领域的适用性错误地解释为“自动”，这将允许在数字领域使用武力。我们的西方同事还试图将他们的国家观点说成是全球共识的产物。因此，任何通过联合国安全理事会对在指定的大会论坛上达成的平衡协议进行修改的企图，我们都予以反对。

正如俄罗斯联邦总统普京在 2021 年 3 月 26 日俄罗斯联邦安全理事会会议上指出的，在发展确保国际信息安全的全球体系方面，俄罗斯的理论办法仍然是公开、透明和不变的。这套办法载于总统于 2021 年 4 月批准的《国际信息安全国家政策基本原则》。这是一份公开文件，我鼓励大家阅读。

我们的理论基于以下前提：信息和通信技术仅用于和平目的、需要防止信息空间的冲突、为此有必要加强多边和双边合作。我们认为，应缔结普遍的国际法律协议，以便有效地处理这些任务。为实现这一目标，必须共同努力，为信息空间中的国家行为制定和商定普遍、公平和全面的规则，这些规则应考虑到当前现实。还必须共同努力，以明确区分信息空间中允许和不允许的活动；使这些规则具有法律约束力，以确保所有国家严格遵守。

与此同时，我们维护国家主权在数字领域的不可侵犯性。应由每个国家来决定管理自己的信息空间和相关基础设施的参数。

同样重要的一项任务是，建立一个确保国际信息安全的和平、公平、公正的体系，该体系兼顾所有国家的利益，无论其数字潜力如何。应大力支持由联合国牵头、以缩小数字鸿沟为目的的建设这种能力的努力。我们相信，新的不限成员名额工作组将能够根据其任务规定，继续详细审查这一问题并提出相关建议。

此外，我们必须共同打击将信息和通信技术用于犯罪目的的行为。我们呼吁各会员国为指定的特别委员会的工作作出建设性贡献，该特别委员会负责在 2023 年前拟定一项关于这一问题的公约草案。

大会仍然是讨论国际信息安全的关键论坛。正是在这个论坛上，将在今后五年内就这一议题的所有方面进行专家讨论。让我们集中精力支持这一独特的进程。我们必须维护国际信息安全多边合作的建设性气氛。这一多边合作由联合国主持、以不限成员名额工作组的形式进行，其有效性和相关性已得到证明。这将使新的不限成员名额工作组真正有机会取得切实可行的成果。作为联合国安全理事会成员，我们有共同责任为这一努力作出充分贡献。

附件十六

突尼斯常驻联合国代表塔里克·拉德卜的发言

首先，我想对主席国爱沙尼亚组织这次关于网络安全和维护网络空间国际和平与安全的会议表示感谢。

我感谢副秘书长兼裁军事务高级代表中满女士所作的内容丰富的通报。

突尼斯对近年来网络空间恶意活动的大幅增加深表关切。这些活动可能对国际和平与安全构成严重威胁，特别是在关键基础设施成为目标时。

许多国家还公开发展用于军事目的的网络能力。这一趋势可能引发网络军备竞赛，进一步增加网络攻击和反击的数量，并增加可能导致武装冲突的误判风险。

突尼斯同样担心的是，以前只有国家才有的网络能力，现在已被包括恐怖组织在内的非国家行为者利用并被恶意利用。据报道，这些能力往往是从政府实体的泄漏或盗窃获得的，这进一步提出了国家责任的问题。

不能再排除恐怖组织对核电站等关键基础设施发动毁灭性网络攻击的可能性，应认真对待。

突尼斯重申国际法在处理国家使用信息和通信技术方面的适用性，并在这方面强调必须尊重《联合国宪章》所载的原则，包括以和平手段解决国际争端、不以武力相威胁或使用武力以及尊重人权和基本自由。

我们还想再次强调，国际人道法适用于武装冲突期间的网络行动。

我国代表团欢迎今年早些时候一致通过了从国际安全角度看信息和电信领域的发展不限成员名额工作组的报告、在国际安全背景下促进网络空间中负责任的国家行为政府专家组的报告。这两份报告都有助于加深成员国对国际法如何适用的理解，并就自愿、不具约束力规范如何在预防冲突和促进开放、安全、稳定、无障碍与和平的网络空间方面发挥重要作用提供了进一步的指导。

我们期待着在新的 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会议期间继续就网络安全问题进行公开和包容性的对话，以加强所有国家的能力，防止或减轻恶意网络活动、网络威胁和网络攻击的影响。

在突尼斯国家安全委员会的监督下，在私营部门和民间社会的参与下，突尼斯于 2019 年 10 月通过了一项国家网络安全战略，旨在通过发展国家能力和法律制度，充分尊重基本权利和自由，并通过加强国际合作，提高突尼斯对网络威胁的复原力。

最后，鉴于网络空间的相互关联性，我们认为，分享关于已知脆弱性的信息和为提出要求者进行能力建设，对于减少网络威胁对国际和平与安全构成的风险至关重要。

附件十七

阿根廷常驻联合国代表团的发言

[原件：西班牙文]

阿根廷感谢爱沙尼亚倡议举行公开辩论，以进一步了解网络空间恶意行为带来的日益严重的风险及其对国际和平与安全的影响。安全理事会根据其任务规定和性质，能够处理这一议题，并赋予其应有的相关性和重要性。

世界各地关于严重网络事件的报告经常出现且不断增加。这提请大家注意，需要继续加深对此类事件的理解，其中一些事件可能危及国际和平与安全；以及需要建立合作框架，促进国家能力建设，以迎接影响整个国际社会的挑战。因此，需要在国家、区域和国际各级采取行动。

在国际一级，为解决这个问题最关键的方面之一，阿根廷认为，最重要的是保持广泛和包容的空间，使来自所有区域和持有不同观点的国家都能积极参与，就负责任的国家行为的规则、规范和原则以及如何在网络空间适用国际法等问题建立共识。阿根廷的理解是，联合国大会所有成员以协商一致方式接受了一大批自愿规范、规则和原则，以指导各国使用信息和通信技术以及网络空间中负责任的国家行为。这对维护网络空间的和平利用和稳定至关重要。这是一个起点和基础，应得到维护和发展。

我们特别重视第一个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取得的共识，它以公开性特点为基础。我们还特别赞赏最新的在国际安全背景下促进网络空间中负责任的国家行为政府专家组的报告。应该指出的是，这两个小组今年都发布了共识报告，提出重要建议并作出重要贡献，以便继续在过去达成的共识的基础上再接再厉。

为继续巩固已达成的协议并达成新的协议，有必要继续保持一个开放和包容的论坛，推动更广泛的讨论。因此，我们欢迎设立一个新的信息和通信技术安全和使用问题不限成员名额工作组，其任务期限将延长至 2025 年。我国将继续积极和建设性地参与其中。

在这个问题上，为采取更有效的办法，阿根廷与所有区域的其他一些国家一起，支持关于在国际安全背景下发展信息和通信技术的行动纲领的国际倡议。该行动纲领正在进行全面的概念拟订。它提出一个开放、包容、灵活和持续的框架，供在联合国主持下、由各国进行、并由参与网络空间的多个行为者适当参与的讨论。我们邀请所有国家关注这一倡议。

阿根廷认为，我们理解的基础和原则应是保护和保障《联合国宪章》和国际条约所载的人权和基本自由。性别问题和对弱势群体的特别保障必须是我们采取的所有行动中一项贯穿各领域的因素。

在该领域不断创新的背景下，我们必须积极努力，确保所有国家都能公平地享受这些技术的好处。因此，我们认为，缩小国家之间和国家内部的数字鸿沟应该是辩论中持续关注的问题。

这种关注与国家能力的发展是相辅相成的。这一领域有巨大的行动空间，这是与参与网络空间的其他行为者，如私营部门、民间社会、学术界和技术部门发展协同增效的原则之一。

事实证明，区域和次区域组织是发展国家能力、促进共同理解和推动国际合作的重要和决定性的行为者。

毫无疑问，各国必须在国家一级做出重大努力，发展有效的能力、规范和结构，使这一问题得到应有的重视和优先考虑。

我们相信，这次活动将使我们能够找到新的理解途径，帮助我们实现自由、开放、安全、可互操作和稳定的网络空间。

附件十八

澳大利亚常驻联合国代表米切尔·菲菲尔德的发言

澳大利亚感谢爱沙尼亚给我们机会向安全理事会就网络空间的国际和平与安全问题发言。随着网络空间的战略意义的增强，将有更多团体试图通过网络空间施加力量。网络问题已成为所有国家迫切关注的战略性外交政策问题——国际社会将其视为战略问题至关重要。

尽管恶意网络事件的频率、规模、复杂性和严重性都在增加，联合国在促进国际合作以了解这些威胁和促进开放、自由、安全、可互操作、和平的网络空间方面有着深厚的历史。

联合国所有成员以协商一致方式商定，现有的国际法、尤其是整个《联合国宪章》，适用于网络空间，对维护和平与稳定以及促进开放、安全、稳定、无障碍、和平的信息和通信技术环境至关重要。[3]

澳大利亚就国际法的特定原则如何适用于网络空间中的国家行为阐明了观点(2017 年；2019 年；2021 年)，并发表了假想的法律案例研究(2020 年)。[4]

国际人道法(包括人道、必要性、相称性和区分等各项原则)适用于武装冲突中的网络活动。国际人道法规定了适用于武装冲突中不构成或未达到“攻击”程度的网络活动的规则，包括向平民和平民个人提供的一般保护，使其免受军事行动带来的危险。

国际人权法也适用于网络空间中的国家行为。根据国际人权法，国家有义务保护其管辖范围内个人的相关人权，包括隐私权，如果这些权利是通过网络空间或在网络空间行使或实现的。

认识到网络空间的独特属性，2015 年，所有会员国同意在使用信通技术时以 11 条自愿、不具约束力的网络空间负责任国家行为规范为指导。[5] 这些规范是对国家现有法律义务的补充，而不是取而代之。国际法与规范一起确立了对国家负责任行为的明确预期，从而促进了可预测性、稳定性和安全性。

所有国家还认识到，需要采取建立信任措施并协调能力建设。[6] 这些努力旨在防止导致冲突的误解，现在比以往任何时候都更加重要。还需要进行有针对性的能力建设，以确保所有国家都能够应对挑战，抓住互联互通增加带来的机遇。

[3] 见大会第 68/243 和 70/237 号决议、第 75/564 号决定。

[4] 见 www.internationalcybertech.gov.au/international-security-at-the-un。

[5] 见大会第 70/237 号决议。

[6] 同上。

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《联合国网络空间负责任国家行为框架》(《框架》)，为安全、稳定和繁荣的网络空间提供依据。该框架的每个要素都相辅相成，任何一个要素都不应孤立考虑。

该框架得到所有会员国的普遍赞同，[7] 这是在促进网络空间国际和平与稳定方面取得的重大进展。该框架如果得到遵守，将为应对国家产生、国家支持的恶意网络活动构成的威胁提供坚实基础。

澳大利亚重申致力于按照《网络空间负责任国家行为框架》行事。2010 年、2013 年、2015 年和 2021 年的政府专家组报告[8] 以及不限成员名额工作组 2021 年报告[9] 都阐述了该框架。澳大利亚呼吁所有国家也这样做。

然而，尽管国际社会提出明确期望，少数国家和国家支持的行为者却日益藐视国际法和规范。他们的做法威胁到国际和平与稳定。

我们需要的不是更多的规则，也不是新的规则，而是遵守我们已经商定的规则，以及在规则破坏时加强问责。为阻止恶意活动，必须让违反现有国际法以及商定的负责任国家行为规范的人承担实际后果。

澳大利亚致力于打击、威慑和阻止恶意网络活动，特别是国家及其代理人的恶意网络活动。澳大利亚将与合作伙伴合作，加强对网络空间不可接受行为的协调应对。威慑恶意活动可以保护国际稳定。澳大利亚网络威慑政策的目标是，防止损害澳大利亚和我们国际合作伙伴利益的重大网络事件的发生。

国家与多利益攸关方社区(包括民间社会、私营部门、学术界和技术界)之间的有效合作对安全产生了实际影响，提升了能力，并在网络空间创造了一个发展、开放和稳定的强化循环。往往是最先受到网络事件影响的人、关键基础设施的保护者、技术专长的受益者、网络空间非政府利益攸关方不断发展的权益，为维护和平的在线环境提供了互补利益。

性别不平等破坏了网络空间的全球和平、稳定和安全。它助长并往往加剧了一系列挑战，如贫困、治理不力、冲突和暴力极端主义。性别平等和妇女参与与网络空间国际和平与安全相关的决策、领导、和平建设的价值是毋庸置疑的。澳大利亚将继续采取切实步骤，支持妇女积极有效地参与讨论网络空间的国际和平与安全的所有论坛。

恶意网络活动造成的潜在损害或破坏相当严重，且不断增加。国际社会对这些问题日益关注并提高了认识，这一点不应浪费。应抓住这个机会——加深对国际法如何适用于网络空间的理解，促进负责任国家行为准则和建立信任措施的切实执行，协调能力建设，以便所有国家都理解并能够执行该框架，并确保听到不同的声音。

[7] 大会第 75/564 号决定；A/75/816。

[8] A/65/201；A/68/98；A/70/174。

[9] A/75/816。

附件十九

奥地利常驻代表团的发言

奥地利感谢爱沙尼亚以安全理事会 2021 年 6 月主席的身份召开本次关于网络空间国际和平与安全的公开辩论会。奥地利赞同欧洲联盟的发言。我们希望以我国的名义补充以下几点意见。

今天标志着安全理事会首次将网络安全作为一个单独的问题来处理——这是一个值得欢迎的发展。为了保持相关性并履行其任务，安全理事会必须继续应对当代对国际和平与安全的威胁。

过去几年，越来越多的恶意网络活动增加了网络空间的威胁。在今天的互联世界中，当基础设施越来越依赖于数字控制系统时，网络攻击的影响可能与传统攻击相似，有时甚至更糟。这些事态发展，再加上网络攻击归因方面的挑战，增加了不安全因素、误判的风险以及在决定如何应对来袭攻击时可能出现的人为错误。

虽然网络空间的运作与物理世界不同，但有一个简单的事实不会有错：整个国际法也完全适用于网络空间。最近，信息和通信技术(信通技术)不限成员名额工作组以及网络安全政府专家组的成果都重申了这一点，这两个工作组都以协商一致的方式达成了实质性的成果文件，进一步加深了我们对网络空间面临的挑战的理解。随着越来越多的国家不仅发展防御性网络能力，而且发展进攻性网络能力，所有国家在使用信息和通信技术时都必须遵守现有的国际法以及关于在网络空间负责任行为的规范。我们希望这些文件能提醒各国注意自己的义务，从而有助于提高网络空间的稳定性。

不言而喻，《联合国宪章》的基本规定应指导所有国家在网络空间的行为。特别是，各国有义务遵守禁止使用武力的规定，这是国际安全制度的核心支柱。此外，过去的政府专家组已就网络空间负责任国家行为准则达成一致，这些准则已得到所有会员国的认可。因此，很明显，造成不稳定、不安全的不是缺乏规则和规范，而是执行不力。因此，我们呼吁所有国家充分遵守国际法，全面遵循负责任国家行为规范。

如果网络空间出现武装冲突或冲突因素，必须尊重和遵守国际人道法——人道、必要性、相称性、区别等原则在网络空间完全适用。

在 COVID 大流行的背景下，我们关切地注意到，最近对医疗和卫生设施的网络攻击有所增加，这公然违反了关键基础设施，包括医疗基础设施，在任何时候都应禁止恶意网络活动的规范。

为避免冲突情况，关键是要建立信任——各国应建设性地参与分享他们对网络空间的理解以及参与军事活动的方式，避免误判。在这方面，区域组织的作用不可低估——许多组织开展了建立信任的活动。我们特别欢迎欧洲安全与合作组织在这一问题上的参与，我们相信，在其网络安全事务联络点网络的经验基础上，我们也可以在联合国层面推出一个全球网络。

尽管国家、国际和区域组织在制定国际法和负责任国家行为规范方面一直走在前列，但它们无法独自应对我们面前的挑战。商业行为者在网络空间有着重要的作用和责任，而民间社会和学术界则帮助我们将不同的观点带入讨论。这就是为什么未来关于网络空间的讨论应该以一个整体、多利益攸关方的方法为指导，以确保在维护自由、安全、开放和稳定的网络空间方面发挥作用的人的声音被听到，并为我们寻求的共同目标作出贡献。

尽管在网络安全领域取得了所有进展，但仍有许多未解决的问题——这将取决于国际社会是否能找到这些问题的共同答案。合作仍将是关键，奥地利随时准备在相关进程中作出建设性贡献。本着这一精神，我们希望安理会未来的公开辩论将恢复以往的做法，即允许非成员进行口头发言，以便让所有感兴趣的国家都能看到。

附件二十

巴林常驻联合国代表贾迈勒·法里斯·阿尔鲁瓦韦的发言

[原件：阿拉伯文]

技术和数字转型以及现代技术的出现正在帮助实现全人类的进步、繁荣和发展。2019 冠状病毒病(COVID-19)大流行期间，所有部门对远程工作、教育和服务提供的依赖使其重要性得到了放大。尽管技术发展有许多好处，但也有许多风险。在缺乏一个明确的保护信息安全和网络空间的体系的情况下尤其如此。正如我们所见，各种网络攻击针对国家的基本基础设施，并威胁到重要部门、机构或个人。

联合国对这一问题给予极大关注。安全理事会在几次关于维护国际和平与安全的会议上以及在阿里亚模式会议上，都间接提到这个问题。大会还建立了一些机制，包括 2021-2025 年信息和通信技术(信通技术)安全和使用问题不限成员名额工作组。该工作组成立于 2020 年，旨在审议国际安全背景下使用信通技术带来的威胁、制定国家的网络空间行为准则、在使用信通技术方面适用国际法、建立信任措施和能力建设。

巴林坚信，务必保护网络空间不受攻击并确保国家和人民利益，因此支持建立这样的机制。巴林参加了从国际安全角度看信息和电信领域的发展不限成员名额工作组的工作，该工作组于 2021 年完成工作。巴林期待着积极参加新成立的工作组。

随着信通技术的数字化转型和巨大飞跃，巴林高度重视网络安全。作为这种关注的一部分，巴林通过内政部国家网络安全中心(负责处理王国各部门的网络安全问题)、信息和电子政务管理局(负责保护巴林王国政府数据网络的信息安全)，努力建立一个明确和全面的治理系统来保护网络空间。电信管理局试图加强公共和私营部门的合作，以确保做好应对网络安全威胁的准备。

巴林还注意制定信息安全的立法和法律框架，以保护个人和机构。此类立法包括关于保护个人数据的第 30(2018)号法案、关于保护信息和国家文件的第 16(2014)号法案、关于信息技术犯罪的第 60(2014)号法案。

在区域一级，巴林积极参与海湾阿拉伯国家合作委员会网络安全常设委员会的工作。它提议建立一个电子平台，以便在成员国之间交流关于网络安全的信息和数据。每个成员国都任命了一名联络官负责交流网络安全信息，包括关于威胁和最佳做法的信息。

巴林王国于 2017 年批准了《阿拉伯打击信息技术犯罪公约》。

最后，巴林王国申明支持国际网络安全合作，以满足世界各国人民的愿望，并在实施 2030 年可持续发展目标方面实现进步、繁荣和增长。

附件二十一

比利时常驻联合国代表菲利普·克里德尔卡的发言

首先，请允许我感谢主席国爱沙尼亚主持安全理事会关于网络空间和平与安全的首次公开辩论会。本次及时的辩论显示处理这一议题的紧迫性以及安全理事会这样做的相关性。网络空间恶意活动带来的风险确实在增加，对国际和平与安全的影响比以往任何时候都更加有害。因此，最重要的是，重申会员国对国际法和负责任国家行为框架的承诺，将其作为预防冲突和维护网络空间和平与安全的关键因素。

实现这一目标既需要国际社会对网络空间治理达成共同的国际理解，也需要采取实际行动在实地落实这一愿景。

关于网络空间治理的国际辩论正处于关键阶段。比利时坚决支持联合国框架内正在进行的辩论，其中包括第一委员会、各种不限成员名额工作组和政府专家组。以下是关键因素。

首先，比利时主张建立全球、自由、开放、稳定、和平、安全的网络空间的共同愿景，在这个空间，人权和基本自由以及法治均适用。这一共同理解基于包容性的办法，倾听所有利益攸关方，包括民间社会、私营部门和学术界的意见。

其次，国际社会必须继续努力为负责任国家行为建立一个真正普遍的网络安全框架。这一框架必须建立在充分应用现有国际法，包括整部《联合国宪章》、国际人道法和国际人权法的基础上。去年，比利时作为安全理事会非常任理事国参加了关于关键基础设施网络攻击的安全理事会阿里亚模式会议。针对关键基础设施的网络攻击正在危及人的生命，必须受到国际社会的谴责。针对医院等医疗设施的网络攻击绝不可接受。

关于联合国的网络空间负责任国家行为框架，必须强调的是，联合国会员国通过了联合国第 70/237 号决议，认可了政府专家组 2010 年、2013 年和 2015 年报告的结论，这些结论构成了进一步工作的坚实、协商一致的基础。联合国及其会员国作出重大努力，建立了关于网络空间治理的共同国际理解，还制定了在实地落实这一共同愿景的实际行动。在一个高效和有效的多边体系中，我们必须在这一共识基础上推进任何进一步的讨论，以避免重蹈过去艰难妥协的覆辙，避免使未来的努力陷入困境。

第三，我们认为，应使国际刑事司法更好地适应 21 世纪的挑战。这就是为什么比利时与列支敦士登一起倡议设立关于《罗马规约》适用于网络战的顾问委员会，以探讨国际刑事法院在这一新的监管框架中可以发挥的作用。我们期待着收到顾问委员会的最后报告。该报告定于今年提交。

指导原则之后要有行动跟进，才能有所作为。在这方面，比利时相信，埃及和法国提议建立的行动方案是落实我们愿景的正确架构。比利时自豪地与其他 50 多个国家一起支持这一倡议，我们希望其他许多国家也加入。

在国家层面，比利时最近在 2021 年 5 月通过了新的“2021-2025 年国家网络安全战略 2.0”。该战略阐述了我国在提高网络复原力和打击网络威胁方面的跨领域办法。这项国家战略的主要目标是“推动比利时跻身欧洲最不脆弱国家之列”。

比利时的网络安全政策还规定了一个新的归因机制，该机制被设想为一种威慑工具。如果我们想在网络攻击的数量和复杂性不断增加的环境中有效地预防和威慑恶意的网络活动，针对比利时重要组织的恶意网络活动的正式归因是一项重要工具。还可以启动国家归因程序，帮助遭到类似攻击的盟国受害者。

此外，该国家战略还规定了明确的国际承诺。这是因为比利时言行一致，坚信需要加强国际合作来促进网络空间的安全与稳定。

加强国际合作也意味着更多的能力建设和对建立信任措施的更多支持，包括通过欧洲安全与合作组织(欧安组织)等区域组织的努力。比利时积极参与欧安组织的工作，使这些建立信任措施具体化、可操作。能力建设方面的需求在全球范围内都是重要而紧迫的。现有的合作或能力建设方案，如欧洲联盟或全球网络专门知识论坛提供的方案，需要予以加强和扩大。增强全球抵御网络威胁的能力符合我们所有人的利益。

附件二十二

巴西常驻联合国代表团的发言

首先，我要祝贺爱沙尼亚提出这一伟大倡议，首次推动安全理事会在维护国际和平与安全的更广泛背景下举行关于网络安全的正式公开辩论。信息和通信技术(信通技术)快速发展，已渗透到人类生存的各个领域，促使我们更新威胁的概念，使现有的规范框架适应这一新的现实，并制定负责任国家行为的新模式，以克服现代挑战，遏制冲突的出现。

虽然对维护国际和平与安全负有主要责任的这个机构刚刚才提出网络安全议题，但会员国就这一议题的辩论已超过 20 年——至少从 1998 年这个议题首次被列入大会议程起。在此期间，我们目睹政府专家组通过了四份共识报告，其中两份由巴西专家主持。不限成员名额工作组也通过了一份同样的共识报告。这些文件共同构成了一个由共同理解、不具约束力的自愿性规范、规则和原则组成的既有成果体系，有助于指导各国使用信通技术。

这一体系对维护国际和平与安全的最大贡献之一是，主张国际法、包括国际人道法适用于网络空间。在我们为上一个政府专家组正式汇编提供的国家自愿贡献中，我们重申了巴西的坚定信念，即各国在使用信息和通信技术时必须遵守国际法，包括《联合国宪章》、国际人权法、国际人道法。联合国和其他区域组织已认识到，国际法，特别是《联合国宪章》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、无障碍的信息和通信技术环境至关重要。因此，在目前的讨论中，问题不再是国际法是否适用，而是国际法如何适用于各国对信通技术的使用。

虽然确定如何适用在大多数情况下可参照物理世界的类似情况，但网络空间的独特性创造了新情况，而国际法最初并不是为了规范这些情况。信息系统的互联性、信通技术环境的无形性以及网络空间恶意和攻击性行为的责任归属问题的复杂性，对国际法提出新的挑战。而国际法的发展一直以有形的领土国际秩序为基础。

各国对国际法如何适用于信通技术的使用解释不同，这增加了不可预测的行为、误解和紧张局势升级的风险。因此，有必要逐步确定各国在这一问题上的共同点，并在分歧之处共同致力于提高对现有规则解释的一致性。如有必要，还应考虑制定额外的规范，作为填补潜在法律空白和解决其余不确定性的一种手段。

维护国际和平与安全在很大程度上取决于国家之间的信任程度。因此，除了承认国际法的适用性以及建立和实施负责任国家行为的规范、规则和原则之外，最重要的是各国政府实施建立信任措施。在技术和政治层面建立联络点网络，以及就威胁和信通技术事件管理交流国家意见，则是重要的合作和透明措施。这些举措不仅有助于防止误会和误解，还有助于处理严重的信通事件，并在危机情况下缓解紧张局势。

能力建设也是促进和平的信通技术环境的重要工具。与其他领域一样，国家间的不平等也会在网络空间产生不安全感，对动能世界产生直接影响。为发展国

家机构、人力资源和公共政策而开展的国际合作有助于降低国家的脆弱性，对普及执行国际法和网络空间负责任国家行为的规范、规则和原则至关重要。如果说疫情教会了我们一件事，那就是在人人安全之前，没有人是安全的。同样的道理也可适用于高度相连、相互依存的网络空间。

鉴于网络空间的多利益攸关方性质，巴西认为，如果没有民间社会、学术界和私营部门的贡献，任何关于网络安全的有效讨论都不会成功。多利益攸关方的办法对于识别和抗击威胁、防止冲突、促进共同理解、提高网络复原力和促进合作至关重要。不同国家的公共和私营行为者之间进行更广泛的互动，交流经验和分享最佳做法，对于实现一个更加开放、安全、和平、无障碍的信通技术环境至关重要。

巴西一直积极参加联合国内部关于网络安全的讨论。在政府专家组和上一个不限成员名额工作组中，我们始终力求主动。新的不限成员名额工作组将在 12 月举行第一次实质性会议。巴西将在新工作组的辩论中保持建设性态度。在可能建立的其他定期机构对话机制，如网络安全行动纲领的对话机制中，巴西也将保持建设性态度。与此同时，作为新当选的安全理事会非常任理事国，我们还打算在本机构为发展关于在国际安全背景下使用信通技术的影响的讨论作贡献。巴西认为，安理会应首先以以下目标为指导：促进遵守大会就网络安全问题通过的过去和未来的建议。

谢谢各位！

附件二十三

加拿大常驻联合国代表团的发言

[原件：法文]

我们感谢爱沙尼亚组织这次安全理事会会议，讨论如此及时和相关的议题。加拿大很高兴有机会为这次讨论作贡献。

世界越来越依赖数字技术和互联网。来自网络空间对国际和平与安全的威胁不胜枚举。对民主进程的干扰是一个特别令人关切的领域。另一个是最近勒索软件事件的增加。因此，我们必须继续采取措施，维护自由、开放和安全的网络空间。

商定的网络空间负责任国家行为框架是这一空间和平与稳定的基础。该框架包括承认国际法对网络空间的适用性、遵守国际商定的规范、能力建设，以及运用建立信任措施。这些因素加在一起减少了升级和冲突的风险。

联合国不限成员名额工作组和政府专家组最近通过的共识报告重申了这一框架。所有联合国会员国现在都已承诺以该框架为指导。

国际法对于确保基于规则的国际秩序延伸到网络空间至关重要。最近的不限成员名额工作组和政府专家组报告重申了国际法在网络空间的适用性，并在这方面取得了重要进展。工作组报告建议在国际法的能力建设方面加强合作，使更多的国家能够发展本国观点并建立共同理解。政府专家组报告重申了国际法的适用性，并特别提到了国际人道法。

政府专家组 2021 年 5 月编写的报告为执行 2015 年通过的、并经所有会员国通过大会第 70/237 号决议认可的 11 条自愿的负责任国家行为规范提供了指导。加拿大认为，这些商定的规范和国际法基本上足以指导网络空间中的国家行为。然而，在其传播和执行方面仍有工作要做。最近由犯罪集团实施的高调勒索软件事件导致能源和食品供应等关键行业大范围中断。它们还影响了金融市场。

尽管犯罪集团应对这些行为负责，但这些例子突显了国际法和 11 条政府专家组规范的重要性，其中一些规范直接或间接涉及对关键信息和通信技术基础设施的威胁。一项规范规定，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。另一项规范指出，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。

从事勒索软件和其他犯罪活动的犯罪行为者在各国生活和工作。他们利用国家的数字基础设施进行恶意活动。他们受这些国家的法律约束。当被告知恶意活动可能来自其领土时，各国有责任作出反应、执行其法律并与其他国家合作。通过同意以政府专家组规范为指导，我们都已承诺这样做。这也是越来越多国家通过强有力的法律打击网络犯罪的原因。在许多情况下，各国以《欧洲委员会网络犯罪公约》(又称《布达佩斯公约》)为基础制定法律。该公约的缔约方现来自世界所有地区。

不幸的是，正如我们在最近局势中所看到的，所有国家并不总是尊重负责任国家行为框架。一些国家允许网络罪犯在其领土上逍遥法外。其他国家正在使用代理或故意从事与违背该框架的恶意网络活动。对于这种行为及其对国际和平与安全构成的威胁，加拿大多次与国际伙伴一起呼吁并作出应对。

加拿大是 2019 年 9 月《促进网络空间负责任国家行为的联合声明》的 27 个签署国之一。除了重申负责任国家行为框架外，我们承诺在自愿基础上共同努力，在国家违反这一框架时追究其责任，包括采取透明和符合国际法的措施。

这就是我们一直在做的事情，我们将继续这样做。为维护负责任国家行为框架，有必要强调反规范行为。我们鼓励其他国家也这样做。

关于联合国未来的道路，加拿大期待着建设性地参加 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。我们还将积极推动网络安全行动纲领的制定。加拿大是该行动纲领的共同提案国，因为我们认为，该行动纲领可以作为一个有益、务实的论坛，促进负责任国家行为框架的实施。

这两个进程的成功将取决于它们在其工作方法和产出中纳入不同声音和观点的能力。在不限成员名额工作组中，加拿大主张非政府利益攸关方的切实参与。民间社会、学术界、技术界和私营部门可以为这些讨论作出很多贡献，因为他们在执行政府专家组和工作组的建议中发挥着重要作用。我们还将倡导利益攸关方大力参与正在制定的行动纲领。

同样重要的是，无论是在不限成员名额工作组还是在行动纲领中，都必须确保切实听取妇女的意见。应从一开始就将性别问题纳入这两个进程的主流，以确保这两个小组的工作解决网络安全的性别问题。有资料显示，妇女有意义参与的冲突调解进程产生更有力的结果，减少了和平进程结束后敌对行动再现的可能性。联合国的网络进程也同样可以通过让妇女有意义的参与而得到加强。包容对这两个进程的成功非常重要。

简而言之，加拿大仍然是网络空间负责任国家行为框架的坚定支持者。我们将继续促进过去的政府专家组和最近的不限成员名额工作组的建议的实施。我们还将坚持不懈地呼吁并依法应对违背该框架的恶意网络活动。我们期待着继续与国际社会一道，加强网络空间的稳定和安全，以促进国际和平与安全。

附件二十四

智利常驻联合国代表团的发言

智利重申其立场，即国际法特别是《联合国宪章》对于维护和平与稳定以及促进开放、安全、稳定、无障碍与和平的信息和通信技术(信通技术)环境是适用和必要的。这一点以及《联合国宪章》的具体原则，特别是和平解决争端、禁止对任何国家的领土完整或政治独立使用或威胁使用武力、不干涉他国内政、尊重人权和基本自由，在物理领域和数字领域都是不可分割的，因此，智利将继续促进这些原则的实施。

包括国家和其他行为者在内的持续威胁行为者开展的恶意信通技术活动，对国际安全与稳定、经济和社会发展以及个人的安全和福祉构成重大威胁。针对在国内、区域或全球范围内提供服务的关键基础设施的恶意活动已日益严重，其中包括影响以下方面的恶意信通技术活动：关键信息基础设施、向公众提供基本服务的基础设施、对互联网的普遍可用性或完整性至关重要的技术基础设施以及卫生部门实体。在未来的冲突中，这些恶意活动可能更具破坏性，严重影响人们的福祉和生活。在这个意义上，各国可能会受到武装冲突背景下产生的网络攻击的严重影响。

在武装冲突期间，各国在领导和执行其在网络空间的行动时应严格遵守国际法规则，并特别考虑到国际人权法和国际人道法。

智利坚决支持政府专家组的工作及其在 2010、2013、2015 和 2021 年通过的报告和建议，因为它们代表了在信通技术领域的国际法、规范和建立信任措施方面的巨大进展。智利还支持不限成员名额工作组的工作及其建议。为减少对网络能力的恶意使用并建立一个更稳定的网络空间，必须在各个层面遵循和执行这些建议。

推进网络空间负责任国家行为行动纲领是一项积极、建设性和现实的倡议，可以帮助我们在信通技术环境的框架内向前迈进并取得具体成果。该行动纲领可以是永久、包容、基于共识和务实的国际文书，以推进在国际安全背景下使用信通技术的负责任行为。作为这一倡议的共同提案国，智利认为，该行动纲领将提供一个通过业务建议的平台，促进国际合作，推动适合受惠国需要的援助方案，特别是在能力建设方面。

关于遵守现有的国际法和执行网络空间负责任国家行为规范，重要的是各国能够就国际法在网络空间如何适用发表看法并与其他国家分享。这一领域的能力建设也至关重要。制定执行规范的准则是一个重要步骤，应有助于各国在这一问题上取得进展。区域组织可以在协助各国执行规范和遵守国际法、制定这方面的区域战略以及培训和能力建设方面发挥关键作用。

智利认为，加强网络空间的建立信任措施和能力建设至关重要，区域组织必须在这方面发挥最重要的作用。在这方面，我们强调美洲国家组织通过其网络空间合作和建立信任措施工作组正在开展的工作，以及欧洲安全与合作组织和东南亚国家联盟的工作和进展。

有必要促进各区域就这一问题的对话，而且是能力建设和执行或规范方面的对话。这种对话应考虑交流经验、信息、准则、最佳做法、经验教训，并邀请各组织成员参与这些区域进程。各国应加强国家联络点和外交部在网络空间和信通技术政策方面的作用。网络外交是一项帮助各国改善合作、建立信任的重要工具。各国还应考虑建立双边机制，就网络安全和网络空间进行对话和合作。

智利认为，多边进程必须尽可能包容和透明。关于信通技术的讨论应包括私营部门、学术界、民间社会、工业界和技术界等。如果我们不能保证所有利益攸关方的参与和工作，就不可能在网络空间建立稳定和安全的环境。参与讨论的行为者越多，我们就越有可能取得对所有人都有利的结果。在这个意义上，我们认为，我们有必要听取所有相关方的意见，他们也可以在正式会议上发表自己的观点和意见。从这个意义上说，各国在制定旨在预防冲突、建立共识和提高网络复原力的政策、战略和其他倡议时，应包容所有利益攸关方。

附件二十五

捷克共和国常驻联合国代表团的发言

捷克共和国感谢爱沙尼亚共和国历史性地组织了安全理事会关于国际和平与安全背景下网络安全议题的首次公开辩论。各国在网络空间遵守国际法和负责任国家行为是预防冲突和维护国际和平与安全的关键因素。

捷克共和国赞同欧洲联盟提交的发言，并希望补充以下两点意见。

当前和正在出现的对国际和平与安全的网络威胁

网络空间为人类和经济发展带来巨大好处，但它也正在成为依赖性和安全挑战日益加剧的领域。在 2019 冠状病毒病(COVID-19)大流行期间，我们对信通技术的依赖日益增强，而恶意行为者不断利用信通技术为自己谋利，这清楚地提醒我们，网络空间面临着日益严峻的挑战。值得注意的是，我们看到针对向公众提供基本服务的关键基础设施的恶意信息和通信技术(信通技术)活动出现了惊人的增长，如针对医疗设施、水、能源、卫生设施、选举基础设施和互联网普遍使用的恶意活动。特别是，越来越多的网络攻击破坏了医疗服务的提供，导致更多的生命损失，破坏了我们应对 COVID-19 的集体能力，并最终威胁到国际和平与稳定。

这种旨在故意破坏关键基础设施的鲁莽的信通技术活动还有可能造成毁灭性的人道主义后果。如果这是国家所为，则违反了国际法规定的国家义务。因此，捷克共和国欢迎所有会员国最近通过政府专家组和不限成员名额工作组的最后报告申明，针对关键基础设施的信通技术活动是不可接受的。虽然政治承诺是第一个必要步骤，但保护关键基础设施免受信通技术威胁还需要国际社会作出持续的实际努力，包括通过加强技术合作和具体的网络相关能力建设方案。安全理事会还可以发挥决定性作用，确保国家支持的针对关键基础设施的信通活动承担后果。

新的和正在出现的网络威胁不仅影响各国的国家安全，还日益威胁到个人的福祉和安全。捷克共和国特别关切的是，主张保护网络空间个人自由的国家与呼吁加强技术监控的国家之间的政治分歧越来越大。我们认为，通过信通技术扩大国家支持的大规模监控技术、部分或完全关闭互联网以及广泛的内容审查引起了严重的人权关切。必须采取果断行动，保护公民免受国家权力在网络空间的任意和非法行使。这些趋势，加上将人工智能引入我们生活的各个方面所带来的潜在风险，带来新的安全挑战，威胁到人们对网络空间的信任和信心，并可能最终削弱我们维护国际和平与安全的能力。

加强对国际法和负责任国家行为规范的遵守

捷克共和国重申，各国遵守国际法规定的义务是维护自由、和平、稳定、安全、可互操作和无障碍的网络空间的基本要素。所有国家都肯定现行国际法对国家使用信通技术的适用性，特别是通过大会第 68/243 号和第 70/237 号决议普遍认可了 2013 年和 2015 年政府专家组报告。

在这方面，捷克共和国还回顾，各国对其领土上的信通技术行使专属管辖权的权利不仅产生了国际法规定的权利，还产生了具体的义务。特别是，捷克共和国希望重申，包括国际人道法和国际人权法在内的现有法律体系毫无例外地适用于网络空间中的国家行为。

令人遗憾的是，少数国家继续质疑现有国际法对网络空间的适用性，包括国际人道法对武装冲突背景下使用信通技术的适用性。捷克共和国希望强调，在它看来，国际人道法对信通技术行动的适用性不会促进网络空间的军事化，也不会促进任何其他领域的军事化。相反，国际人道法对使用武力施加了限制，要求在武装冲突背景下使用的所有战争手段和方法都必须符合其规则，包括人道、区分和相称性规则等原则。

此外，捷克共和国回顾，根据国际不法行为责任法，所有国家都有义务尽职调查，在其能力范围内采取具体措施，确保其领土不被用于对其他国家进行恶意网络活动。

捷克共和国同样认识到，国家执行网络空间负责任国家行为现行框架的能力，包括充分开展尽职调查的能力，与该国的能力有内在联系。在这方面，捷克共和国强调，需要加强国际努力，在全球范围内建设网络能力和提高网络复原力，包括尽早制定联合国网络空间负责任国家行为的行动纲领，这将使会员国能够通过实际和注重成果的行动，推动现有承诺的落实。

最后，捷克共和国完全致力于对网络安全采取以人为本的办法，强调必须保护个人在信通技术环境中的安全和安保，无论是通过保护关键基础设施免受信通技术威胁，还是通过确保网络安全措施不被用作限制在网络空间充分享受人权和基本自由的借口。

附件二十六

丹麦、芬兰、冰岛、挪威和瑞典常驻联合国代表团的联合发言

我荣幸地代表北欧国家：芬兰、冰岛、挪威、瑞典和我的国家丹麦发言。我们感谢主席国爱沙尼亚将这一非常相关的议题列入安理会议程。这对所有会员国都是一个很好的机会，使我们在致力于在网络空间适用国际法以及建立网络空间负责任国家行为框架的基础上再接再厉，促进和平与稳定。

信息和电信技术的发展给世界带来无数好处。它带来巨大的经济进步和社会发展。在当前的大流行病中，网络空间使我们许多人能够与家人、朋友和同事保持联系，并维持社会的重要功能，包括对管理卫生危机至关重要的关键基础设施的运作。然而，网络空间也被用来传播有关 2019 冠状病毒病(COVID-19)的虚假信息，暴露了我们在信息空间被破坏和滥用方面的共同脆弱性。此外，这场疫情还暴露了严重的数字鸿沟，尤其是性别数字鸿沟。作为北欧人，我们坚信，全球无障碍、自由、开放和安全的网络空间不仅对当今世界的运作方式至关重要，对我们塑造更美好、更绿色、更安全的未来的共同雄心也至关重要。

不幸的是，恶意的网络活动继续挑战网络空间的安全和稳定。过去一年半的情况表明，国家和非国家行为者将利用任何机会，甚至是全球大流行病，在网络空间开展恶意活动。这种活动是不可接受的。它们威胁到我们社会的完整、安全和繁荣，破坏了国际和平与稳定。

让我强调对国际和平与安全构成挑战的三个相互关联的趋势。

首先，最近针对公司、组织和政府的供应链的网络攻击增加，使数万甚至数十万计算机系统暴露于危险之中。这种攻击显示出对受影响者的公然漠视。其目的往往是窃取敏感信息和知识产权，以便在地缘政治竞争中获得优势。这种攻击可能会产生额外的意想不到的效果，因为后门是敞开的，人人都可利用。

第二，国家支持的破坏性网络攻击，如 WannaCry 和 NotPetya，已在世界范围内发动，并完全无视在全球产生的负面的系统性影响。这类攻击不仅造成巨大的经济损失，还造成包括医院在内的信息和通信技术系统以及影响关键电力供应的工业控制系统的瘫痪。这些活动危害我们公民的健康和安全。

第三，各国需要采取行动，应对来自其领土的网络犯罪日益严重和破坏稳定的影响。最近针对美国的燃料供应、爱尔兰的医院以及巴西、美国和澳大利亚的食品生产的勒索软件攻击表明，网络犯罪的后果已成为国家安全问题，可能影响到国际和平与安全。国家和非国家团体日益混杂在一起，使威胁进一步复杂化。

日复一日，网络空间中可容忍行为的门槛正在向错误的方向发展。我们必须扭转这一趋势，履行我们会员国在认可政府专家组报告和不限成员名额工作组共识报告时作出的共同承诺。本着这一精神，我们再次重申，国际法，包括整个《联合国宪章》、国际人道法和国际人权法，适用于网络空间中的国家行为。我们还呼吁更严格遵守 2015 年政府专家组报告中制定的关于网络空间负责任国家行为的

11 条自愿、不具约束力规范，同时铭记 2021 年政府专家组报告对这些规范的指导和进一步理解。这将对解决上述挑战大有裨益。

我们必须通过集体追究责任人的责任来提高恶意网络活动的成本。所有国家都必须尽职调查并采取适当行动，处理来自其领土的恶意网络活动。不应允许黑客组织不受惩罚地运作。

我们支持在联合国内部继续交流信息和最佳做法，特别是在执行负责任国家行为准则、建立信任措施和在网络空间适用现有国际法方面。我们应在大会认可不限成员名额工作组报告和政府专家组报告后已商定的共识框架基础上，走一条务实的道路。这构成了任何进一步讨论的基础。提议制定行动纲领是迈向全面实施已商定规范的一个好办法。

我们必须认识到，虽然网络威胁是一项全球性挑战，但它在不同国家和区域有着不同的表现。在我们各个社会中保持强大的网络复原力不仅对我们的共同安全至关重要，对享受人权同样至关重要。我们需要在全球范围内合作建设能力。

国家不能单独行事。应对网络空间的威胁需要多利益攸关方采取办法，以帮助预防冲突，建立共同理解，增强信心和能力建设。我们需要联合国作为召集人和平台，在政府、民间社会、学术界和私营部门之间建立有效合作。我们支持秘书长数字合作路线图，特别是在涉及私营部门的参与时，这对管理关键基础设施、收集信息、保护系统和个人数据至关重要。

所有国家都必须履行其责任，遵守国际法，尊重网络空间规范。否则，恶意网络活动对国际和平与安全的威胁将不断增加。网络攻击将继续增加冲突风险，危及生命，侵犯人权，扼杀经济活动，加深分歧，引发争端。所有国家都可在促进和维护基于规则、可预测、开放、平等、自由、无障碍、稳定和安全的网络空间方面发挥作用，以造福所有人。

附件二十七

厄瓜多尔常驻联合国代表克里斯蒂安·埃斯皮诺萨的发言

[原件：西班牙文]

首先，请允许我感谢爱沙尼亚在关于该议题的阿里亚模式会议一年后将该项目列入安全理事会正式议程。我们还注意到卡拉斯总理在这方面的领导作用，并欢迎副秘书长兼裁军事务高级代表中满泉的介绍。

2020-2021 两年期是网络外交领域的一个里程碑，这不仅是因为第一个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任务和 2021 年 3 月 12 日取得的实质性成果，以及网络空间负责任国家行为政府专家组 5 月 28 日达成的共识，还因为 2019 冠状病毒病(COVID-19)大流行加速了数字转型。

这场大流行病以不同方式对和平与安全的各个层面产生了影响。网络安全也不例外。基本服务的安全成为一个主要的关注点，同时还需要保护关键基础设施，使其免受可能在物理世界造成破坏的网络攻击。

我们今天面临的威胁大部分是跨国的，无论是在物理世界还是在虚拟世界，对抗这些威胁的唯一途径是通过国际合作和对话。因此，如果一个会员国不安全，那么没有一个会员国是安全的。

因此，厄瓜多尔重申致力于按照国际法执行政府专家组的报告和不限成员名额工作组的成果所反映的现行规范。我国代表团谨强调，任何领域都不能置身于包括国际人权法和国际人道法在内的国际法范围之外，这并不意味着网络空间军事化是可以接受的。

相反，厄瓜多尔坚持应完全和平利用网络空间。《联合国宪章》禁止使用武力，因此，网络空间的所有国际争端都应通过和平手段解决。

因此，我们促进信任和能力建设。为此，我们认为需要一个业务平台，以促进各国执行现有框架。该平台可以采取行动纲领的形式。

我们捍卫和支持任何将促进更大的国际合作以减少执行负责任国家行为规则能力方面失衡的机制。

此外，我们认识到区域组织可以为能力发展和执行此类规范作出贡献。美洲国家组织在这一领域的宝贵工作，特别是其打击网络犯罪和恐怖主义的努力就是一个例子。

最后，我回顾需要维护和促进负责任地使用信息和通信技术，作为网络空间稳定与安全的关键保障。同样，我们认为，考虑到技术的快速发展，应加强现有规范。安全理事会必须考虑建立机制，加强利用技术作为巩固和平的手段，以此作为对常规努力的补充。

谢谢。

附件二十八

埃及常驻联合国代表团的发言

埃及高度重视信息和通信技术(信通技术)的国际安全问题，并强烈呼吁联合国发挥核心和主导作用，通过所有国家参与的包容和公平的进程，促进和制定各国使用信通技术的规则和原则。

一些国家正在发展可能用于恶意用途和进攻性军事目的的信通技术能力。在未来国家间冲突中使用信通技术正在成为现实，针对关键基础设施的有害信通技术攻击的风险既真实又严重。这场新的军备竞赛对国际和平、安全和稳定产生深远影响，特别是在常规武器与非常规武器之间的界限继续被侵蚀的情况下。

此外，各国开发的相关技术正在被恐怖主义分子和犯罪分子转让、复制或翻版。恐怖主义分子和犯罪组织恶意使用信通技术是对国际和平与安全的严重威胁，特别是考虑到与归因有关的挑战。

根据国际法和《联合国宪章》，所有会员国应避免采取任何明知或故意破坏或以其他方式损害他国关键基础设施的使用和运作以及干涉他国内政的行为。

毫无疑问，信通技术的国际安全问题已变得非常重要和具有战略意义，不能在国际层面上没有明确的具有约束力的规则。联合国系统内的包容性进程是在这一领域建立公平、全面和有效安排的最佳、最有效的方式。

联合国已采取一些步骤来建立一个补充国际法原则的规范性框架。随着最近以协商一致方式通过了大会第 73/27 号决议所设不限成员名额工作组关于从国际安全角度看信息和电信领域发展的最后报告，联合国已确立网络空间预防冲突和稳定框架的初步要素。

大会呼吁会员国在使用信通技术时遵循第一委员会辖下政府专家组连续报告中所载的负责任国家行为规范。然而，由于这些规范的自愿性质和缺乏任何后续机制，这些适度规范的实施仍少之又少。

不限成员名额工作组是关于这一重要议题的第一个包容性进程，它的成功以及根据大会第 75/240 号决议设立新的不限成员名额工作组代表着会员国可能在一些关键方面的重要相互理解达成协议上取得可喜进展。

主要是在大会主持下的联合国内部的包容性进程是这一领域建立公平、全面和有效安排的最有效方式。我们鼓励安全理事会在审议维和与反恐等议题时考虑到新兴技术带来的机遇。然而，安理会不应用作一个立法机构，试图代表会员国就必然需要包容和透明程序的事项制定规范和规则。

大会以协商一致方式认可的建议可以构成政治或法律上具有约束力的规则的基础，特别是这些规则源自国际法原则和《联合国宪章》。

埃及还鼓励考虑建立一个包容性的机构平台，专门就保障信通技术的和平利用和减少其相关风险开展国际合作。

我们认为，国际法和《宪章》的原则确实适用于包括网络空间在内的所有领域，但我们同时认为，亟需确定具体义务，使网络空间中的国家行为符合国际法和《联合国宪章》的目标。

在一个联系日益紧密的世界中，任何关于网络安全的国际管理制度只有加强最薄弱的环节才会强大。幸运的是，我们的共识是，必须加紧和加强能力建设工作，防止对关键基础设施的潜在攻击，并发展发展中国家所需的能力和技术技能。联合国应领导协调努力，向发展中国家提供必要援助。

总之，信通技术既带来巨大机遇，也带来巨大挑战。我们强调，迫切需要确定和制定负责任国家行为规则，以加强全球信通技术环境的稳定和安全，防止网络空间成为冲突和军备竞赛的另一个舞台。

附件二十九

萨尔瓦多常驻联合国代表团的发言

[原件：西班牙文]

萨尔瓦多感谢爱沙尼亚代表团以安全理事会 2021 年 6 月主席的身份举行本次公开辩论会，这是安全理事会首次以实质性的正式方式处理网络安全问题。该举措是本机构履行国际承诺、在多边层面审议信息和通信技术领域现有和潜在安全威胁的一项非常重要的措施。

新技术的发展是促进各国经济和社会发展的一个重要机会。然而，这些信息系统很容易受到攻击，攻击者打算为意识形态目的或为自身利益而操纵通信网络。鉴于犯罪分子和恐怖主义分子利用新的信息和通信技术来实现他们的目标，务必投入努力和资源，为制定和采用共同规范拟定专门准则。这将有助于我们防止此类犯罪，并使我们更容易将那些在准则之外活动的人绳之以法。

因此，我们强调与打击网络犯罪有关的国际和区域文书的重要性，以及该领域取得的进展，例如设立不限成员名额工作组，以制定一项打击将信息和通信技术用于犯罪目的的全面国际公约。

我们满意地欢迎联合国会员国在国际和平与安全议程范围内打击恐怖主义的努力。然而，我们注意到，在该领域具有国际约束力的文书中，仍然无法找到任何直接提及网络空间的内容。这是我们都必须尽快弥补的一个差距。我们赞扬安全理事会努力以实质性方式讨论这一重大威胁，以期提供有效的解决方案。我们敦促本机构继续这些努力，抛开所有政治和/或个人利益，坚持预防新冲突和为其发展创造条件的目标。

萨尔瓦多回顾 2004 年通过的大会第 58/199 号决议，其中载有国家关键信息基础设施要素的清单。由于技术上的相互依存度越来越高，这些关键基础设施面临的威胁越来越多，种类也越来越多。该决议还认识到，关键信息基础设施的脆弱性继续构成重大的安全问题。

此外，为了创造条件帮助在实现国际和平与安全、充分行使人权以及经济和社会发展的共同目标方面取得进展，我们认为，除了目前为防止网络空间成为宣传激进主义、招募和为犯罪活动筹集资金的平台所作的努力外，还应扩大大会第 58/199 号决议提供的框架，以解决保护关键基础设施活动免受网络攻击的需要。

世界将继续面临本组织成立以来的最大挑战之一，2019 冠状病毒病(COVID-19)大流行的暴发暴露了各国基本系统的脆弱性。我们已经看到，在 COVID-19 大流行期间，针对国家卫生系统的网络攻击有所增加，它们危及数百万人的生命，并直接影响到最脆弱的社区和部门。我们希望利用这个论坛谴责近几个月来针对世界卫生组织的网络攻击和盗窃身份的企图。毋庸置疑，随着互联互通的增加，假设这些攻击在未来几年里还会增加。

最近几个月，对信息和通信技术的恶意使用已经扩展到针对能源、金融和粮食供应部门的网络攻击；与其他部门比较，这些部门极易受到网络攻击。同样，我们已经看到，旨在影响政府官员和机构的看法的虚假信息活动有所增加，这些活动往往能够使这些官员和机构的工作失去合法性，引发不稳定和社会冲突。

所有上述情况促使我们必须继续推动预防工作，编纂旨在防止恶意使用信通技术的国际法，承认与适用的国际人道法的相互关系，并涵盖武装冲突期间的网络行动领域。

我们强调，必须在协商一致的基础上开展工作，不得意图强加不符合各国实际的解决方案，并确保考虑到大会通过政府专家组和不限成员名额工作组从国际安全角度看信息和电信领域的发展的各种共识协议所取得的进展。我们尤其欢迎不限成员名额工作组 2021 年以协商一致方式通过的协议，联合国 193 个会员国、包括安全理事会 15 个成员和该进程的其他相关方都参与其中。

萨尔瓦多期待建设性地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。该工作组将在 2021-2025 年期间开展实质性工作。我们赞赏新加坡常驻联合国代表布尔汗 • 加福尔作为该进程候任主席所做的工作。

应该指出区域组织、私营部门、民间社会、学术界和其他相关部门在预防和打击这些威胁方面的根本作用。迫切需要通过积极交流信息和良好做法、能力建设、法律框架的标准化和使用新技术作为发展和打击有组织犯罪的途径，继续加强区域和国际合作机制的工作，以预防和应对这些挑战。

附件三十

欧洲联盟驻联合国代表团团长奥洛夫·斯科格的发言

我很荣幸代表欧洲联盟及其成员国在关于网络安全的公开辩论中发表意见。

候选国土耳其、北马其顿共和国、* 黑山* 和阿尔巴尼亚，* 参与稳定与结盟进程的国家和潜在候选国波斯尼亚和黑塞哥维那，以及乌克兰和摩尔多瓦共和国，均赞同本发言。

首先，我们赞扬爱沙尼亚就这一关键议题举行公开辩论。目前恶意网络活动继续增加，加剧的挑战危及网络空间的国际安全与稳定，特别是在疫情的特殊情况下。

数字化对我们的安全、经济和整个社会的影响越来越大，既创造机遇也带来挑战。交通、能源和卫生、电信、金融、安全、民主进程、空间和国防都严重依赖日益紧密相连的网络和信息系统。

有鉴于此，我们尤其感到震惊的是，最近针对全球基本运营商(包括保健部门)的恶意网络活动有所增加，影响了信息和通信技术(信通技术)产品和服务的可用性、安全性和完整性，从而影响了业务的连续性，这可能会产生溢出效应和系统效应，并增加冲突风险。

因此，我们欢迎有机会在对维护国际和平与安全负有主要责任的安全理事会讨论这一重要问题。这是一个机会，可以强调面临的一些挑战，重申联合国社会迄今取得的成就，并对如何在联合国内解决这些问题提出展望。

在这方面，欧洲联盟及其成员国欢迎最近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(不限成员名额工作组)和联合国促进网络空间中负责任的国家行为政府专家组以协商一致方式通过的有意义的报告。

这些报告大大有助于提高人们的认识，并有助于加强预防、应对网络威胁和恶意网络活动并从中恢复的能力。这是非常必要的，因为随着所有国家都越来越依赖信通技术，缺乏认识和能力本身就构成威胁。

因此，必须提高全球的网络复原力，因为这会降低潜在的犯罪者为恶意目的滥用信通技术的能力，使各国能够根据国际法以及联合国政府专家组 2010、2013、2015 和 2021 年在国际安全背景下的信息和电信领域的共识报告，对从其领土上开展此类活动的行为者进行尽职调查并采取适当行动。

历届联合国政府专家组和不限成员名额工作组的报告为网络空间的预防冲突、合作和稳定提供了基线，即重申适用国际法，处理负责任国家行为规范、网络空间的建立信任措施和网络能力建设。

* 北马其顿共和国、黑山、塞尔维亚、阿尔巴尼亚继续是稳定与结盟进程的一部分。

欧洲联盟及其成员国重申，网络空间预防冲突、合作和稳定框架只能以现有的国际法为基础，其中包括大会自 2013 年以来认可的整个《联合国宪章》、国际人道法和国际人权法。

加深对国际法如何适用于网络空间的理解是为了进一步减少误解，提高网络空间的问责，考虑到网络空间的国际安全和稳定，联合国会员国应继续推进和实施这一框架。

例如，欧洲联盟及其成员国认为，国际人道法完全适用于武装冲突背景下的网络空间。我们重申，不应将国际人道法适用于网络空间误解为使任何不符合《联合国宪章》的武力使用合法化。国际人道法规定向没有或不再参与敌对行动者给予基本保护，除其他外，保护平民免受敌对行动的影响，保护战斗人员免受不必要的痛苦等。国际人道法还对允许的战争手段和方法、包括新的战争手段和方法加以限制。

第二，遵守负责任国家行为规范最为重要。一套商定的规范反映了国际社会的共同期望，确立了负责任国家行为标准。它使国际社会能够评估国家的活动和意图，以预防冲突并加强网络空间的稳定和安全。

第三，与网络有关的建立信任措施是预防冲突的实际手段。事实证明，通过合作和信息共享，区域建立信任措施能够降低信通技术事件可能引起的误解、升级和冲突的风险。

最后，该框架包括能力建设这一重要问题。我们积极支持加强协调的呼吁，包括通过我们与世界各地的合作伙伴的众多努力，在使用信通技术的能力建设工作上加强一致性，以消除数字鸿沟。

欧洲联盟通过其外部融资工具支持网络能力建设工作。该工具涵盖一系列具有全球影响力的方案，其中包括非洲、亚洲和拉丁美洲以及欧盟邻国和西巴尔干国家实施的行动。具体而言，欧洲联盟目前正在对世界各地的活动进行投资，以支持与执行伙伴合作实施的活动，如欧洲联盟的网络复原力促进发展、Glacy+、欧盟网络直线、加强亚洲安全倡议等项目。

为了强调网络空间预防冲突、合作和稳定框架，欧洲联盟将继续促进网络空间中负责任的行为。有鉴于此，欧洲联盟及其成员国致力于通过和平手段解决国际争端，发生在网络空间的此类争端也包括在内。

因此，欧洲联盟联合外交反应框架是欧洲联盟网络外交办法的一部分，有助于预防冲突、降低网络安全威胁、提高国际关系的稳定性。为了促进和保护开放、自由、稳定和安全的网络空间，欧洲联盟将继续使用其网络外交工具箱，并为此与国际伙伴合作。

鉴于网络空间的复杂性，从一开始，各国和多利益攸关方群体就必须应对网络空间带来的挑战、改善合作并加强能力。我们还有一项主要责任，即让所有利益攸关方都能负起责任，推动建立一个以人权、基本自由、民主和法治为基础，开放、自由、安全和稳定的网络空间，我们还需支持他们的努力。欧盟的网络外

交办法还考虑到性别视角在缩小“性别数字鸿沟”和促进妇女有效和有意义地参与在国际安全背景下使用信通技术相关决策过程中的突出作用。

为加强合作，我们认为联合国应发挥核心作用，推动落实迄今取得的成就。为促进有效的多边多利益攸关方辩论，以推进网络空间的和平与安全，显然需要推进联合国网络空间负责任国家行为框架。欧洲联盟与 53 个成员国一起，提议制定一项行动方案，以促进网络空间中负责任的国家行为。

在大会认可的现有成果的基础上，该行动纲领为联合国内部的合作和交流最佳做法提供一个永久性平台。行动纲领还提供机会，有助于根据受益国确定的需要制定能力建设方案。它还在联合国内部设立一个体制机制，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，各司其职，维护开放、自由、安全、稳定、无障碍、和平的信通技术环境。

由于这一平台的永久性和务实性，我们认为行动纲领建议是及时的，值得国际社会进一步探讨。它为进一步开展网络空间预防冲突、合作和稳定框架方面的工作，确保各国能够从全球开放、稳定和安全的网络空间中获益奠定了坚实和务实的基础。

附件三十一

格鲁吉亚常驻联合国代表团的发言

我们感谢主席国爱沙尼亚就这一重要问题召开今天的高级别辩论会，并感谢各位尊敬的发言者。

格鲁吉亚长期以来致力于发展负责任和有道德的网络空间，包括网络安全和复原力，以促成安全、可靠、可信赖的数字环境的全面框架，以造福整个国家。过去十年中，我们建立了必要的信息和网络安全的法律基础，并确定了关键的信息系统主题；通过并实施两项网络安全战略和相关行动计划；第三个国家网络安全战略也正在通过中。

然而，众所周知，网络空间在带来重大的经济和社会机遇、创新和发展的同时，也带来新的安全威胁。近年来，我们看到网络空间不仅被用于恐怖主义、欺诈和犯罪的目的，还被用作混合战争和干涉国家内部事务的有力工具。

不幸的是，混合战争也成为一些国家推进国家利益的有力工具，正如本机构所了解的，格鲁吉亚在应对来自某一常任理事国的混合威胁方面有着长期和痛苦的经验。自 90 年代初以来，俄罗斯联邦不断对格鲁吉亚发动混合战争，在企图破坏我国的主权、领土完整、欧洲和欧洲-大西洋的愿望方面，俄罗斯从未停手。

这些事件不胜枚举。2008 年 8 月，在俄罗斯对格鲁吉亚的全面军事侵略期间，我们目睹了俄罗斯在进行侵略的同时发动大规模网络攻击的第一个先例。2019 年，格鲁吉亚总统府、法院、各市议会、国家机构、私营部门组织和媒体机构的网站、服务器和其他操作系统遭到大规模网络攻击。格鲁吉亚当局与我们的合作伙伴合作进行的调查得出结论认为，这次网络攻击是由俄罗斯联邦武装力量总参谋部主任局策划和执行的。

令人遗憾的是，正当国际社会与 2019 冠状病毒病(COVID-19)大流行作斗争之时，俄罗斯联邦仍然试图通过加强对格鲁吉亚抗疫最成功的机构之一——理查德-卢加尔(Richard Lugar)公共卫生研究中心的宣传战来获得政治红利。俄罗斯的指控代表了针对这个独特实验室的典型的错误信息和宣传活动。建立该实验室的目的正是为了识别和应对像这场大流行病一样的疫情。

今天，我们都看到俄罗斯不仅在我们的地区，而且在全球范围内积极应用混合工具包。俄罗斯混合工具包中最突出的工具是军事存在、信息行动、网络攻击、支持代理政治团体、干涉国内事务以及施加经济影响。

最后，我们必须强调，针对主权国家的网络攻击和混合战争严重违反了国际法、国际法规范和原则，破坏了国际和平与安全。我们重申致力于继续加强国家和国际层面的网络安全，我们同时呼吁国际社会更加关注俄罗斯联邦在格鲁吉亚和其他地方的恶意信息和通信技术活动。

附件三十二

德国常驻联合国代表团的发言

一年半前，2019 冠状病毒病(COVID-19)大流行袭击世界，以戏剧性的突然性让我们意识到，数字技术在多大程度上塑造了我们的日常生活和经济复原力。同时，它也无情地暴露了我们的弱点。网络攻击，包括针对关键基础设施的攻击，可以对国际和平与安全构成威胁。德国仍相信，这是安全理事会的一个重要议题。

国际和平与安全正受到不同方面的压力：首先，网络犯罪活动破坏了目前对我们的经济、政府和现代社会整体运作至关重要的技术的可靠性和可信度。仅举几例，自 COVID-19 大流行爆发以来，拒绝服务攻击、网络钓鱼和恶意软件的传播急剧增加。对欧洲和北美的关键基础设施的攻击以及作为敲诈工具的网络攻击也在增加。

第二，国家支持的以间谍、破坏、造谣和破坏稳定或经济利益为目的的恶意网络活动正在破坏国际信任和缓解冲突的合作机制，从而威胁到全球安全。

第三，整个公民社会，特别是人权维护者在网络空间中受到越来越大的压力。互联网旨在提供的表达自由、透明度和真正沟通的空间不断缩小。

为应对这些日益增长的威胁，需要采取多支柱办法。其中一个支柱是加强我们国内和国际的复原力。这包括改善技术基础设施、政治和法律能力，以及加强国际合作。

第二个支柱是进一步推进和界定我们对网络空间负责任国家行为的共同理解，并划定不得逾越的红线。因此，我们必须捍卫不限成员名额工作组和政府专家组取得的现有成果，并进一步推动负责任国家行为规范的发展。

德国的立场是，包括《联合国宪章》和国际人道法在内的国际法在网上和网下一样适用。各国应严格避免支持违反其国际法义务的信息和通信技术(信通技术)活动，特别是考虑到这些活动有可能造成国家间紧张局势并使之升级。信通技术活动不得故意破坏关键基础设施或以其他方式损害关键基础设施的使用和运作。特别是，任何行为者都不应危及互联网公共核心的普遍可用性或完整性，这对网络空间的稳定至关重要。我们呼吁所有国家严格遵守其尽职调查的义务，并根据国际法对从其领土进行恶意网络活动的行为者采取迅速行动。

为促进正在进行的关于网络空间国际法的讨论，德国已发表一份关于国际法在网络空间的适用性的政策文件，我们鼓励其他国家也这样做。

然而，仅商定共同的既有成果是不够的。还须对不可接受的行为作出坚定的回应。可以考虑采取各种手段，包括对话、交流、国家或国家集团的政治声明，揭露和谴责不负责任的行为，或对相关个人和实体实施制裁。我们与欧洲联盟的伙伴一起，已建立与网络有关的制裁制度，这使我们能够以坚定、有效和有针对性的方式并在完全符合国际法的情况下应对网络攻击。我们过去用过这一手段，

如果我们的安全受到损害，我们将毫不犹豫地再次使用它。此外，归因文化可以加强规范性框架，促进网络空间的问责制。

与民间社会、私营部门和学术界的持续交流对于增加我们的网络空间复原力和推动互联网治理事业至关重要。这些努力必须利用和纳入公共当局以外的丰富专业知识，目的是维护网络空间的国际和平与安全。

附件三十三

希腊常驻联合国代表团的发言

数字技术深刻促进了当前的经济和社会转型，为经济增长以及可持续和包容性发展提供了重大机遇。尤其是网络空间已成为我们社会的支柱之一。与此同时，网络空间恶意行为的增加，包括国家和非国家行为者为恶意目的滥用信息和通信技术(信通技术)，已经成为新风险、新挑战的来源。这种行为威胁经济增长，并可能导致破坏稳定和连带效应，增加冲突风险。

因此，我们强烈支持大会批准的网络空间预防冲突、合作和稳定的战略框架，我们强调需要将我们的集体努力集中在发展充分应对网络威胁的技能和能力上。当前的全球卫生危机凸显了全球网络复原力的必要性，在这场危机中，我们看到了针对保健部门的网络威胁和恶意网络活动。

全球网络复原力降低了潜在犯罪者滥用信息和通信技术的能力，加强了各国有效应对网络事件并从中恢复的能力。作为我们加强全球复原力和制定实际合作措施的最新努力的一部分，我们目前正在组织区域网络安全研讨会，与会者来自西巴尔干国家。

通过积极参与国际组织，如联合国、北约、欧洲安全与合作组织，我们寻求合作，交流经验和最佳做法，并在制定应对网络威胁的适当手段方面做出最大程度的贡献。此外，作为欧洲联盟的成员，我们实施了包容性和多方面的网络空间预防冲突和稳定战略框架。在欧盟内部，网络安全是成员国之间协调一致的集体努力，开创了多边合作的独特和宝贵的先例。

我们高度致力于建设一个受国际法管辖，充分适用人权、基本自由和法治的全球、和平、安全、开放和独立的网络空间。在我们参加的所有区域和国际论坛上，我们一直积极分享我们在双边和多边执行规范、建立信任措施和能力建设方面的经验。我们坚定地致力于积极参与联合国关于网络安全问题的进一步讨论，并重申我们愿意积极参与，努力取得建设性进展。

附件三十四

危地马拉常驻联合国代表团的发言

危地马拉感谢爱沙尼亚代表团以安全理事会主席的身份召开本次公开辩论会，讨论一个对各国无疑都极为重要的问题。网络空间已成为全球活动的一个核心和不可或缺的领域，通过负责任国家行为来保护网络空间对于确保维护国际和平与安全至关重要。我们相信，此类会议是我们各国就一个日益重要的议题的不同实施层面交流意见和良好做法的绝佳机会。

世界目前面临着几项安全挑战，而网络安全问题等新威胁的出现加剧了这些挑战。回顾过去的网络攻击，以及 2019 冠状病毒病(COVID-19)大流行期间网络攻击的增加，显然有必要解决这一议题，特别是如果我们考虑到它可能影响我们社会最脆弱的部门。

网络威胁和攻击的产生和发展源于数字媒体互连而发展的各种活动。这代表着情况的复杂性，即需要我们各国所有部门参与和合作，以便制定加强国内和全球网络安全的技术和法律框架。

所有国家的情况如出一辙，我们社会的所有部门都普遍增加了信息和通信技术(信通技术)的使用。这一新情况有助于信息交流和通信的空前发展，但同时也带来可能影响我们人民安全的新风险、新威胁。

有鉴于此，我国代表团对这些新技术表示关切，特别是考虑到网络空间和数字网络的民用和双用途性质，它们可能被犯罪和恐怖主义团体利用。令人极为担忧的是，一些国家正在发展用于军事目的的信息和通信技术能力，在未来国家间冲突中使用这些技术的可能性越来越大。

危地马拉认识到，网络空间的相连性和复杂性要求各国政府、私营部门、民间社会和学术界共同努力，以全面和平衡的方式应对网络安全挑战。维护开放、自由、安全、稳定的网络空间是所有这些部门的责任。

为此，我国促进在次区域、区域和国际各级建立信任和透明度措施，支持能力建设活动、信息交流和传播最佳做法。

我国代表团强调，国际法对网络空间国家行为的适用性、适用于和平时期的自愿、不具约束力的国家行为准则以及执行建立信任措施仍然至关重要。此外，在目睹各国在网络安全和防御方面的现有差距后，我国特别关注能力建设工作，以便找到一个有助于维护国际和平与安全的更公平的竞争环境。

危地马拉认为，区域组织在实地建立和平方面发挥着不可或缺的作用。在区域和全球范围内加强它们在网络空间的存在，以创新方式推进持续和平议程，具有相当大的潜力。区域和次区域组织注重改善各国的安全，在不同区域实施切实的建立信任措施以改善网络稳定方面取得了长足进步。毫无疑问，如果没有这些组织的贡献，预防冲突和稳定的努力就会减少。

危地马拉目前有一项国家网络安全战略，其主要目标是加强国家能力，为确保人民参与、发展和行使网络空间权利创造必要的环境和条件。此外，危地马拉还有一个网络事件响应中心(CERT)，提供网络安全审计、漏洞扫描和警报分类服务。这两项工作都是在美洲国家组织的协助下实现的。

除此之外，危地马拉正在制定一部关于网络犯罪的法律，明确界定行动路线以及与信通技术有关的犯罪类型，以便通过国际合作促进能力建设，并制定明确的监管链和数字证据处理协议，以实行正当程序。还有必要提及的是，我国很荣幸成为布达佩斯公约的观察员国，该公约旨在通过协调各国的法律、改进调查技术和加强各国之间的合作来打击计算机犯罪和互联网犯罪。

我国代表团认为，有必要继续以统一方式对各国法律加以改变和调整，并设计制度，以便在保障个人权利的框架内发现、调查和起诉可能的犯罪，同时降低利用计算机网络破坏信息保密性、完整性和可用性的风险。我们希望，我们今天的讨论将积极促进和补充大会正在进行的网络规范制定过程，特别是通过政府专家组和 2021-2025 年不限成员名额工作组的有意义的工作。

最后，我们回顾所有国家必须和平利用信通技术，为人类的共同利益服务，促进所有国家的可持续发展，无论其科学和技术发展水平为何。

附件三十五

印度尼西亚驻联合国临时代办穆罕默德·库尔尼亚迪·科巴的发言

请允许我感谢爱沙尼亚召开这次会议。我也要感谢通报人所作的宝贵通报。

随着人们对数字连接的依赖性增加，信息和通信技术(信通技术)已成为我们日常生活中不可或缺的一部分。

此外，在 2019 冠状病毒病(COVID-19)大流行期间，信通技术为公共和私营部门提供了一条向民众提供基本服务的生命线。

在这方面，必须强调的是，国家和非国家行为者的恶意网络活动，特别是针对关键基础设施的恶意网络活动，可能会危及国家稳定以及国际和平与安全。

在这种情况下，印度尼西亚希望强调以下几点：

第一，在指导我们使用信通技术的行为及其对国际和平与安全的影响方面，法治至高无上。

国际法原则和《联合国宪章》规定了指导各国使用信通技术的基本法律规则，包括在应对任何恶意攻击方面。

所有国家都必须遵循同一套规则和法律。任何人都不应被豁免。

此外，印度尼西亚支持大会第 70/237 号决议中概述的负责任国家行为规范。

在继续满足在确定和发展有关这一事项的国际法律框架方面日益增长的需要的同时，我们的努力也应着眼于解决各国和各区域之间的差距。

除了技术上的差距，当务之急是加强国家政策框架以及现有国际法和网络空间自愿、不具约束力规范的实施。

第二，双边、区域和多边办法在加强网络空间信任方面的作用。

双边、区域和多边层面的合作措施在增进理解和加强网络空间稳定方面是相辅相成的，特别是在能力和建立信任领域。

通过建立联络点、定期信息交流、对话和分享最佳做法，东盟建立信任措施一直在为东南亚区域和其他区域的网络稳定作出贡献，特别是通过东盟区域论坛。

此外，印度尼西亚强调，与其他多利益攸关方实体建立有意义的伙伴关系，帮助各国在使用信通技术时采用负责任行为框架是有价值的。

在这方面，我们强调发达国家需要与发展中国家分享信通技术。正如所有其他全球问题一样，确保其他国家拥有正确的工具和能力来应对这一威胁，将有助于信通技术领域的总体稳定。

第三，联合国可发挥领导作用，协调努力解决信通技术事件可能引发的冲突。

今天的讨论是安理会就信息和通信技术对维护国际和平与安全的影响的首次正式专门辩论。

它标志着联合国在这一问题上向前迈出重要一步。

今后，安理会需要预测网络领域威胁的增加，以及信通技术环境中可能发生的导致重大战争的重大事件。

我们强调，必须确保继续协调和协同联合国的行动。安理会应继续应对信通技术领域的事态发展涉及的国际和平与安全以及人道主义影响。

同时，安理会必须以大会正在审议和制定的规范和规则为指导。

最后，请允许我重申，印度尼西亚致力于推动我们的共同努力，以适当应对与使用信通技术有关的维护和平与安全方面日益严峻的挑战。

附件三十六

红十字国际委员会的发言

红十字国际委员会感谢有机会为本次安全理事会关于“维护网络空间的国际和平与安全”的公开辩论作贡献。

过去二十年来，敌对的网络行动已成为维护国际和平与安全的一个日益重要的问题。随着社会的数字化，国家和其他行为者的军事能力也日益引起关切。今天，国际社会认识到，“一些国家正在发展用于军事目的的信通技术能力”，而且“在未来的国家间冲突中使用信通技术的可能性越来越大”。[10]

鉴于这一现实，红十字国际委员会希望回顾使用网络技术可能对人类造成的伤害，然后介绍各国如何通过国际和国家层面的行动减轻这些不利的人道主义后果。

今天，众所周知，针对关键民用基础设施的网络行动已造成巨大的经济损害、社会混乱和国家间的紧张局势。在“从国际安全角度看信息和电信领域的发展不限成员名额工作组”的最后报告中，所有国家都承认，针对关键基础设施的网络行动有可能产生“潜在的破坏性人道主义后果”。[11] 虽然红十字国际委员会无法证实任何造成人员伤亡的网络行动，但我们对网络行动的破坏性影响感到担忧，例如电力供应、供水系统或医疗服务中断。[12] 这类行动在任何时候都会给人类带来严重风险。然而，我们的经验表明，破坏重要的民用基础设施在已受到武装冲突削弱的社会中具有特别严重的后果。

不利的人道主义后果并非不可避免。各国必须采取果断措施，确保武装冲突期间网络行动的使用符合现行国际法规则。红十字委员会认为，这需要在国际和国家层面采取行动。

在国际层面，各国已确认国际法适用于信通技术环境。这首先包括《联合国宪章》规定的国家义务，特别是禁止使用武力以及以和平手段解决国际争端的义务。最近，政府专家组还指出，“国际人道法仅适用于武装冲突局势”。专家组回顾了“既定的国际法律原则，包括 2015 年报告中指出的适用的人道、必要性、相称性和区分原则”，它承认“需要进一步研究这些原则如何以及何时适用于各国使用信息和通信技术，并强调回顾这些原则绝不是将冲突合法化或鼓励冲突”。[13] 红十字国际委员会完全支持这一观点，即：武装冲突期间的网络行动并非发生在“法律空白”或“灰色地带”，它们受国际人道法既定原则和规则的约束。

为确保国际人道法得到理解和有效应用，红十字国际委员会欢迎进一步研究如何以及何时适用这一领域的法律。为避免不利的人道主义后果和社会混乱，我们要求各国在解释和应用国际人道法的规则和原则时，考虑到信通技术环境的具

[10] 不限成员名额工作组，2021 年最后报告，第 16 段；政府专家组，2021 年最后报告，第 7 段。

[11] 不限成员名额工作组，2021 年最后报告，第 18 段。

[12] 可查阅 www.icrc.org/en/document/potential-human-cost-cyber-operations。

[13] 政府专家组，2021 年最后报告，第 71(f)段。

体特点。保护平民生活的基本问题需要各国进一步研究和明确定位。例如，在一个日益受数据驱动的世界中，各国应优先同意民用数据享有免受攻击的保护，就像民用纸质文件一样。此外，各国应申明，通过扰乱民用物体的功能而损害民用物体的网络行动应受所有关于敌对行动的国际人道法规则的约束。[14]

虽然对国际法如何限制武装冲突期间的网络行动进行进一步研究和达成一致很重要，但这些规则只有通过在国家层面的实施才能生效。红十字国际委员会在与军事人员和专家讨论后确定了一些关键步骤，说明各国如何能够并且应该避免武装冲突期间的军事行动对平民的伤害。[15] 今天，我们要强调其中四个步骤。

- 首先，每个国家都对其参与网络行动的所有机构以及按照该国指示或在其指挥或控制下行事的其他行为者负责。各国必须确保所有这些行为者尊重国际人道法。

- 第二，各国应制定明确的内部程序，确保在使用与网络有关的战争手段或方法时，遵守适用的法律框架。

- 第三，各国有义务采取一切可行的预防措施，在实施攻击时，包括通过网络相关的战争手段和方法进行攻击时，避免或至少将平民的附带伤害降至最低。在信通技术环境中，这可能包括实施“系统围栏”、“地理围栏”或“终止开关”等技术措施。[16]

- 第四，各国还有义务制定措施，保护平民人口免受军事网络行动带来的危险。其中一些措施可能在和平时期就必须实施。

最后，红十字国际委员会赞扬各会员国努力推动国际对话，并就网络行动的潜在人类代价以及预防和减轻人类伤害的措施达成一致。我们认为，国际人道法必须成为这种辩论的一部分，红十字委员会将继续为这些辩论提供专门知识。

[14] 另见红十字国际委员会，“武装冲突期间的国际人道法和网络行动：红十字国际委员会立场文件”，2019 年。

[15] 红十字国际委员会，“在武装冲突期间避免军事网络行动对平民的伤害”，2021 年。

[16] “系统围栏”表示除非与目标系统精确匹配，否则阻止恶意软件自行执行；“地理围栏”表示将恶意软件限制为仅在特定因特网协议范围内运行；“终止开关”表示在给定时间后或远程激活时禁用恶意软件的一种方法。

附件三十七

国际刑事警察组织(国际刑警组织)警务执行主任的发言

导言

网络犯罪是数字时代的一个全球性挑战。其影响远远超出被报道或被发现的范围，影响了逾 45 亿网民的日常生活。最近各方对数字环境的依赖性增加，导致网络空间出现更多犯罪机会。如今，网络犯罪将目标转向政府、企业、关键基础设施甚至医院，对全球安全构成严峻挑战。由于网络犯罪规模和严重程度快速增长，国际刑事警察组织(国际刑警组织)已将打击网络犯罪作为优先事项。

作为全球性的中立政府间组织，国际刑警组织知悉旨在维护网络空间和平与安全的国际法、规范、建立信任措施和能力建设努力。鉴于本次公开辩论的目的是为了更好地了解网络空间恶意活动所带来的日益增长的风险，国际刑警组织向安全理事会提交本书面发言，以支持其对实现和平与安全网络空间的承诺。本发言概述了最新的网络犯罪趋势及其影响，以及国际刑警组织的全球机制和解决方案，国际刑警组织 194 个成员国可利用这些机制和解决方案应对相关紧迫挑战。

当前和正在出现的网络威胁

过去一年，国际刑警组织分析了广泛的网络威胁。国际刑警组织最近的评估强调，2019 冠状病毒病(COVID-19)大流行为网络犯罪分子开辟了新途径，使其可不分地区地进行各种形式的网上犯罪活动。突出的威胁包括基于勒索软件的敲诈、商业电子邮件破坏、非法数据采集操作、错误信息以及为利用全球疫情而重新出现的旧类型恶意软件。

已查明趋势还包括，网络犯罪分子将目标转移到大公司、政府和关键基础设施。[17] 网络犯罪分子和欺诈者正在利用基本的社会需求和焦虑。自 2020 年 3 月以来，国际刑警组织一直收到成员国提出的一些请求，要求处理针对医院等处于抗击冠状病毒前线的机构的勒索软件攻击。[18] 犯罪分子通过攻击这些在应对疫情中发挥关键作用的关键基础设施，可最大限度地造成损失和勒索赎金。

勒索软件攻击并不新鲜，却是增长最快的网络犯罪形式。勒索软件使用双重勒索和勒索软件即服务模式，为网络罪犯提供了一种非常诱人的、有利可图的商业模式。我们还看到一种形势，即此类攻击不受地域限制，表明犯罪分子正在扩大目标锁定范围，全球各地任何机构都可能成为攻击目标。例如，导致欧洲一家医院关停的同一种勒索软件在亚洲也被使用。

[17] INTERPOL, Assessment Report of the Impact of COVID-19 on Cybercrime, retrieved from https://www.interpol.int/en/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf.

[18] https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware。

此外，我们还看到复杂的欺诈犯罪侵害了欧洲受害者，而赎金在几个小时内即被转移到西非和东南亚。大规模数据泄露事件也在继续发生，给世界各地企业造成了巨大经济损失。与此同时，网络犯罪分子藏匿在保证匿名和不可追踪访问的暗网中。因此，国际刑警组织通告的重要性和关联性上升，特别是“紫色通告”，[19] 成员国可利用这一工具分享有关此类欺诈计划作案手法的信息。目标是迅速传播这一关键信息，预防下次攻击。

此外，网络犯罪和金融犯罪之间的融合也带来了复杂挑战。这类犯罪包括多个阶段，从网络攻击到数据利用，再到洗钱阶段的分层和最终兑现。在这一过程中，加密货币的使用也阻碍了有效、及时的反应。鉴于此类犯罪非常复杂，需要一种联合行动模式，将不同执法专门单位的能力结合起来，以更好地打击网络欺诈和洗钱。为在这方面提供全方位的行动和分析支持，国际刑警组织在 2020 年底启动了国际刑警组织全球金融犯罪工作队。

减轻网络威胁的全球机制

事实上，国际警务合作对于保持高度互联的世界的安全和安保至关重要。正如联合国毒品和犯罪问题办公室关于网络犯罪的综合研究所确认的，国际刑警组织在促进警察之间的合作方面发挥着独特作用。[20] 为支持 194 个成员国，国际刑警组织的任务是本着《世界人权宣言》的精神，在不同国家现有法律的范围内，促进跨境执法合作，并酌情支持以预防或打击犯罪为使命的政府和政府间组织、当局和服务机构。

由于国际刑警组织的中立性和全球存在，国际刑警组织在领导和协调全球对网络犯罪的执法反应方面具有独特地位。它还有助于世界各地执法部门分享有关网络犯罪和威胁行为者的信息，并提供广泛的专业知识、技术指导和业务支持。基于这种独特作用，国际刑警组织在联合国各种政策进程(如联合国综合研究网上犯罪问题专家组[21] 和联合国信通技术安全问题不限成员名额工作组)中倡导并强调了国际警察合作的重要性。

2020 年 11 月 23 日，大会一致通过了关于联合国与国际刑警组织合作的决议的第二次半年期审查，将这种伙伴关系推向了新高度。[22] 这一成就意义非凡，在包括网络犯罪在内的关键合作领域引入了新措辞，为这两个组织在这一领域的进一步合作提供了更大合法性。

在当前数字化时代，国家解决方案甚至区域解决方案都已不够用。为帮助实现网络空间的国际和平与安全，国际刑警组织能够作为有效打击网络犯罪的全球机制，为成员国提供多种服务和工具，包括：

---

[19] https://www.interpol.int/en/How-we-work/Notices/About-Notices。

[20] 毒品和犯罪问题办公室关于网络犯罪的综合研究，第 195 页。

[21] https://www.unodc.org/documents/Cybercrime/IEG_cyber_comments/INTERPOL.pdf 和 https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/Statements/Item-3/INTERPOL_item_3.pdf。

[22] 大会关于联合国同国际刑事警察组织(国际刑警组织)的合作的第 75/10 号决议。

- 名为 I-24/7 的全球警察安全通信系统，以安全、实时的方式分享紧急警务信息；
- 19 个帮助向国际社会发出警报和支持跨国调查的数据库[23] 和通告；[24]
- 国际刑警组织的“全球网络犯罪方案”，在预防、发现、调查和阻止网络犯罪方面提供警务能力，目的是减少网络犯罪的全球影响，保护社区，建设更安全的世界；
- 国际刑警组织全球网络犯罪专家组和与网络犯罪部门负责人组成的区域工作组，讨论与网络犯罪有关的紧迫问题，并制定业务和战略计划；
- 交流平台，如“网络犯罪知识交流平台”，用于在更广泛的执法社区内安全地分享信息；“网络犯罪合作平台——业务”平台，用于业务闭门讨论；
- “网络融合平台”，汇总网络犯罪数据并进行深入分析；
- 国际刑警组织的 24/7 网络犯罪联络点，实时连接来自不同国家的网络犯罪部门，进行执法合作；
- 国际刑警组织全球网络事件反应小组(I-CIRT)框架，协调全球执法部门对重大网络事件的反应；
- 国际刑警组织全球金融犯罪工作组，通过加强国际合作和创新，减少全球金融犯罪的数量和影响，重点关注网络欺诈和洗钱计划。

多利益攸关方办法

网络犯罪调查存在许多物理领域没有经历过的挑战。对执法部门来说，很难直接知道是否发生了攻击，而且，举报率也很低。调查网络犯罪还需要特定的技能和技术，而这些技能和技术并非随处可得。网络犯罪本质上是全球性的，如果证据和嫌疑人同时位于多个司法管辖区，警方往往难以有效应对。

为克服这些挑战，国际刑警组织将伙伴关系置于打击网络犯罪努力的核心。在 2019 年举行的国际刑警组织大会第 88 届会议上，成员国批准了旨在促进国际刑警组织与私营部门公司分享信息的名为“网关”的法律框架。[25] 这一决定所基于的事实是，执法部门需要与私营部门密切合作，因为在网络犯罪方面，大部分数据和专长都掌握在私营部门手中。

国际刑警组织的全球网络犯罪方案目前在这一框架下有 12 个私人合作伙伴，这些伙伴分享最新的网络犯罪信息和专长，并为执法机构提供技术援助。国际刑警组织借助公共和私营部门的数据，可向成员国提供量身定制的业务支持和技术指导。

[23] https://www.interpol.int/en/How-we-work/Databases/Our-19-databases。

[24] https://www.interpol.int/en/How-we-work/Notices/About-Notices。

[25] https://www.interpol.int/en/News-and-Events/News/2019/INTERPOL-s-General-Assembly-sets-roadmap-for-global-policing。

此外，与全球网络安全生态系统中的各种行为体合作至关重要，多样化的数据集可帮助形成对网络犯罪的有效政策和行动反应。也有助于我们集思广益，增加韧性和敏捷度，特别是在充满不确定性的情况下。去年年底，国际刑警组织支持尼日利亚警方及其私人合作伙伴逮捕了一个有组织犯罪集团的多名成员，该犯罪集团此前开展的网络钓鱼活动和商业电子邮件泄露骗局祸害了150多个国家的政府和私营部门公司。[26]

国际刑警组织还特别强调预防。为预防网络犯罪，国际刑警组织与公共和私营伙伴密切合作，开展了一系列全球宣传活动，促进良好网络环境。还支持执法机构帮助公众进一步了解犯罪行为本身、自己保护方法以及发生网络犯罪时的应对措施，克服打击网络犯罪方面的众多挑战。

结语

在打击网络犯罪方面，由于犯罪行为人、基础设施和受害者之间的联系超越国界和管辖权，地方执法部门并非总有能力或实力处理这些跨境因素。成员国应牢记，各区域在执法、网络能力或实力方面的差距仍是犯罪网络将其基础设施和活动分布在风险较低地区的根本因素。

为减轻网络空间不断变化的威胁和风险，成员国应借助和最大限度地利用警务合作，及时作出有效反应。国际刑警组织在每个国家都有当地存在，能够将这些点联系起来；与成员国和合作伙伴一起，识别和瓦解网络空间的犯罪行为。

显然，只有通过全球协调和快速反应，才能有效打击网络犯罪。我们需要保护系统，让领导层做好准备，分享解决方案并鼓励正确应对措施。特别是，执法部门必须是值得信赖和有效的合作伙伴，因为数据交换是关键——包括国家警察部队、私营部门和国际刑警组织等全球专家之间的数据交换。在打击网络犯罪的共同目标下，必须以“敢于分享”的态度增进全球执法者之间的信任。

在国际社会面临特殊压力之时，唯有加强合作和包容，才能确保我们的共同安全。国际刑警组织的主张是：协助国际执法合作，建设一个更安全的世界。我们坚信，安全和司法是实现和平与可持续网络空间的关键，国际刑警组织通过促进国际执法合作，与联合国并肩开展工作。为使这一努力取得成功，国际刑警组织将继续支持成员国打击网络犯罪。

[26] https://www.interpol.int/en/News-and-Events/News/2020/Three-arrested-as-INTERPOL-Group-IB-and-the-Nigeria-Police-Force-disrupt-prolific-cybercrime-group。

附件三十八

伊朗伊斯兰共和国常驻联合国代表马吉德·塔赫特·拉万希的发言

网络空间为人类不断发展和提升生活的方方面面提供了良机。因此，网络空间作为重要推动力，不仅必须在全世界范围内、特别是在发展中国家得到推广，还必须得到保护，使其免受威胁。

网络空间也可被用来实施侵略行为、破坏和平、“以武力相威胁或使用武力”、“干涉本质上属于任何国家国内管辖的事务”、侵犯国家主权或胁迫其他国家。这些也必须得到有效防止。

作为一项指导原则，现有的“适用的”国际法原则和规范，当然不能有误解或任意解释，必须规范各国在网络空间方面的权利、义务和行为。

然而，当对国际法的适用性没有共识，甚至缺乏与网络空间有关的国际规范时，国际社会必须努力制定必要规范。

为此，鉴于《宪章》授权大会负责“国际法的逐渐发展和编纂”，大会必须继续不断努力，发展和编纂网络空间所需的国际原则和规范，包括以具有法律约束力的国际文书的形式。

在作出这些努力的同时，各国必须尽一切努力促进尽可能广泛地利用网络空间促进自身发展，并在这样做时，负责任地按照适用的国际法、特别是联合国的宗旨和原则行事。

各国对维护有保障、安全和可信赖的网络空间负有首要责任。因此，鉴于目前网络空间治理的复杂情况，必须促进和确保各国在全球层面的网络空间环境治理中，特别是在政策和决策方面，发挥突出作用并认真参与。

同时，所设想的网络空间治理的发展方式必须不会对各国在网络空间环境方面的发展、治理和立法选择的权利产生不利影响。

各国有权“自由获取信息，不受干扰地充分发展其信息和大众传媒系统，并利用其信息媒体促进其政治、社会、经济和文化利益和愿望”，以及“各国有权利和义务在其宪法特权范围内打击传播虚假或歪曲的新闻”，大会在 1981 年《不容干涉和干预别国内政宣言》中也重申了这一点，必须得到充分遵守。

在履行维护有保障、安全和可信赖的网络空间的责任时，各国必须采取合作而非对抗的方式。

正如大会在 1965 年《不容干涉各国内政和保护各国独立和主权的宣言》中所重申的，“任何国家都无权以任何理由直接或间接干涉任何其他国家的内政或外交事务”。因此，所有国家必须防止和避免这种行为，特别是针对国家的政治、经济和文化要素或与网络有关的关键基础设施的行为，包括通过与网络有关的方式和手段。

此外，大会通过 1981 年《不容干涉和干预别国内政宣言》重申，一国有义务“确保其领土不被用于侵犯另一国的主权、政治独立、领土完整和国家统一或

破坏其政治、经济和社会稳定的任何方式”；“不以任何形式或借口采取任何行动或企图破坏另一国或其任何机构的稳定”，以及“不以干预或干涉他国内部事务为目的进行任何诽谤运动、中伤或敌对宣传”。各国在网络空间方面也必须遵守这些规则。

根据大会在 1970 年《关于各国依联合国宪章建立友好关系及合作之国际法原则之宣言》中重申的原则之一，各国不得使用“任何类型的措施来胁迫另一国家，使另一国家在行使主权权利时有所屈从，并从该国获取任何利益”。因此，各国不得将与网络空间有关的进展作为经济、政治或任何其他类型胁迫措施的工具，包括通过限制或阻止针对其他国家的措施。

同样，各国必须避免在网络空间环境内或通过网络空间环境使用或威胁使用武力。各国还必须避免并防止滥用在其控制和管辖下开发的网络空间相关供应链来制造或协助开发产品、服务和维护方面的漏洞，损害他国的主权和数据保护。

各国还必须适当管控本国管辖范围内的网络空间相关公司和平台，并采取适当措施，使其对自己在信通技术环境中的行为负责，包括对侵犯其他国家的国家主权、安全和公共秩序的行为负责。无论如何，国家应对其在网络空间内或通过网络空间开展的国际不法行为负责。

此外，所有与网络空间有关的国际争端必须完全通过和平手段解决，并以 1970 年《关于和平解决国际争端的马尼拉宣言》所述的“国家主权平等和自由选择手段的原则”为基础。

在此方面值得回顾的是，近年来，我们看到了一种令人震惊的趋势，即某些国家系统地指控其他国家在网络空间发起网络攻击或类似活动。鉴于目前与网络空间环境中的归责有关的挑战，以及缺乏一套国际上制定和商定的关于证实归责的真正、可靠和充分证据的标准，此类指控必须被视为纯粹出于政治动机。

总而言之，网络空间及其相关的手段、技术和工艺必须完全用于和平目的，为此，各国必须以合作、负责任的方式行事，并充分遵守适用的国际法。

最后，我们赞同大会必须继续审议网络空间相关问题的观点。就伊朗伊斯兰共和国而言，作为网络攻击的受害者之一(曾遭到 Stuxnet 恶意计算机蠕虫攻击，据信由美国和以色列政权联合制造，旨在对伊朗的和平核设施造成破坏)，伊朗伊斯兰共和国随时准备为大会制定网络空间所需原则和规范的努力作出贡献。

附件三十九

意大利常驻联合国代表团的发言

意大利赞扬爱沙尼亚提请安全理事会注意网络安全问题，并高兴地参加今天的公开辩论。

我们还赞赏裁军事务高级代表中满女士的支持和奉献精神，以及她在会员国对网络安全事件数量上升感到关切的时刻，愿意向安全理事会通报情况。

意大利赞同欧洲联盟的发言，并愿以本国身份补充以下意见。

此次辩论正逢其时。大会已经肯定第一委员会过去两年在信息和通信技术领域的发展、国际安全和促进网络空间负责任国家行为方面开展的工作。不限成员名额工作组和政府专家组在本期通过的两份报告是重要成就，应有助于在会员国之间建立信任。这两份报告还使网络安全这一多年来被认为技术性很强的领域受到关注。

数字化的步伐正在全球范围内加快，伴随着这一发展带来的好处，维护网络空间作为一个全球的、开放的和稳定的领域的挑战也随之而来。近几个月来事件激增，有时针对关键基础设施，给世界经济带来高昂成本，令人遗憾。其中一些袭击让我们得以一窥这些行动可能造成的生命损失，特别是在疫情期间。滥用新技术的破坏性潜力正变得越来越明显，加以管控的必要性也越来越明显。意大利认为，联合国是执行这一任务以及促进网络和平与稳定的最佳机构。

意大利赞同欧洲联盟关于包括国际人道主义法和人权法在内的国际法在网络空间的适用性、遵守负责任国家行为规范的重要性以及将建立信任措施作为预防冲突的实际手段的有效性的发言。我们还希望强调区域组织在网络安全领域可发挥的重要作用。作为多边主义的坚定支持者，我们鼓励联合国与区域组织之间的对话，在这方面，我们欢迎联合国秘书长与欧洲理事会之间最近的讨论，这是就我们所面临的挑战交换意见的良机。我们还赞赏欧洲安全与合作组织主席国瑞典的努力，这凸显了人权、性别问题和网络安全之间的相互联系。

在相互联系日益紧密的世界里，对话对于增进共识、增加合作机会变得更加重要。本着这一精神，我们支持欧洲联盟与联合国和区域组织，特别是非洲联盟、东南亚国家联盟区域论坛和特别顾问办公室的对话。

通过区域组织，会员国可最大限度地扩大自己的双边接触，分享最佳做法和经验教训，确保区域做法不会出现分歧。应进一步致力于和平解决争端的机制，以及发展网络外交和网络调解的倡议。

我们认为，网络领域应保持开放、自由、安全和稳定，作为各国实施政策的一种手段，促进社会繁荣，保障所有人的可持续发展，为实现可持续发展目标做出贡献。能力建设的重要性不可低估，因为它保证了各国的同等复原力，提高了认识，并刺激了能力发展。这一领域需要做的工作还很多，我们认为，与其他 52 个会员国共同推动的“推进网络空间负责任国家行为”的行动纲领可成为协调和促进这一努力的优先平台。我们已经表示，愿意在第一委员会讨论的范围内进一

步探讨这一倡议，并愿在今天重申我们的决心。行动纲领也可成为形成多利益攸关方办法和发展公私伙伴关系的论坛。

2020 年和 2021 年的这场大流行病造成巨大挫折。我们的共同努力需要专注于重新启动可持续发展，而网络领域是这方面的一个重要组成部分。意大利作为七国集团成员正在努力实现这一目标，并在其目前担任二十国集团主席的背景下推动这一愿景。今天的辩论是朝着提高认识和确保与数字化相关的发展在安全稳定的网络领域发生、同时保护一切努力不受破坏的重要一步。

本辩论进行时，20 国集团外长正在马特拉开会，讨论复苏和可持续发展问题，目的是不让任何人掉队。我们希望这些努力是相辅相成的，安全理事会将继续关注网络问题，监测进展情况，并准备呼吁不遵守规定的国家履行其义务。希望不遵守规定的国家将非常少，因为会员国一致认为需要将时间和精力用于制定积极的网络安全议程——一个发展信任、透明度和包容性的议程。

附件四十

日本外务省联合国事务与网络政策大使赤崛毅的发言

日本谨表示衷心感谢爱沙尼亚总理卡娅·卡拉斯组织本次关于网络安全的公开辩论会。日本感谢爱沙尼亚在概念说明中肯定 2017 年在日本主持下组织的关于当代国际和平与安全的复杂挑战的公开辩论。

日本欢迎 3 月通过不限成员名额工作组的报告和 5 月通过第六届政府专家组的报告，两者均以协商一致方式获得通过。

不限成员名额工作组报告的最大价值在于，该报告在所有会员国都可充分参与的进程中以协商一致方式获得通过。会员国直接肯定了相关法规、包括国际法、特别是整个《联合国宪章》适用于网络空间。

政府专家组的报告具有额外价值。对于 2015 年政府专家组报告所列 11 项规范中的每一项，新报告都提供了指导和实施实例。日本希望这些内容能进一步促进各国合作，推进负责任国家行为。此外，现在更清楚的是，可归责于国家的国际不法行为需要国家承担责任。国际人道主义法的适用性得到了明确表述。专家组再次指出，各国有采取《宪章》所承认措施的固有权利。

我们期待着今后在各种论坛上深化关于在网络空间适用国际法的具体讨论。日本希望它提供给政府专家组的国家立场汇编的立场文件将有助于这种讨论。在此，我想与大家分享日本立场中最重要的几点。

日本认为，一国不得通过网络行动侵犯另一国的主权。此外，一国不得通过网络行动干预另一国国内管辖范围内的事务。一国在网络空间实施的国际不法行为会带来国家责任。

根据国际法，各国对网络行动有尽职调查义务。规范 13(c)和(f)以及 2021 年政府专家组报告第 71(g)段的第二句话均与此项义务有关。关于最近的科洛尼尔管道运输公司事件，美国总统提到了努力实现“某种国际标准，以便政府在知道犯罪活动在其领土上发生时，对这些犯罪企业采取行动”。我们认识到，难以将网络行动归责于某个国家。尽职调查的义务可提供理由，以援引不可归于任何国家的网络行动源自其领土的国家的责任。

根据《联合国宪章》第二条第三款的规定，任何涉及网络行动的国际争端都必须通过和平手段解决。为确保和平解决争端，在网络行动引起的争端中，应利用安全理事会基于《联合国宪章》第六章和第七章的权力以及联合国其他机构的职能。日本对建立新的国际归责机制的想法持保留态度。

日本的观点是，当网络行动构成《联合国宪章》第五十一条规定的武装攻击时，各国可以行使该条承认的固有的单独或集体自卫权。

国际人道主义法适用于网络行动。这一申明有助于对战争方法和手段的监管。那种认为该申明将导致网络空间军事化的说法是毫无根据的。

国际人权法也适用于网络活动。个人在网络操作方面享有与其他方面相同的人权。

关于国际法和自愿性规范之间的关系，为稳定网络空间，必须同时运用国际法和规范，防止利用信通技术的国际不法行为，促进网络空间负责任国家行为。正如不限成员名额工作组报告中明确表示的那样，规范不会取代或改变国家在国际法下的义务。

日本希望大量会员国自愿就如何适用国际法发表本国立场。

日本认为，现在正逢其时，应将执行商定的自愿规范和国际法义务以及建立信任措施和能力建设措施作为优先事项。

在执行方面，日本希望邀请各国政府在发生恶意网络行动时主动宣布相关法律评估，包括评估其是否构成违反国际法行为。这种做法将促进对国际法如何适用于网络行动的共同理解。国际和国内法院及法庭对网络事件适用国际法将产生类似效果。日本希望，通过积累这种实践，网络空间的恶意活动将得到遏制。

日本坚决支持该行动纲领。我们认为，行动纲领将成为确保和监测商定规范、国际法义务、建立信任措施和能力建设执行情况的有效机制。我们期待着深化关于行动纲领的讨论。我们还将继续积极参加新的不限成员名额工作组。

日本致力于维护一个自由、公平和安全的网络空间，并将继续积极推动促进网络空间法治的讨论和努力，包括在联合国开展的讨论和努力。

附件四十一

哈萨克斯坦常驻联合国代表马格占·伊利亚索夫的发言

我们感谢主席国爱沙尼亚组织和主持题为“维护国际和平与安全：网络安全”的辩论会。

在全球面临威胁的情况下，为确保安全，国际社会需要共同协调，解决政治和经济方面诸多问题。在这一背景下，应指出，世界上出现了一个新的同时也很复杂的组成部分-网络安全。

应该明确的是，信息和通信技术具有促进各国发展的巨大潜力。同时，它们为犯罪分子创造了新机会，可能导致犯罪率和复杂性上升，以及滥用包括人工智能在内的新兴技术的潜在风险。在这方面，预防和制止为犯罪目的使用信息和通信技术行为应是各国现阶段的工作重点。

在这方面，我们欢迎大会 2019 年 12 月 27 日通过的第 74/247 号决议所规定的设立一个代表所有区域的不限成员名额特设政府间专家委员会，以拟订一项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，同时充分考虑到关于打击为犯罪目的使用信息和通信技术行为的现有国际文书和国家、区域和国际各级的现有努力。

我们认为，联合国在这一领域的工作将进一步参考 2021 年 3 月通过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的最后实质性报告、第 75/240 号决议(该决议设立了 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)形成的共识、以及 2021 年 5 月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通过的共识报告。

各国应继续加强措施，保护所有关键基础设施免受信通技术威胁，并就这一领域的最佳做法加强交流。

在这方面，我们欢迎联合国网络安全谈判进程，欢迎与会者和会员国理解，关于这一特定议程的所有决定都必须以协商一致方式作出。

附件四十二

拉脱维亚常驻联合国代表团的发言

信息和通信技术(信通技术)的发展在经济、服务、教育和通信领域为国家和社会带来了诸多好处。在应用信通技术产生巨大积极影响的同时，拉脱维亚越来越关注信通技术的恶意和破坏性使用对国际和平、安全、稳定和人权的影响。

更多时候，国家遭受此类犯罪，包括影响民主机构和关键基础设施的犯罪。更令人震惊的是，恶意的网络活动正在利用冠状病毒病大流行，将对维护人类健康、疫苗研究以及信息空间至关重要的医疗保健系统作为攻击目标。

去年联合国安全理事会阿里亚模式会议上的广泛参与和讨论证实了网络安全对国际和平与稳定议程日益重要的意义。因此，将网络安全问题列入安全理事会的正式议程是非常及时和适当的。拉脱维亚完全支持爱沙尼亚努力促使各方适当反思减轻网络空间不负责任行为对国际和平与安全的影响。

联合国必须继续发挥重要的全球作用，以促进和平、安全与稳定，包括在网络空间。从国际安全角度促进网络空间负责任国家行为政府专家组和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在过去几年的积极工作为今天的讨论奠定了实质性基础。

政府专家组和不限成员名额工作组的两份基于共识的最后报告是值得欢迎的垫脚石，有助于进一步开展工作，以便就广泛的问题形成共识。

在这方面，关于各国在国际安全方面负责任地使用信通技术的行动纲领是政府专家组和不限成员名额工作组报告的宝贵成果。与网络有关的行动纲领应成为进一步工作的坚实基础，最重要的是，应以行动为导向，以便在执行负责任行为规范方面取得切实进展。

在这方面，拉脱维亚希望强调网络空间的多利益攸关方性质，这需要来自私营部门、民间社会和学术界的一系列非国家行为体参与讨论。考虑到这些利益攸关方在信通技术生态系统中的主导地位，这些利益攸关方可通过许多不同方式做出重大贡献，分享观点、知识和经验。

各国应继续积极努力，并准备好在未来的联合国进程中深入讨论，在国际安全背景下推动网络空间负责任国家行为。我们都必须不懈努力，加强对自身信通技术的保护和安全，同时各国不应允许另一国家或非国家行为体在本国境内利用信通技术实施国际不法行为。我们呼吁所有国家不要开展、支持或容忍不符合包括《联合国宪章》在内的国际法的活动，以避免妨碍与使用信通技术相关的安全。责任、建立信任和可预测性必须成为网络安全领域国际合作的关键因素。

为了一方面防止误解和误会，另一方面建立关于信通技术事件的沟通实践，我们必须在会员国之间建立公开的沟通渠道。在联合国建立政策和技术层面的联络点网络，可为在全球一级进行更有效的沟通作出有意义的贡献。事实证明，欧洲安全与合作组织的联络点网络在区域一级是有效的。

最后，拉脱维亚要赞扬所有会员国表现出合作和共同努力的决心，以便在政府专家组和不限成员名额工作组进程中就报告达成共识。这是一条正确的道路，也是进一步加强国际合作的绝佳机会，以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。

附件四十三

列支敦士登常驻联合国副代表兼临时代办乔治·施帕贝尔的发言

网络行动已成为现代战争的平衡器，为所有行为体、包括资源较少的行为体，提供了新的进攻和防御行动的途径。因此，近年来，网络行动的频率和严重程度都在加强，威胁着国际和平与安全。令人震惊的是，此类袭击有可能给平民造成严重痛苦，包括生命损失和基本服务中断。在这方面，我们回顾，各国越来越同意将国际法(特别是整个《联合国宪章》和源自《宪章》原则的习惯国际法规则，以及《国际刑事法院罗马规约》和国际人道主义法)适用于网络空间。

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使联合国内关于网络背景下国际和平与安全的讨论制度化。此外，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(政府专家组)发布的最后报告重申了国际法在网络空间的适用性和必要性。列支敦士登注意到不限成员名额工作组和政府专家组在进一步讨论国际法、特别是《联合国宪章》如何适用于网络空间方面所作的共同贡献。

《联合国宪章》的标志性成就之一是禁止使用武力。除非得到安全理事会根据《宪章》第七章授权或根据《宪章》第五十一条进行自卫，否则禁止使用武力。然而，第五十一条越来越多地被援引为在没有必要法律理由的情况下使用武力的法律依据。随着新技术和国家能力的发展，这种趋势有延伸到网络空间的实质性风险。我们应确保网络空间不会为不正当的自卫行动提供便利。而且，我们回顾，先发制人地援引第五十一条需要有证据表明武装攻击迫在眉睫，而且总是需要证明必要性和采取的应对措施的相称性。

《联合国宪章》规定，安全理事会将在最严重违反国际法有关规则、构成侵略行为的情况下发挥执法作用。除《宪章》所载工具外，安理会现在还可选择将有关情况提交给国际刑事法院，以启动对侵略罪行为人的个人刑事责任。在这方面，列支敦士登认为，明确了解《罗马规约》如何适用于网络行动，将有助于为安理会的工作提供参考。

为阐明《罗马规约》对网络行动的适用性，列支敦士登与其他十个国际刑事法院缔约国一起成立了一个顾问委员会，以探讨国际刑事法院在监管网络战争方面的作用。顾问委员会由 16 位知名国际律师组成，在 2019 年和 2020 年期间召开了三次会议，讨论《罗马规约》的核心条款适用于网络行动的程度。最后报告定于今年提交。我们希望，这将有助于在网络行动的背景下就问责问题达成共识，并从一开始就威慑此类犯罪。

列支敦士登强调，为了国际和平与安全，需要一个强有力的法律框架来规范网络空间。我们很高兴通过我们即将提交的以《罗马规约》为重点的报告，为打击恶意网络行动的全球努力做出贡献，我们将继续坚定不移地拥护国际法，努力维护国际和平与安全。

附件四十四

马耳他常驻联合国代表团的发言

马耳他感谢爱沙尼亚就我们认为应列入安全理事会议程的这一问题组织了本次及时的辩论。尽管安全理事会多次辩论都提到了网络安全问题，但我们认为，考虑到网络安全问题是国际和平与安全面临的最重要和不断变化的挑战之一，应得到更加突出的重视。

马耳他赞同欧洲联盟所作发言，并希望以本国名义强调几点。网络空间的发展为全球会员国和公民带来了诸多机遇，促进了繁荣、互联互通和经济增长。然而，网络领域也为恶意活动打开了大门，这些活动旨在破坏和利用社会中的漏洞并进行攻击，可能对会员国及其公民产生相当大的影响，例如在敏感数据和关键基础设施方面。事实上，我们越向虚拟和互联的世界转变，就越容易受到这类恶意活动的影响。

马耳他认为，联合国在规范国家在网络空间的行为方面可发挥核心作用，特别是因为联合国已经建立了广泛的国际法体系。我们还对政府专家组(政府专家组)和联合国不限成员名额工作组(不限成员名额工作组)取得的成果感到非常鼓舞，两者通过了关于推进国家在网络空间行为等方面的共识报告。我们需要这两个进程继续在联合国系统内提供信息，并阐述国际法在网络空间的应用、建立信任措施的重要性以及提供更多的指导和规范。我们重视会员国对这些进程的参与和贡献，我们敦促各方继续推进这些讨论，跟上这一领域的快速发展。

我们已经目睹网络攻击对敏感数据和基础设施可能产生的破坏性影响。至关重要的是，对网络领域国家行为的规范和条例应得到妥善概述。这将提高可预测性，并避免在评估网络威胁时出现任何误判。对网络空间的恶意使用具有持久影响，因此也需要在国际层面进行合作，以避免可能出现的任何潜在冲突。

通过应用良好做法和既定规范在国家之间建立信任措施是向前推进的一个重要组成部分。这将减少任何潜在误解，并更好地评估恶意行为。

国际社会还必须就这一问题接触各类其他利益攸关方，包括民间社会和私营部门，以确保建立公平的竞争环境和公平的规则。网络空间所有潜在用户都需认识到自身在提高网络抗御能力和防止恶意使用所掌握的工具方面所发挥的作用。

马耳他认为，在涉及可能对国际和平与安全产生影响的新技术时，安全理事会可发挥重要作用。安全理事会必须确保网络空间所有相关行为体遵守国际法以及既定规则和准则，以避免网络攻击引起的潜在冲突。我们敦促安理会继续处理这一问题，并确保我们共同促进增进理解和互信。

附件四十五

摩洛哥常驻联合国代表团的发言

[原件：法文]

首先，摩洛哥王国感谢爱沙尼亚组织安全理事会第一次公开辩论会，讨论维护网络空间的国际和平与安全这一重要而及时的问题。摩洛哥欢迎爱沙尼亚共和国总理卡娅·卡拉斯女士的详细发言，以及爱沙尼亚共和国在网络事务和网络空间安全方面的出色领导。摩洛哥还感谢裁军事务高级代表中满泉女士就当前维护网络空间国际和平与安全的挑战所作的内容丰富的通报。

摩洛哥王国作为一个互联互通水平很高的发展中国家，很快就对信息和通信技术(信通技术)的发展及其作为可持续发展引擎的优势表现了特别兴趣。然而，尽管我们一致认识到这些技术的进步对人类日常福祉的好处和优势，但我们开始意识到可能出现的威胁，从简单的“假新闻”传播到对和平与安全的实际攻击，在国家和国际层面都是如此。

然而，在物联网、数字革命或网络战争等术语被普遍使用的当下，我们对抗网络威胁的能力仍远远低于对这些必要工具的高度依赖。除此之外，需要注意的是，目前以 COVID19 大流行为标志的背景使我们更加进入网络时代，同时也成倍地、不可逆转地增加了我们对网络攻击和威胁的暴露和脆弱性，包括针对关键基础设施的攻击和威胁。

这些恶意行动，除威胁国家主权之外，还有一种不幸的可能性，即增加网络空间冲突的风险，同时造成相当大的人员和物质损失。这很可能破坏国际和平与安全的结构，使网络攻击成为新兴重大威胁。

正如秘书长在 2018 年《裁军议程》启动仪式上所说的，“我们生活在危险的时代”。

的确，现在国际社会和联合国会员国比以往任何时候都更面临与网络空间威胁相关的潜在和现实风险。只有通过集体和单独努力防止恶意使用信通技术，才能保证网络空间继续成为和平、安全、稳定和发展的引擎。

在这方面，摩洛哥认为，保障和保护网络空间仍是各国作为领导者的共同责任。因此，摩洛哥根据皇家指令，在立法、组织和预防层面迅速采取了以下重大行动：

- 网络安全战略的定义围绕着四个战略因素：评估行政部门、公共机构和极其重要的基础设施内的信息系统的风险；保护和防御这些信息系统；加强安全基础(法律框架、宣传、培训和研发)；促进和发展国家、区域和国际合作。

- 2020 年 7 月 25 日颁布了关于网络安全的第 05-20 号法，目的是建立法律框架，要求各实体拥有一套基本的最低限度的安全措施和规则，以确保其信息系统的可靠性和韧性。其目标还包括发展数字信任、经济数字

化，以及更广泛地保证摩洛哥经济和社会活动的连续性，以促进国家网络安全生态系统的发展。

- 在本十年期间，成立了数个旨在确保国家治理网络安全的组织，例如2011 年成立的信息系统安全战略委员会、信息系统安全总局、国家电信管理局、国家个人数据监测和保护委员会，以及开展全国打击网络犯罪运动的摩洛哥理工学院研究和创新中心。

在本次公开辩论前夕，2021 年 6 月 28 日，摩洛哥还批准了一项与网络安全有关的法令草案，规定了适用于信息系统安全的规则，以及《非洲联盟网络安全和个人数据公约》。

然而，鉴于网络威胁的全球性，国际上商定的重大措施应能与在国家层面实施的法规相配合。因此，摩洛哥已经批准了《欧洲委员会网络犯罪公约》(又称《布达佩斯公约》)，并在 2018 年加入了《网络空间信任与安全巴黎呼吁》。在联合国主持下，摩洛哥参加了从国际安全角度看信息和电信领域的发展不限成员名额工作组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，以及 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，并参与制定即将出台的促进网络空间负责任国家行为的行动纲领。摩洛哥也是电子政务和网络安全之友小组的成员，爱沙尼亚和新加坡是该小组出色的共同主席。

最后，摩洛哥王国强调，各国都有责任证明其保护网络空间的共同和坚定的意愿，这主要是由于网络空间的预防和安全方面是使用信息和通信技术的必然结果。

尤其需要安全理事会发挥关键作用，特别是在发生对国际和平与安全构成直接威胁的网络攻击的情况下，而且需要安全理事会在预防领域发挥先锋作用。

摩洛哥再次热烈感谢爱沙尼亚组织这次必要而及时的公开辩论，我们需要对维护网络空间的国际和平与安全问题有更多的认识和讨论，并将这一问题列入安全理事会议程。

附件四十六

荷兰常驻联合国代表约卡·布兰特的发言

荷兰王国感谢爱沙尼亚和卡拉斯总理组织本次关于维护网络空间国际和平与安全的公开辩论会。

鉴于国家和非国家行为体的网络攻击急剧增加，本次会议非常及时。这些恶意网络活动可通过相对有限的资源对社会造成潜在的巨大破坏。其后果是破坏国际关系的稳定。

因此，现在是时候共同努力，通过推进负责任国家行为，谴责不负责任的行为并施加后果，确保开放、自由和安全的网络空间。

虽然这个问题还有许多其他相关角度，但荷兰将重点关注对加强网络空间稳定始终至关重要的三个具体因素：

- 守法
- 归责
- 能力建设

守法

多年来，针对关键和民用基础设施的网络行动已被证明是真实、可信的威胁。过去一年更是如此，我们目睹了网络攻击在范围、规模、严重程度和复杂性方面的演变。作为社会，我们越来越多地将生活的几乎方方面面转移到数字世界，我们必须认识到，正是互联网促进了世界各地的这些连接。因此，毫不奇怪，针对关键基础设施、政府或社会的恶意网络行动的有害影响将被立即、广泛感受到。对国际安全稳定、经济社会发展以及个人安全福祉构成重大风险。

随着最近就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(政府专家组)的报告达成共识，各国现在具备了一项有关网络空间负责任国家行为的框架。使各国能够更好地理解国际法和商定的 11 项自愿非约束性规范的适用性。荷兰回顾，现有国际法、特别是《联合国宪章》适用于网络空间，对维护和平与稳定以及促进自由、开放和安全的网络空间，包括尊重网络空间的人权和基本自由至关重要。

各国同意禁止对支持公共基础设施基本服务的基础设施和信息基础设施进行恶意网络行动，并确认政府专家组规范 13(f)。每个国家都有权确定其指定为关键的基础设施，可能包括：医疗设施、金融服务、能源、水、交通和卫生设施。荷兰一直专注于三项(非详尽的)基础设施：

对互联网的普遍可获得性或完整性至关重要的技术基础设施；

选举所必需的技术基础设施；

医疗保健部门。

本着这一精神，我们鼓励各会员国通过发表国家声明，详细说明本国对遵守负责任国家行为框架的立场，公开界定和分享本国认为重要的基础设施。这是我们提高透明度、形成共识、创造可预测性和建立信任的唯一途径。需要继续努力执行商定的框架，以降低事态升级的风险，并使所有国家都遵守法律。

归责

我们似乎都同意网络空间的规则和规范。然而，我们继续看到网络威胁的增加。荷兰对 2019 冠状病毒病(COVID-19)大流行被滥用于针对关键基础设施、卫生部门、对互联网的普遍可用性或完整性至关重要的技术基础设施以及选举的技术基础设施的恶意网络操作感到震惊。

让我们明确一点——我们将在自愿的基础上共同努力，在国家违反这一框架的行为时追究其责任，包括采取透明和符合国际法的措施。网络空间不良行为必须承担后果。

能力建设

数字韧性是管理网络风险和减轻其影响的关键。然而，不同国家之间的网络安全能力水平不同，放大了这个相互关联的世界的脆弱性。因此，开展有针对性的能力建设努力，确保所有负责任的国家都能落实这一框架，更好地保护网络不受重大破坏性、毁灭性或其他破坏稳定的网络活动的影响，符合我们的共同利益。此外，有效的网络能力建设需要国家和非国家行为体之间的合作。有鉴于此，荷兰建立了全球网络专家论坛，该论坛已经成熟为一个强大的公私能力建设平台，利用和巩固现有的 700 多项网络能力建设工作，为建立技术复原力提供援助，帮助起草确保安全、安保和尊重人权的立法。

我们赞扬爱沙尼亚为安全理事会今后的网络讨论奠定了基础，并欢迎今天关于网络安全的首次正式辩论。

附件四十七

新西兰常驻联合国代表团的发言

新西兰谨指出，我们赞赏爱沙尼亚将维护网络空间国际和平与安全这一重要问题提上安全理事会议程。

网络威胁是所有会员国面临的一个紧迫而普遍的问题。网络威胁对新西兰的繁荣与安全以及国际和平与安全构成重大风险。

我们必须共同建设稳定安全的网络环境，让所有人都能享受数字互联互通带来的好处，数字互联互通是经济社会文化发展的重要推动因素。

我们珍视有这一机会分享新西兰对维护网络空间和平与安全的国际努力的看法。为此，我们重申关于网络空间负责任国家行为的商定框架的极端重要性：

- 我们必须遵守现有国际法规定的义务，我们都同意这些义务在网上网下都适用；
- 我们必须执行网络空间负责任国家行为规范，每个会员国都已通过大会第 70/237 号决议认可这些规范；
- 我们必须确保建立信任措施得到广泛采纳和利用；
- 我们必须加倍努力进行能力建设，以确保我们都具有网络韧性。

这个框架提供了用于鼓励网络空间负责任行为的所需要素，但需付诸实践，才能发挥效力。我们需要继续以务实、有意义和具体的方式落实这一框架。新西兰承诺将继续与大家一道为此而努力。

国际法

作为小国，新西兰坚定地支持基于规则的国际秩序。在跨界威胁方面尤其如此。新西兰在地理上的孤立并不能保护新西兰免受网络威胁。

确保该系统促进开放、安全、稳定、无障碍、和平的在线环境，并鼓励网络空间负责任国家行为，是新西兰的重要优先事项。

就如何在网上准确适用国际法达成共识是对维护和平与稳定的重要贡献。我们都同意，国际法在网上和在网下一样适用。适用的国际法包括：《联合国宪章》；国家责任法；国际人道法;国际人权法。

但我们承认，在这些问题上仍然存在一些分歧。为支持对国际法如何在网上适用的理解，2020 年 12 月，新西兰发布了一份国家立场声明。我们鼓励其他会员国分享各自国家观点，以发展和加强我们对这些问题的共同理解。

负责任国家行为规范

新西兰致力于预防、发现、威慑和应对恶意网络活动，维护 2021 年联合国不限成员名额工作组报告认可的负责任国家行为规范。我们所有国家都承诺遵守

的规范是网络空间稳定和安全的核心组成部分。我们需要继续对所做承诺负责--并也对其他国家问责。

除其他外，我们必须促进国家间合作，保护关键基础设施，保障全球供应链，在需要时提供援助，尊重人权和隐私，并防止在国家领土上恶意使用数字技术。

我们继续思考 2019 冠状病毒病(COVID-19)大流行如何突显强调安全和有保障的网络空间的重要性。我们看到国际上有报告称，国家和非国家行为体在网上进行了一系列不同的恶意活动。除其他外，这项活动的目标是关键的卫生保健基础设施；从事应对工作的官员；公众成员。这是不可接受的，突显出网络空间的威胁将生命置于危险之中。新西兰和其他一些国家公开谴责了破坏疫情应对的恶意网络活动。

建立信任措施

我们将继续致力于取得建设性、务实和具体成果，改善国际和地区网络安全。建立信任措施为实现这一目标提供了重要途径，我们欢迎促进网络空间的相互理解、透明度、可预测性和稳定性的实际举措。

对新西兰来说，东南亚国家联盟(东盟)地区论坛是讨论区域网络安全的重要论坛。我们欢迎与该论坛内成员的合作，并期待着在未来几年继续与大家合作。新西兰欢迎有机会在区域内和区域间分享经验教训，以提高区域伙伴在网络空间的透明度、理解和信心。

能力建设

新西兰希望帮助确保所有国家降低与增加连通性相关的风险，同时继续从中受益。这包括支持更广泛和更深入地理解和遵守网络空间负责任国家行为框架。

为实现这一目标，我们需要确保所有人都有必要的工具和能力，有意义地参与正在进行的讨论和辩论领域，并在国内和区域内实施支持国际稳定的举措。

新西兰仍然致力于建设区域网络安全能力，并特别注重与太平洋和东南亚邻国的合作。我们继续在新西兰 1 000 万新西兰元的"支持太平洋地区网络安全 "方案下实施各项举措，并支持东盟-新加坡网络安全卓越中心。

结语

我们有很多工作要做，但我们并非从零开始。我们再次欢迎最近联合国政府专家组和不限成员名额工作组进程的成果。这些进程以及由此产生的报告是重要的互补和相辅相成的成就。我们必须继续在大会批准的这项以及其他共识协议所建立的基础上再接再厉。

重要的是，这些讨论必须涉及各种不同的观点，包括小国和非政府利益攸关方的观点。会员国对网络安全的广泛兴趣使我们感到振奋——网络空间的和平与安全确实影响到我们所有国家——看到如此广泛的国家真正参与到应对这些挑战的努力中，令人鼓舞。新西兰随时准备与大家一起应对这一挑战。

附件四十八

巴基斯坦常驻联合国代表的发言

我谨对爱沙尼亚共和国常驻代表团就“维护网络空间的国际和平与安全”这一主题召开这次重要而及时的安全理事会公开辩论会深表赞赏和感谢。

信息和通信技术(信通技术)为国际社会提供了巨大机遇，其重要性也在继续增加。同时，信通技术使用所固有问题的复杂性给国际和平与安全带来了严重风险。

对网络技术的敌意使用正迅速接近可能构成破坏和平或威胁国际和平与安全的阶段。

滥用和不规范地使用信通技术，可能导致关键基础设施受到网络攻击，对国际和平与安全造成严重影响。最近发生的疑似网络攻击事件就是例证。

有必要紧急处理日益增长的网络安全前景，作为联合国预防冲突的更广泛努力的一部分。

在这方面，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在今年 3 月通过了共识报告，这对支持全球努力实现创造安全、可靠、稳定、和平的信通技术环境的共同目标具有历史意义。

这也有力彰显了国际社会有能力在最困难情况(如大流行病)下共同应对关键的全球挑战。

虽然我们理解报告没有解决所有会员国的关切，但我们认为必须巩固迄今已取得的进展，并保持继续这一包容和透明进程的势头。

巴基斯坦仍然积极和建设性地参与不限成员名额工作组的工作，并欢迎根据大会第 75/240 号决议设立 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。

新的不限成员名额工作组在以往建议的基础上，为取得有意义的进展提供了极为有用的论坛，以便加强网络空间负责任行为的规则，实现有意义的国际合作，最大限度地减少恶意使用信通技术对国际安全造成的威胁。

2015 年政府专家组和不限成员名额工作组最近的报告商定了一系列重要结论，有助于在会员国之间达成广泛共识，即国际法、特别是《联合国宪章》适用于维护信通技术环境中的和平与稳定，而且至关重要。

《联合国宪章》毫不含糊地明确维护主权、领土完整和不干涉别国内政的原则。在驾驭复杂的网络治理的过程中，这些原则应作为指向性明灯。

同时，需要认真考虑国际法及其解释在国家行为和使用信通技术方面的适用程度、范围和性质。

简单断言现有国际法适用于网络空间，不足以应对信通技术带来的多方面法律挑战。需要根据网络空间的独特特点进行调整。

巴基斯坦认识到，必须制定一项具有法律约束力的国际文书，特别是针对信通技术的独特属性，提供旨在创造网络空间稳定和安全的监管途径。这种法律框架应考虑到所有国家的关切和利益，应以协商一致为基础，并在所有国家平等参与的情况下在联合国内推行。

关于国家负责任地使用信通技术的自愿、非约束性规范可有助于降低国际和平与安全面临的风险。然而，鉴于信通技术环境面临的前所未有的威胁和技术发展的快速步伐，有必要加强国际努力，制定具有约束力的规则，帮助维护和平与稳定，促进开放、安全、稳定、无障碍、和平的信通技术环境。

我们应该确保网络空间不被滥用以致使国家支持的造谣运动、煽动暴力、仇恨言论和包括仇视伊斯兰在内的其他相关形式的不容忍行为永久化。

联合国在促进会员国之间的对话和国际合作方面发挥着核心作用，以便在关键方面形成共识，包括适用国际法和规范、负责任国家行为的规则和原则、促进建立信任和透明度措施以及支持能力建设和传播最佳做法。

巴基斯坦拥有 2 亿多人口，数字环境蓬勃发展，在线用户数量不断增加，因此，巴基斯坦非常重视利用数字技术促进社会经济发展，并促进更有效和高效的治理和公共服务提供。

巴基斯坦致力于促进信通技术及网络安全方面的国际合作，以此作为弥合数字鸿沟的手段。在制定数字经济和网络空间及信通技术安全的规则方面，所有国家都是平等的利益攸关方。

附件四十九

秘鲁常驻联合国代表团的发言

[原件：西班牙文]

秘鲁欢迎主席国爱沙尼亚倡议召开安全理事会本次高级别公开辩论，讨论对维护国际和平与安全日益重要的问题。我们也欢迎其他发言者的通报。

我们意识到使用信息和通信技术(信通技术)在国际安全方面的相关性、其迅速演变及其带来的好处。COVID-19 大流行引发的卫生危机突显了我们对信通技术的依赖、缩小数字鸿沟的紧迫性以及保护关键基础设施的重要性。

同样，我们也意识到恶意使用信通技术可能带来的危险，从而增加网络空间发生冲突的风险。恐怖主义团体、犯罪组织、武装团体和其他代理人恶意使用信通技术，对国际和平与安全构成严重和系统性威胁。

考虑到这些威胁不是来自技术本身，而是来自对它们的使用，我们必须加深对了解信通技术的适当使用以及如何通过促进开放、自由、稳定和安全的网络空间来避免蓄意恶意使用。

为此，我们承认《联合国宪章》作为安全坚实基础的首要地位，我们支持在网络空间适用国际法和国际人道法。此外，我们认为，通过确立具有法律约束力的义务来制定这一领域的国际规范至关重要。

我们赞赏联合国在制定促进适用国际法和执行国家在国际安全背景下的网络空间负责任行为规范的要素方面作出的显著努力和取得的进展。我们赞扬不限成员名额工作组和政府专家组通过的实质性报告，我们希望通过协调这两个进程的工作，我们将能够在网络安全方面发表一致的声明和行动方案。

除国际努力外，我们认为区域和国家行动至关重要，特别是在促进建立信任措施、能力建设、信息交流和分享最佳做法以保障网络安全方面。对于技术发展水平较低的国家，在我们看来，由于缺乏避免冲突的能力而产生的潜在影响，它们必须具体说明避免使网络空间成为冲突舞台的谅解和协定。

考虑到网络空间相互关联和复杂的性质、信息和通信技术的不断创新以及新兴技术的日益融合，我们支持私营部门、特别是信息产业、民间社会和学术界参与应对这些挑战。我们深信，他们的贡献将继续丰富关于这一问题的多边审议。

最后，我们强调整个国际社会需要协调工作，需要采取新的行动来研究现有的威胁以及可能的合作措施，以应对这些威胁。安全理事会在预防冲突和促进和平与安全方面的作用将是至关重要的，以保障网络空间是开放、和平、安全和有益的，并促进可持续发展和人民的福祉。

附件五十

波兰常驻联合国代表团的发言

联合国安全理事会有史以来第一次关于网络安全的公开辩论，是我们对当代国际和平与安全挑战的看法的一个重要里程碑。

我们感谢并赞扬主席国爱沙尼亚使我们能够在这个非常及时的时刻处理网络安全问题。

2019 年，在我们担任成员期间，波兰已提请联合国安全理事会注意中东地区的网络事件问题。

现在是时候提高整个国际社会对网络空间恶意活动稳步上升的认识。20 年来，在数字技术空前发展的同时，我们在世界各地观察到越来越多复杂的网络攻击和网络事件。波兰每天都在经历这种事件的发生。

当然，其性质各有不同。有些事件纯粹是有犯罪背景的，另一些事件的动机是经济目标，而且往往越来越多是政治目标。然而，这些活动有一个共同点，即都是非法的。恶意的网络活动，无论如何都是无法辩解或辩护的。

正如你在概念说明中正确指出的：“现行国际法，特别是《联合国宪章》，为各国开展网络活动提供了充分的指导。”制定共同接受的网络空间活动模式是国际社会的一项重大任务。

波兰坚决支持政府专家组取得的成就，并积极参与不限成员名额工作组的工作，该工作组在其报告中重申了国际法在网络空间的适用。我们希望第二届不限成员名额工作组将有助于对和平利用网络空间的重要性有更好的共同理解。我们也高度重视大会第三委员会特设委员会的工作。

除了对形势的共同评估之外，更重要的是共同采取精心策划的行动。因此，波兰支持多方利益攸关方、非政府组织、私营部门和学术界广泛参与关于网络安全的国际辩论。

我们也坚信，各区域内应开展关键的工作。在区域组织、个别国家和民间社会代表的参与下，我们可以就能力建设或建立信任措施制定有用的文书。

为促进全球和区域层面的国际努力，我们需要汇集我们的资源和外交能量。这就是为什么我们坚定支持和推动将《行动纲领》确立为网络空间活动国际合作的最终形式。

通过这次公开辩论，我们希望网络安全将在联合国安全理事会议程上占据永久位置。网络空间恶意活动的政治和经济代价太高，联合国这样的重要机构不容忽视。

请放心，波兰将不遗余力地为所有全球和区域进程作出贡献，以便在尊重国际法和共同商定的准则的基础上加强网络秩序。

附件五十一

卡塔尔常驻联合国代表团的发言

[原件：阿拉伯文]

请允许我感谢裁军事务高级代表中满泉的通报。裁军事务厅的工作有助于在联合国裁军议程上给予网络安全应有的位置。

我们每天都看到世界对网络空间的严重依赖所产生的变革性影响。然而，数字技术和全球连通性也为滥用网络空间提供便利，鉴于重要的公共基础设施和服务对数字领域的依赖，这一点尤其令人担忧。政府和非政府行为体滥用网络空间以及信息和通信技术(信通技术)对国家安全构成威胁，影响区域和国际和平与安全以及国际关系。此外，恐怖组织正在利用新兴的数字技术来增强其犯罪能力。

显然，任何国家都不能幸免于滥用网络空间的威胁。因此，必须采取集体行动应对这一全球挑战。幸运的是，网络空间本身可以为协调这些努力提供一个极好的工具。正如我们在过去一年中所看到的，数字平台已被证明是联合国机构和其他国际合作论坛继续工作不可或缺的手段。

我们必须评估潜在的威胁以及网络盗版和滥用网络空间对和平与安全的影响。面对这些威胁，需要集体努力加强区域和国际安全环境，促进和平利用网络空间和相关先进数字技术。

在这方面，必须适当考虑将国际法适用于各国使用信通技术，并从国际安全的角度促进与国家电子空间有关的负责任行为。

与此同时，必须在开放和安全的、所有人都可以进入的数字环境中维护信息自由流动以及对人权和基本自由的尊重。

除国际框架外，国家战略对于指导相关利益攸关方之间的行动和协调也很重要。其中包括在数字技术中发挥关键作用的私营部门。

保护信息安全和信息基础设施是卡塔尔的优先事项之一。卡塔尔正采取综合措施，开发这方面的资源，重点是促进国际合作和能力建设。

信息安全和网络安全列入联合国议程已有数年。然而，必须采取步骤，跟上这一领域的快速发展。因此，我们欢迎秘书长对这一问题的重视，他已将促进和平的信息和通信技术环境作为其主要优先事项之一。我们还高兴地看到，政府专家组内部再次达成共识。我们也期待不限成员名额工作组的下一届会议，以期为扩大这方面的国际共识作出贡献。

最后，我想重申，卡塔尔国将继续在各个层面努力，为促进网络空间的和平、安全和稳定的全球努力作出贡献。

附件五十二

大韩民国常驻联合国代表赵显的发言

首先，我要感谢你及时召开今天关于“维护网络空间国际和平与安全”的公开辩论。我还要感谢裁军事务高级代表中满泉女士阁下的深入通报。

在过去几十年里，人类见证了数字技术领域前所未有的技术进步。网络空间的概念曾经只存在于科幻小说的想象中，现在已成为我们所有人的日常现实；我们周围的虚拟和实体空间正整合成一个生态系统。尽管这种进步给我们带来了前所未有的经济和社会利益，但我们也变得更加容易受到恶意网络活动的影响。过去一年里，在全球大流行期间，随着越来越多的人上网，我们的生活变得更容易受到网络威胁的影响。与此同时，针对关键基础设施、包括世界各地的医疗基础设施和设施的网络攻击越来越多，这一点越来越令人担忧。

在此背景下，我想强调我国代表团认为尤其重要的四点。

第一，大韩民国支持联合国在目前正在进行的关于如何应对当前挑战和推进网络空间中负责任国家行为的讨论中发挥核心作用。在这方面，我国代表团欢迎通过联合国从国际安全角度看信息和电信领域发展不限成员名额工作组的共识报告，以及上个月通过的政府专家组第四次共识报告。这些成就反映了在负责任的国家使用信通技术行为的累积和演变框架方面所取得的进展，并通过这些活动加强整个国际社会对这一关键领域的了解。

正如所有联合国会员国在不限成员名额工作组上一次报告中一致同意的那样，国际法适用于国家对信通技术的使用，各国应以政府专家组报告中概述的负责任的国家使用信通技术行为框架为指导。国际法的首要地位和以规则为基础的秩序必须同样适用于网络空间，以确保和平与安全。

第二，我国代表团高度赞赏政府专家组最近的共识报告，其中就负责任的国家行为准则、建立信任措施、能力建设以及国际法如何适用于国家使用信通技术等问题提供更深一层的理解。该报告重申了包括《联合国宪章》等国际法的适用性，特别是国际人道法在武装冲突局势中的适用性。我们还强烈支持政府间专家组的建议，即对于包括涉及使用信通技术在内的任何国际争端，当事方应首先寻求以《联合国宪章》第三十三条所述和平方式解决争端。

具体地说，我国代表团高兴地看到，该报告进一步阐述关于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规范。这一“尽责”原则是由韩国提出的，并首次反映在 2015 年政府专家组报告中，其中指出每个国家在知道或被告知有国际不法行为时，应采取适当和合理的步骤来处理情况。

第三，我们必须进一步提升我们在建立信任和促进共同理解方面的努力。大韩民国作为负责任的联合国会员国及数字和技术领域的领先国家，一直积极参加各种区域和多边论坛并作出贡献。就在上周 6 月 22 日，韩国与欧安组织密切合作，成功举办了“第三届区域间网络/信通技术安全会议”，讨论当前网络安全趋势，促进区域组织之间的网络安全合作。我们还在 2020 年主办了第 19 届韩国-

联合国裁军与不扩散问题联席会议，重点讨论新兴技术的发展和影响，并将共同主持2021-23年东盟地区论坛信通技术安全问题闭会期间会议。此外，今年11月，韩国将启动一个国际论坛来进一步活跃讨论，在国际和平与安全的背景下应对包括网络攻击和恶意使用新兴技术在内的新出现安全威胁。在包容、透明、开放的原则下，该论坛将为各利益攸关方提供一个令人欢迎的国际平台。

第四，网络安全需要多方利益攸关方参与，因为网络空间的国际安全层面跨越多个领域和学科，这一点我们怎么强调都不为过。虽然各国政府仍然是中心，但只有当我们让私营部门、学术界、公民社会和技术界等其他主要利益攸关方参与这一进程时，我们才能真正有效。我们还应牢记，与其他利益攸关方的接触可大大有助于促进达成共识并落实网络空间负责任行为框架。

最后，我愿借此机会重申，大韩民国将致力于与联合国和所有会员国一道，进一步推动建设开放、安全、稳定、无障碍、和平的网络空间。

附件五十三

罗马尼亚常驻联合国代表团的发言

1. 我们赞赏爱沙尼亚主动组织首次网络安全公开辩论，将其作为联合国安理会议程上的正式具体议题。这是进一步加强以规则为基础的国际秩序的及时倡议，也是我们在维护国际和平与安全这一至关重要的问题上开展多边合作的及时举措。

2. 今天的辩论加强了联合国会员国在上一次政府专家组和不限成员名额工作组的共识报告中在以现有国际法、规范、建立信任措施和能力建设为前提、巩固网络空间负责任国家行为规范框架方面取得的显著进展。

3. 在不断演变的国际安全环境中，信息和电信技术既带来了显著的好处，也带来了当今一些最突出和尖锐的威胁。这些威胁既来自国家行为体，也来自非国家行为体，针对目标是各关键部门，如能源、交通、金融和卫生等，这些部门依赖有形和数字关键基础设施在国内、区域或全球提供服务。数字技术也可能被滥用，试图削弱我们的民主体制，侵蚀公众对民主原则的信任。此外，数字技术还可以被用来为地缘政治目的而利用系统的脆弱性。COVID-19 大流行最近一个可怕的例子，表明旨在破坏或改变疫苗研究和分配的战略信息的网络行动的破坏性影响。

4. 在这种环境下，负责任的国家之间多边合作的价值怎么估计都不为过，加强公共行政部门、私营部门、民间社会和学术界之间的伙伴关系也是如此。我们需要共同努力，共享有关威胁和可信应对措施的可靠、准确、及时、值得信赖的信息，协调努力，加强全球、区域和国家各级的相关防范机制。最重要的是，我们需要集中精力发展我们社会的应对能力，以抵御对我们的关键基础设施——无论是有形、数字还是体制方面的基础设施——的威胁影响。

5. 考虑到这一点，值得注意的是，罗马尼亚在担任民主政体共同体现任主席期间，将积极促进技术与民主进程之间的联系作为其主要优先事项之一；作为在布加勒斯特新成立的欧洲网络安全产业、技术和研究能力中心的东道国，罗马尼亚欢迎并积极促进欧盟成员国和产业界之间计划的共同管理伙伴关系投资；作为新设立的欧洲-大西洋复原力中心的发起国和东道国，罗马尼亚将努力提出新的主张和战略，使社会适应和平、安全和民主稳定面临的新挑战。

6. 作为欧盟成员国，罗马尼亚正在努力推动和实施欧盟新的数字十年网络安全战略的各主要方面，特别是网络外交工具箱，包括欧盟针对恶意网络活动的网络威慑和战略通信工具。欧盟网络外交工具箱在预防、威慑和应对影响欧盟和成员国安全的网络事件方面具有重要作用。

7. 罗马尼亚将网络安全视为国家安全的一个关键方面，努力确保制定和调整适当的国家法律框架，以促进主管当局之间的合作和有效信息交流，并履行其国际义务。负责任的国家行为涉及以下主要积极义务：制定现代和有效的国家立法、网络战略和体制；促进和参与实质性国际合作；非常重要的是，透明度、维护商定的规范、促进民主原则和充分尊重人的尊严。

8. 网络空间的安全是罗马尼亚最高的政治和外交优先事项之一，通过促进负责任国家行为和巩固全球、区域和国家各级的预防性和规范性机制来实现。我们致力于支持一个全面适用人权和基本自由以及法治的全球、开放、安全和有保障的网络空间。我们还认为，无法想象一个开放、安全、稳定、无障碍、和平的网络环境可以存在于在主要以国际法为基础的国际规则体系之外。

9. 罗马尼亚积极参与旨在巩固网络安全框架的两个联合国进程(政府间专家组和不限成员名额工作组)，以便通过商定有关防止网络空间冲突的重要建议(从巩固对网络空间适用国际法的理解，到关于负责任的国家行为的不具约束力的自愿规范以及关于未来制度化对话的建议)，顺利完成工作。

10. 展望未来，罗马尼亚认为，制定《联合国促进网络空间负责任国家行为行动纲领》将推动采取具体的务实措施，以开放、包容、透明和永久的方式进行能力和信任建设，并为获得资金来源提供便利，从而协助联合国所有会员国努力预防冲突，形成对威胁的共同看法，增强网络复原力。

11. 在未来的所有联合国进程中，罗马尼亚将积极宣传其有关国际法适用于网络空间的立场。我们坚信，没有理由认为现行国际法不能适当指导在网络空间/或通过网络空间媒介开展的国家间关系。这包括作为武装冲突(无论是国际冲突还是非国际冲突)一部分实施的网络行动背景下的国际人道法。在这种情况下，网络行动的规划和实施必须符合指导敌对行动的原则，即区分、相称、必要和预防。

12. 然而，促进各国间对话和交流有助于澄清国际法适用于网络空间的一些具体情况。考虑到这一点，我们注意到，罗马尼亚就这一专题发表了初步意见，以便根据大会第 73/266 号决议对政府专家组的工作作出贡献。

附件五十四

塞内加尔常驻联合国代表团的发言

[原件：法文]

首先，我要感谢爱沙尼亚共和国总理卡娅·卡拉斯女士主持这次关于网络安全的重要高级别虚拟公开辩论，鉴于网络空间的安全威胁不断增加，这个主题在联合国系统内变得越来越重要。我还要感谢裁军事务高级代表中满泉女士，我国代表团饶有兴趣地听取了她的通报。

事实很清楚：网络空间恶意行为的扩散是对国际和平与安全的真正威胁，需要安全理事会采取行动。让我们今天聚在一起的辩论表明，安理会意识到这一威胁，辩论是大会十多年来在网络安全问题上持续不懈努力的一部分。

本着这一精神，四个政府专家组和不限成员名额工作组分别就各国在网络空间的负责任行为以及在国际安全背景下的信息和电信发展进行了各种审议。这些审议都是积极的，清楚地表明各国就网络空间监管方式达成共识的意愿。

在承认现有国际法若干原则和规范的适用性并宣布国家对其可能在网络空间实施的国际非法行为的责任时，不限成员名额工作组和最新的政府专家组 2021 年 3 月和 5 月的报告结论是对理解在网络空间行使国际法的又一贡献。

此外，与一些国家一样，塞内加尔认为，建立信任措施和透明度对于促进各国在网络空间采取负责任的行为至关重要，因此应予以加强。

事实上，通过定期交流有关其网络活动的信息，各国可以帮助避免认识上的错误和误解，预防和管理因使用网络空间而产生的危机，并视情况为在数字事务上进行富有成效的合作奠定基础。

尽管如此，由于该部门的巨大变化和新网络威胁的出现，塞内加尔认为，实在国际法规则以及建立信任措施和透明度本身不足以适当监管网络空间，而应辅之以一项具有约束力的国际法律文书。

因此，将自愿建立信任和透明度措施与具有约束力的国际公约结合起来的一般方法将变得十分必要，这不仅是为了制订网络空间规则，而且也是为了顾及所有会员国的立场和利益。2021-2025 年期间，新的信息和通信技术安全和使用问题不限成员名额工作组的审议工作应倾向于这一方法。

塞内加尔政府坚定致力于为这一领域的工作作出积极贡献，自 2017 年 11 月通过《国家网络安全战略》以来，这仍是塞内加尔政府的优先事项之一。这份文件的愿景是在 2022 年在塞内加尔建立一个对所有人来说都值得信赖、安全和具有复原力的网络空间，其中包括对塞内加尔网络安全战略背景的评价，同时考虑到当前和未来的威胁。该文件确定了以下 5 个战略目标：加强网络安全的法律和体制框架；保护关键信息基础设施和国家信息系统；促进网络安全文化；在所有部门建设网络安全能力和技术知识；参与区域和国际网络安全努力。

根据最后一个目标，塞内加尔是第一个加入《非洲联盟网络安全和个人数据资料保护公约》(马拉博公约)的国家。它还加入了《欧洲委员会网络犯罪公约》(布达佩斯公约)和《欧洲委员会关于在个人数据自动处理中保护个人的第 108 号公约》(欧洲条约汇编第 108 号)及其关于监督机构和跨界数据流动的附加议定书(欧洲条约汇编第 181 号)。此外，它还通过了 2011 年 8 月 19 日西非国家经济共同体(西非经共体)关于打击网络犯罪的指令，并批准了 2018 年 11 月 12 日的《网络空间信任与安全巴黎呼吁》和 2019 年 5 月 15 日的《消除网络上恐怖主义和暴力极端主义内容的克赖斯特彻奇呼吁》。

在国内，国家已建立数字监管和使用的法律框架。除了 2008 年 1 月 25 日《关于电子交易的第 2008-08 号法》外，我们还可以提及 2008 年 1 月 25 日《关于信息社会的第 2008-10 号指导法》，2008 年 1 月 25 日《关于网络犯罪和保护个人数据的第 2008-11 和 2008-12 号法》以及 2018 年 11 月 28 日《关于电子通信守则的第 2018-28 号法》；并按照同样的思路，对《刑事诉讼法》进行了修订，以考虑到利用信息和通信技术犯罪领域的程序。

同时，通过设立数据和信息系统安全中央技术服务机构、打击网络犯罪特别司和数据保护委员会，加强体制结构。为实施《2022 年国家网络安全战略》，成立国家网络安全咨询委员会和国家网络安全局，很快将进一步丰富这一结构。

建设网络能力是另一个挑战，对发展中国家来说尤其如此。因此，塞内加尔在提供信息安全培训方面作出了多重努力。目前，国家在该领域设有几个培训机构，其中最引人注目的是 2018 年 11 月开设的达喀尔国家和地区网络安全学校，以及 2015 年 10 月成立的信息安全专业学院。

网络安全不应阻碍新的信息和通信技术提供的创新和发展机会，也不应用于限制这些技术的发展。

作为预防和打击恶意利用网络空间的一种手段，网络安全举措的最终目标应该是促进建立一个无障碍、安全、和平与繁荣的数字环境，并根据《2030 年议程》目标 9 的具体目标 9.c，不让任何人被排除在外。

考虑到这一雄心壮志，塞内加尔政府根据《新兴塞内加尔计划》制定了《2016-2025 年数字塞内加尔战略》。这份文件体现了塞内加尔保持非洲数字创新领先国家地位的雄心，其核心口号是“到 2025 年，塞内加尔将实现人人享有数字服务并用于所有用途，在有效的生态系统中建立充满活力和创新的私营部门。”

附件五十五

新加坡常驻联合国代表布尔汗·加福尔的发言

感谢你召开这次重要会议，这是安全理事会首次正式讨论网络安全问题。

这是一个及时的议题。COVID-19 大流行加快了数字化速度，我们的生活也以新的方式从中受益，同时也给我们带来了新的脆弱性。网络威胁和恶意网络活动正变得更加频繁和复杂，其后果也更加严重。2020 年，恶意网络活动估计造成了近 1 万亿美元的损失。最近此类活动的激增清楚地提醒我们，国际社会必须继续防范和准备应对这些全球和跨界威胁。在这方面，我想强调五点。

首先，我们必须认识到，网络空间从根本上是一个管理全球公域的问题。作为小国，新加坡一贯支持以尊重国际法为根基、以规则为基础的多边体系。我们在网络空间方面的做法也没有什么不同。为维护一个安全、可信任、开放和可互操作的网络空间，我们必须采取基于全球规则和规范以及遵守国际法的全球方法。考虑到地缘政治紧张局势加剧导致全球局势动荡不安的背景下，要做到这一点将是具有挑战性的。然而，我们别无选择，只能继续倡导和支持国际法和规范的适用性，以鼓励国家在网络空间的负责任行为。我们需要加倍努力开展国际合作，以提高网络复原力和稳定性。

新加坡致力于发挥联合国作为唯一普遍、包容和多边论坛的作用，制定管理网络空间的规则。我们对联合国日益成熟的网络安全讨论感到鼓舞。自 1998 年信通技术安全首次被列入联合国议程以来，6 个政府专家组研究了滥用信通技术在国际安全背景下构成的威胁，以及如何应对这些威胁。其中 4 个小组商定了实务报告，其中包括刚刚完成工作的最新版本。

在第七十三届联合国大会上，网络安全讨论首次被提交给广大会员国。这是通过设立关于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(不限成员名额工作组)来实现的。我们对不限成员名额工作组最近顺利通过共识报告感到鼓舞。该报告有助于我们在许多问题上达成共同理解，并确定了需要进行更多讨论的领域。

新加坡积极参加了不限成员名额工作组和最近设立的政府专家组。新加坡还荣幸地当选为新的 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主席。作为该机构的主席，新加坡坚定地致力于在联合国继续就网络安全进行公开、包容和透明的讨论。我们希望，新的不限成员名额工作组的工作将有助于在网络空间建立一个基于规则的多边秩序，并给予所有国家，无论大小，信心、可预测性和稳定性，这对经济进步、创造就业机会和采用技术至关重要。我们期待在这方面与所有会员国密切合作。

第二，所有国家都容易受到恶意网络活动的影响，而这种活动的规模和复杂性正日益增加。但小国尤其脆弱，特别是发展中国家和最不发达国家。如果我们认真对待网络安全的全球方法，我们必须对需要帮助的国家的能力建设保持高度关注。这是联合国可以帮助协调努力的一个领域。新加坡与联合国裁军事务厅合

作，开发了一个对所有联合国会员国开放的在线培训课程，以促进加深对信通技术的使用及其对国际安全的影响的理解。我们仍将致力于与联合国合作并支持联合国提供进一步的能力建设方案。

第三，新加坡认为可以做更多的工作，以促进提高对现有 11 项关于负责任国家使用信通技术行为的自愿、不具约束力的规范的认识和执行。我们支持就执行规范交流最佳做法和经验。这将有助于确定我们应应对的挑战和可能需要额外规范的不足之处。新加坡支持进一步拟订现有规范的工作。例如，针对任何跨境关键信息基础设施(如云端和金融体制)的恶意网络活动可能会对多个国家的基本服务、包括与国际贸易、运输和通信相关的服务造成大范围的中断。各国应考虑如何促进与相关基础设施所有者和运营者开展跨境合作，以加强针对此类基础设施的信通技术安全措施。

这就引出了我要谈的第四点，即加强与其他利益攸关方、特别是私营部门的接触。由于关键信息基础设施的很大一部分归私营部门所有，国际社会必须找到与私营部门密切合作的方法，以防止和减轻这种中断所带来的影响。新加坡支持公共部门与私营部门合作交流最佳做法，以支持强有力的网络安全框架。

第五，新加坡认为，区域组织在支持联合国讨论和协助执行联合国所制定的规则和规范方面发挥至关重要的作用。网络安全是新加坡 2018 年担任东南亚国家联盟(东盟)主席国期间的优先事项。那一年，东盟成为第一个原则上赞同 11 项关于负责任国家使用信通技术行为的自愿、不具约束力的规范的区域组织。东盟目前正在制订一项行动计划，以执行这些规范。在东盟内部，新加坡也一直在支持能力建设方案。东盟-新加坡网络安全卓越中心成立于 2019 年，是一个多学科的能力建设中心，涉及建立信任措施、政策、战略、立法和行动等领域。我们期待与联合国会员国共同努力，加强集体网络能力建设工作。

最后，我要指出，一个安全可靠的数字基础设施必须支撑我们对数字经济的雄心。成员国应以持续、全面、协调的方式共同应对网络安全挑战，这一点比以往任何时候都更加重要。新加坡愿与各国一道，为建设安全、可信任、开放、可互操作的网络空间打造伙伴关系与合作。

附件五十六

斯洛伐克常驻联合国代表米哈尔·姆利纳日的发言

斯洛伐克赞同欧洲联盟的发言。我方想以本国代表身份补充一些意见。

感谢你组织这次及时的讨论，让我们有机会反思网络空间恶意活动带来的日益增加的风险及其对国际和平与安全的影响，并讨论促进网络空间和平与稳定的全球努力。

COVID-19 危机使加强网络空间安全与稳定的必要性更加突出和紧迫。这场危机表明，数字能力已成为提供基本服务和持续进行有效治理的关键。关键基础设施的运作中断可能会造成严重后果。针对重要部门和服务的恶意网络活动会破坏稳定，可能最终威胁到国际和平与安全。

由于网络威胁在很大程度上属跨国性质，保持国家之间以及国家与多方利益攸关方群体之间的国际合作与对话十分重要。只有通过各国政府、私营部门和民间社会共担责任，共同努力，我们才能有效地支持维护网络空间国际和平与安全并保护人权。

联合国在推动国际辩论方面发挥重要作用，提高人们对网络对国际和平与安全的挑战的认识，在促进网络空间负责任国家行为方面取得进展。

斯洛伐克坚决支持多边主义，因为多边主义有助于管理和应对网络空间当前和未来的挑战。我们深信网络空间稳定应基于现行国际法，包括整个《联合国宪章》、国际人道法和国际人权法。正如大会 2010、2013 和 2015 年核准的政府专家组 3 份共识报告所确认的那样，斯洛伐克完全支持现行国际法适用于网络空间中的国家行为。我们将尽最大努力进行透明和建设性的讨论，以便相互借鉴经验、良好做法和专门知识。

斯洛伐克也是不限成员名额工作组内《推动国家在网络空间的负责任行为行动纲领》的共同提案国。我们相信包容性和建设性的机构对话，注重结果、规律和基于共识的方法。在我们看来，《行动纲领》提案为所有联合国会员国开展此类对话提供了依据。

在谈到网络空间的信任措施和能力建设时，斯洛伐克认为，这两项内容是维护网络空间稳定的最重要措施。欧洲安全与合作组织(欧安组织)等区域组织在预防冲突和加强国家间合作方面是非常有用的工具。各国在网络空间方面的定期沟通和互动有助于避免冲突，缓解日益加剧的潜在紧张局势，同时也为对话提供一个平台。

国际法是国家间关系稳定和可预测的主要支柱之一。斯洛伐克坚决支持那些重申现行国际法——特别是整个《联合国宪章》以及国际人道法和人权法——确实适用于国家在网络空间的行动的国家。《联合国宪章》规定了对维持和平与稳定特别重要的国际法规则和原则。毫无疑问，人权在网上和网下都一样适用，各国必须尊重和捍卫这些权利。

附件五十七

斯洛文尼亚常驻联合国代表团的发言

斯洛文尼亚欢迎安全理事会举行首次公开辩论，专门讨论网络安全这一具体专题。讨论网络安全问题对所有成员国都是及时和有益的。安全理事会就这一议题举行公开辩论有助于在国际和平与安全框架内提高认识。在这方面，斯洛文尼亚欢迎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(不限成员名额工作组)和联合国促进网络空间负责任国家行为政府专家组最近达成的共识报告。

斯洛文尼亚赞同欧洲联盟的发言，并谨以本国代表的身份补充几点意见。

我们生活在一个相互联系、瞬息万变的世界。一个全球性的、开放的、自由的、稳定的、安全的网络空间有助于经济和社会效益，但同时也存在恶意的网络活动。对网络空间的滥用可能会影响到重要的经济部门和向公众提供的医疗保健和能源等基本服务及其他基本基础设施。国家或非国家行为体恶意使用信通技术可能破坏各国政府之间的信任，产生负面影响，进而破坏国际和平与安全。

为缓解现有和新出现的威胁，斯洛文尼亚坚信，网络空间的治理应充分尊重现行国际法，特别是整个《联合国宪章》、国际人道法和人权，并执行负责任的国家行为规范和规则。为此，我们的第一个目标应该是促进现行国际法的适用，并将我们的集体努力集中于推动执行现行负责任国家行为规范，包括对在一国管辖范围内运作的私人实体提起刑事诉讼。

负责任的国家行为规范与建立信任和能力建设措施的政策齐头并进。这是我们可以真正有所作为之所在。斯洛文尼亚坚定支持——在联合国 53 个会员国的框架内——有关制订《推动国家在网络空间的负责任行为行动纲领》的提议。《行动纲领》将建立在联合国大会现有成果的基础上。《行动纲领》将提供一个促进能力建设方案的机会，并将在联合国内部提供一个与其他利益攸关方合作和交流最佳做法的体制机制。

此外，在执行负责任国家行为规范时，斯洛文尼亚将继续促进和支持突出反映性别观点，以缩小“数字性别鸿沟”，并让妇女有效和有意义地参与与在国际安全背景下使用信通技术有关的决策进程。

斯洛文尼亚将于 2021 年 7 月 1 日起担任欧盟理事会主席国，将加强在网络安全领域的合作，精简欧盟与西巴尔干地区之间的网络问题。让西巴尔干地区更接近欧洲网络生态系统，是为数字发展、更好的连通性以及更好地进入数字经济和社会构建值得信赖和安全的环境方面的重要因素，也是有助于网络空间的全球稳定。

为此，斯洛文尼亚计划于 2021 年 10 月初组织召开欧盟和西巴尔干非正式峰会。斯洛文尼亚还将与欧盟国际空间站合作，组织一次关于西巴尔干国家的网络安全会议。此外，我们将协助审查与西巴尔干国家在预防和调查儿童性虐待和性剥削方面的合作情况并取得进展。

斯洛文尼亚作为即将上任的欧洲联盟理事会主席国，还将推动欧洲加强网络复原力和网络危机管理的监管工作，审查《网络和信息系统安全指令》(NIS 2 指

令)，概述在整个欧盟范围内实现高度共同网络安全的措施，并努力积极推动实施欧盟网络外交工具箱，以促进预防冲突、缓解网络安全威胁和加强国际关系稳定。我们将努力加强国际合作，减少误解、升级和冲突的风险。

最后，请允许我重申，安全理事会在支持网络安全领域的工作方面发挥核心作用，这对维护国际和平与安全至关重要。通过组织这次公开辩论，你已积极鼓励营造一个促进合作的环境，在信通技术以及全球、开放、自由、稳定和安全的网络空间方面建立信任。

附件五十八

南非常驻联合国代表团的发言

南非饶有兴趣地注意到，联合国安全理事会召开本次公开辩论，首次将维护网络空间国际和平与安全作为专门主题事项进行审议。我还要感谢裁联合国军事务高级代表中满泉女士的通报。

我们进一步注意到为今天的讨论提供的指导性问题，我们将努力在发言中作出回应。

首先，南非要强调，网络空间和平与安全问题是一个普遍而复杂的问题，需要联合国所有会员国的充分参与。正因为如此，我们认为，处理这一问题的适当地点是大会第一委员会的议事程序，该委员会已经在处理这一问题。

在这方面，会员国已通过一些政府专家组的工作进行了参与，其中最新的工作重点是促进网络空间负责任国家行为，在巴西大使吉列尔梅·德阿吉亚尔·帕特里奥塔阁下的干练领导下，于 2021 年 5 月底提出了共识报告。

此外，2019 年以来，联合国所有会员国广泛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，该工作组于 2021 年 3 月底通过了共识报告；并参与新设立的 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，该工作组将由新加坡共和国常驻代表布尔汗·加福尔大使阁下担任主席并提供指导。

因此，联合国会员国在以下方面的讨论取得了长足的进步：网络空间新出现的对国际和平与安全的威胁；规范国际和平与安全这一方面的国际法框架；指导会员国的规范、规则和原则；所需的建立信任措施；能力建设要求；如何在这方面继续对话。

请允许我在这方面简略地提出以下几点意见。

南非认为，面对众多新出现的威胁，有必要让包括民间社会和私营部门在内的所有相关行为体参与进来。因此，必须理解这些威胁的性质以及在全社会范围内开展合作，以应对国家和非国家行为体在网络空间构成的威胁并充分应对这些威胁。

南非强调有必要弥合数字鸿沟和性别鸿沟，并将数字鸿沟转变为数字机会，这是建立复原力同时促进更大发展的关键。然而，有害信通技术事件日益复杂，这是南非等发展中国家关切的问题。

南非仍对关键基础设施和关键信息基础设施受到越来越大的网络攻击威胁感到关切。我们认为我们应通过加强合作和建立最佳做法机制来应对这些威胁，但这些努力应支持国家优先事项以及确定和指定此类基础设施的努力。我们还意识到，尽管面临威胁，但信通技术可能带来的积极经济和社会机会不应因恶意使用这些技术而黯然失色。因此，令人担忧的不是技术本身，而是对这些技术的滥用。

为规范网络空间的使用，特别是对国际和平与安全构成的威胁，南非支持国际法、特别是整个《联合国宪章》的适用性。

鉴于已经做了大量工作，我们认为，我们应侧重于执行现有规范、规则和原则上。发展中国家共有的一项基本原则是，我们还必须认识到，鉴于各国防范网络空间恶意行为威胁的能力各不相同，我们都处于不同的风险境地。因此，我国代表团强调，国家和其他利益攸关方都需要实施能力建设方案，以协助各国打击网络领域恶意行为体破坏稳定的威胁。南非认为，能力建设对于使各国在改善全球网络空间安全方面处于同等地位至关重要，因为这确实是一个全球挑战，需要制订全球解决方案。

最后，南非仍致力于继续参与解决这些问题，特别是在将于 12 月开始实质性工作的信息和通信技术安全和使用问题不限成员名额工作组的框架内进行参与。这将成为一个包容各方的单一轨道，以讨论我们可如何应对网络空间国际和平与安全所面临的复杂和普遍的新威胁。

附件五十九

瑞士常驻联合国代表团的发言

[原件：法文]

感谢爱沙尼亚组织本次公开辩论，并感谢高级代表所作的通报。网络空间已成为我们社会不可或缺的一部分，并为社会和经济发展带来巨大的机遇。与此同时，恶意网络行动构成不稳定风险，已成为对国际和平与安全的威胁。我们感到关切的是，网络空间正被用来投射力量，并变得越来越分散和不稳定。

一个开放、安全、稳定、无障碍、和平的网络空间对所有人都有利。联合国在这方面发挥至关重要的作用。瑞士欢迎最近以协商一致方式通过政府专家组和不限成员名额工作组的报告。这些报告是各国在网络空间采取负责任行为的重要步骤。

为促进网络空间的和平稳定，我想强调几点。

首先，国际法适用于网络空间。尊重国际法是预防冲突和维护国际和平与安全的必要条件。通过和平手段解决争端的义务也适用于各国在网络空间的活动。此外，国际人道法适用于事实上存在武装冲突的情况，无论是国际冲突还是非国际冲突。瑞士欢迎政府专家组的最新报告明确指出这一点。这是一个重要的里程碑。国际人道法及其基本原则对在武装冲突背景下执行网络行动实行重要限制。

其次，瑞士对恶意网络行动的人道主义影响感到担忧，自疫情发生以来，恶意网络行动一直在增加，并且经常涉及医疗基础设施。瑞士强调指出，正如 4 月份的公开辩论所表明的那样，此类基础设施是受到保护的。政府专家组的报告为保护关键基础设施不受恶意网络活动影响提供一个框架。此外，为人道主义目的收集的数据必须受到保护。我们还鼓励各国遵守有关网络空间负责任行为的自愿规范以及政府专家组其他相关执行导则，以避免损害关键基础设施，减轻人道主义影响，并确保保护平民。

第三，建立信任措施对于防止网络空间出现不信任氛围非常重要。在区域层面，瑞士致力于推动欧洲安全与合作组织在促进网络稳定方面发挥作用。瑞士正与德国一起拟订一项关于实施建立信任措施的提案，其中规定在发生严重网络事件时进行磋商。瑞士还致力于透明度和能力建设。我们的国家网络安全中心在发生事件时向其他国家提供技术支持，并分享有关可能威胁的数据和信息。安全理事会和联合国各组织应考虑到已证明有助于促进网络空间和平与稳定的区域倡议和建立信任措施。

最后，民间社会组织、学术界、技术界以及私营部门在支持国际网络稳定方面发挥重要作用，特别是在尊重网上和网下的人权和基本自由方面。瑞士作为自由在线联盟的成员，与 30 多个国家的政府和利益攸关方网络合作，促进互联网上的表达自由。我们鼓励安全理事会和会员国让不同行为体参与执行《网络空间负责任国家行为框架》。

多边合作和遵守国际法，包括遵守人权和国际人道法，对于网络空间的和平与安全至关重要。瑞士鼓励就这些议题进一步开展工作，包括在新的不限成员名额工作组和未来促进网络空间负责任国家行为的行动纲领中开展工作。作为安全理事会候选国，瑞士期待在现有成就的基础上开展多利益攸关方建设性对话。

附件六十

泰国常驻联合国代表团的发言

泰国赞赏爱沙尼亚在此关键时刻，努力组织安全理事会高级别公开辩论：“维护网络空间国际和平与安全”。我们还赞扬爱沙尼亚发挥领导作用，成为第一个举行安理会网络安全正式会议的国家。我们希望，确保和防止滥用网络空间及信息和通信技术(信通技术)将继续在安理会议程上占据重要位置，同时继续欢迎联合国广大会员国参与这些重要讨论。

泰国认为，网络空间造福了人类，这在大流行病期间表现得很明显，它使人们能够获得基本的社会服务，最重要的是，让人们相互联系，并有助于实现《2030年可持续发展议程》。尽管如此，包括恐怖分子在内的国家和非国家行为体将信通技术用于攻击关键民用基础设施等恶意目的，不仅破坏国际和平与安全，而且影响到我国人民的安全。因此，根据相关国际法和规范，各国有责任解决这些问题。

泰国认为，联合国可以在支持努力创建稳定和安全的网络空间方面发挥重要作用。事实上，20 多年来，网络空间安全问题一直在联合国会员国的议程上。最明显的成功是最近以协商一致方式历史性地通过了 从国际安全角度看信息和电信领域的发展不限成员名额工作组(不限成员名额工作组)(2019-2021 年)的报告以及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(政府专家组)(2019-2021 年)的报告。

泰国欢迎新的信息和通信技术安全和使用问题不限成员名额工作组(2021-2025 年)。我们确信，在新加坡常驻代表兼不限成员名额工作组主席布尔汗·加福尔先生阁下的干练领导下，各国将进行富有成效的讨论，包括就加强各国之间的信任、合作和透明度以及进一步拟订网络空间负责任国家行为规范进行讨论。

在新的不限成员名额工作组中，泰国希望以下问题可得到解决或澄清：进一步制订关于如何实施负责任国家行为规范的指导意见和建议；就国际法如何适用于网络空间以及是否存在漏洞达成共同理解；制订可持续的、需求驱动的建立信任措施，并采用“定期机构对话”。

泰国还注意到其他政府间机构、私营部门和民间社会组织和进程所作出的良好努力，以促进我们为建设安全和有保障的网络空间作出集体努力。泰国支持在工作中采取多方利益攸关方办法，以确保包括妇女和青年在内的相关利益攸关方和伙伴切实参与社会。

为此，泰国支持通过加强对商定规范的切实实施，弥合现有的分歧和能力需求，并确保现有多边和双边渠道保持开放以继续对话，从而加强规范基础。所有国家必须继续共同努力，维护我们共同的愿景，即为所有人创造一个开放、安全、无障碍、和平的网络空间和信通技术环境。

附件六十一

土耳其常驻联合国代表团的发言

感谢爱沙尼亚组织本次公开辩论，着重讨论一个重要议题，特别是在当前大流行病造成的情况下。也感谢联合国裁军事务高级代表中满泉女士所作的通报。

信息和通信技术(信通技术)的使用影响到世界各地的经济和发展。大流行病突显了我们对数字技术的严重依赖。确保自由、开放和安全地使用信通技术无疑是至关重要的。

土耳其对日益增多的网络攻击感到担忧。针对关键基础设施的恶意网络活动、恐怖主义、数字间谍、欺诈、网络虐待和剥削儿童以及滥用个人数据等都是当前的威胁，也对国际和平与安全构成风险。

由于技术的发展，网络攻击变得更容易实施，而受害者所承受的负面影响和代价也迅速增加。网络攻击也变得越来越“有针对性的”。网络攻击每年带来的代价正成倍增加。要防御这些攻击，就需要有新的和最新的方法和手段。

土耳其欢迎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(不限成员名额工作组)以及最近联合国促进网络空间负责任国家行为政府专家组的共识报告。这些报告对联合国框架下现有网络安全工作作出了宝贵贡献。同样重要的是，不限成员名额工作组和政府专家组的报告应相互兼容和互补，以提高网络空间的稳定性、复原力和国际合作。我们希望在未来看到这种努力有更多的凝聚力。

随着数字化的快速发展，土耳其一直注重采取必要的措施，以改善其国家网络安全。目前正在实施涵盖 2020-2023 年的《国家网络安全战略和行动计划》。该《行动计划》的主要战略目标是保护关键基础设施和提高复原力、能力建设、有机网络安全网络、新一代技术(即物联网、5G、云计算等)的安全、打击网络犯罪、发展和培育国内和国家技术、将网络安全纳入国家安全、加强国际合作。

此外，土耳其国家网络应急小组在实施和协调防范网络威胁的措施方面发挥至关重要的作用。

培训方案以及国家和国际网络安全演习与我们的努力相辅相成。土耳其信息和通信技术局(信通技术局)提供关于网络安全和其他相关领域的在线公共培训。在过去 4 年里，5 000 多人接受了网络安全不同方面的培训。

每年举办的“互联网安全日”是信通技术局的提高意识活动之一，旨在提高人们对有意识地安全使用互联网的认识。此外，土耳其采取措施应对网络安全面临的更高的数字安全风险，并与相关利益攸关方合作采取措施，以保证在大流行病期间的业务连续性、可及性和对消费者的保护。

我们还采取步骤加强我们的国家立法框架。

鉴于网络风险的跨境性质，加强国际合作至关重要。基于这种认识，土耳其参与网络威胁情报共享，并为包括欧安组织、G20 和经合组织在内的区域和国际

组织内的政策和合作战略作出贡献。土耳其还参加国际演习，包括国际电联和北约内部的演习。

联合国在各国就信通技术使用开展更具战略性和有效的合作方面发挥核心作用。土耳其支持国际法在网络空间的适用性。现在正当其时，我们应该在联合国系统内以前开展的工作的基础上，找到有意义的方法，将网络空间负责任国家行为的规则、规范、原则和建议付诸实施。

我们未来工作的一个优先领域是就国际法如何在网络空间适用达成共同理解。这对于减少误解和促进网络空间的问责确实是必要的。

还需要在会员国之间建立紧急情况沟通渠道，并通过这些渠道分享信息和资源。这将极大地促进建立信任和加快我们的能力建设工作。

此外，我们还需要紧急审查和加强现有国际文书，以加强在云计算、物联网、5G 和人工智能等新技术框架内的合作。

对确保新技术安全的国家监管办法进行调查，并拟订行为守则，以便为国家框架提供指导和参考，这样做可以成为有用的工具。此外，我们需要对威胁建立共同的理解和定义。

在能力建设方面，我们认为，联合国和区域组织可以推动网络安全专家交流方案，建立共同的培训平台。必须鼓励开展国际演习，以加强国家网络事件的准备和应对能力。

由于网络空间是一个无国界领域，网络安全是一个多利益攸关方问题，国家当局需要与用户、私营部门、非政府组织和国际对口单位合作，以打击网络威胁。全球供应商、服务提供商和安保公司也应与各国政府和国际组织更有效地合作，为全球网络安全作出贡献。

土耳其承诺继续参与和对话，以促进区域和全球网络安全。

附件六十二

乌克兰常驻联合国代表团的发言

感谢爱沙尼亚发起召开安全理事会如此重要的会议，并感谢裁军事务高级代表中满泉夫人所作的通报。

信息和通信技术的飞速发展逐渐导致互联网空间的“重新格式化”：如今，它不再是一个舒适的交流平台，而是一种真正的武器，在黑客、犯罪分子、某些国家行为体及其代理人手中变得越来越危险。

令人遗憾的是，尽管在国家、区域和国际层面上建立了打击网络犯罪的现有法律规范和体制机制，但现代数字世界的优势往往被滥用，网络攻击呈上升趋势，已成为混合战争的新方法。

国际政策越来越容易受到网络威胁。在过去几年里，世界上一些国家已成为网络攻击有利可图的目标。

自 2014 年以来，网络攻击成为破坏我国主权的外部企图的主要因素之一。乌克兰因此深受其害。2014-2021 年期间，乌克兰面临数量空前的针对我们关键基础设施重要目标的网络行动。其中大部分攻击是由俄罗斯联邦控制的黑客组织实施的。

针对主要关键基础设施、能源、运输、石油和天然气部门的网络行动是对国际和平与安全的挑战和威胁。最近，科洛尼尔管道运输公司成为网络攻击的对象，严重影响了管理管道的计算机设备，造成严重的后果。

在 COVID-19 大流行的时候，恶意网络行动的破坏性影响是显而易见的。一些国家和非国家行为体滥用全球危机发起网络行动，包括针对卫生部门的行动，这是国际社会迫切关切的问题。

然而，不仅是关键基础设施，而且国际政治也越来越容易受到恶意使用越来越复杂和先进的信通技术能力的影响，克里姆林宫黑客对重大竞选活动和候选人的履历进行干扰的头条新闻证实了这一点。

因此，网络稳定已成为确保更广泛和平与安全的重要组成部分，因此要求严格遵守国际法，最近在不限成员名额工作组和政府专家组报告中重申了国际法在网络空间的适用，并要求适当实施有关负责任行为的规范、规则和原则以及加强国际合作，以维护自由、开放、稳定和安全的网络空间。

我们强调，应特别注意拟订打击网络威胁的统一标准，分享最佳做法，在网络安全领域建立互信，防止网络空间被用于政治、恐怖和军事目的，并提供财政和技术援助，以提高国家抵御网络威胁的能力，缓解风险，增强韧性。

如今，针对关键基础设施和政府机构的网络行动以及可能煽动恐怖主义的虚假信息运动，是干涉包括乌克兰在内的主权国家内政的一种广泛使用的方法。

毫无疑问，俄罗斯利用高科技来实现自己的政治和地缘政治目标，即通过支持和加剧邻国的冲突，进行侵略性的信息战。

我们强烈鼓励国际社会在确定某个国家或国家行为体为敌对目的准备或实施有针对性的恶意使用信通技术或传播谎言的情况下，彻底考虑问责问题。

毕竟，如果没有可靠的机制来发现、惩罚并将负责协调和资助全球网络空间非法活动的个人和相关国家绳之以法，那么在这一领域所作出的国际努力就是徒劳的。

附件六十三

阿拉伯联合酋长国常驻联合国代表团的发言

COVID-19 大流行突显了世界对信息和通信技术的依赖，这些技术对于保持我们了解情况和相互联系至关重要，即使我们仍然相距甚远。

在过去 18 个月里，我们看到针对医疗设施的恶意网络行动有增加的趋势，包括针对致力于疫苗研究和开发以抗击 COVID-19 的组织的行动。我们身处于一个动荡的地区，而中东也不能幸免于恶意网络活动带来的风险——它往往是重大网络行动和间谍活动的目标。在过去几年里，我们地区发生了影响电信、银行和公共部门的严重事件。石油和天然气设施也成为袭击目标，造成数亿美元的破坏。这种针对该地区关键基础设施的恶意网络活动有可能在本已紧张的环境中引发冲突，并对国际和平与安全构成威胁。

阿联酋致力于建立必要的基础设施和机制，以增强其网络安全能力，这样既保护自己免受网络威胁，也可以更好地与其他国家合作，应对共同的挑战。2020 年 11 月，我们成立了阿联酋网络安全委员会，以便制订国家网络安全综合战略和国家网络事件应对计划。我们主办了最大规模的网络安全和数字转型会议，包括 GITEX、GISEC 和 Cybertech，以建设国内能力，我们还建立一个公私合作平台，以促进信息共享。我们还与各国、国际组织和私营部门实体合作，在政策和技术层面共享信息。例如，阿联酋为海湾合作委员会新的恶意软件分析联合平台等区域组织的工作作出贡献，并且是伊斯兰合作组织计算机安全事件应急小组的现任成员。这些合作性透明度建立信任措施是阿联酋为减少国际和平与安全面临的网络风险所做的一些努力。

阿联酋欢迎信通技术问题不限成员名额工作组和政府专家组报告中的建议。这些报告着重指出，必须支持进一步实施网络空间负责任国家行为自愿规范的努力，并需要就国际法对网上活动的适用性达成共同理解。但还需要做更多的工作，既要鼓励和支持各国执行这些建议，也要在快速变化的环境中提供进一步的指导。《网络空间负责任国家行为行动纲领》为今后的工作提供了理想的路线图，并将有助于应对国际和平与安全面临的网络风险。

将国际和平与安全面临的网络风险降至最低仍将是一项挑战。阿联酋提出了两项有助于完成这项任务的建议。

首先，各国应在双边、区域和国际各级提供培训和能力建设，包括通过培训方案和制订指导意见，以协助实施负责任国家行为规范。这些行动可以作为建立信任措施，应对国家之间在网络空间的不信任和误解，因为这种不信任和误解可能对国际和平与安全构成风险。

其次，各国应继续与秘书长分享其观点和评估，并积极参与与网络有关的国际论坛和跨区域模式。分享最佳做法和交流经验可以帮助各国适应不断发展的规范，成为网络空间负责任行为体。

所有国家都有责任在线上和线下促进国际和平与安全。遵守负责任国家行为规范和履行国际法规定的义务是最好的起点。