联合国 S/PV.9662 (Resumption 1)

安全理事会

第七十九年

临时逐字记录

第九六六二次会议

2024年6月20日星期四下午3时举行

纽约

主席:	赵炫禹先生	（大韩民国）
成员:	阿尔及利亚	卢阿费先生
	中国	王振江先生
	厄瓜多尔	杜朗·梅迪纳先生
	法国	斯特雷海亚诺先生
	圭亚那	帕尔马南德女士
	日本	铃木先生
	马耳他	西斯卡尔迪先生
	莫桑比克	伊拉尚德·古维亚先生
	俄罗斯联邦	德尔加乔夫先生
	塞拉利昂	申克斯先生
	斯洛文尼亚	Burkeljc先生
	瑞士	斯特里特先生
	大不列颠及北爱尔兰联合王国	佩奇女士
	美利坚合众国	吴女士

议程项目

维护国际和平与安全

应对网络空间不断演变的威胁

2024年6月7日大韩民国常驻联合国代表团给安全理事会主席的信（S/2024/446）

24-17607 (C)

下午3时05分开会。

主席（以英语发言）： 我谨提醒所有发言者将发言时间限制在三分钟以内，以便安理会能够快速开展工作。麦克风颈圈上的灯将在三分钟后闪烁，提示发言者结束发言。

我现在请古巴代表发言。

加拉·洛佩斯先生（古巴）（以西班牙语发言）：信息和通信技术的使用必须完全用于和平目的，以促进各国人民之间的合作和发展。

古巴坚决反对网络空间军事化，反对将信息和通信技术用作使用或威胁使用武力，或用于旨在干涉他国内政的行动的工具。《联合国宪章》第五十一条并不适用，也不能在网络空间问题上援引。因此，令人担忧的是，一些国家在其国家安全战略中纳入了使用网络武器和可能发动网络攻击的内容，据称是为了威慑敌国。

必须采取一切必要措施，防止滥用信息和通信技术以及媒体平台，包括社交网络、电台和电子广播，作为违反国际法宣扬仇恨言论、煽动暴力、发动颠覆、破坏稳定、传播虚假新闻和歪曲国家现实以达到颠覆和干涉目的的工具。个人、组织和国家秘密和非法利用国家信息技术系统对第三国进行网络攻击也是不可接受的。

古巴主张在联合国框架内谈判并尽快通过一项具有法律约束力的国际文书，以填补网络安全方面的重大法律空白，并通过国际合作等方式有效应对这一领域日益增多的挑战和威胁。为投资于发展中国家信息和通信技术基础设施的安全，有必要克服巨大技术差距和强加给发展中国家的障碍，因为它们限制了这些国家应对威胁的能力。

大会第一委员会授权设立的信息和通信技术安全和使用安全不限成员名额工作组是就我们各国所面临威胁和挑战进行交流和达成一致的适当机制，这些威胁和挑战涉及恶意使用信息和通信技术。该工作组是一个包容、民主和透明的论坛，所有会员国都可以在其中平等地为在这一领域找到以协商一致为基础的解决方案作贡献。

主席（以英语发言）：我现在请巴林代表发言。

萨勒曼女士（巴林）（以阿拉伯语发言）：首先，我谨欢迎大韩民国外交部长赵兑烈先生阁下主持今天上午的公开辩论会，并感谢大韩民国常驻联合国代表团举行本次会议，讨论由于网络空间的重大事态发展而越发重要的一个话题。我还谨感谢联合国秘书长安东尼奥·古特雷斯先生阁下和其他通报人的宝贵发言。

网络空间的恶意活动、如勒索软件攻击、加密货币盗窃以及窃取敏感信息与资产等构成的风险与日俱增，不仅危及关键基础设施的安全，而且加剧全球稳定已经面临的挑战。这些活动充当了成倍增加威胁的强大工具，增加传统的安全关切，并且形成新的脆弱性。数字系统彼此互联的性质意味着，网络事件可迅速升级成为国际性危机，破坏国家间的信任与稳定。

巴林王国强调多层面做法的重要性，这种做法包括利用现有的创新工具、平台、框架以及战略，来减少与网络威胁有关的风险，此外还要让所有利益攸关方参与进来，因为网络工具和网络技术已不再是政府专有的领域。巴林王国还强调能力建设与分享技术、知识以及最佳做法的重要性，以增强国家防止和应对网络事件的能力。

在此背景下，巴林王国支持大会在加强合作以维护网络安全方面的多项举措，其中包括 政府专家组、信息和通信技术安全和使用安全不限成员名额工作组以及《推进从国际安全角度使用信息和通信技术的负责任国家行为的行动纲领》。

在国家一级，巴林王国高度重视在一项全国综合战略的支持下，在明确的网络安全治理系统的基础上实现网络安全。我们还成立了国家网络安全中心，通过制订有效的治理标准，提供防御、监测和应对电子攻击的手段，以及提高个人和机构的认识，从而在巴林王国提供安全的网络空间。

国家网络安全战略加强了区域和国际伙伴关系。该战略查明了五个根本支柱，每个支柱都 是实现巴林王国网络安全愿景的一个至关重要且必不可少的组成部分。这些支柱结合在一起，组成了一个维护安全可靠的网络空间的全面和具有凝聚力的框架。这些支柱首先是强有力的具有韧性的网络保护机制；其次，它们是有效的网络安全治理和标准；第三，它们构筑了一个有网络安全意识的社会；第四，它们通过伙伴关系与合作加大了保护力度；以及第五，它们培养了国内骨干。

最后，鉴于与信息和通信技术有关的动态引发不断演变的威胁，巴林王国期待在联合国、尤其是安全理事会就网络安全问题进行更多富于成果的对话。

主席（*以英语发言*）：我现在请波兰代表发言。

什切尔斯基先生（波兰）（*以英语发言*）：数字技术、包括电子政务的发展与实施以及对关键基础设施资源的电子行政管理遍布世界各地，导致对网络空间的依赖日益增多。这对国家的安全与主权构成严重挑战。我们日复一日地看到，非国家行为体和国家行为体在网络空间开展越来越多的恶意活动，把国家和社会的稳定与安全作为攻击的目标。

波兰秉持国际法适用于网络空间的国家立场，将其作为保障国际和平与安全的首要措施。在这方面，有两点对于我国至关重要。第一点是，在某些情况下，网络空间的行为构成对禁止使用武力的违反。第二点是网络攻击可被定性为武装攻击。就我们而言，自卫权适用于网络空间。

我们常常面临的一个挑战涉及网络攻击的归因。无论如何，我们不得放弃把肇事的国家与网络罪犯绳之以法的努力。重要的是要认识到，有些国家不是打击在其领土上活动的网络罪犯，而是美化和保护他们以谋取政治或经济利益，由此破坏它国的稳定与安全。它们企图模糊得到国家支持的行为体和以犯罪为动机的行为体之间的界线，并且在目标实体试图保护自己、追究肇事者责任时，给这些实体制造含混不清。

与此同时，大批国家具备执行国际法和自愿规范的政治意愿，但是有可能缺乏这样做的必要能力。与这些国家密切合作，帮助它们，并且提供充分和有针对性的能力建设符合我们的共同利益。这一切不会一夜之间发生。因此，我们需要联合国框架内开展这种合作的一个常设平台。在此背景下，根据以欧洲联盟名义所做的发言，波兰大力支持制订行动纲领。我们鼓励联合国所有会员国支持该行动纲领，并为其落实做出积极贡献。

网络攻击和恶意活动寻求破坏国际和平与安全。因此，我们呼吁安全理事会加大力度，制止和防止网络空间的恶意活动。我们还想呼吁安理会的一个成员国——俄罗斯联邦——遵守国际法，不仅停止在实地对乌克兰的非法侵略，而且停止在网络空间和针对其邻国的侵略。

主席（*以英语发言*）：我现在请罗马尼亚代表发言。

费鲁策先生（罗马尼亚）（*以英语发言*）：我谨感谢大韩民国举行关于一个如此重要的话题的辩论会。

我谨发表几点意见，以补充以欧洲联盟名义所做的发言。

网络空间的威胁持续存在、错综复杂，具有破坏性，并且变得更加频繁。罗马尼亚对针对政府机构和民主进程的恶意网络活动数量之多感到震惊。这是一种严重威胁——网络行动往往与虚假信息相结合，可破坏民主进程的完整性和我们社会的整体韧性。

我们还对关键基础设施和基本服务遭到网络攻击、由此可能受到干扰与破坏性影响感到担忧。我们强烈谴责意在破坏我们的民主机构、国家安全与自由社会的恶意网络活动。网络空间不负责任的行为给国际和平与安全带来风险，是不能容忍的。安全理事会有权处理这些问题，并鼓励加强问责。

国际法适用于网络空间。在网络空间，国家负有根据国际法、包括 《联合国宪章》负责任地行事的义务。我们鼓励安全理事会谴责网络空间的恶意行

为。国家以不符合国际法和不遵守联合国负责任地使用信息和通信技术（信通技术）国家行为框架所规定义务的方式使用信通技术的任何做法有损国际和平与安全。

增强安全理事会的作用，以一种与信通技术方面的其它联合国进程相辅相成的方式处理网络威胁，对于维护网络空间的和平与安全既是及时的，也至关重要。本次公开辩论会和先前于2023年5月和2024年4月召开的阿里亚模式会议确认了安全理事会可做出的重要贡献。

罗马尼亚高度重视加强网络空间复原力的必要性。我们需要加强对国家关键基础设施的保护，因为恶意行为体企图严重扰乱我们社会的运作。我们仍然致力于国际反勒索软件倡议，并期待它得到加强，成为应对这一系列威胁的协调一致的国际对策。此外，网络空间本身的性质要求各方对人工智能技术加剧网络攻击规模和复杂性的潜力进行前瞻性讨论，同时防止和更迅速地对抗网络攻击、乃至减轻其影响。

最后，我们呼吁所有国家尊重其维护国际法的国际义务和承诺，并在网络空间负责任国家行为的商定框架内行事。我们必须忠于我们的核心价值观和原则，并以负责任的方式行事。

主席（*以英语发言*）：我现在请奥地利代表发言。

普雷特霍夫先生（奥地利）（*以英语发言*）：奥地利要感谢大韩民国召开今天这场及时的公开辩论会。

奥地利赞同以欧洲联盟的名义所作的发言。我要以本国代表的名义补充以下几点。

主席先生，为了回答你关于安全理事会作用的指导性问题，我们认为，通过我们都赞同的共同语言即国际法来进行这场辩论可以使概念更加清晰。所有会员国一致商定，国际法，尤其是《联合国宪章》，完全适用于网络活动。《宪章》很明确：它授权安全理事会对国际和平与安全的威胁作出反应。为了履行任务，安全理事会必须继续应对国际和平与安全受到的当代威胁。同样重要的是，要强调《宪章》第六章规定的安全理事会在和平解决争端方面的作用。网络活动不是发生在一个单独的虚拟网络空间，而是在现实世界中。因此，网络活动并不构成一个需要自己的新规则或特别适用国际法的新领域。归根结底，安理会负责应对国家行为。只要与安理会的任务授权相关，它就不应回避某种形式的国家行为——网络活动——这完全顺理成章。例如，关于制裁，所有旨在违反安理会决定的具有约束力的制裁的活动，包括网络活动，都值得安理会关注。在这方面，将网络安全纳入安全理事会所涉问题的主流至关重要。

奥地利致力于网络环境内外的法治，最近发表了关于网络活动和国际法的立场文件。奥地利欢迎今天的辩论会，它强调了安全理事会在履行《联合国宪章》规定的应对国际和平与安全威胁的任务方面的重要作用。

主席（*以英语发言*）：我现在请哈萨克斯坦代表发言。

乌马罗夫先生（哈萨克斯坦）（*以英语发言*）：我谨表示，我们感谢大韩民国组织今天这场非常重要的会议。

数字化的步伐比人类历史上任何一次创新都更快。在短短二十年里，数字技术改变了社会，影响了发展中国家大约50%的人口。通过利用技术改善连通性和获得金融、商业和政府服务的渠道，可以显著减少人们的不平等。医疗保健行业正在利用先进技术，使用人工智能来拯救生命、诊断疾病和延长预期寿命。虚拟学习环境和远程教育的出现使学生有可能参加以前无法参加的课程。

与此同时，信息和通信技术（信通技术）正被包括犯罪集团和恐怖分子在内的许多非国家行为体用于身份盗窃、欺诈和网络攻击。它们还被用来制造不和，传播错误信息，破坏国家稳定，破坏国家间的信任。网络空间的恶意行为可以破坏能源、交通和通信等关键基础设施，因此可能成为现有冲突的威胁倍增因素，这要求安全理事会的介入。这证实了网络威胁正成为地缘政治挑战的趋势。

在这方面，哈萨克斯坦支持通过制定普遍接受的使用标准，对使用信通技术和人工智能采取全球通用的负责任方法。我国的专家正在积极参与信息和通信技术安全和使用问题不限成员名额工作组以及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特设委员会的工作。我们支持5月份推出的全球政府间联络点名录。同许多会员国一样，哈萨克斯坦目前正在为该名录指定外交和技术联络点。

最后，我要强调，在地缘政治不稳定的情况下，重要的是避免将问题政治化，要寻求共同立场。安全理事会可以在协调国际作出努力和实施具体措施以应对网络威胁方面发挥关键作用，包括以下方式：支持各国的能力建设举措，特别是在发展中区域；提高它们预防和应对网络事件的能力；让非国家行为体参与，包括技术公司和民间社会组织；加强应对网络风险的集体努力；当然，还有提高对网络安全问题的认识，并组织对不断变化的网络威胁形势的定期审查。

主席（*以英语发言*）：我现在请伊朗伊斯兰共和国代表发言。

伊拉瓦尼先生（伊朗伊斯兰共和国）（*以英语发言*）：主席先生，我感谢你召开了这场公开辩论会。

要应对信息和通信技术（信通技术）环境中不断变化的威胁，需要采取包括技术、法律和合作战略在内的多层面办法。

伊朗一直是针对我国基础设施的大量网络攻击的主要目标和主要受害者，这些攻击严重扰乱了公共服务和政府职能。一些明显的例子包括对伊朗和平核设施的“震网”和“毒曲”攻击，以及对关键工业基础设施，如钢铁和石化行业以及加油站的网络攻击。这些恶意活动凸显了信通技术环境被武器化，从而对国家基础设施造成破坏的可能性。

鉴于信通技术治理的复杂性，我想强调以下几点。

第一，维护安全、有保障和值得信赖的信通技术的首要责任在于各个国家。必须加强和确保各国在全球层面信通技术环境治理中的突出作用和积极参与，特别是在政策和决策方面。信通技术治理的发展方式不应对各国决定自身发展、治理和信通技术环境立法的权利产生不利影响。各国必须按照国际法的基本原则，尤其是联合国的宗旨和原则，负责任地采取行动。

第二，缺乏普遍具有法律约束力的信通技术规范仍然是一个挑战。当前的国际法往往落后于技术变革的快速步伐，为恶意行为体制造了可乘之机。因此，制定和执行针对信通技术环境具体特点、并且具有法律约束力的国际规范至关重要。

第三，各国必须避免使用信通技术进步作为经济、政治或其他胁迫措施的工具，包括针对其他国家的限制或封锁措施。它们还必须防止和避免滥用在其控制和管辖下的与信通技术相关的供应链，确保这些供应链不会出现危及其他国家主权和数据保护的薄弱环节。各国必须确保对在其管辖范围内具有域外影响的信通技术公司和平台采取适当措施，并让追究其在信通技术环境中的行为的责任，特别是在它们侵犯其他国家主权、安全或公共秩序的时候。

第四，我们坚信信息通信技术环境必须完全用于和平目的。为此，联合国必须通过信息和通信技术安全及和使用不限成员名额工作组继续发挥核心作用，制定具有法律约束力的义务，防止出于恶意目的使用信息通信技术，继续使这一领域仅用于和平目的。

主席（*以英语发言*）：我现在请巴基斯坦代表发言。

阿克兰先生（巴基斯坦）（*以英语发言*）：我们感谢大韩民国代表团召开本次重要辩论会，讨论应对网络空间中不断演变的威胁问题。我还要感谢秘书长和其他通报人的富有见地的发言。

信息通信技术（信通技术）的应用为社会经济发展做出了巨大贡献。然而，这些技术也扩大了冲突范围。网络战，包括国家和非国家行为体发动的信息战以及实际网络攻击，已成为战争的一个新的重要领域。巴基斯坦认识到不断变化的网络威胁形势的严重性及其对国际和平与安全的影响。我们还认识到迫切

需要应对网络空间中的其他恶意活动，包括勒索软件和盗窃敏感信息。

包括巴基斯坦在内的一些国家是虚假信息的受害者。总部位于布鲁塞尔的欧盟虚假信息实验室在其2019年和2020年报告中揭露了针对巴基斯坦的反巴宣传和虚假信息活动以及网络战行为。2019年的报告提供了15年来针对巴基斯坦的大规模行动的证据，涉及10多个以欺骗手段获得人权理事会认证的所谓非政府组织、750多个假媒体机构和550个假网站，甚至就连死人都复活了。这是一场由国家主导的系统性运动，旨在传播虚假信息并滥用联合国和欧洲机构，目的是诽谤巴基斯坦。欧盟虚假信息实验室揭露的这一虚假信息活动需要全球关注。我们必须制定各种方式，防止此类非法和公然滥用网络工具来宣扬敌对国家言论和目标的做法。

2021年12月，大会以协商一致方式通过了巴基斯坦提出的题为“打击虚假信息以促进和保护人权和基本自由”的第76/227号决议。该决议确认各国有责任制止散布破坏促进各国间和平与合作的虚假信息。作为持续恶意网络宣传和其他宣传的受害者，巴基斯坦仍然致力于打击虚假信息这一病毒。我们将通过国际合作，包括在安全理事会内的合作，来推动就此采取行动。

我们承认安理会在应对挑战国际和平与安全的具体网络威胁方面发挥着重要作用，但我们认为，信息和通信技术安全和使用不限成员名额工作组最适合促进国际合作以及以协商一致方式应对信息通信技术快速发展带来的挑战和机遇。

《联合国宪章》明确敦促各国遵守主权、领土完整、不使用武力和不干涉各国内政的原则。这些原则应作为网络治理的指导框架。

然而，只是说国际法适用于网络空间还不够。巴基斯坦和其它国家一样，认为必须针对信息通信技术的独特属性制定一项具有法律约束力的国际文书，才能提供网络空间稳定和安全所不可或缺的监管框架和治理机制。这样的法律和制度框架应照顾各方关切和利益，并在联合国范围内以及所有国家平等参与下进行谈判。

妥当的建立信任措施，例如自愿交流信息和最佳做法，有助于提高网络空间的透明度和可预测性，减少误解的可能性，从而降低冲突风险。上个月启用的信息通信技术安全问题全球联络点名录是促进各国在信息通信技术安全领域信任与合作的重要一步。我们必须以此类机制和合作为基础，加强网络安全，确保信息通信技术能力充分用于经济社会发展。

主席（*以英语发言*）：我现在请乌拉圭代表发言。

冈萨雷斯夫人（乌拉圭）（*以西班牙语发言*）：我们欢迎秘书长今天上午与会，也欢迎网络和平研究所首席执行官以及利兹贝克特大学法律和技术教授、非洲联盟网络安全专家组副主席的发言。

我们认为安理会现任主席大韩民国召开本次公开辩论会非常及时。本次辩论会突出了这一问题，并丰富了关于这个对国际和平与安全议程至关重要且与本组织职权范围内许多其他问题密切相关的问题的对话和讨论。乌拉圭支持这一举措和其他类型的举措，它们旨在针对恶意使用信息和通信技术（信通技术）对全球和平、安全与稳定造成的破坏性影响采取积极行动。

没有任何地区或国家可以免受这种不分国界的危险。大多数会员国都遭受过这种性质的攻击，这使网络空间成为一个不安全的地方，并进一步加剧了困扰我们社会的祸害，例如恐怖主义、贩毒、人口贩运和关键基础设施遭受攻击等。

今天上午，我们认真听取了秘书长的讲话，我们赞同数字技术用作武器的危险正在增加的看法。我们还谴责使用人工智能加剧网络空间威胁，以及以类似方式使用会进一步增强伤害能力的量子技术。

乌拉圭提倡自由、开放和安全地使用网络空间，从而能够发展技术的积极方面和互联网的使用——这是一种积极做法，使我们能够实现可持续发展目标，

促进国际贸易, 继续取得可增进我们民众福祉的科学和医学进步。

为此, 我们必须要有提供这种安全性的具体工具和安全监管框架。然而, 实际上, 由于构成网络安全的技术发展水平不同, 并非所有国家和地区都能够以同样的方式应对这些网络威胁, 或是使自己免遭这些威胁。

在这方面, 我们对能力建设和国际合作方面缺乏重大进展感到关切。发展中国家比以往任何时候都更需要转让有效应对恶意使用信息通信技术带来的挑战所需的技术、知识、良好做法和设备。

在网络空间产生的不利环境中, 联合国在国际和平与安全方面发挥着根本作用, 而国际和平与安全是任何繁荣的先决条件。

在这方面, 我们着重强调大会通过第一委员会发挥的作用。我们重视并支持信息和通信技术安全和使用安全不限成员名额工作组的工作, 就像我们过去重视并支持从国际安全角度促进网络空间负责任国家行为政府专家组的工作一样。他们的工作产生了关于国家负责任行为的建议和标准化规范, 形成了可作为参考的共识基础, 为进行讨论和辩论提供主要论坛。各国也有责任适用所产生的这些规范和基础。

随着技术的进步, 各种组织也必须持续动态发展。它们必须不断发展并通过一个常设机制应对这些不断演变的事态带来的挑战, 从而改善其体制框架和治理。它们必须避免重复, 并最终走向适用于所有国家的强制性规则。网络空间不能免受国际法和国际法规的约束, 这为我们提供了法律确定性。

我们借此机会表示, 即将举行的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特设委员会届会十分重要, 这项公约也称网络犯罪公约。我们希望它能尽快获得通过, 并希望各国据此制定国家标准。我们认为, 这是本组织在这方面可以采取的积极步骤。

最后, 我要重申加强网络复原力和能力建设的重要性, 这是本组织大部分机构的共识, 而区域组织在其中发挥着关键作用。我们重视并赞赏各个国家的支持, 这些国家建立了合作方案, 推动开展培训, 培养能够应对网络空间相关挑战的技术人员和专业人员, 我们敦促这些国家继续沿着这条道路前行, 这无疑将促成一个对所有人都更有益的网络生态系统——一个基于国际合作而不是对抗也不是将这些问题政治化的网络生态系统。

与其他领域一样, 安全理事会和大会在应对网络威胁方面发挥协同作用至关重要。像这样的定期通报会和辩论会十分必要, 有利于采取有效行动, 打击在整个国际安全领域, 包括在冲突中滥用技术的行为, 从而亦促进在网络空间相关方面保护平民的工作。

主席先生,我感谢你将这一项目列入今天的议程。

雅尼娜夫人(阿尔巴尼亚)(*以英语发言*): 在今天的数字化世界中, 网络安全对所有会员国来说都是一个重要问题。我们要感谢主席国韩国在安全理事会召集本次重要讨论, 感谢各位通报人提供了有用意见。

我们许多人都曾遭遇过某种形式的网络攻击。我们看到, 这些恶意活动不仅影响到我们各国公民的日常生活, 而且更广泛地说, 极大影响到整个国际社会, 直接危及国际和平与安全。网络攻击越来越多, 对不同地区国家产生了严重的负面效应, 国内生产总值减少, 其中发展中国家最易受影响。

随着网络威胁更加复杂多样, 我们的应对应是灵活敏捷的。通过促进国际合作和信息共享, 我们应当有能力制定这种应对措施, 减轻我们单独和集体面对的网络威胁。两年前, 阿尔巴尼亚成为多个伊朗伊斯兰共和国关联黑客团体所发动空前大规模网络攻击的目标, 其明确目的是摧毁政府基础设施, 使公共服务瘫痪, 在我国制造混乱和不安全。我们仍然是复杂网络攻击的目标。

在这方面, 阿尔巴尼亚正投资于国家网络复原力, 同时高度重视区域和国际网络安全办法。我们所

在的西巴尔干地区继续面临越来越多的持续演变的网络威胁。我们正通过网络安全、网络犯罪和网络外交等方案努力建设本地区的网络能力。将于7月在我国阿尔巴尼亚举行的网络安全地区峰会将寻求加强西巴尔干地区的网络复原力。

我们坚信，国际一级可以且应该做更多的工作。

在这方面，我要着重强调三个要点。

第一，安全理事会作为维护国际和平与安全的主要机构，可以且应该更多地参与其中。安理会是讨论网络威胁和应对方法的有益平台。讨论应具包容性，对不同行为体开放。在这方面，我们认为政府与私营部门之间的合作为加强防御网络威胁增添价值。

第二，在我们共同建设安全网络空间的工作中，应更加重视追究恶意国家和非国家行为体的责任。这与尊重网络空间负责任行为国际准则是相辅相成的。

第三，有必要加强能力建设。发达国家拥有强大而稳固的网络态势，而许多发展中国家缺乏应对网络威胁的资源和专门知识。这可能导致关键基础设施出现危险漏洞，极易遭遇网络攻击、网络间谍和其他破坏性活动。

最后，请允许我再次重申，只有在全球一级共同努力，才有可能实现安全的网络空间，本次会议是朝正确方向迈出的一步。

主席（*以英语发言*）：我现在请希腊代表发言。

瑟克里斯先生（希腊）（*以英语发言*）：首先，我要感谢大韩民国组织这次非常重要的高级别讨论，我还要感谢我们的通报人所作耐人寻味的发言。

希腊完全赞同欧洲联盟代表团代表早些时候所作发言，并愿以本国名义发表以下看法。

我们这个时代的数字发展是人类进步的催化剂，改变了我们的社会和经济，扩大了合作机会。新兴技术为人类提供了经济增长以及可持续和包容性发展的重大机遇，涉及到本组织工作的所有三大支柱：和平与安全、人权和可持续发展。

随着我们的经济、民主和社会比以往任何时候都更依赖安全、可靠和日益互联的网络和信息系统，网络安全是建设开放、自由、稳定、安全的全球网络空间的关键。

与此同时，恶意利用这些技术已成为新的风险和挑战的来源。近年来，网络空间恶意行为有所加剧，包括针对关键基础设施、供应链和知识产权的网络攻击持续激增，针对政府、组织、企业和公民的勒索软件攻击数量上升。

此外，更令人震惊的是，网络攻击正成为武装冲突中行动的组成部分。希腊对此类活动深表关切，这些活动破坏国际和平与安全，可能导致不稳定和连带影响，增加冲突风险。

然而，网络空间并非法外之地。作为被称作“网络空间负责任国家行为框架”的一部分，所有国家一致认为，现有国际法，特别是《联合国宪章》,适用于维护和平与稳定，且不可或缺。在这一领域，国际法必须像适用于国际关系所有其他领域一样得到维护和执行。

由于安全理事会对维护国际和平与安全负有主要责任，我们希望它今后将在涉及新威胁和现有威胁的问题上发挥更积极的作用。这种作用可包括努力加强上述负责任国家行为框架和应对不符合维护国际和平、稳定与安全目标的网络活动。

作为坚决支持国际法至上地位以及和平解决争端的国家，我们重申对和平、安全网络空间的愿望，我们完全致力于进一步讨论这一非常重要的议题，包括在我国担任安全理事会2025-2026年非常任理事国期间。

主席（*以英语发言*）：我现在请西班牙代表发言。

戈麦斯·埃尔南德斯先生（西班牙）（*以西班牙语发言*）：我欢迎召开本次公开辩论会。作为维护国际和平与安全的坚定倡导者和积极贡献者，西班牙重申致力于打击网络威胁，致力于在联合国会员国负责任

行为框架内开展区域和国际合作, 以推广网络空间国家负责任行为。

虽然威胁的性质在迅速变化, 迫使我们调整方法和工具, 以联合和综合的方式应对这些威胁, 但全球和国家网络抗攻击能力的关键仍在于使用更多、更好的网络工具, 以确保世界各地的关键基础设施受到保护。

一些最令人担忧的趋势是: 数据劫持现象骤增, 特别是针对关键基础设施的数据劫持; 通过数字技术操纵信息和认知; 以及利用各种脆弱性攻击国际供应链并造成经济损失。

随着混合战略、灰色地带和不对称战争的出现, 冲突概念本身也在演变。战争与和平之间的鲜明区别在某些情况下已不再适用。恶意使用信息和通信技术(信通技术)现已成为用来在冲突中获取优势的各种不断变化的复杂工具的组成部分。迫切需要拓展视角, 如此方能全面应对当代冲突。

因此, 与信息和通信技术有关的任何可能的国际机制或承诺都应基于就信通技术方面负责任国家行为框架一致达成的协议, 并通过公开、包容和透明的进程产生。

主席(*以英语发言*):我现在请葡萄牙代表发言。

Vinhas先生(葡萄牙)(*以英语发言*): 我谨赞扬大韩民国组织今天的辩论会, 并赞同欧洲联盟代表今天早些时候所作的发言。

作为国际和平与安全的保障者, 安全理事会必须能够应对现有、新出现和未来的威胁。我们正在辩论网络空间威胁问题, 这一事实表明, 安理会在受到提示时能够在新的挑战面前作出调整。

敌对的网络活动和行动已被证明是对数字化转型所带来的繁荣的最严重挑战。它们也证明是对我们机构的信誉和我们公民对这些机构的信任的严重挑战。更令人担忧的是, 网络不安全对现实世界的影响不容低估。

敌对网络行为体的攻击能力不断增强, 导致预防攻击和从攻击中恢复的成本不断增加。特别是网络犯罪集团的作用, 增加了网络威胁形势的复杂性。继2022年据称是勒索软件团伙的破坏性攻击之后, 葡萄牙加入了国际反勒索软件倡议。值得注意的是, 国家支持的行为体也越来越多地以勒索软件为掩护, 以实现各种战略目标。

人工智能已成为多种威胁行为体极为有效的能力“平衡器”, 为不成熟的操作者提供更大的可能性, 并有可能扩大攻击范围。面对此种威胁形势, 我们相信, 未来的联合国打击网络犯罪公约将很快定稿, 并且能够促进国际执法合作。这种打击国家支持的行为体实施的网络犯罪的合作, 反过来又将促进执行联合国关于网络空间负责任国家行为的法律、规范和建立信任措施框架。

能力建设也发挥着至关重要的作用, 葡萄牙打算与联合国大学合作, 为发展中国家启动一个年度数字能力建设方案。预计将从2026年起实施的未来常设制度性机制或行动纲领也将有助于弥合数字鸿沟。

安理会可以发挥重要的补充作用, 同时保持信息和通信技术(信通技术)安全及使用问题不限成员名额工作组作为加深我们对威胁、规范和法律的理解, 以及促进各国间能力建设和建立信任的主要平台的作用。

第一, 安全理事会可以重申在不限成员名额工作组中以协商一致方式商定的一套负责任国家行为准则, 如为此发表一项主席声明。仅这一措施就能让人们认识到网络威胁可能对国际和平与安全产生的影响, 具有重要意义。

第二, 也是最后一点, 安全理事会还可以尝试酌情将与信通技术有关的关切纳入其相关任务。在某些情况下, 建设关键基础设施抵御敌对网络活动的能力, 可为促进长期稳定起到决定性的作用。

主席(*以英语发言*): 我现在请萨尔瓦多代表发言。

冈萨雷斯－洛佩斯夫人（萨尔瓦多）（*以西班牙语发言*）：我谨感谢大韩民国召开本次重要辩论会，讨论我们在网络空间面临的不断演变的威胁。

如我国代表团在其他场合所指出的那样，国际安全范畴内与使用信息和通信技术（信通技术）有关的威胁在规模和强度上继续演变。这些威胁与滥用人工智能或量子计算等新兴技术有关，可产生新的攻击媒介，导致信通技术系统的脆弱之处遭利用。由于数字基础设施在治理的各个领域——即社会、经济和政治领域——的连接性日益增强，我们可能看到影响难以预测的连环效应。

信通技术领域的恶意活动可能产生超越国际和平与安全界限的破坏性影响。同样，它们也可能对平民造成直接伤害，特别是当这种攻击针对的是社会运作所必需的关键基础设施，如公共卫生系统或水和能源供应及运输系统等基本服务时，或者当它们扰乱或损害互联网的功能和可用性时。

我国认为，安全理事会这一机构应更系统、更积极地处理和平与安全面临的网络威胁，这是其维护国际和平与安全的任务和责任的一部分。为做到这一点，可进行具体的讨论，在以下几个方面取得实际成果：保护关键基础设施和关键信息基础设施；网络安全事件的发现、应对和恢复；以及网络安全能力建设的跨领域愿景等。

此外，还可以考虑是否有可能在安理会专题议程中列入一个项目，以应对数字领域，包括信通技术和人工智能等其他新兴技术，给和平与安全带来的威胁，从而对在大会和其他附属机构框架内所做努力形成补充。

还必须指出，应进一步处理数字技术对武装冲突中保护平民和民用物体的影响，包括在数字领域适用和充分尊重国际人道法原则。我们认为，虚假信息的增加和影响、通过数字平台传播错误信息和仇恨言论也是值得安全理事会关注的问题。

由于时间关系，发言全文将通过秘书处提供。

主席（*以英语发言*）：我现在请保加利亚代表发言。

斯托伊娃女士（保加利亚）（*以英语发言*）：保加利亚赞同以欧洲联盟名义所作的发言。我想以本国代表的身份强调几点。

我们赞扬大韩民国组织今天的高级别辩论会以及提请安全理事会注意这一重要议题。我们要感谢通报人内容丰富、富有见地的介绍。

网络空间威胁不断变化的问题对于我们各国社会的安全和稳定越来越重要。如今，网络空间越来越多地被用于政治和意识形态目的，国际上日益加剧的两极对立阻碍了有效的多边主义。

正如通报人所述，恶意使用网络给我们带来的更大风险是，助长了虚假信息活动，而这些活动试图利用社会的脆弱性，破坏民主进程和机构，播下不信任的种子，最终削弱社会。此外，针对关键基础设施和基本服务的恶意攻击也构成了重大的全球威胁。所有这些活动都损害了国际安全与稳定以及网络空间为经济、社会和政治发展带来的惠益。

虽然包括网络安全在内的国家安全仍然是只有各国政府才有权处理的问题，但网络事件潜在的跨境影响表明需要作出共同努力。因此，在国际层面加强网络问题合作非常重要。尽管地缘政治紧张局势造成关于网络空间国际安全的有效多边辩论总体呈现颓势，但安全理事会显然需要在这个问题上采取更加积极主动的立场。

保加利亚认为，国际安全与稳定取决于全球性、开放、稳定和安全的网络空间。在这个空间中，国际法特别是《联合国宪章》应当得到尊重，关于负责任国家行为的自愿、不具约束力的规范、规则和原则应当得到尊重。为此，国际合作至关重要。因此，必须加强安全理事会在应对网络威胁方面的作用。安理会按照维护国际和平与安全这一首要责任的要求，在网络安全问题上主动积极开展工作，会使其能够很好地应对恶意网络活动。

网络空间互联互通的特点，要求所有利益攸关方就网络空间交流信息，承担各自的责任，共同维护全球性、开放、稳定、安全的网络空间。因此，多方共同参与的做法对于妥善应对网络空间不断变化的威胁至关重要。各国和包括安全理事会在内的国际机构应努力加强与私营部门、学术界和民间社会等所有利益攸关方定期、有条不紊的交流。这也是促进和推动网络空间预防、准备、韧性和快速响应的必由之路。

最后，值得指出的是，不同国家的网络韧性以及发觉和应对恶意网络活动的能力在能力和成熟度方面存在很大差异。因此，有必要通过能力建设提升网络安全整体水平，确立网络安全特别是关键基础设施以及新技术开发和应用的共同标准。

主席（以英语发言）：我现在请安德里亚尼女士发言。

安德里亚尼女士（以英语发言）：我很荣幸今天就现代技术的滥用和网络空间日益严重的威胁这一重大问题在安理会发言。

网络犯罪会加剧威胁，助长其他形式的犯罪活动，加剧全球冲击，破坏可持续发展、和平与安全。

国际刑警组织支持本次公开辩论会，将就加强全球安全架构以应对非国家犯罪行为体构成的网络威胁谈三点看法。

首先，我们必须加强对迄今为止仍然是散布于各个地区和部门的当代网络威胁状况的认识。在这方面，国际刑警组织开发了一个网关模型，推动获取行业数据，作为成员国信息共享的补充。我们在自己的I-24/7平台上实现了196个成员国在线连接，实现了全球警务信息的安全交换。

此外，我们还提供定制的网络犯罪问题平台，用于交流最佳做法和进行分析。此外，我们的24/7联络点名单和区域工作组有助于在紧急情况下快速做出反应并在机构之间建立信任。通过共同努力以及利用现有和已建立的信息交换机制，我们可以在保护网络空间和确保全球安全方面取得重大进展。

其次，我们必须弥合能力差距。网络韧性方面仍然存在显著差异。国际刑警组织通过提供技术援助和能力建设支持成员国消除数字鸿沟。我们寻求为执法部门提供应对当今网络挑战所需的知识和技能。

第三，我们必须通过定期机构对话和多边机制最大程度实现协同增效。我们要记住，合作，而不是重复工作，才是关键。正因如此，国际刑警组织积极参与联合国内外的各种网络进程，包括信息和通信技术安全和使用问题不限成员名额工作组以及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特设委员会。

网络威胁不分国界，我们的防御也应如此。国际刑警组织始终致力于通过合作、创新和不懈的孜孜以求精神，确保所有人拥有一个更安全的网络世界。

主席（以英语发言）：我现在请印度代表发言。

拉古塔哈利先生（印度）（以英语发言）：我祝贺大韩民国担任安全理事会六月份主席。我欢迎就“应对网络空间不断演变的威胁”举行公开辩论会这一倡议。我还要感谢秘书长和民间社会代表发表见解。

当今世界是数字时代。数字化转型超越了所有传统的地理、政治和经济界限。随着人工智能等新兴技术的快速进步和采用，我们的生活与数字领域越来越紧密地交织在一起。在从个人通信到关键基础设施都互联互通的世界上，人们严重依赖于网络空间。

数字化转型也让我们面临无数的网络威胁。针对关键基础设施、信息和金融系统以及政府网络的网络攻击的频度和隐蔽程度正在加大。盗窃加密货币、劫持数据、深伪技术、错误信息和煽动现在司空见惯。此外，人工智能有可能导致网络攻击范围和规模扩大的情况也值得注意。

构成网络空间基石的信息和通信技术（信通技术）产品的安全无虞性正在受到损害。这些行为是由国家支持的行为体和非国家行为体以及跨国犯罪网络实施的。此类邪恶行为破坏了人们对全球信息通信技术供应链的信任和信心，损害了安全，造成了国家

之间潜在的冲突点。据世界银行估计，2019年至2023年网络攻击可能给全球造成约5.2万亿美元的损失。

恐怖分子也在寻找通过网络空间实施暴力的新办法；使青年变得激进；进行招聘；开展训练和筹集资金。虚拟资产和加密货币这些新方法正在成为恐怖分子金融交易的常态。恐怖主义正在利用网络世界的新渠道和新融资方式，这使该问题成为每个国家安全与繁荣的关键问题。印度几十年来一直是恐怖主义的受害者，知道网络恐怖主义挑战的严重性。

在这方面，我要强调四点。

网络空间的威胁不仅有可能危害国家安全，还可能破坏全球稳定与合作的基础。没有哪个国家或组织能够单独应对网络威胁——这需要结成统一战线。

国际文书越来越需要处理来自网络空间的威胁。现行国际法在支持应对网络攻击方面处于不利的位置。针对关键基础设施、信息和金融系统以及政府网络的网络攻击应被作为恐怖袭击对待。应思考现有反恐条约对网络空间的适用性。国际社会应确保打击恐怖主义犯罪的法律的一致性。该领域的全球合作将有助于统一网络安全基准、最佳做法以及规章。

印度参加了联合国授权的支持全球包容和透明的政府间参与以旨在实现网络空间安全与安保的各种网络进程与磋商。我们认为，多利益攸关方的协作对于了解和领会网络空间的新兴威胁至关重要。

最后，印度是世界上推进数字技术、联接以及复原力的先导之一。印度致力于一个开放、安全、自由、便捷以及稳定的网络空间环境。印度将继续同国际社会一道努力，处理网络威胁，确保数字革命继续为人类造福，而不削弱人类的集体福祉与稳定。

主席（*以英语发言*）：我现在请柬埔寨代表发言。

毛先生（柬埔寨）（*以英语发言*）：主席先生，首先，我谨感谢你举行今天的高级别公开辩论会，使会员国得以分享对网络空间的看法，因为网络威胁正在日益引起各国的关切。我也感谢安东尼奥·古特雷斯阁下、我们的各位通报人以及发言者富于见地的发言。

无可否认的是，我们的世界现在高度依赖数字技术。信息和通信技术（信通技术）的飞速进步带来了重大机会，但是也使我们面临威胁国际和平与安全的新的不断演变的风险。近来网络攻击事件的增多就证明，信通技术系统的处境比以往任何时候都更加脆弱。

在这方面，柬埔寨致力于为所有人营造一个安全的数字环境。我们借用东南亚国家联盟（东盟）这个平台来推动能力建设方案，促进最佳做法的交流。我们坚信国际合作的力量，并敦促国际社会提供技术援助，分享知识，以加强网络安全，特别是发展中国家的网络安全。

在国家一级，今年早些时候，柬埔寨采取果断行动，成立了数字安全委员会。该委员会由相关部委组成，领导了我们在网络安全、防止网络犯罪、网络防御以及网络外交方面的工作。这种协调一致的做法使我们得以评估需求，处理技能缺口，并且执行有效战略，以保护我们的数字基础设施。

柬埔寨重视网络安全能力建设的重要性。上个月，我国邮政和电信部长积极参加了全球信通技术安全能力建设圆桌会议。我们赞扬由新加坡担任主席的信息和通信技术安全和使用安全不限成员名额工作组不懈努力，促进在这个关键问题上的国际对话与合作。

此外，柬埔寨倡导促进网络空间负责任行为、维护国家主权以及防止恶意行为的有力的法律框架和国际规范。政府、企业以及民间社会之间的协作对于分享信息和开发创新的解决方案至关重要。我们还把教育和提高认识举措作为优先事项，用安全地畅游数字世界所需的知识与技能来增强我国民众的权能。

最后，柬埔寨致力于同各国一道努力，建设一个安全和具有复原力的数字未来。我们重申我们对合作与协作的承诺，以寻求为所有人实现一个更加强大、安全并且具有网络复原力的未来。我国代表团认为，

通过共同努力, 我们就能够营造一个促进创新、经济增长以及所有民众福祉的网络空间。

主席(以英语发言): 我现在请巴西代表发言。

弗兰萨·达内塞先生(巴西)(以英语发言): 我感谢大韩民国举行本次会议。

正如我们在4月份大韩民国举行的阿里亚模式会议上所指出的那样, 巴西与许多其它代表团一样, 对网络安全威胁的格局不断演变表示关切。我们也同意, 需要能够提高所有人网络复原力的多边解决方案。

但是, 我们依然坚信, 实现该目标的最佳方式是保持我们讨论的包容性, 同时避免与现有工作重叠。我们赞赏大韩民国真诚努力, 通过阿里亚模式会议和本次公开辩论会, 寻求在安全理事会进行更广泛的讨论, 但是我们认为, 进行这些讨论的合适论坛仍是大会。

今年, 我们目睹了安理会为新领域制订规则的能力局限, 它两次未能通过有关外层空间中的武器问题的一项决议草案(见S/PV.9616和S/PV.9630)。多个代表团两次对在安理会处理最好由联合国全体会员国处理的复杂问题提出关切。这些关切在此也是有效和适用的。

当前的信息和通信技术安全和使用安全不限成员名额工作组恰恰具备讨论这个话题的授权, 并且在查明网络威胁方面一直富于成效。它强调了勒索软件和加密货币以及其它攻击媒介的威胁, 包括对关键基础设施的威胁。它辩论了网络攻击的溢出效应, 并且讨论了如何保护和区分具有特定人道主义重要性的系统。它澄清了国际法和国际人道法对网络空间的适用性。目前它正在讨论执行网络空间负责任国家行为框架的具体措施。这些是重要成果, 说明在适当的论坛进行这些辩论是可行而且重要的。

这并不是说安理会没有要发挥的作用。根据《联合国宪章》规定的权力与职能, 本机关可应对那些威胁国际和平与安全的特定和具体网络事件。

在裁军进展几乎陷于停滞的时候, 网络安全领域由于在大会取得重要进展而引人瞩目。让我们努力保持这种势头。

主席(以英语发言): 我现在请危地马拉代表发言。

罗德里格斯·曼西亚女士(危地马拉)(以西班牙语发言): 危地马拉谨感谢大韩民国以安全理事会主席的身份举行本次重要的公开辩论会。

我国代表团承认, 网络空间已成为全球活动的一个核心和不可或缺的领域, 由于其民用性和两用性, 它不止一次被犯罪分子和恐怖团体所利用。这导致对关键基础设施的盗用和网络攻击增多, 电网、交通系统、医院、学校等受到影响, 由此给民众的生活和经济造成破坏性影响。网络的全球互联和全球经济的数字化提供了空间, 使破坏网络安全的行为有可能对经济和国际安全构成严重威胁。

网络空间的恶意活动可以多种方式导致冲突成倍增加。这些恶意活动使隐密攻击继而可信地否认成为可能, 使归因变得复杂, 并且制造不信任, 由此加剧国家间的紧张。此外, 国家和非国家行为者可能利用网络空间进行宣传、造谣和间谍活动, 挑起内部分裂, 助长国内和跨国冲突。

此外, 不可否认的是, 人工智能提供了一个非常重要的机遇, 有助于人类在各个领域取得进步, 从预防和解决危机, 到落实医疗保健和教育服务, 扩大政府、民间社会和联合国在各个领域的工作。然而, 恶意使用人工智能会破坏人们对机构的信任, 削弱社会凝聚力, 威胁民主。鉴于上述情况, 我国代表团认为有必要加强现有努力, 先做好预防, 再应对现有的和潜在的威胁。

目前已经采取了一些步骤, 将网络安全问题纳入本组织的工作方案。然而, 还有必要采取有力行动, 加强努力, 切实将这些问题列入安全理事会议程。这些行动具体包括: 建立实施制裁的机制, 规范网络空间行为; 增加对各国的援助, 加强其网络安全能力;

继续与私营部门和民间社会合作，制定雄健战略监控信息和通信技术。

安全理事会必须发挥更大的领导作用，打击破坏国际和平与安全的网络威胁。

主席（以英语发言）：现在请比利时代表发言。

克里德尔卡先生（比利时）（以英语发言）：首先，请允许我衷心感谢大韩民国组织本次会议。

我荣幸地代表比荷卢三国——卢森堡、荷兰王国和我国比利时——发言。比荷卢三国赞同欧洲联盟由代表所作的发言。另外我们还要强调四点。

第一，关于威胁，正如先前在安理会指出的，比荷卢三国一直十分关切恶意网络活动日益严重和不断演变的威胁。这种威胁的规模继续扩大，并可能因人工智能和量子计算进步等新兴技术而进一步加剧。我们观察到的一个令人担忧的趋势是，勒索软件攻击、勒索软件即服务的使用以及恶意网络威胁正在增加，它们将目标对准关键性基础设施，包括卫生和教育部门。这些事件的影响和外溢效应的风险对国际和平与安全构成威胁。

接下来我要谈第二点。在大会第一委员会，我们一致通过了联合国网络空间负责任国家行为框架。其中确认，国际法、特别是《联合国宪章》适用于网络空间。执行该框架，对于解决危及国际安全的信息和通信技术相关的现有和潜在威胁，具有至关重要的意义。在这方面，比荷卢三国支持制定一项行动纲领，促进在国际安全背景下使用信息和通信技术的负责任国家行为。联合国其他相关进程包括制定一项联合国打击网络犯罪公约。

此外，我要说的第三点是，根据《联合国宪章》第六章，安全理事会在和平解决争端、包括在网络领域解决争端方面具有明确的职能，有权呼吁各方解决任何可能危及维护国际和平与安全的争端。作为比荷卢三国，我们认为安理会在推动建立一个开放、自由和安全的网络领域方面可以发挥重要作用。因此，我们欣见安理会日益关注网络安全，这从2016年以来越来越多地举行关于网络问题的会议就能看得出来。目前正在发生的冲突表明，网络问题本质上是对国际和平与安全的更广泛威胁的一部分。因此，主席先生，比荷卢三国也赞同您关于将网络问题纳入安理会现有工作主流的建议。

最后，我要讲的第四点是，比荷卢三国呼吁更多地关注网络行动的受害者。人们往往从地缘政治竞争的角度来看待恶意网络活动，但这些活动也对人们造成破坏性影响，严重剥夺了他们的人权。因此，为了将人类福祉和尊严放在讨论的首位，我们呼吁采取以受害者为中心的做法。

我们也不要忘记，数字化转型，包括网络空间的数字化转型，会给受人道主义危机影响的人们带来重大的保护风险。我们看到，红十字国际委员会及其设在卢森堡的全球网络中心，站在第一线应对一些此类挑战，包括开发和测试新工具，以中立、公正和独立的方式向受影响民众提供数字服务。

主席先生，我们比荷卢三国再次感谢您组织本次辩论会，同时赞扬您努力普及认识和讨论网络威胁的重要性。

主席（以英语发言）：请挪威代表发言。

勒沃尔德先生（挪威）（以英语发言）：我高兴地代表丹麦、芬兰、冰岛、瑞典和我国挪威等五个北欧国家发言。

首先，请允许我感谢大韩民国倡议召开本次适时的会议。这还只是安理会第二次正式讨论网络安全这一重要议题。

自从安理会在2021年爱沙尼亚担任主席期间首次讨论这个问题（见S/2021/621）以来，网络威胁的事态发展一直令人担忧。

请允许我简要地谈谈三种威胁。

首先，来自国家支持的网络行动的威胁继续存在，最明显的是在俄罗斯对乌克兰的非法侵略战争中的网络行动威胁。俄罗斯的网络能力已在乌克兰境内

被用作武器，企图破坏对当局的信任并摧毁关键基础设施。我们继续重视乌克兰的网络防御，也重视保护我们自己的社会免受恶意行为者的侵害。在这方面，我们要再次强调，国际法也适用于网络空间。

第二，国家支持的行为体、非国家行为体和犯罪行为体之间的界限越来越模糊。令人关切的主要问题包括勒索软件攻击日益增多，能够用上先进网络工具和技术的国家行为体和非国家行为体更加广泛。

最后，与所有这些威胁相关的一个特别关切问题是，恶意行为体越来越多地将关键部门和基础设施作为攻击目标。

为应对这些威胁，北欧国家特别要强调多利益攸关方参与网络安全的重要性。我们必须努力加强政府与包括民间社会、学术界和私营部门在内的所有相关利益攸关方之间的协调。私营部门可以获取信息，在网络空间中发挥着至关重要的作用，因为技术和网络安全公司在预测和应对威胁方面扮演着关键角色。必须更好地利用相关利益攸关方的知识和能力，支持自由、开放、和平与安全的网络空间。

鉴于威胁形势不断变化，北欧国家认为，安全理事会更经常地讨论网络安全问题越来越有益。安全理事会在专题讨论和针对具体国家的讨论中，讨论当前和新出现的网络威胁，有助于提高对威胁的认识，分享经验教训，以及制定适当的应对措施。

安理会的工作也是对其他论坛讨论的补充。有鉴于此，最后我谨重申，北欧国家支持制定一项网络安全行动纲领，作为一个常设、包容各方和注重行动的机制，推进这一领域的负责任国家行为。

主席（以英语发言）：我现在请克罗地亚代表发言。

西蒙诺维奇先生（克罗地亚）（以英语发言）：主席先生，感谢你组织本次及时的公开辩论会会。克罗地亚赞同欧洲联盟的发言，我谨以本国代表身份讲几句。

我们面临着越来越多、越来越狡诈的网络威胁。其中包括使用勒索软件针对关键基础设施的攻击、持续的活动以及外国对民主进程的干预等等。这些活动中的每一项都有可能破坏政府的稳定，乃至破坏和平与安全。

在冲突地区，网络行动可能会放大常规战争的影响，特别是在针对关键基础设施时，从而导致敌对行动升级和平民遭到更大伤害。在这方面，我们赞扬红十字国际委员会所做的工作，强调网络空间并非法外之地，并申明国际人道法既适用于现实世界也适用于网络世界。

正因为此，安全理事会应考虑进一步加深对这一高度复杂问题的认识，不仅通过在网络安全领域与多个利益攸关方定期交流，而且在建设和平以及预防冲突和调解努力方面进行交流。实现这一点的办法可以是，通过定期通报和报告网络威胁情况，确保安理会和会员国都能够了解最新事态发展和趋势。

此外，安全理事会在应对网络威胁方面的作用可与联合国其它机构和多边倡议的现有工作相辅相成。这包括信息和通信技术安全和使用不限成员名额工作组以及其他相关未来框架（例如《行动纲领》）开展工作，确保采取协调和全面的全系统方法。安理会还可促进各国之间的对话和建立信任措施，降低网络冲突升级为武装对抗的风险，探讨如何推动缓和紧张局势。

安理会可以通过采取主动积极措施了解和减轻网络威胁、促进国际合作以及将网络考虑因素纳入其更整个授权，在现有的联合国网络安全生态系统中发挥重要作用，更好地维护数字时代的国际和平与安全。

主席（以英语发言）：我现在请智利代表发言。

纳尔瓦埃斯·奥赫达夫人（智利）（以西班牙语发言）：我们很高兴有机会参加本次公开辩论会。我们注意到今天发言者的介绍和发言。我们借此机会祝贺大韩民国担任安全理事会本月主席。

正如我们之前指出的那样，智利认为网络攻击和网络空间恶意活动对国际和平与安全构成威胁，并可能对各国造成各种影响，这具体取决于各国的数字化水平、能力、维安、基础设施和发展情况。

我们特别强调，这些威胁也会对不同群体和实体，特别是妇女、女孩、男孩和青少年产生不同影响。

关于网络空间恶意活动新出现和不断变化的趋势，我们可以提到人工智能和机器学习的使用、各种攻击向量策略的结合、损害产品和服务完整性的供应链攻击、对物联网设备的攻击等等。

勒索软件、擦除器、木马等恶意软件以及网络钓鱼和分布式拒绝服务攻击等技术带来的风险也值得注意。如果恶意行为体实施这些威胁，可能会对各国的运作造成严重破坏，并影响其经济和人民的福祉。

为此，我们认为加强各国之间的共同努力与合作至关重要。这包括交流经验教训、执行网络空间国家负责任行为的现行规范、适用国际法和国际人道法、建立信任措施和能力建设，所有这些都有助于减少各国之间的不信任，助力网络空间的稳定。

智利提倡上述做法，并指出应让相关各方，例如民间社会、学术界、私营部门、技术界以及其他相关行为体参与所有辩论和讨论。

我们强调应当加强安全理事会在应对网络空间威胁方面的作用，并相信安理会可以为建立安全、开放、和平的网络空间做出重大贡献，从而造福所有国家。智利高度重视这一问题，因为恶意行为体会利用缺乏必要工具和培训来应对此类威胁的国家的脆弱性。

从这个意义上说，安理会可以成为在能力建设和技术援助方面创造对话与合作空间的宝贵工具，而这可以使最需要这种援助的国家受益。我们呼吁该机关应对不断变化的网络空间威胁形势带来的挑战，同时开展国际合作，我们认为国际合作应该成为共识。

主席（*以英语发言*）：我现在请尼泊尔代表发言。

塔帕先生（尼泊尔）（*以英语发言*）：我感谢主席大韩民国召开本次公开辩论会。我还要赞扬通报人富有见地的宝贵发言。

信息通信技术和人工智能的快速发展彻底改变了我们的生活，为加速社会和经济发展提供了前所未有的机遇。我们对技术的依赖一直在增长。然而，它们的滥用造成了新的严重威胁。我们对世界其他地方勒索软件攻击、网络犯罪、错误信息传播和仇恨案件激增感到担忧。

没有任何基础设施或系统能够免受网络攻击；无论是金融机构、医院、交通、供水或能源供应系统等民用基础设施，还是核武器军事指挥和控制系统或自主武器系统都是如此。这对国际和平、安全、稳定与发展构成挑战。

我们尼泊尔也面临着这种威胁的巨大挑战，尼泊尔的银行机构、政府网站和服务器不时遭受网络攻击和勒索软件攻击。

为此，我想强调几点：第一，我们需要在《联合国宪章》等国际法公认准则的基础上，实施一套强有力的规则，同时确保网络空间的开放、稳定和安全。我们应该就规则的适用达成共识，促进网络空间建立信任措施以及推动网络空间负责任的国家行为。

其次，我们必须定期举行通报会和评估会，纳入科技主导型公司、私营部门、民间社会和学术界的见解，分享知识和最佳做法，让自己为不断变化的网络威胁形势做好准备。

第三，尼泊尔等国家更容易受到此类新威胁的影响。

（接上段）我们面临的挑战包括缺乏充足的法律和监管框架、人力和财力有限等，以便做好准备以防止和应对这些威胁。因此，持续的国际支持与援助对于提高尼泊尔这样的国家的能力从而使它们能够防止和应对网络攻击至关重要。我们需要促进多利益攸关方的伙伴关系，以便弥合体制、技巧、能力、技术以及资源方面的缺口。

第四, 我们应通过弥合国家间的数字鸿沟, 促进所有人的包容性发展与繁荣, 从而促进网络安全。

最后, 我们面临的网络威胁是严重的。通过主动采取综合和协调一致的行动, 我们就能够确保所有人享有一个安全、开放并且和平的网络空间。在我们推进所有人享有可持续的数字未来议程的同时, 我们必须共同建设一个能够抵御和克服数字时代威胁的具有复原力的全球社会。

主席(*以英语发言*): 我现在请孟加拉国代表发言。

穆希特先生(孟加拉国)(*以英语发言*): 我感谢安全理事会现任主席大韩民国举行本次重要的公开辩论会。我也感谢各位通报人富于见地的通报。

在不断演变的数字格局中, 网络威胁已变得无处不在, 而且常常迫在眉睫, 扰乱全球的金融、民主、社会文化以及安全架构。《2024年全球风险报告》强调指出, 网络威胁是当代最严重的挑战之一, 到2027年可能的网络犯罪成本估计为24万亿美元。如此惊人的数字要求我们立即采取紧急行动。但是, 网络犯罪不仅造成经济成本, 它对个人和社会的严重影响也不能低估。

为探讨主席提出的引导性问题, 我谨强调几点意见。

首先, 网络威胁的扩散给全球和平与稳定带来严重风险, 这些网络威胁包括勒索软件攻击、网络间谍活动以及通过深度伪造和其它手段开展的错误信息和虚假信息活动。这些威胁把关键基础设施作为目标, 并且通过散布仇外理念、不容忍以及成见, 来破坏民主进程与社会和谐。此外, 人工智能和量子计算领域的进步扩大了网络威胁的范围, 使其更趋复杂。由于数十亿民众的日常活动依赖数字平台, 处理这些威胁的紧迫性达到前所未有的程度。

其次, 我们坚信, 面对这些严重威胁, 我们的实力取决于我们最薄弱的环节。因此, 当今加强国际合作与协调不可或缺。加强网络安全措施, 搭建信息共享机制, 以及对能力建设举措进行投入, 这些对于提高复原力以抵御网络威胁至关重要。在这方面, 我们强调在数字领域坚持主权平等和国际法原则的重要性。我们必须想方设法, 在表达自由和必须打击散布错误信息的有害行为两者之间达成平衡。

第三, 在这个快速演变的网络格局中, 我们赞扬信息和通信技术安全和使用安全不限成员名额工作组促进重要的国际论辩与协作。反映国际社会总体意志与愿望的大会仍是进行这些关键讨论的主要平台, 使各国能够积极参与塑造我们集体的网络未来。我们还希望, 当前的《全球数字契约》将为处理该问题发挥关键作用。我们倡导采取大会与安全理事会协作的做法, 以有效执行该《契约》。

最后, 关于处理网络空间不断演变的威胁是否属于安理会职权范围的问题, 由于这不是传统安全概念的一部分, 我们认为, 鉴于该问题给和平与安全带来的新兴威胁, 网络安全理应得到联合国最高层的关注。处理这个关键问题的合适平台需要通过开放和透明的对话来决定, 而不是使它成为又一个分歧与极化的领域。

与此同时, 我们认为, 安理会可在制定建立信任措施方面发挥重要作用, 包括通过有效的信息共享和交换看法。我们必须共同努力, 无论是在安理会还是联合国任何其它适当论坛、包括不限成员名额工作组的主持下共同努力, 以制订规范、标准以及规章, 倡导所有人享有一个安全、有保障、非歧视并且稳定的数字环境。孟加拉国重申, 我们致力于同全球社会协作, 处理不断演变的全球网络安全威胁格局。

主席(*以英语发言*): 我现在请越南代表发言。

邓先生(越南)(*以英语发言*): 网络空间的威胁无论是在规模上还是复杂性上一直在不断演变, 对国际和平与安全构成重大挑战。这些威胁涵盖一系列恶意网络活动, 包括间谍活动、针对关键基础设施的攻击和数据泄露, 还有错误信息、虚假信息以及网络心理战。这些活动可严重危及国家安全, 造成严重的经济损失, 并且削弱公众对机构的信任。

任何国家均无法幸免这些威胁。尤其是发展中国家，它们往往缺少强大的网络安全能力，无疑是最脆弱的，有时被民族国家作为打网络战和非国家行为体制造网络犯罪的试验场。

在全球层面，由于网络空间没有边界和存在归因的挑战，网络攻击可引发冲突，加剧地缘政治紧张。因此，处理这个复杂问题要求采取一种多层面的做法，联合国在其中发挥着重要作用。

首先，至关重要的是，国家要遵守和执行适用国际法的现有规范与规则，它们为网络空间的国家行为提供了全面指导。

与此同时，为进一步促进数字领域国家间的和平、安全以及合作，我们需要继续加强管理网络活动的国际框架，尤其是致力于与该领域有关的进行之中的进程，包括 《全球数字契约》和一项关于打击网络犯罪的公约。

其次，能力建设对于维护开放、安全、稳定、具有复原力的和平的网络空间至关重要，特别是对那些网络能力有限的国家来说，以便有效地阻止、防备和应对恶意网络活动的影响。至关重要的是，各国要抱着共同的目标，即： 增强能力，缩小国家间和区域间在信息和通信技术方面的发展差距。

第三，考虑到安理会的任务授权，它应更多地关注这个问题，处理网络威胁与其议程上如防止冲突、打击恐怖主义和保护关键基础设施等其它重要问题之间的关联。安理会还亟须同联合国其它机构、区域组织以及私营部门开展协作，以便制订应对网络威胁的统一和全面的对策。

越南政府采取了一种综合性的全社会的做法来处理网络威胁，于2018年颁布了我国的网络安全法。越南重申，我们支持全球协调一致地努力搭建有力的框架与机制，以旨在维护网络空间的主权、不干涉和负责任行为的原则。通过建设性的对话与合作，我们可有效处理技术不断演变带来的挑战，同时保护全球网络空间和信息生态系统的完整性。

奥蓬-恩蒂里女士（加纳）（*以英语发言*）：主席先生，首先我感谢你举行今天关于一个如此重要的话题的公开辩论会。我们也感谢各位通报人提供了深刻的视角。

加纳在迎接信息和通信技术（信通技术）革命空前巨大的影响的同时，也清楚意识到这场革命也给国际和平与安全带来的风险。在我们身边，即非洲大陆，我们目睹了信通技术的迅猛发展对各种国家安全挑战和威胁产生的影响和作用。无论是网络钓鱼和身份盗窃、恐怖分子招募追随者、还是在暗网上进行小武器和弹药交易，来自数字领域的安全风险一直没有停歇。私营企业和重要的公共基础设施也未能幸免，在某些情况下对和平与稳定构成严重威胁。即使在民主治理领域，信通技术对增强非洲公民权能、从而在结社和集会自由框架下推进其所选政治事业产生了积极影响，但这种影响也因为信通技术被滥用于传播假新闻、虚假和错误信息而大受打击——这对国家统一和凝聚力带来了很高风险。

必须建立强有力的网络防御能力，以应对这些削弱公众信心和信任的日益增长的趋势，同时我们要告诫的是，需要一个精心调节的对策，以避免政府越权，避免削弱公民权利和自由的行动，这些行动本身就可能成为严重不满和不稳定的根源。事实上，在认识到非洲所面临挑战的同时，我们大陆的领导人一直在采取多项措施加强网络防御。在今年举行的非洲联盟国家元首和政府首脑会议第三十七届常会期间，网络安全占据了中心位置，会上作出了推进非洲议程数字化转型战略的重要决定。除了推动加快创建大陆网络安全战略，非洲领导人还就国际法在网络空间的应用商定了共同立场。我们赞同，若要建立一个值得信赖并有能力应对不断变化的威胁的网络空间，还有许多工作要做。我们必须尽一切努力，通过能力建设和技术援助来弥合数字鸿沟。

为了回答关于安全理事会在应对网络空间对国际和平与安全的威胁方面可发挥作用的问题，加纳想补充以下三点。

第一, 为了充分利用网络空间促进增长和繁荣的巨大潜力, 必须采取协调一致的全球行动来应对新兴风险, 并为所有人创造一个可靠、安全和有韧性的网络空间。这凸显了信息和通信技术安全和使用问题不限成员名额工作组和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协商一致报告的重要性, 也让我们确信, 国际法和《联合国宪章》在信通技术环境中维护和平、安全和稳定方面是适用且必不可少的。

第二, 今天的公开辩论会是近年来关于这一主题为数不多的公开辩论之一, 是认识到网络空间恶意行为体对全球和平与稳定构成越来越大危险的又一重要步骤。安理会的行动应旨在补充大会在制定和促进网络空间负责任行为规范方面的作用。它还可以考虑鼓励为数字领域建立一个有法律约束力的框架, 以规范威胁国际和平与安全的政府或非政府实体的任何行动。这种框架可以利用信通技术领域关键利益攸关方的专门知识, 协调国际努力, 从而应对网络犯罪并认定责任, 以确保问责。成立一个专门处理此事的附属机构可以作为一个起点。

第三, 鉴于信通技术、特别是人工智能快速发展以及它们被滥用的潜在危险, 安理会可以考虑在最终将其纳入各种专题和地域性议程之前, 创建一个侧重于网络安全的具体议程项目。这种方法将为安理会提供充足的时间来审议其影响并充分把握这一问题, 使其能够制定全面的战略来保障全球和平与安全免受网络威胁。

主席(*以英语发言*): 我现在请巴拿马代表发言。

康塞普西翁·哈拉米略女士(巴拿马)(*以西班牙语发言*): 在数字时代, 恶意网络活动造成的威胁持续增长。巴拿马认识到建立全球网络安全架构以有效打击这些不断变化的网络威胁的重要性。安全理事会等行为体在其授权范围内, 可以在应对这些挑战和加强国际合作、从而捍卫我们共有的数字环境方面发挥关键作用。它对维护国际和平与安全负有首要责任, 这一责任在网络空间领域同样关键。通过积极主动地参与网络安全工作并熟悉新兴威胁, 安理会可以为所有国家建立一个安全与和平的网络空间作出重大贡献。我们必须探索如何提高安理会应对恶意网络活动的能力, 因为这些活动可能影响重要基础设施、平民和人道主义努力。

在应对这些网络威胁的复杂局面时, 必须考虑到正在进行的关于拟定一项打击非法使用信息和通信技术的全面国际公约的讨论, 它将有助于补充《欧洲委员会网络犯罪公约》。该公约及其议定书有助于促进打击网络犯罪方面的国际合作, 同时, 网络威胁不断变化的性质要求我们调整和加强法律框架。通过更新和改进这些框架, 我们可以更好地应对网络空间的新挑战, 并确保更具韧性的全球网络安全架构。

考虑到恶意网络威胁的跨国性质, 安全理事会必须与会员国、国际组织和其他利益攸关方合作应对这些多层面的挑战。通过在网络空间促进合作、分享最佳做法和促进负责任的国家行为, 我们可以共同减轻与这些威胁相关的风险和脆弱性。巴拿马认为, 可以在安理会的一些委员会中推动这些努力, 例如第1540(2004)号决议所设委员会。总的来说, 安全理事会可以在应对网络空间带来的国际和平与安全挑战方面发挥具体作用并采取具体行动, 包括制定关于网络威胁的评估和战略, 并将网络安全纳入其关于具体问题的讨论。网络威胁与安全理事会议程上的其他问题相互关联,包括保护平民、武装冲突中的和平与安全、打击恐怖主义、反恐以及妇女与和平与安全主题。评价和战略应考虑性别视角和妇女参与决策, 同时考虑到她们各不相同的脆弱性。

为了有效地将网络空间相关关切纳入自身工作, 安理会可以探索加强网络复原力、促进国际合作和全面应对网络威胁的方法。通过加强协调与合作, 提高网络安全能力, 我们可以建设一个更安全、更有韧性的数字环境, 造福所有国家。巴拿马呼吁安全理事会在这方面采取果断行动, 并呼吁我们共同努力, 为今世后代确保一个更安全、更和平的网络空间。

主席(*以英语发言*): 我现在请意大利代表发言。

约万诺维奇先生（意大利）（*以英语发言*）：主席先生，我谨感谢你及时召开这次公开辩论会。随着我们进入一个以快速技术进步为标志的时代，对强大而统一的网络安全方法的需求从未像现在这样紧迫。

意大利赞同以欧洲联盟的名义所作的发言，并希望以本国代表的身份补充一些思考。

意大利对恶意网络活动日益增多以及为军事目的发展信息和通信技术（信通技术）能力感到关切。我们坚定致力于加强所有会员国在新数字技术领域的合作。意大利担任七国集团主席期间，寻求在国际社会努力的基础上，促进一个开放、可互操作、安全、有保障、有韧性和尊重人权的网络空间，并遵循国际法的原则和规则。意大利呼吁尊重《联合国宪章》和现有国际准则，以维护和平与稳定，加强我们的共同安全。

安全理事会肩负着维护国际和平与安全的首要责任，在应对网络安全威胁以造福所有国家方面可发挥独特的作用。安理会的这种参与确实应对联合国现有其他进程，如推进从国际安全角度使用信息和通信技术的国家负责任行为拟议行动纲领，形成补充。安全理事会前几次会议上提出的建议旨在优化应对信通技术对全球安全影响的集体举措。其中一项建议是，在审议具体的国家案例或其他更广泛的专题，如维持和平与建设和平任务、不扩散和反恐问题时，考虑相关的网络安全关切。

此外，我们还应加强联合国应对恶意使用信通技术危害国际和平与安全行为的能力。在保护平民、关键基础设施和人道主义行动方面，这一点尤其重要。在向前迈进的过程中，我们必须考虑恶意活动的主要趋势——这些趋势有时因人工智能等新技术而加剧——及其在现有冲突中成为威胁倍增因素的可能性，并考虑安全理事会和整个联合国可设想采取哪些具体行动来应对我们面前日益严峻的挑战。

我们都意识到，恶意网络活动可能会对我们各国人口中的弱势群体造成格外严重的影响。我们都面临关键基础设施，如医疗保健或能源设施，或公民个人和私营企业沦为网络攻击目标的风险。要阻止网络攻击实施者因其不法行为而获得回报，能力建设至关重要。有鉴于此，意大利将于7月2日主办一次全国会议，讨论加强负责全世界网络能力建设活动的公共和私营实体的生态系统问题。这将有助于以包容各方的多利益攸关方做法实施今后的项目。

意大利致力于使这一做法取得成功，为证明这一点，我要重申，我国愿与所有会员国合作，发展和加强必要的技能、进程和资源，以适应日新月异的网络空间，最终确保所有国家都有一个更安全的未来。

主席（*以英语发言*）：我现在请以色列代表发言。

卡尔马先生（以色列）（*以英语发言*）：以色列要同其他国家一道，祝贺大韩民国组织和主持本次非常适时的关于网络安全威胁的重要辩论会，并要从我们的角度就网络空间中现有不断演变的威胁补充一些看法。

以色列是前所未有的网络侵略浪潮首当其冲的受害者。我们的对手并不局限于发动常规战争和恐怖袭击，还试图利用数字领域来破坏我国的安全，在我国民众中播撒不和的种子，扰乱我们的生活。网络攻击已成为以色列每天面对的现实。我国的关键基础设施，无论是政府、金融还是社会基础设施，都面临着国家和非国家行为体的无休止攻击。这些攻击企图危害我国公民的安全和福祉，威胁我国的经济稳定，并挑战我国的民主体制。我们在网络空间面临的威胁是真实而普遍的，需要我们集体保持警惕并采取行动。

与许多国家一样，以色列清楚网络威胁的深远影响。我国的经验告诉我们，这些威胁并不是理论上的。2023年10月7日星期六，数千名哈马斯恐怖分子渗透到以色列南部边境，屠杀、焚烧、强奸、残害了1200名无辜者——妇女、男子、老人、儿童和婴儿。此外，还有数千人受伤，240多名无辜公民被恐怖分子绑架，沦为人质。自2023年10月7日以来，以色列还不断遭受大规模网络攻击。这些攻击是伊朗在其代理人——真主党、哈马斯和其他恐怖团体——的积极支持和参与下策划的，这些团体针对我国最关键、最敏感的基础设

施, 如我国的供水、能源基础设施和医院, 发动了大规模网络攻击。必须谴责伊朗公然违反网络空间负责任国家行为准则, 违反基本的人道和道德标准。除了网络攻击, 我们还是伊朗大规模操弄公共舆论行动所针对的目标, 其目的是恐吓以色列公民, 滥用我们社会的自由和民主, 并给哈马斯残暴袭击的受害者及其家人带来更多痛苦。攻击者将网络空间作为其实施恐怖活动的工具和场所, 企图损害以色列社会的根基。

全球各地的以色列和犹太社区正在经受一场全球性的煽动、仇恨言论和反犹主义浪潮, 而社交媒体上的协调一致的不真实行为大大加剧了这一浪潮。我们注意到, 一些大型科技公司及其社交媒体平台为消除仇恨和暴力所做的努力在不断改进, 但仍有许多工作要做。我们呼吁所有社交媒体平台在这方面表现出更多的责任感。不应允许任何形式的仇恨言论、要求毁灭或暗示消灭某个群体的呼吁在世界各地回响。

如人们在法国总统马克龙在2023年10月7日袭击事件后成立的打击哈马斯煽动和筹资活动国际联盟最近于5月15日在海牙举行的会议上所指出的那样, 哈马斯对网络空间的利用结合了一系列战略和目标。哈马斯特工利用各种在线平台实施激进化、洗脑、煽动暴力、散布仇恨和虚假信息以及筹集资金, 而所有这些都是为了实现该组织的既定目标, 即通过暴力和圣战摧毁以色列国。哈马斯在网络空间传递信息, 巧妙使用各种图标和符号, 以绕过人工智能语言监测系统, 使各种群体和个人认同哈马斯的暴力世界观, 并将这些想法从网络空间转移到现实世界。这一转移表现在, 向哈马斯账户提供的捐款和筹款数额大幅增加, 达数千万美元, 大批抗议者参加充满仇恨的示威活动, 以及哈马斯在网上发表的反以色列和反犹太言论引发的持刀袭击事件。国际社会尚未将网络恐怖活动作为恐怖主义来处理。网络恐怖分子有着独特的动机, 不受国际准则的影响。当今世界仍然缺乏应对网络恐怖的适当手段。

所有爱好和平的国家都应考虑尽早填补这一缺口。始于中东的事件很少只发生在我们区域。在这个相互关联的世界上, 没有一个国家能够独善其身。从导致关键基础设施瘫痪的勒索软件攻击到损害公众信任的造谣活动, 最近全球各地网络事件激增, 凸显了我们共担责任的紧迫性。这些威胁不仅危及我们的技术进步, 影响我们的经济, 而且还危及我们民主体制的结构和全球稳定。以色列强调国际协调的重要性。没有任何一个国家能够单独应对这些威胁。我们必须加强我们的伙伴关系, 加强信息共享机制, 并要求每个国家执行网络空间负责任行为的准则和规则。这对于创造一个安全稳定的数字环境至关重要。在这个环境中, 创新可以蓬勃进行, 而不必担心被利用。国际社会必须团结一致, 谴责网络侵略, 并确保那些试图通过网络手段损害我们集体安全的人承担后果。

最后, 让我们借此机会重申, 我们致力于维护网络空间的信誉与安全。通过对话、合作和果断行动, 我们可以共同减轻我们面临的威胁, 并利用数字技术的变革潜力, 造福全人类。

主席(*以英语发言*): 我现在请摩洛哥代表发言。

海拉尔先生(摩洛哥)(*以法语发言*): 主席先生, 首先, 请允许我祝贺你在安全理事会举行本次公开辩论会, 讨论一个在我们世界目前面临困难时期, 并且鉴于网络空间固有威胁不断变化的复杂性质而具有至关重要意义的议题。我欢迎大韩民国外务部长官赵兑烈先生、秘书长安东尼奥·古特雷斯先生和各位通报人与会, 我感谢通报人的全面通报。

摩洛哥引以为豪的是, 我们与其他62个国家一道, 共同提出了关于从国际和平与安全角度利用信息和通信技术(信通技术)的联合声明。

摩洛哥一贯主张会员国在网络空间领域加强合作, 并申明支持在联合国主持下采取的旨在建立一个安全、可靠和有韧性的网络空间的举措, 该空间作为一个共享领域, 应始终保持其和平与繁荣的性质, 并充分利用负责任地使用信通技术带来的机遇。

面对如此复杂和不可预测的地缘政治环境, 呼吁国际社会为全球可持续与和平的数字转型奠定基础, 转型情况将取决于我们在以下方面的共同努力: 促进互信、透明度、最佳做法交流, 应缔约国的要求并

根据其需要开展能力建设和技术援助，缩小发达国家与发展中国家在信通技术领域日益扩大的差距，尤其是尊重会员国的国家主权和领土完整。

摩洛哥王国在穆罕默德六世国王陛下的领导下，始终积极倡导负责任地使用信通技术、数字信任和数字化，这要归功于我国新的2030年国家网络安全战略，该战略旨在巩固和扩大自2012年通过国家网络安全战略以来所取得的成就，以期更好地支持数字转型，将其作为社会经济发展的重要杠杆。

摩洛哥的网络安全方针也基于国际合作，包括与兄弟般的友好阿拉伯国家和非洲国家的合作，以期在南南合作和三方合作的框架内，最大限度地受益于这一重要领域所代表的优势和机遇。

联合国正在建立专门审查网络和数字威胁的多种机制和平台。摩洛哥认为，鉴于网络威胁不分国界的性质，安全理事会应该更加积极和主动地参与这一敏感领域的工作，以履行其任务，特别是维护网络领域的国际和平与安全。

我们认为，安全理事会应考虑更深入地讨论对国际和平与安全构成直接和持续风险的网络威胁的定义和优先次序，包括重点关注以下方面。第一，安理会应重点关注决定威胁是否达到足以由安全理事会审议的警戒级别的关键参数。第二，安理会应讨论为防止网络威胁升级而应采取的措施。第三，安全理事会应举行年度辩论会，概述网络空间新出现的威胁。第四，它应注重加强妇女、青年、私营部门、民间社会和学术界的参与，使安全理事会能够及时了解信通技术领域新出现的威胁及其对国际和平与安全的影响。

摩洛哥强调，在安全理事会内进一步讨论网络威胁问题，将使安理会有机会发挥主导作用，制定注重行动的对策，减轻会员国每天面临的集体网络威胁。

最后，我们认为，现在是时候了，应该保持过去十年在联合国内部产生的势头，维护我们对一个可靠、安全、有韧性的网络空间的集体和建设性承诺。网络安全和网络犯罪不是孤立存在的，而是具有广泛的后果，对整个国际社会产生格外严重的影响。

主席（*以英语发言*）：我现在请列支敦士登代表发言。

韦纳韦瑟先生（列支敦士登）（*以英语发言*）：我们感谢大韩民国继续开展爱沙尼亚启动的进程，让安全理事会参与处理网络安全问题（见S/2021/621）。安全理事会参与处理这一议题，有助于确保法治有效应对现代技术挑战，包括不断变化的网络空间威胁，这是安理会任务的核心。

在当今相互联系的世界中，新网络技术的出现不仅为国际合作提供了前所未有的机遇，而且也带来了可能造成灾难性影响的恶意网络行动的风险。在俄罗斯对乌克兰的侵略等局势中，网络攻击的复杂性和频率不断升级，这要求我们明确国际法如何适用于网络空间。

首先，我们重申国际法适用于网络空间的广泛共识，包括国际人道法、国际人权法、国际刑法，当然还有《联合国宪章》。红十字国际委员会申明，国际人道法涵盖武装冲突期间的网络行动，强调在数字领域也必须遵守法律标准。此外，由于许多网络行动越来越多地被用来实施国际犯罪，包括战争罪和危害人类罪，亟需了解其在国际刑事法院（国际刑院）《罗马规约》体系下的影响。相关评估确认，刑院已经可以调查和起诉相关的网络攻击。这完全符合逻辑：国际人道法适用于网络行动，因此达到国际刑院严重性门槛的违反国际人道法行为是可以起诉的。列支敦士登于2020年和2021年召集的顾问委员会编写了一份报告，阐明了《罗马规约》四种核心罪行——侵略罪、战争罪、危害人类罪和种族灭绝罪——中的每一种罪行如何适用于网络行动领域。

在国际刑院起诉借助网络实施的犯罪，有助于有效应对不断变化的网络威胁形势。在顾问委员会报告的基础上，国际刑事法院检察官最近与微软公司共同启动了一个多利益攸关方磋商进程，以制定一项国际刑院政策，应对借助网络实施的犯罪。这将有助于国际法从业人员更深入地了解与起诉借助网络实施的犯罪相关的复杂性。此外，加强刑院、联合国、各国政

府、私营部门和民间社会之间的对话，将促进网络领域的重要政策制定工作，并最终支持刑院作为国际和平与安全架构的关键组成部分发挥作用。

最后，安全理事会可以在确保追究网络攻击的责任方面发挥关键作用，因为安理会有权向国际刑院移交案件，并将相关局势送交刑院调查。刑院与安全理事会之间的关系对于确保正义不被战争工具不断变化的性质和发展所超越至关重要。

主席（以英语发言）：我现在请土耳其代表发言。

切廷先生（土耳其）（以英语发言）：主席先生，我们感谢你组织本次公开辩论会，讨论不断变化的网络空间威胁。

信息和通信技术（信通技术）已成为社会和经济不可或缺的一部分，影响到生活的方方面面。

今天，各国开发和利用技术的能力在其发展和增长中发挥着重要作用。技术的发展为我们提供了许多机遇，同时网络威胁在不断变化，变得更加复杂。信通技术系统的安全漏洞往往威胁着经济、公共秩序和国家安全。恐怖主义、数字间谍、欺诈、网上虐待儿童以及通过信通技术利用和滥用个人数据等威胁也对国际和平与安全构成危险。

我们对日益增多的网络攻击尤其感到震惊。研究表明，2023年，全球有3.17亿多次勒索软件攻击和60多亿次恶意软件攻击。由于技术发展，网络攻击变得更加容易实施，同时对受害者造成的不利影响和负担在迅速增加。打击这些攻击和应对威胁需要在实践中和法律上采用最新的方法和手段。

鉴于网络威胁的跨界性质，加强该领域的国际合作和能力建设至关重要。基于这一认识，土耳其参与了网络威胁情报共享，并为区域和国际组织内的政策和合作战略做出了贡献。

就国际法而言，土耳其加入了《欧洲委员会网络犯罪公约》。我们还积极参与在联合国开展的各种努力，尤其是通过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特设委员会参与这些努力。我们认为，通过信通技术实施的恐怖主义方面的犯罪也应在未来的一项公约中做出规定。

还存在国际法在网络空间的适用性的问题。土耳其是《推进从国际安全角度使用信息和通信技术的负责任国家行为的行动纲领》的共同提案国之一，我们大力支持大会第77/37号和第78/16号决议。

网络空间是无疆界之域，而网络安全是一个涉及多利益攸关方的问题，因而国际合作至关重要。服务提供方和安保公司应该更加有效地同政府和国际组织合作，以便为全球的网络安全做出贡献。我们欢迎安全理事会侧重于利用网络空间来处理不断增加的威胁，并且承诺继续我们在这方面的参与和对话。

主席（以英语发言）：我现在请沙特阿拉伯代表发言。

阿勒瓦西勒先生（沙特阿拉伯）（以阿拉伯语发言）：首先，我谨祝贺大韩民国常驻代表黄浚局大使阁下担任安全理事会主席。我祝大韩民国代表团在其主席任期内取得圆满成功。我还谨感谢安东尼奥·古特雷斯秘书长阁下、网络和平研究所首席执行官Stéphane Duguin先生和法律与技术教授Nnenna Ifeanyi-Ajufo女士的通报。他们为应对网络安全面临的危险和不断增多的网络威胁做出了超凡和重要的不懈努力。

我们比以往任何时候都更加迫切需要一个能够促成增长与繁荣的安全和有保障的网络空间。这凸显出加强网络安全作为国家优先事项对于保护国家切身利益和国家安全的重要性。沙特阿拉伯王国认为，加强这方面的国际合作和整合国际上为减少网络威胁所做的努力至关重要而且必不可少。现在是时候了，国际社会要采取一种严肃和务实的做法，通过联合国委员会相关的和专门机构，团结国际上的努力以应对网络威胁。

沙特阿拉伯王国的网络安全领域取得了充满活力的快速进步，其基础是《沙特2030年愿景》及其使能因素和目标。沙特阿拉伯王国在集中治理、分散运行

的基础上，开发了本国的依赖国内机构行使职责的网络安全模式，由此开启了我国的转型之路。

在这方面，我们于2017年设立了国家网络安全局，作为沙特王国负责网络安全的机构和我国的国内参考点。沙特王国采纳了一种综合模式，处理网络安全的各个层面，无论是立法、安全、经济还是发展层面。沙特王国的网络安全工作在国际上受到肯定，最值得一提的是通过国际电信联盟的“全球网络安全指数”受到肯定，根据该指数，我国在全球排名第二，在阿拉伯世界、中东和亚洲名列第一。此外，根据国际管理发展学院的“世界竞争力排名”，沙特阿拉伯王国连续两年即2022年和2023年在网络安全方面全球排名第二。2024年，沙特王国在《世界竞争力年鉴》中名列第一，由此确认了我国作为全球网络安全先锋的地位。

沙特阿拉伯王国相信要加强网络安全方面的国际合作。为此，沙特王国设立了全球网络安全论坛，这个全球性平台汇聚了来自世界各地的决策者， 讨论与网络安全有关的战略性问题。120多个国家参加了该论坛去年的会议。此外，沙特王国设立了网络安全国际论坛，一个总部设于利雅得的组织，旨在加强全球的网络安全，促进这方面的国际合作与社会经济发展，进一步整合网络安全领域的国际努力，以便为实现人类在世界各地的繁荣提供支持。

沙特阿拉伯王国参加了对多个国家和国际组织的能力建设。40多个国家和组织参加了沙特王国举行的网络演练。此外，我们寻求集合区域的努力，以增进地区网络安全。这些努力导致根据沙特王国的建议，在海湾阿拉伯国家合作委员会的主持下设立了一个专门处理网络安全问题的部长级委员会。此外，根据沙特阿拉伯王国提出的建议，在阿拉伯国家联盟下设立了阿拉伯网络安全部长级理事会。阿拉伯国家领导人在最近的首脑会议上决定，该部长级理事会、其秘书处以及执行办公室将设于利雅得市。

最后，加强网络安全人人有责，它要求我们大家开展合作与伙伴协作，以便营造一个安全和有保障的网络空间，使世界各地的所有人得享增长与繁荣。

主席（*以英语发言*）：我现在请阿根廷代表发言。

马伊内罗先生（阿根廷）（*以西班牙语发言*）：我们谨感谢大韩民国举行本次关于网络安全这个对阿根廷极为重要的问题的高级别公开辩论会。

阿根廷认为，我们必须应对的主要威胁并非与世界各地的地缘政治动态无关，考虑到网络空间的全球性和网络事件的跨国性，情况更加如此。在这方面，我们愿强调，在查明潜在或现有威胁以及国家防止和减少威胁所必须采取的措施时，此外还有在开展合作和进行能力建设时，绝不能违反国际法，包括国际人权法和国际人道法，也不应损害《联合国宪章》所载的原则，如有关国家领土完整与主权、不干涉国家内部事务以及和平解决争端的原则。

我们认为，安全理事会的作用及其在网络安全领域的工作绝不能与其它工作重叠，而应补充和借鉴2004年成立的从国际安全角度看信息和电信领域的发展政府专家组的长期工作以及信息和通信技术安全和使用安全不限成员名额工作组当前的工作，该工作组将于7月份审议第三次年度进展报告草案，以期通过该报告。

关于举行定期通报会来评估涉及安理会当前任务授权和议程的不断演变的网络威胁格局的建议，我们认为，至关重要的是，要考虑邀请裁军事务厅的代表以不限成员名额工作组秘书处的身份参加这些通报会的可能，以及邀请工作组主席和学术界、民间社会以及私营部门的代表与会的可能。

尤其是，关于网络空间的新威胁，我们认为，安全理事会将从私营部门代表的报告或介绍中受益，因为在大多数情况下，私营部门是关键基础设施的所有者和运营者。它们还拥有更强大的能力和资源来探索恶意软件的运作情况，这使它们能够随着时间推移不断更新其威胁名单。

我们也欢迎主席在概念说明（S/2024/446，附件）中承认能力建设是一个不可或缺的因素。我们认为，能力建设对于弥合网络安全差距至关重要——这一差距会不加区分地平等影响所有国家，无论其发展

水平如何。那些网络安全能力较差的国家往往存在可被恶意行为体利用的弱点。由于网络空间固有的互操作性，全球网络空间任何地方的漏洞都可能产生重大而广泛的影响。因此，能力建设方面的合作至关重要。只有通过能力建设方面强有力和持续的国际合作，我们才能确保为所有人提供一个真正有韧性、开放、安全、稳定、无障碍、和平、自由和可互操作的网络空间。

在这方面，我们主张，能力建设与执行网络空间负责任国家行为框架有着内在联系。在执行网络空间负责任行为的规范、规则和原则时，必须以促进创新、能力建设技术援助和促进网络韧性技术转让作为补充，这应符合现有国际法，并顾及发展中国家的需求。这不仅将有助于我们各国的福祉和经济发展，也有助于在平等基础上执行和采纳在使用信息和通信技术（信通技术）方面负责任行为不断发展的累积框架，从而促进国际和平与安全。

阿根廷尤为关切使用恶意软件、勒索软件和网络钓鱼的日益频繁的行动及其对关键基础设施的影响。这个关键基础设施中的弱点生态系统已经大大增加，这是国家、私营部门和民间社会共同关切的问题。在这方面，我们强调多利益攸关方合作的重要性，以便继续分析网络空间的现有和潜在威胁，并促进全球层面的行动，如交流经验。与此同时，我们饶有兴趣地注意到信通技术和其他新兴技术为我们社会的发展带来的机遇。我们明白新兴技术是中性的，问题在于我们对它们的控制和使用。在这方面，我们认识到，需要在正在建立的信通技术转让监管框架与所有国家为了自身福祉和社会经济增长而获取新兴技术的权利之间找到一种公平的平衡，并为了造福所有人而促进网络空间的韧性。

最后，安全理事会可以继续发展在信息和通信技术安全和使用问题不限成员名额工作组和其他相关论坛开展的工作，在网络安全领域发挥关键作用。必须确保安理会的行动符合既有的规范和建议。多边协调将促进各国和国际组织之间的合作，推动对网络安全采取统一的方法。

主席（以英语发言）：我现在请格鲁吉亚代表发言。

伊纳什维利先生（格鲁吉亚）（以英语发言）：格鲁吉亚赞同以欧洲联盟的名义所作的发言，并希望以本国代表的身份补充一些意见。

首先，我们感谢主席国大韩民国召开今天的公开辩论会。我们还要感谢各位通报人今天早些时候的深刻介绍。

网络空间的最新动向为创新、经济进步和发展提供了重大机遇。它有潜力提高会员国加强保护开放与和平社会的能力。然而，如果遭到滥用，它也可能造成潜在的威胁。网络安全威胁随着技术进步不断演变，包括恶意软件、网络钓鱼、数据泄露等。面对全球相互关联的危机，安全理事会在应对和尽量减少国际和平与安全所受威胁、包括来自网络空间的威胁方面的作用仍然关键。

近年来，国际社会目睹了某些国家和非国家行为体如何通过将常规作战方法与新开发的非常规手段相结合，威胁到基于规则的国际秩序。一些人使用网络战术来获得战略优势，如破坏通信网络、攻击关键基础设施和破坏军事系统。

在此背景下，格鲁吉亚仍然致力于促进网络空间中负责任的国家行为。我们的网络安全态势符合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和信息和通信技术安全和使用问题不限成员名额工作组制定的规范框架。

过去几年来，由于妇女的参与，我们看到了对和平与安全的更大贡献。妇女更多地参与网络安全领域为更加包容和多样的视角铺平了道路。然而，尽管格鲁吉亚政府努力确保在网络空间负责任的行为，但我们正在目睹俄罗斯激进地使用混合工具侵犯格鲁吉亚主权。在2008年俄罗斯发动全面军事侵略的过程中，格鲁吉亚是第一个在常规军事行动之外成为大量网络攻击的目标的国家案例。

因此, 我们认为能力建设是多边合作不可或缺的因素。在加强国家网络安全能力的同时, 它将促进更高效的国际合作, 以应对复杂的网络威胁, 这些威胁往往超越国界, 需要协调应对。鉴于信息和通信技术能力分布不均, 我们认为, 联合国可以更好地支持各国建立规范性框架的努力, 并协助会员国进行能力建设, 以缩小现有差距。

最后, 我们重申致力于在国家和国际层面加强网络安全, 同时强调网络威胁的跨领域性质以及通过集体行动有效应对这些威胁的必要性。

主席(以英语发言): 我现在请澳大利亚代表发言。

拉尔森先生(澳大利亚)(以英语发言): 我感谢大韩民国召集我们讨论这一重要议题。

我很高兴代表加拿大、新西兰和澳大利亚发言。

网络威胁破坏了数字技术的变革机会。它们的规模和复杂性越来越大, 若在武装冲突中使用, 就构成了特殊的挑战。作为公民和消费者, 我们每天都依赖这些服务, 这意味着涉及关键基础设施的网络事件可能会对整个社会产生毁灭性的连锁影响。它们是现有风险的威胁倍增器, 能够在最基础、最根本的层面上威胁政府的有效运作和公众对政府的信任。

在世界各地, 我们已经看到重大网络事件瘫痪了关键基础设施, 扰乱了基本服务和政府运作。在我们这些国家, 我们非常直接地经历过这种现象。在澳大利亚, 一起涉及医疗部门的勒索软件事件暴露了数百万人的个人信息。在加拿大, 一起勒索软件事件导致省级医疗服务提供者的系统瘫痪, 造成严重延误, 并危及与数千名工作人员和患者有关的敏感信息。在新西兰, 出于经济动机的网络活动的比例首次超过了国家支持的活动。

在当前各个武装冲突局势中, 我们看到军事网络运营方对政府和私营部门网络部署破坏性的恶意软件, 损害参与危机应对的民用关键基础设施和实体, 包括应急服务和能源、运输和通信网络。

[接上段]我们还看到, 使用勒索软件工具实施金融犯罪——包括盗窃加密货币, 直接资助核计划和大规模毁灭性武器计划——与破坏我们实现全球稳定和裁军的努力之间存在明显联系。安全理事会在防止这一联系方面可发挥关键作用。我们欢迎像这样讨论网络威胁的机会, 这有助于将这些问题纳入安全理事会讨论的主流, 提高对这些问题的关注度, 吸纳多利益攸关方的专门知识, 包括民间社会组织的专门知识。

我们共同发出了一个明确信息, 即所有国家在网络空间的活动都要受制约, 都要遵守义务, 就像在实体空间一样。联合国所有会员国一致同意, 现行国际法——特别是整个《联合国宪章》——适用于网络空间。各国必须明确承诺按照国际法和商定的非约束性规范所设定的期望行事。

最后, 我们有两个主要要求。

第一, 我们要求安全理事会确认商定的网络空间负责任国家行为框架, 该框架是和平与稳定的基础, 并促进一个开放、安全、稳定、可进入、和平的网络空间。要实现这些关键目标, 就必须履行和遵守相关承诺, 并辅之以协调开展的能力建设, 以支持所有国家提高应对挑战的能力。

第二, 我们呼吁安全理事会申明, 国际人道法适用于武装冲突局势中的网络空间。这种申明将增强我们对保护关键基础设施和支持国际法特别是《联合国宪章》的集体承诺。

主席(以英语发言): 我现在请库尔图瓦女士发言。

库尔图瓦女士(以英语发言): 红十字国际委员会(红十字委员会)与大韩民国一样, 对武装冲突期间网络行动可能造成的人员损失感到关切。

红十字委员会致力于保护和援助世界各地受120多场武装冲突影响的人。在越来越多的此类冲突中, 网络行动给人民安全和福祉带来更多风险。有三个趋势尤其令人担忧。

第一, 网络行动扰乱了平民基本服务的提供, 如电、水和医疗保健。这种网络行动危及已遭受武装冲突所致破坏和不安全之苦的人们, 且往往构成无视国际人道法的行为。

第二, 我们对民间行为体——个人、黑客团体和科技企业——越来越多地参与到与武装冲突有关的网络行动中深感关切。平民和民用物体越接近敌对行动, 他们受到伤害的风险就越大。

第三, 红十字委员会和整个国际红十字与红新月运动作为人道主义组织也面临日益严重的网络操作威胁, 包括数据泄露和有害信息行动。如果我们的救援行动受到干扰, 或者对我们行动和工作的信任遭到破坏, 则我们援助和保护人民的能力就会削弱。

在安全理事会, 成员们负有维护国际和平与安全的首要责任, 并在武装冲突期间保护平民方面发挥关键作用。安全理事会一贯明确： 战争是有限度的。安理会明确表示, 交战方不得以平民或民用物体为目标, 医疗设施以及人道主义救援行动和人员必须得到尊重和保护。因此, 红十字委员会鼓励安全理事会将网络行动可能造成的人员损失纳入其工作主流, 并有系统地维护国际人道法对所有战争手段和方法——无论新旧、网络战还是热战——施加的长期限制。

最近通过的第2730 (2024) 号决议是朝这一方向迈出的重要第一步, 该决议明确表示关切针对人道主义组织的恶意信息和通信技术 (信通技术) 活动, 并谴责针对人道主义人员的散布虚假信息和煽动暴力行为。在当今数字化世界中, 安全理事会不应忽视信通技术活动在武装冲突期间对平民构成的威胁。

主席（以英语发言）： 我现在请基里巴斯代表发言。

提托先生（基里巴斯）（以英语发言）： 基里巴斯感谢有机会分享对国际和平与安全范畴内信息和通信技术 (信通技术) 使用的看法。我们要感谢秘书长以及来自非政府组织和学术界的通报人分享了各自观点。

本周早些时候, 基里巴斯表示赞同大韩民国就此问题发表的联合声明。我们要赞扬大韩民国在这一问题上发挥的领导作用, 感谢主持本次会议的大韩民国外交部长赵兑烈先生出席会议。主席先生, 我感谢你突出强调安全理事会的作用, 即确保信息和通信技术被负责任地用于促进世界和平与安全, 而不是用于危害国际和平与安全的目的, 特别是在区域战争和暴力冲突呈上升态势之时。

我们同样关切针对民用基础设施的恶意网络活动及其对人们生活和福祉的影响, 特别是对我们社会中最边缘化、最弱势成员的影响。我们对针对水电等关键民用基础设施的网络行动深表关切。这些民用物体受国际人道法的保护。此外, 根据国际人道法, 医疗设施必须得到尊重和保护。在武装冲突时期, 人道主义救济行动也必须受到尊重和保护。

当各利益攸关方就武装冲突局势中的有害网络行动发表意见、呼吁适用国际人道法并就此展开讨论时, 他们这样做是出于对其民众安全的真诚关切。让我们设想一下, 假如有一个这些保护措施不适用于网络行动的世界, 让我们扪心自问, 这样一个世界是否是我们想要生活在其中并称之为家的世界。对我们国家来说, 答案是否定的, 尤其是在太平洋, 我们与大自然、与我们自己和谐共处。

我们必须坚持国际人道法适用于网络领域。因此, 我们坚持认为, 国际社会, 特别是安全理事会, 应听取来自非政府组织和学术界的利益攸关方和行为体对网络犯罪分子的恶意活动表达的关切。我们必须随时准备维护和应用国际人道法原则。因此, 我们强烈鼓励安全理事会将网络行动的人道主义关切纳入主流, 并维持对所有战争手段施加的限制, 包括对国际人道法定义的网络行动。我们不能冒国际人道法在新现信通技术网络领域遭侵蚀的风险。

最后, 我谨回顾美国前总统哈里·杜鲁门79年前为欢迎新诞生的《联合国宪章》而发表的讲话：

“只有当我们理解《宪章》的内涵以及它对世界和平的意义，这份文件才会成为真实存在的人类现实。”

让我们所有人都尊重整个《联合国宪章》，并呼吁控制所有全球技术公司——其中大多数不受政府控制——控制好所有信息和通信技术，确保这些技术被负责任地使用，从而促进对《宪章》的充分尊重，推进《宪章》的崇高目标，为所有人建设一个更加和平、繁荣、人性化和充满爱的世界。

主席（*以英语发言*）：伊朗伊斯兰共和国代表要求再次发言。

艾哈迈迪先生（伊朗伊斯兰共和国）（*以英语发言*）：我知道，今天的会议已经开了很长时间，我不打算占用安理会成员太多时间。然而，我要求再次发言，因为阿尔巴尼亚和以色列政权的代表滥用本会议厅，对伊朗提出毫无根据的指控，诬告我国支持网络攻击。

我们断然拒绝并谴责这些毫无根据的说法。关于阿尔巴尼亚代表在发言中无端提及伊朗一事，我们在2022年9月10日给安全理事会的信（S/2022/685）中回应并驳斥了这一不实之词。我们认为，阿尔巴尼亚政府被恐怖组织、即人民圣战者组织提供的错误信息所误导，错误地将网络攻击归咎于伊朗。

目前以阿尔巴尼亚为基地的人民圣战者组织在包括以色列政权在内的某些国家的协助和支持下，已经对伊朗的关键基础设施发动了数次网络恐怖袭击。这个恐怖组织通过恐怖爆炸和暗杀，使许多伊朗官员和平民成为殉难者，自1981年以来已夺走近17 000名伊朗公民的生命。

尽管如此，伊朗伊斯兰共和国政府还是真诚地向阿尔巴尼亚政府表示，愿意进行建设性的合作和接触，以澄清对伊朗的毫无根据的指控。不幸的是，我们的请求没有得到回应。

关于以色列政权毫无根据的指控，我们坚决予以拒绝。具有讽刺意味的是，一个以在网络和真实空间从事恶意、犯罪和恐怖活动而臭名昭著的政权的代表却指责其他人实施了以色列政权一再实施的行动。

九个多月来，占领政权以色列公然违反包括国际人道法和国际人权法在内的所有国际法律规则、原则和准则，对手无寸铁的巴勒斯坦人民发动了灭绝种族战争和军事侵略，并在本区域从事恶性恐怖行动。该政权直接违反安全理事会相关决议，无耻地使用一切可能的手段来屠杀弱势群体，包括将饥饿作为一种战争方法，无差别袭击包括妇女和儿童在内的平民，蓄意攻击重要民用基础设施，以及阻挠向平民提供基本的人道援助和服务。

此外，该恐怖政权对主权国家的关键基础设施发动网络攻击的历史悠久而黑暗。如伊朗早些时候在本会议厅所作的发言中提到的那样，震网病毒和毒区病毒对伊朗和平核设施的攻击是以色列从事犯罪活动，对关键基础设施发动网络攻击的明显例子。这些犯罪行为为该政权公开承认，是其从事恶意网络行动的明证。

鉴于其历来严重违反国际法基本原则，以色列政权根本不配在遵守这些原则一事上指责或教训其他国家。该政权不应逍遥法外，安全理事会必须追究其已经并继续犯下的所有国际罪行的责任。

下午5时55分散会。