联合国 S/PV.9662

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日星期四上午10时举行
纽约

主席：	赵兑烈先生/黄先生	（大韩民国）
成员：	阿尔及利亚	本贾马先生
	中国	傅聪先生
	厄瓜多尔	德拉加斯卡先生
	法国	德里维埃先生
	圭亚那	佩尔绍德先生
	日本	山崎先生
	马耳他	弗雷泽夫人
	莫桑比克	阿丰索先生
	俄罗斯联邦	涅边贾先生
	塞拉利昂	卡努先生
	斯洛文尼亚	日博加尔先生
	瑞士	尚达夫人
	大不列颠及北爱尔兰联合王国	吴百纳女爵士
	美利坚合众国	托马斯-格林菲尔德夫人

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)

24-17601 (C)

上午10时开会。

通过议程

议程通过。

维护国际和平与安全

应对网络空间不断演变的威胁

主席（以英语发言）：我热烈欢迎秘书长、各位部长和其他高级代表来到安理会会议厅。他们今天的出席凸显了所议主题的重要性。

根据安理会暂行议事规则第37条，我邀请阿尔巴尼亚、阿根廷、澳大利亚、奥地利、巴林、孟加拉国、比利时、巴西、保加利亚、柬埔寨、智利、哥斯达黎加、克罗地亚、古巴、捷克、埃及、萨尔瓦多、爱沙尼亚、冈比亚、格鲁吉亚、德国、加纳、希腊、危地马拉、印度、印度尼西亚、伊朗伊斯兰共和国、以色列、意大利、哈萨克斯坦、基里巴斯、拉脱维亚、列支敦士登、摩洛哥、尼泊尔、挪威、巴基斯坦、巴拿马、菲律宾、波兰、葡萄牙、罗马尼亚、沙特阿拉伯、新加坡、西班牙、土耳其、乌克兰、阿拉伯联合酋长国、乌拉圭和越南代表参加本次会议。

根据安理会暂行议事规则第39条，我邀请以下通报人参加本次会议：网络和平研究所首席执行官Stéphane Duguin先生；利兹贝克特大学法律和技术教授Nnenna Ifeanyi-Ajufo女士。

根据安理会暂行议事规则第39条，我还邀请下列人士参加本次会议：欧洲联盟驻联合国代表团代表、临时代办海达·萨姆森夫人阁下；国际刑警组织驻联合国特别代表罗赖玛·安娜·安德里亚尼女士；红十字国际委员会常驻联合国观察员Laetitia Courtois女士。

安全理事会现在开始审议其议程上的项目。

我谨提请安理会成员注意文件S/2024/446，其中载有2024年6月7日大韩民国常驻联合国代表给安全理事会主席的信，转递关于正在审议的项目的概念文件。

我现在请秘书长安东尼奥·古特雷斯先生阁下发言。

秘书长（以英语发言）：我感谢大韩民国召开这次高级别辩论会，讨论影响我们所有人的问题——网络空间的和平与安全。

从信息和通信技术、云计算到区块链、5G网络、量子技术等，数字技术的突破正在飞速发生。数字进步正在彻底改变经济和社会。它们使人们走到一起；通过点击屏幕或点击鼠标来传递信息、新闻、知识和教育；使公民得以获得政府服务和接触政府机构；并大力助推经济、贸易和金融包容性。

但正是给网络空间带来巨大惠益的无缝和即时连接为也可能使个人、机构和整个国家陷入深深的脆弱之中。数字技术被用作武器的危险逐年增加。网络空间令大门洞开，任何人都可以乘隙而入，很多人的确也乘隙而入。国家和非国家行为体以及彻头彻尾的犯罪分子在网络空间实施的恶意活动呈上升趋势。

严重的网络安全事件司空见惯，令人不安。医疗保健、银行和电信等基本公共服务遭到侵入；非法活动，包括犯罪组织和所谓的网络雇佣军的活动持续不断；大批宣扬仇恨者在信息高速公路上散布恐惧和分裂；网络空间越来越多地被用作持续武装冲突中的另一种武器。所谓的平民黑客活动分子正在加入进来，并在许多情况下模糊了战斗人员与平民之间的界限。数字工具与武器系统（包括自主系统）的日益集成带来了新的隐患。

与此同时，数字技术的滥用正变得更加狡猾和隐蔽。恶意软件、擦除工具和木马正在激增。人工智能辅助的网络行动正在加剧威胁，量子计算则可能因其破坏加密的能力而破坏整个系统。软件漏洞被利用，网络入侵能力甚至通过互联网出售。公司的供应链正成为黑客起劲攻击的目标，造成严重的、破坏性的连锁效应。勒索软件就是一个令人悲痛的例子——对公共和私人机构以及人们依赖的关键基础设施构成巨大威胁。据估计，2023年勒索软件造成的支付总额将达到11 亿美元。

但远甚于金钱损失的是我们共同的和平、安全和稳定遭受的损害——无论是在国家内部还是在国家之间。破坏公共机构、选举进程和网络诚信的恶意活动会侵蚀信任，加剧紧张局势，甚至播下暴力和冲突的种子。

数字技术提供了一个难以置信的机会，为所有人创造一个更加公正、平等、可持续与和平的未来。 但突破必须朝着好的方向发展。《新和平纲领》将预防摆在所有和平努力的核心位置。它呼吁制定符合国际法、人权和《联合国宪章》的强有力框架，并呼吁所有国家集中努力，防止网络空间内部和通过网络空间造成冲突扩大和升级。正如《法治新愿景》所反映的那样，法治必须像存在于现实世界一样，存在于数字领域。

我还欢迎大会承诺在该领域采取行动，其中包括专门负责信息和通信技术安全及使用的不限成员名额工作组。各国正在得到普遍认可的、网络空间方面负责任国家行为规范框架的基础上推进工作。它们正在积极考虑国际法是否适用于国家在该领域的活动。在大会主持下，会员国在努力在未来几个月内就新的网络犯罪条约达成共识，该条约应在保护网络人权的同时深化合作。但鉴于网络空间与全球和平与安全的联系日益明显，安理会也可以通过将网络相关考虑纳入其现有工作流程和决议来发挥关键作用。

这是安理会第二次就此问题举行正式会议。但是，在这个会议桌旁审议的许多问题都受到网络空间的影响并与网络空间相关联，包括在武装冲突中保护平民、和平行动、反恐和人道主义行动。将这一问题纳入安理会的审议，将是为更有效地应对这一重要问题奠定基础的有益方式。

（以法语发言）

为保障实体世界的和平与安全，我们需要采取新的方法来处理数字世界的和平与安全问题。9月份的未来峰会将是加强合作应对重大全球挑战和重振多边体系的重要契机。峰会将产生的未来契约为支持维护网络空间国际和平与安全提供独一无二的机会。除其他优先事项外，未来契约第二章旨在重申全球共识，即保护关键基础设施免受有害数字做法的危害，为包括人工智能在内的数据驱动技术建立更强的问责制。与此同时，我的人工智能高级别咨询机构正在完成其最终报告，探讨我们如何为人类治理人工智能，同时解决其风险和不确定性。我期待与安理会、大会和所有会员国合作，确保技术得到适当利用：为全人类和我们共同的地球的进步和安全而努力。

主席（以英语发言）：我感谢秘书长的通报。

我现在请Duguin先生发言。

Duguin先生（以英语发言）：今天很荣幸在安全理事会就一个至关重要的问题发言：如何应对网络空间不断演变的威胁。作为设在瑞士的独立中立非政府组织网络和平研究所的首席执行官，我的发言内容属于经验之谈，因为本研究所向最弱势的非营利组织群体提供免费网络安全服务，监测威胁行为体，提供威胁检测和分析，并倡导尊重网络空间的法律和规范。

在我们分析这一威胁的演变时，我想谈一谈威胁形势发生的重大颠覆性变化及其产生的叠加效应，这些变化综合在一起对维护国际和平与安全产生了直接影响。我将谈到各种主题：威胁行为体扩散并愈加以关键基础设施为攻击目标；威胁在今天的突变——特别是网络攻击与虚假信息相结合，以及利用网络攻击规避国际制裁；威胁在明天的演变——人工智能对网络安全构成的独特风险。这些演变给国际和平与安全带来了独特的挑战，特别是阻碍了归责，即确定网络攻击或行动实施者或源头的过程。

我首先谈威胁行为体扩散。自2022年俄罗斯联邦入侵乌克兰以来，网络和平研究所一直在记录支持交战双方的威胁行为体的扩散。战争不再是国家的专属。一系列非国家行为体——犯罪集团、具有地缘政治动机的黑客活动组织和其他平民——正在武装冲突中参与网络攻击和行动。他们追求四个目标：摧毁基础设施，扰乱基本服务的正常运作，同步进行虚假信息散布和网络攻击，以及通过渗透和间谍活动窃取

数据并用作武器。在这方面，我们网络和平研究所追踪了127个威胁行为体的3000多次网络攻击活动，涉及56个受影响国家和24个被针对的关键基础设施部门。这些网络攻击造成的伤害远远超出了交战国的边界，所有网络攻击中有近70%影响到非交战国的组织。这些衡量指标可在我们的冲突时期网络攻击平台上免费获得。这种攻击扩散导致缓和局势成为问题，阻碍停止敌对行动。在这种情况下，如何才能使这127名威胁行为体停止恶意活动或使其受控？

这种攻击扩散对关键基础设施的安全产生了直接影响。我要举两个例子。2022年2月，一次网络攻击以乌克兰宽带卫星互联网接入为目标，使用了名为“AcidRain”的雨刷恶意软件。攻击的重大影响超出了乌克兰边界。它到欧洲各地风力涡轮机的运行，德国一家主要能源公司失去了对5800多台风力涡轮机的遥控监测，德国、法国、匈牙利、希腊、意大利和波兰的数千名卫星互联网服务用户受到影响。这种重大影响不仅仅发生在武装冲突时期。在2019冠状病毒病（COVID-19）大流行期间，网络和平研究所在大流行的两年时间里监测到500起针对医疗卫生机构的网络攻击。500次网络攻击连冰山一角都算不上——也就是冰山一角上的一小块冰。仅这500次攻击就使43个国家的医疗卫生服务被中断扰乱，导致2000万患者的数据被盗，相当于医疗卫生服务五年时间里累计遭到的扰乱数量。这意味着五年累计的救护车改道、预约取消、患者医疗服务机会减少。

但不断演变的威胁的另一个方面是利用网络攻击来逃避国际制裁以及资助非法活动。例如，一些民间社会行为体、网络安全组织和国家分析了两个被控犯罪团体——Kimsuky和拉撒路集团——的活动，从其战术、工具、程序和意图看系朝鲜民主主义人民共和国所为。这两个犯罪集团协调进行所有类型的全球网络攻击：供应链、勒索软件、加密货币交易所和金融机构。除了主要造成直接重大危害之外，此类攻击还成为规避国际制裁依托的载体。根据最近的估计，拉撒路集团和Kimsuky从此类攻击中获利超过30亿美元。这种升级造成了巨大危害。2017年5月的WannaCry攻击在不到24小时内影响了150多个国家的25万多台计算机，引发严重的服务中断，对医疗卫生、金融和交通等部门造成大范围影响。

有关威胁演变的最后一点，预见新风险十分重要，如前面提到的量子计算对密码学的威胁，以及生成式人工智能对犯罪模型的威胁。自生成式人工智能和大型语言模型出现以来，人工智能已被恶意行为体用来增强能力。今天，人工智能被用来扩大所谓网络杀伤链中的现有程序，这是任何攻击者实施网络攻击的必经标准程序。例如，使用人工智能可节省识别目标的时间，自动化漏洞搜索，提高网络钓鱼的产能。这只是第一步，因为已经有组织在试验使用生成式人工智能来自动化网络攻击的不同环节。这带来了不可接受的风险。若测试成功，就有可能使整个网络杀伤链的自动化程度大大提高，以至于恶意行为体可能故意也可能意外触发自主网络攻击。

鉴于几大变化相互交汇——威胁扩散、攻击关键基础设施或规避制裁出现特定新模式、新人工智能技术带来新变化，很难用一个单一战略来应对。尽管如此，还是可以采取几种措施，我最后就来谈这个方面。

我们可以落实法律、规范以及制裁，特别是通过透明地记录违犯行为和采取一种前瞻式的做法，以防止恶意使用网络空间，包括滥用人工智能或量子计算。

揭露违犯者、执行制裁以及采取妥善和充分的措施非常重要。不进行归因，就不可能有局势的缓解，因为它对于做出知情的决定以采取措施和防御至关重要。归因可具有威慑作用，因为追究违犯者的责任可促成法律和外交上的回应，加大政策制订的力度。

最后，至关重要的是，要能够全面、可量化地衡量网络攻击造成的损害。网络和平研究所正在制订这样一种方法，以衡量网络攻击造成的损害，因为迄今往往从金钱或能力损失的角度来进行描述，而人口和社会架构遭受的损害也同样重要。

这些方面对于维护国际和平与安全至关重要。

主席（以英语发言）：我感谢Duguin先生的通报。

我现在请Ifeanyi-Ajufo女士发言。

Ifeanyi-Ajufo女士（以英语发言）：我深感荣幸地受邀在本次论坛上发言，探讨维护国际和平与安全，并处理网络空间不断演化的威胁，尤其是通过提供区域视角和审视非洲的局势。

在有关网络空间的和平与安全的任何讨论中，都有必要通过现有的区域现状和视角，来衡量网络空间的安全。我们必须承认，有效实现网络安全常常与发展中国家、特别是非洲地区发展中国家的现状相抵触，这些国家仍处在数字鸿沟的末端，缺乏充足的能力、技能以及基础设施，按照预期的标准有效确保和平与安全。因此，在承认我们在网络安全方面的共性的同时，我们也必须承认不同地区之间的差异与挑战，从特定的国家和区域现状的角度来思考网络威胁。

网络空间的和平与安全层面已成为许多地区的一项根本议程。例如，2022年11月，非洲联盟和平与安全理事会首次从根据国际法的规则来进行监管的角度处理了网络空间的和平与安全问题。此后，非洲联盟采纳了网络安全，作为《非洲联盟2063年议程》的一个旗舰项目，并且作为非洲联盟《2020年至2030年非洲数字化转型战略》的一个贯穿各领域的主题。重要的是，《非洲联盟网络安全和个人数据保护公约》于2023年6月生效，这为减少网络威胁和保护信息通信技术（信通技术）基础设施提供了一个统一的监管框架。今年1月，非洲联盟还通过了有关国际法适用于网络空间中的信通技术使用的非洲共同立场。我必须补充的是，非洲的立场是首项包含了一个能力建设部分的有关国际法适用于网络空间的立场文件。非洲也是首个制订区域共同立场的地区。

我们还必须承认，在各地区如何能够维护网络空间的和平、安全与稳定方面存在各种挑战。例如，去年以来，我们看到非洲联盟委员会总部遭到网络攻击，电子邮件系统的运作遭到破坏。肯尼亚通信局宣布，仅2023年，肯尼亚就记录了8.6亿次网络攻击，该国的关键信息基础设施遭到策划精密的攻击。仅2023年7月，肯尼亚非常重要的eCitizen平台就遭到引起高度关注的网络攻击，使得部委、县政府以及机构提供的5000多项政府服务无法接入。一个自称为“匿名苏丹”的团体声称对肯尼亚和非洲其它地区的这些网络袭击负责。数月前，有组织的网络攻击迫使马拉维政府暂停发放护照，此前移民局的电脑网络遭到网络攻击，被视为一起严重的破坏国家安全事件。

由此提出了重要问题，包括区分国家行为体和非国家行为体所负责任的界限模糊，以及这些新兴网络威胁如何加剧已有冲突的分裂的动态。我们看到有组织的恐怖团体和极端团体的活动如何因为非洲多地区的冲突而变得更加嚣张。我们不仅看到网络空间的犯罪活动加剧该地区国际和平与安全已经面临的威胁与挑战，而且还看到国家如何以网络安全为名违反国际人权，关闭互联网接入，特别是在武装冲突期间。这些行为不仅侵犯民众的通信权与信息自由，而且使得无法在冲突期间在非洲、当然还有其它地方开展有效的人道主义行动。我们还看到，网络促成的虚假信息和错误信息正在越来越多地被作为工具，用来破坏部分地区的和平与安全。在这些情况下，人工智能的使用进一步加剧了局势。

但是，我们相信，安全理事会能够带来巨大变化，加强网络空间的和平与安全，尤其是采取一种区域性视角。确实，现有的不平等要求进行复杂的互动，以便界定安全理事会在网络空间的和平与安全方面的任务授权。网络安全基础设施和数字能力方面的这些差距加上诸如非洲这样的地区持续存在的政治冲突，提出了重大挑战。对于网络空间环境下的不干预、尽职以及和平解决争端方面的义务似乎也缺乏认识。

因此，在安全理事会确定其维护网络空间的和平与安全的任务授权时，重要的是，要思考那些可被有效利用来反击现有威胁并且增强能力的协作式措施。有必要建立和增强区域一级的能力。但是，我们必须指出，这不只是一个法律、技术以及业务能力的问题，而且也是一个涉及社会、经济以及政治现状的问题。鉴于网络安全的成熟度和当地背景各有不同，需要进

行战略性的区域能力建设。必须顾及不同地区的特定现状，因为各地区的能力差距未必一样。尝试开发不同地区的网络能力并进行地区间转让的做法必须有目的地进行，但是也必须基于已界定的问责机制进行战略规划。

在诸如非洲这样的地区，需要进行能力建设以处理与网络有关的威胁的优先领域包括治理、政策制订、技术工具与基础设施以及研究。有必要开发用于保护关键基础设施的能力。重要的是，要确保在尚未设立地区一级网络安全事件应对小组的地方设立这些小组，并且授权设立24/7的地区联络人。开发和实施在这些小组中开展区域和国际协作的机制也非常重要。

为促进网络空间的信任与安全，有必要侧重于在所有地区执行联合国网络空间负责任国家行为规范。关于这些规范的自愿性质和有必要在维护网络空间的和平与安全方面采取更多接受问责的做法，已经提出了许多问题，比如制订定义明确的关于在网络空间使用武力、武装攻击以及自卫的指导方针。建立和支持旨在制订建立信任措施的论坛将减少会员国之间的不信任，推动在网络空间和平地解决争端。

重要的是，安全理事会还要开发用于了解跨地区网络威胁格局的机制，借此将能够在监管安全与稳定方面做出知情的决策。这也可能意味着成立一个网络空间和平与安全方面的工作组——首先是思考就冲突和促进网络空间和平与稳定提出建议。发展正常运作的区域网络安全中心以加强跨界合作和信息共享也将有助于实现这些目标。还应重视为制定和实施全面的区域和国家网络安全战略提供能力支持，也应推进一种网络安全领导文化。

区域组织在制定政策和与本区域各国合作来实现和平与安全成果方面可以发挥关键作用。因此，联合国与区域和次区域组织在维护国际和平与安全方面的现有合作现在应该包括一个网络安全议程。最后，安全理事会应推动建立一个平台，促成旨在鼓励各区域发展网络空间和平与安全框架的有效对话。

最后我要补充的是，安全理事会必须推行一项多边议程，明确申明网络空间法治的和平与安全层面。这也需要设立明确的网络治理原则和标准，让所有区域和政府为和平与稳定负责。随着我们的相互联系变得更紧密，同时更加受到人工智能等颠覆性技术的影响，我们也变得更为脆弱。因此至关重要的是，要通过建立对使用网络技术的信任和信心，加强我们保护网络空间的人力和机构能力。

主席（*以英语发言*）：我现在以大韩民国外交部长的身份发言。

首先我要再次感谢古特雷斯秘书长出席今天的会议并作通报。我也要感谢网络和平研究所的Stéphane Duguin先生和利兹贝克特大学的Nnenna Ifeanyi-Ajufo教授分享他们的见解和专业知识。我也深切感谢所有会员国代表参加本次高级别公开辩论会。

今天的会议是联合国历史上安全理事会第二次正式开会讨论网络空间对国际和平与安全的威胁。三年前的2021年6月，安理会就该议题举行了首次公开辩论会（见S/2021/621）。诚然，在安全理事会之外已经完成了一些阶段性目标。大会设立的实体拥有与时俱进的网络空间负责任国家行为规范。还举行了多场关于网络安全的阿里亚办法会议，最近一次是大韩民国与美国和日本共同主办的4月会议。

秘书长也展现了强有力的领导力，呼吁采取措施降低网络相关风险，并建立了人工智能高级别咨询机构，韩国参与了该机构。但自三年前安全理事会第一次会议以来的事态发展清晰表明，为什么安理会现在比以往更加需要积极主动地就来自网络空间的威胁加大互动。除了大量跨界网络攻击之外，世界还目睹了一些大型武装冲突的爆发，其中，攻击不仅发生在传统战场上，也发生在网络空间。

世界也看到了人工智能的爆炸性进步如何大大增强了邪恶行为体在网络空间造成进一步混乱和破坏的能力。世界看到了恶意网络活动如何破坏人们对政治选举的廉正、关键基础设施的安全以及和平与安全结

构的信心，从而对现实世界产生影响。事实上，一个会员国在遭受来自另一个国家的勒索软件攻击后，甚至不得不宣布进入紧急状态。

网络手段本质上具有两用性：任何怀有恶意的人都可以带来新的威胁或引发、扩大或加速现有的威胁。正如著名的未来学家阿尔文·托夫勒曾经指出：“我们的技术力量增强了，但是副作用和潜在危险也增加了。”

大韩民国对恶意网络活动构成的威胁及其对安全的影响并不陌生，因为危及韩国的大规模毁灭性武器的发展在很大程度上是通过此类活动资助的。第1718（2006）号决议所设委员会专家小组的最新报告（S/2024/215）列举了朝鲜民主主义人民共和国大规模毁灭性武器计划的40%资金是如何通过非法网络手段获得的。该小组原先在调查朝鲜民主主义人民共和国在2017年至2023年间对加密货币公司实施的约60起涉嫌网络攻击。可悲的是，该小组现已停止运作，原因众所周知。

朝鲜民主主义人民共和国通过数字手段，系统性地规避安理会通过的专门制裁，并挑战作为安理会工作一部分的国际不扩散制度。在现实世界和网络世界的和平与安全日益交织的时候，安全理事会绝不能把头埋进沙子。至少，它必须跟上安理会之外的趋势，并加强参与，以应对当下来自网络空间的真实威胁。正如安全理事会和大会在讨论小武器、恐怖主义和不扩散问题时协同工作一样，它们同样可以在网络安全问题上发挥互补作用。

虽然对于前进道路还没有定下权威的方法，但大韩民国想提出以下三点建议供安全理事会考虑。

第一，安理会要对当前局势有一个明确的诊断。为此，安全理事会可以要求定期提交报告，以审议网络威胁如何与安理会的任务产生交集，以及不断变化的网络威胁如何影响国际和平与安全。

第二，随后开出的药方必须包括安理会的全部问题。网络安全可以用类似于妇女与和平与安全以及青年与气候变化等其他跨领域问题的方式纳入安理会议程的主流。正如许多会员国在4月份的阿里亚办法会议上指出，恶意使用信息和通信技术与安全理事会职权范围内的各种问题，包括制裁、不扩散和恐怖主义，有着直接联系。本着这种精神，安理会可以将网络安全视为贯穿其区域和专题问题的一个主要组成部分。

第三，从中长期来看，安全理事会应该能够找到应对这一挑战的适当办法。安理会可以就违反国际法和危害和平与安全的恶意网络活动召开会议。此外，它可以敦促所有相关行为体以负责任的方式使用网络技术，并通过安理会所掌握的工具追究责任。不用说，安全理事会应该以补充大会当前讨论的方式制定一项网络安全工作方案。

安全理事会有过根据新出现的安全挑战制定自身议程的经历。《联合国宪章》的设计者想不到气候变化、践踏人权和疫情会成为安全理事会的职权范围。安全理事会要想在应对当代其中一个最紧迫的安全挑战时保持现实意义和灵活性，就必须直面网络安全问题。我真诚希望，今天的公开辩论会将为实现这一目标创造势头。

在结束发言之前，我要补充最后一点。网络空间的无国界性质使所有国家——无论是数字发达国家还是脆弱国家——都面临恶意网络活动的危害。网络空间的国际安全取决于其最薄弱的环节。因此，人道主义-发展-和平的关系在网络世界中同样真实。一个没有恶意网络活动的网络空间将促进数字发展，带来数字机遇，最终促进实现可持续发展目标。一个开放、安全、易于使用、和平的网络空间能够有效遏制网络威胁，也将保护网上自由和人权。

我恢复行使安理会主席职能。

我现在请美国常驻代表、拜登总统内阁成员琳达·托马斯-格林菲尔德夫人阁下发言。

托马斯-格林菲尔德夫人（美利坚合众国）（*以英语发言*）：首先，我要感谢大韩民国再次召集我们开会，讨论这一关涉和平与安全的关键问题和事项。主席先生，我要欢迎你来到安全理事会，并表达我的强

烈赞赏。我几个月前访问首尔时曾有幸与您会面，您能来这里真是太好了。我感谢秘书长和各位通报者的通报，并欢迎其他部长今天莅临会场。

上次4月份的会议之后，我们继续看到建立强有力的网络空间安全势在必行，因此有必要在安理会讨论这个问题。网络安全让我们最基本的系统能够运作起来，包括我们的经济和民主机构、甚至包括联合国本身。美国致力于与所有负责任的行为体合作，保护网络空间的利益，建立数字团结，利用技术实现可持续发展目标。然而，太多的国家和非国家行为体却采取了相反的做法。在世界各地，他们利用数字互联勒索受害者牟利、窃取政府和私营实体的资金和想法、瞄准记者和人权维护者、抢占未来冲突的先机、威胁我们的关键基础设施，甚至在联合国里都这么干。

作为安理会成员，我们必须共同努力，应对国家和非国家行为体带来的网络威胁，加强负责任的国家行为规范，追究网络空间不负责任行为国的责任，支持受这种行为影响的受害者，瓦解全球危险网络攻击背后的犯罪分子网络。目前已经有了这样一个框架。多次以协商一致方式通过的《网络空间负责任国家行为框架》明确指出，国际法适用于网络空间，各国应维护和平时期国家行为自愿规范。这些规范包括各国应调查来自其领土并针对他国关键基础设施的恶意网络活动，并减轻其影响。然而，一些核可该框架的国家却选择对不良行为者视而不见，甚至更糟糕地赋予他们权力。

这一点在四月份关于网络安全的”阿里亚模式”会议上得到强调，其中包括朝鲜民主主义人民共和国开展恶意网络行动，用于资助大规模杀伤性武器和弹道导弹计划。其中还包括俄罗斯在乌克兰、德国、捷克、立陶宛、波兰、斯洛伐克和瑞典的网络活动，在这些国家，俄罗斯总参谋部情报总局除开展其他活动外，还将目标对准了各个政党和民主机构。不仅如此，俄罗斯政府还是勒索软件行为者的避风港，近年来，勒索软件行为者给医院和其他重要基础设施造成了数十亿美元的损失和重大破坏。

就我们而言，2月份，美国和英国宣布采取行动，瓦解LockBit勒索软件集团。该集团以2 000名受害者为目标，索要的赎金总额高达数亿美元，而超过1.2亿美元已经支付。最近几个月，我们公布了一份起诉书，指控俄罗斯人阿图尔·松加托夫和伊万·康德拉季耶夫（又名Bassterlord）部署 LockBit，在美国和全球攻击众多受害者。除此之外，我们还通过2021年成立的国际反勒索软件倡议这一目前世界上最大的网络伙伴关系作出了各种努力。我们呼吁，所有国家应各自通过这一伙伴关系，在联合国等多边论坛上，各尽其责地执行《框架》，促进网络空间的和平与稳定。我们也呼吁安理会确保将网络安全作为贯穿各领域的优先事项，在我们任务授权的各个方面得到考虑。安理会无论是在考虑维和行动如何能够促进良好的网络卫生以限制风险的时候，还是在更好地理解网络安全如何能够加强防扩散努力的时候，都必须继续从网络安全的角度看待各种挑战。

我们有能力保护我们最关键的基础设施和所有依赖这些基础设施的人。我们也有潜能为所有人守卫网络空间福利。因此，让我们以《网络空间负责任国家行为框架》为指导，申明并重申国际法适用于国家对国家的行为。让我们更好地遵守和平时期负责任国家行为自愿规范,帮助减低网络事件引发冲突的风险。让我们维护以规则为基础的国际秩序，确保数字世界对现实世界带来良好的影响。

主席先生，我再次感谢您召集我们讨论这一重要问题。

佩尔绍德先生（圭亚那）（*以英语发言*）：我感谢大韩民国外务大臣赵泰愚先生阁下和大韩民国主席团组织今天的公开辩论会，讨论如何应对网络空间不断演变的威胁。我还要感谢秘书长和通报者为讨论提供真知灼见。

技术快速进步给世界创造了无限的可能，带来了巨大的经济、社会和地缘政治利益。然而，在数字技术变得越来越复杂，并且被恶意行为者所利用的情况下，就给人类安全和国家安全带来前所未有的风险。

数字技术的恶意使用还显示出破坏机构的潜力，带来与治理有关的监管和政策挑战。此外，网络威胁的跨国界性质还使传统的国家安全和国防概念变得过时。

我们现在面临的网络安全威胁可能对公民的健康、安全和安保以及基本服务的运作造成破坏性影响。随着当前的网络安全威胁变得更加错综复杂、具有更多层面，从国家支持网络间谍活动、干预民主进程、侵犯人权、攻击关键基础设施到传播错误信息、虚假信息和仇恨言论，我们的应对措施也必须更加复杂和多面。

对此，我建议从三个方面加以考虑。

首先，必须建立问责和监督机制，防范网络攻击。在这方面，我们注意到最近讨论了针对医疗设施或发电厂等关键基础设施且造成危及生命严重后果的网络攻击，是否构成战争罪、危害人类罪、灭绝种族罪和（或）侵略罪。对此必须进行彻底审查，将其纳入全球法律框架，同时必须确保数字工具和技术的开发和使用应充分考虑道德因素和尊重人权。在这方面，圭亚那认为，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必须完成，而且必须订立一项得到广泛批准的公约。

第二，我们必须将合作、协作和伙伴关系作为优先事项，建设网络安全能力和复原力，并在各国和各区域调查和起诉网络犯罪。在伙伴关系方面，我们必须大力增进信任，加强区域和国际合作，以促进知识共享、信息交流和技术转让。我们还必须寻求在我们负责跟踪和监测网络安全威胁的国家、区域和国际系统之间发展互操作性。为了取得成效，必须制定一个全球框架，以满足各国和相关利益攸关方之间就网络安全面临的新威胁分享情报的需要。联合国和区域机制内正在进行的讨论，包括在秘书长的数字合作路线图和可持续发展目标数字加速议程框架内进行的讨论，为这一努力作出了积极贡献。尽管如此，仍有许多工作要做。我们还必须利用网络领域提供的机会，采取全社会办法，应对网络威胁，加强网络安全。

人工智能系统等新技术可帮助识别和减轻此类威胁。在这方面，作为政府，我们必须加倍努力，与技术公司和私营部门协作，开发更有力的安全工具，制定更有力的政策，并在分析威胁情报方面加强信息共享。此外，圭亚那等许多发展中国家缺乏应对网络威胁和建设抵御威胁能力所需的资源和专门知识。必须将在这些国家建设技术能力视为对我们集体安全的投资，这将有助于消除网络安全能力方面现有的不平等和不平衡状况。考虑到这一点，作为一个全球大家庭，我们可以探讨设立一个全球基金的可能性，以满足培训和能力建设以及软件和硬件开发的需要。此外，圭亚那呼吁拥有先进技术能力的发达国家提供技术援助和资金，以加强发展中国家的网络安全基础设施和应对能力。应不遗余力地确保没有任何一个国家或实体垄断技术工具和能力，因为这可能进一步加剧发展中国家的脆弱性，如通过实施具有域外影响的法律和条例。

第三，尽管在联合国其他论坛内正在开展各种进程，但鉴于恶意网络活动对国际维护和平与安全构成的威胁，安全理事会必须成为网络安全对话的参与方。因此，安理会必须在“阿里亚办法”会议和公开辩论会——包括本次辩论会——的基础上进一步做出努力，加强对这一问题的讨论，以提高人们对新技术构成的新威胁的认识，并共同探讨可采取的有效措施，打击恶意使用这类技术的行为。

最后，网络安全威胁构成的挑战令人生畏，但并非不可战胜。共同努力，展现决心，并一致采取行动，我们就能建设一个能抵御攻击的安全数字世界，促进信任、创新和繁荣，造福每一个人。让我们抓住这个机会，不只要应对我们面前的威胁，更要积极主动地塑造未来，确保没有人掉队。圭亚那随时准备与所有会员国一道，为这一事业而努力。

涅边贾先生（俄罗斯联邦）（*以俄语发言*）：主席女士，我们很高兴看到你主持安全理事会工作。我们感谢秘书长的通报。我们也认真听取了通报人的发言。

联合国启动对国际信息安全问题的讨论时，俄罗斯就在现场。1998年，即26年前，我们介绍了关于这一特定议题的第一项决议（大会第53/70号决议），从而在大会首次提出该议题。就这一议题通过决议自此成为每年一度的活动，得到绝大多数会员国的支持。

在我们的倡议下，设立了相关的联合国政府专家组，以讨论信息和通信技术（信通技术）使用过程中的安全问题。后来，它发展成为一个形式包括各方的工作组——信息和通信技术安全及使用问题不限成员名额工作组，一个在联合国主持下讨论各种国际信息安全问题的独一无二的统一谈判平台。

自开展活动以来，不限成员名额工作组已证明其作用和价值。它的实际成果包括在俄罗斯的倡议下，于5月份推出了一个联络人名录，用于交流计算机攻击或事件信息。对国际信息安全领域的现有和潜在威胁的详细审查正在进行中。目前还在采取具体步骤建设各国的数字能力。去年商定了在这一领域提供援助的普遍原则。

我们认为，国际社会的努力应侧重于继续加强各国在不限成员名额工作组框架内的合作，以便在确保国际信息安全方面取得具体、实际的成果。我们认为，至关重要的是，应在不限成员名额工作组现有任务框架和今后的谈判形式之内，巩固和扩大工作组所取得的成果。俄罗斯已提出在该领域建立一个包容性常设机制的设想。我们认为，在2025年后设立一个具有决策职能的不限成员名额常设工作组，以维护我们的共同成果，将是明智之举。

上述事实清楚地表明，长期以来，联合国一直在国际信息安全方面循序渐进地开展工作。因此，安全理事会参与的必要性受到严重质疑。这一议题有其自身的特点，应在具备相关专门知识的专门论坛上进行讨论。必须保持讨论的专业性和建设性，避免政治化。重复国际社会的努力，将这一议题拿到联合国各论坛讨论，效果只会适得其反，并可能逆转几十年来在大会主持下取得的所有成果。

同样重要的是，不限成员名额工作组的讨论包容各方。所有联合国会员国都可以毫无例外地平等参与，因为决定以协商一致方式作出。把这个问题转交安全理事会将自动把所有不是安理会成员的国家排除在决策之外。今天支持主席呼吁将国际信息安全问题列入安全理事会议程的人显然应铭记这一点。

最后，任何关于潜在风险的讨论都必须考虑到网络空间的技术特性。与现实世界不同，网络空间的威胁极难识别，而识别攻击来源——即所谓的归责——则更加困难。通常需要很长时间才能通过间接证据意识到袭击已经发生的事实。因此，对于哪些恶意使用信息和通信技术的案例可被有把握地视为对国际和平与安全的直接威胁，我们甚至还没有一个基本的认识。在归责问题得到解决，并就这一多方面的具体问题的其他复杂方面，包括法律方面，形成统一的立场之前，安全理事会的任何讨论都可能变成又一次毫无根据的指控，加深国际社会的分歧。这将损害安理会的权威，也完全无助于制定建设性的解决办法。

今天已经发言或将发言的所有国家都是不限成员名额工作组的参与方，提议讨论的问题与工作组讨论的问题类似。5月，举行了一次部长级圆桌会议，讨论了国际信息安全领域的能力建设问题，而不限成员名额工作组第八届会议将于7月举行。事实上，对这一议题的讨论已经在进行，其进展和结果大家有目共睹。

因此，我们不支持通过定期召开安全理事会会议来提高国际社会对国际信息安全问题的认识的呼吁。安全理事会的任务规定所设想的是，对国际和平与安全面临的真正威胁迅速作出反应，而不是就公共领域的共同议题进行哲学式的意见交流。有其他的论坛和模式可供进行此类交流。

西方同事试图提出关于使用信通技术进行恶意活动的指控，然后借此来对付“不受欢迎”的国家，这也令人极为担忧。此外，他们从未提供任何令人信服的证据来支持这些话。

安全理事会第1718（2006）号决议所设委员会朝鲜民主主义人民共和国问题专家小组一再成为这场

肆无忌惮游戏中的工具。根据一个特定会员国的密报，专家小组与俄罗斯方面接触，商讨被认定是平壤所为的计算机攻击。当我们要求提供调查指称事件所需的准确资料时，专家们回答说，他们没有从其“消息来源”收到任何额外资料。然而，完全缺乏细节并不妨碍我们的西方同事毫无根据地指责不赞同他们行动的国家背负着所有“网络原罪”。通常，这种指控被称为“极有可能”，这是西方国家最喜欢的表达方式。这种没有实质内容的影射是不可接受的。确定责任归属需要专业的方法和全面的技术证据。

我们坚决反对任何关于俄罗斯涉嫌鼓励网上恶意行为的猜测。四分之一个世纪以来，我们一直倡导防止网络空间军事化，甚至在西方国家认识到这种风险存在之前，我们就开始提出这方面的具体步骤。

我国的优先事项是制定具有普遍法律约束力的网络安全文书，这将有助于防止该领域的国家间冲突。为此，俄罗斯于2023年向大会提交了一份专门国际条约的原型。这是联合国确保国际信息安全公约的一个概念。通过这样一项普遍协议不仅可以从法律上规定各国在信通技术领域活动的权利和义务，还可以规范国际关系中计算机攻击的政治归因问题。这也将有助于确保在网上充分遵守国家主权平等的原则，而目前许多技术先进国家公然无视这一原则。我们邀请所有会员国根据我们在大会的提议开展实质性讨论。

遗憾的是，西方国家，主要是美国，拒绝这一想法，试图为自己保留尽可能多的自由。鉴于美国高级官员承认利用信通技术对俄罗斯发动了攻击，这一点变得尤为明显。这也反映在华盛顿和北约的理论规定了“进攻性”——实际上是侵略性——方法。

我们今天的通报人和早些时候发言的代表团谈到了网络攻击。然而，他们忘了提到当前一场空前的反俄罗斯假消息战。所有这些恶意活动都是由设在伦敦的组织，即“公共关系和通信协会”和“公共关系网络”，从联合王国协调开展的，还有“乌克兰信息技术军”，它正在不知疲倦地从事造谣活动。通过这些信息技术资源的努力，大量关于俄罗斯和俄罗斯特别军事行动的假消息和谎言正在传播。

我们还担心有人试图淡化关于打击为犯罪目的使用信通技术的全球讨论。一个明显的例子是“反勒索软件倡议”。这种“排外俱乐部”并不特别隐藏其政治化的目标，破坏了会员国为打击为犯罪目的使用信通技术而建立普遍机制的努力，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作出的努力。

在26年多的时间里，俄罗斯联邦一直在推动国际信息安全领域的建设性议程，为维护现实世界和网络上的和平与稳定作出自己的贡献。我们将继续倡导在全球范围内创造一个和平与安全的信通技术环境。

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。

三分钟后，麦克风上闪烁的灯光将提示发言者结束发言。

阿丰索先生（莫桑比克）（*以英语发言*）：主席先生，莫桑比克要感谢你和大韩民国恰当地选择这一重要主题作为担任安全理事会6月份主席期间的标志性活动。我们非常感谢秘书长对这一问题采取了极其深刻的方法，它恰到好处地遵循了《联合国宪章》。我们非常认真地听取了网络和平研究所所长Stéphane Duguin先生以及法律和技术教授Nnenna Ifeanyi-Ajufo教授提出的重要观点。

我们向今天来到会议厅的各位部长和高级别贵宾表示问候。

到目前为止的所有发言都证明了一个事实，即网络空间和现实世界之间的界限继续迅速模糊。结果就是，我们现代生活的几乎所有方面都已经转移到并依赖于数字技术。因此，安理会参与的必要性得到了以下事实的支持：许多国家，无论大小，都严肃地认为没有国界之分的网络空间是一个可能发生冲突的领域，与陆地、海洋、天空和太空一样。

事实上，我们可以认为2013年是一个起点，当时大会商定，包括《联合国宪章》在内的国际法确实适用于网络空间。尽管如此，迄今为止关于网络空间交战规则的全球外交对话进展缓慢。在这方面，信息和通信技术安全和使用问题不限成员名额工作组主持的讨论尚未产生结果。

随着人工智能快速发展，随着一些重大威胁对国家和国际和平、安全和稳定构成新挑战，网络威胁的格局和范围正在迅速演变。随着网络威胁增加，几乎每天都会发生针对公共或私人实体的勒索软件攻击，人工智能生成的栩栩如生的深伪产品的扩散，或者针对一个国家某些领域或其基本服务——如金融、医疗保健、电网、电子政务和其他关键基础设施——的拒绝服务攻击。为了让人们过上现代生活而开发的工具遭到滥用和武器化，网络犯罪随之成为最突出的威胁倍增因素之一，破坏了公众对机构的信任，加剧了政治和社会紧张局势。

不断升温的地缘政治竞争已成为网络安全问题的主导因素，加剧了这些挑战。敌对国家正努力获取军事和情报网络能力，相互指控、指责、报复和升级日益加剧，引发网络军备竞赛。随着网络安全与地缘政治越来越交织在一起，就更好的网络安全规范达成国际协议继续陷于进展停滞甚至可能搁浅。在一个对人类如此重要的问题上这样停滞不前或缺乏进展，有可能破坏我们的集体安全。

鉴于威胁形势快速演变且无商定的接战规则，安全理事会应同意作为紧急事项发挥若干具体作用，采取以下具体行动。

第一，安理会应当在全球合作的基础上，为国家和私人实体制定网络空间负责任行为国际规范和框架。

第二，本着促进我们集体安全的精神，安理会可支持能力建设举措，以加强会员国，特别是资源有限的会员国的网络防御能力。

第三，安理会可推动开展态势感知通报会，促进各国之间分享威胁情报和最佳做法，以提高我们共同的网络安全应对能力。

第四，网络威胁应与安全理事会其他议程项目有机结合，如反恐、干涉选举、保护关键基础设施以及保障和平行动和人道主义行动。

我们认为，更新和扩大关于网络安全的辩论至关重要。与窃取创意思想、数据、知识产权、人权和隐私以及关键消费品和公共设施设计参数有关的问题值得同等关注。对于莫桑比克这样的国家来说，必须要在关于网络安全的全球讨论中听到全球南方的声音和观点。要在建立更公平、更有韧性治理框架方面取得全球进展，关键是在讨论中听取各种不同的观点，避免“一刀切”的做法。通过鼓励开展大韩民国担任主席国期间进行的这种讨论，安理会可在数字时代捍卫国际和平与安全方面发挥关键作用。莫桑比克承诺保持参与。

卡努先生（塞拉利昂）（*以英语发言*）：主席先生，我感谢你召开本次重要的公开辩论会。我还感谢秘书长安东尼奥·古特雷斯先生阁下富有洞察力的通报。我们还感谢Stéphane Duguin先生和Nnenna Ifeanyi-Ajufo女士的深刻见解。我们欢迎各位高级别部长参加本次会议。

塞拉利昂感谢有机会就应对网络空间不断演变的威胁这一关键问题发言，同时认识到信息和通信技术（信通技术）给国际和平与安全带来的巨大益处和相互交错的挑战。我们还认识到消除全球数字鸿沟这一根本发展挑战，以及随着人工智能，特别是生成式人工智能的扩散，鸿沟加深的风险。

在本次发言中，塞拉利昂将具体谈谈指导性问题。对国际和平与安全构成挑战的网络空间恶意活动的主要新趋势和不断演变的趋势，包括恶意软件、诱饵勒索软件、勒索软件即服务模式和加密货币抢劫的扩散。这些活动对平民构成重大风险，对我们各国的国家安全和整体稳定造成破坏性影响，对国际和平构成重大威胁。

我们对网络空间中所使用的不断演变的手段深感关切，它们不仅助长了恐怖主义活动，还危及金融系统和关键服务的信誉。我们特别强调，越来越多地使用勒索软件即服务模式和加密货币盗窃来支持不法活动，突出表明亟须加强合作和能力建设，有效打击这些威胁。最近针对关键基础设施和基本公共服务的勒索软件攻击的频率上升、范围扩大，让人看到网络威胁对公共安全和政治稳定造成的严重影响，要求我们保持警惕。塞拉利昂对网络威胁所涉影响深感关切，包括利用网络犯罪资助非法活动和逃避国际制裁。它们都突出强调亟需加强国际合作和能力建设努力，以有效应对这些威胁。我们呼吁加强会员国间合作，以加强安全理事会有效应对网络空间恶意活动的能力，特别是威胁关键基础设施、人道主义行动和保护平民工作的恶意活动。在数字时代维护和平与安全，整体方法必不可少。

我们经深思熟虑后认为，恶意使用信通技术会加剧现有冲突和挑战，使威胁倍增。针对包括医院和其他医疗卫生系统、金融服务、能源部门、卫星、运输和其他应急系统在内的关键基础设施的恶意网络活动日益盛行，突出表明亟需采取协调一致的全球行动来保护我们的数字网络和系统，突显出安全理事会参与的重要性，对于解决这些问题、管理和化解涉及网络因素的冲突十分重要。

正如我们已经听到的那样，尽管人工智能有巨大益处，但它可被武器化，用以提高网络攻击的规模、速度和复杂程度。自主系统可进行持续自适应攻击，通过所处环境进行学习，从而更有效地利用漏洞。这种人工智能驱动的攻击可针对关键基础设施、金融系统甚至个人隐私，造成大范围的服务中断和破坏。然而，我们也认识到，利用人工智能进行网络防御可帮助我们领先于新出现的威胁。人工智能可增强威胁检测、响应时间和事件管理。通过投资于人工智能驱动的防御技术，我们可建立更具韧性的网络基础设施。通过投资于能力建设和技术转让，我们可提高发展中国家的能力。塞拉利昂认为，安理会可以通过与联合国大会相关委员会以及专门机构全面接触，在应对不断变化的网络威胁和促进国际和平与安全方面发挥关键作用。

过去十年，安理会越来越关注网络空间对国际和平与安全的影响。2016年以来，安理会成员召开了多次阿里亚办法会议，会上各国讨论了网络安全与保护关键基础设施、保护平民以及网络空间中的虚假信息和仇恨言论等主题的各种联系。

因此，塞拉利昂赞扬爱沙尼亚在2021年6月担任主席期间就该主题召开首次高级别公开辩论会。鉴于安理会日益关注网络安全，我们支持以下提议，即定期召开情况通报会，以评估不断变化的网络威胁状况，同时纳入各种利益相关方的见解，以确保全面了解新出现的挑战，未雨绸缪。我们强调安理会必须有效协调、合作和参与，全面打击网络威胁。

我们强调，安全理事会的工作可与联合国正在进行的其他信息通信技术进程相互补充，包括在大会主持下关于使用信息通信技术方面的负责任国家行为准则的相关讨论，以及获得协商一致通过的联合国网络空间负责任国家行为规范框架。

通过纳入联合国系统、私营部门、民间社会和学术界的全面见解，针对不断变化的网络威胁形势制定评估和战略，将确保安理会及时了解新的事态发展及其对国际和平与安全的影响。

会员国应认识到网络威胁与安理会其他议程项目之间的相互联系，探索如何有效地使网络或信息通信技术相关问题成为安理会现有工作的重要部分。塞拉利昂建议将网络相关关切作为安理会关于各种专题，包括维和任务、安理会授权的制裁以及防扩散和反恐努力的讨论的重要内容。

加强国家网络安全能力和促进国际合作是该方法的重要组成部分，也可以纳入每一项努力之中。通过将网络相关主题的考虑纳入其工作，安理会可以更好地全面、整体地应对网络威胁带来的复杂挑战。

就我们而言，塞拉利昂国家计算机安全事件响应协调中心的成立使处理所有网络安全问题的权限得以集中行使，这包括响应塞拉利昂的网络安全事件。

自成立以来，该中心通过多方面的能力建设和协作做法，在增强国家网络安全韧性方面取得了重大的阶段性成果。重要活动包括侧重于应对网络安全和犯罪的能力建设举措。该中心在提高认识以及对各利益攸关方开展培训计划，并与区域和发展伙伴合作，就网络犯罪和电子证据、知识转让以及分享网络安全和网络犯罪调查的最佳做法问题对司法和执法机构进行专门培训方面发挥了重要作用。这种合作通过加强国家能力增强了有效应对全球网络威胁的集体能力。

最后，我首先要遗憾地指出针对我们的多边、国际和司法机构日益明目张胆的网络威胁。在这方面，塞拉利昂明确谴责针对国际刑事法院的攻击。法院将此类攻击描述为“以间谍活动为目的的有针对性的周密攻击，因此可以被解释为严重企图破坏刑院执行任务”。作为缔约国，塞拉利昂重申致力于维护和捍卫《罗马规约》所载的原则和价值观，并维护《罗马规约》的完整性，使法院不受任何干扰和压力，致力于维护和捍卫刑院官员以及与刑院合作者。

其次，我要重申塞拉利昂致力于推动网络安全问题，使之成为国际和平与安全的一个基本方面，并在安全理事会和广大国际社会内部开展合作，应对恶意活动在网络空间构成的复杂且不断变化的威胁。

本贾马先生（阿尔及利亚）（*以英语发言*）：主席先生，我感谢你组织这次重要的公开辩论会，讨论网络威胁对全球安全造成的日益严重的风险。我还感谢秘书长和通报人就有害网络活动令人担忧的增加所作的介绍。

使用勒索软件对关键基础设施实施攻击以及盗窃数字资产和数据使政治稳定面临风险。政府和非政府行为体的参与使情况变得更加复杂、更加危险。网络平台上虚假信息的传播助长分裂、仇恨和宽容，最终是恐怖主义，虚假信息干扰国家事务，阻碍合作，最终威胁世界和平与安全。

包括人工智能在内的新技术正在使网络威胁变得更加严重和难以应对。因此，我们需要在全球范围内紧急应对这些挑战。结合实际，我想强调以下几点。

首先，《联合国宪章》的原则应同样适用于网络空间。信息和通信技术的使用必须符合这些原则。

其次，我们努力维护开放安全的网络空间，这对实现2030年可持续发展议程全球发展目标至关重要。因此，我们需要在联合国内建立一个具有法律约束力的框架。

第三，我们必须帮助发展中国家加强网络威胁防护，缩小数字鸿沟。培养他们的能力对于确保所有国家的网络空间安全至关重要，并且应该成为重中之重。

第四，国际社会必须共同努力，打击网上虚假信息的传播。政府是相关方面，而相关方面必须按照国际法进行合作。国际合作是我们有效应对不断变化的网络威胁的关键。

第五，加强防范和惩治网络犯罪的法律体系。在此，我想强调，我国在打击有害利用技术进行犯罪活动的国际努力中发挥着积极作用。这尤其清楚地体现在阿尔及利亚领导了联合国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。我们希望该委员会将在今年夏季的下次会议上取得成功的结果。

最后，阿尔及利亚大力支持联合国在处理影响国际和平与安全的与使用信息和通信技术有关的问题上发挥作用。信息和通信技术安全和使用安全不限成员名额工作组和大会是包容性地讨论网络威胁的重要平台，它们确保所有会员国能够参与制定应对网络安全挑战的全球对策。我们重申，我们致力于支持它们的宝贵工作。

日博加尔先生（斯洛文尼亚）（*以英语发言*）：我感谢大韩民国举行今天的辩论会。我也谨感谢秘书长的通报，并感谢今天各位通报人的见地与建议。

请允许我谈谈与今天辩论的话题有关的两点意见。

首先，关于网络空间不断演化的威胁，我们认为，敏锐地了解不断演变的网络威胁格局，尤其是在诸如人工智能等新兴技术快速发展的背景下，对于讨论国际社会应对恶意网络活动可采取的合作措施至关重要。在这方面，我们赞扬大会设立的专门的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，但是我们也肯定安理会加大审议力度、比如通过处理秘书长有关网络威胁的报告（A/77/92）结论具有的辅助潜力。恶意网络活动、如勒索软件攻击和针对关键民用基础设施的攻击可给国际和平与安全构成新的挑战，并且加剧现有的威胁，尤其是当这些攻击具有跨界性质时。

由此引出我的第二点意见，即：处理网络空间不断演化的威胁。安理会负有维护国际和平与安全的首要责任。为了根据其任务授权履行其职责，当恶意网络活动威胁国际和平与安全时，安理会应该在缓解紧张和促进问责方面发挥决定性的作用。我们认为，支持恐怖主义或者扩散大规模毁灭性武器或者加剧现有冲突或者把关键民用基础设施作为目标的活动构成此种威胁，因而要求安理会做出回应。本着同样的精神，安理会应处理如虚假信息战等恶意网络活动，这些活动煽动针对平民的暴力，造成人道主义痛苦，或者扰乱人道主义组织、维和行动以及建设和平行动的工作。

在这个冲突日益数字化的年代，强调国际法、包括国际人道法和国际人权法的适用至关重要，这些法律必须得到遵守。

最后，请允许我向安理会保证，我们致力于同安理会成员和联合国广大会员国协作， 继续讨论国际和平与安全面临的网络威胁。我们还继续坚定不移地致力于执行旨在减少这些风险的措施，包括执行现有的网络空间负责任国家行为规范。

弗雷泽夫人（马耳他）（*以英语发言*）：首先，我感谢大韩民国举行本次公开辩论会，讨论这个具有高度现实意义的重要问题。我也感谢秘书长和各位通报人富于见地的通报。

恶意网络活动构成多层面挑战，可给维护国际和平与安全造成严重影响。这些活动包括对政府机构、关键基础设施以及基本公共服务的勒索软件攻击，还包括未经授权获取和使用以电子方式储存的数据。

我们感到震惊的是，恶意网络活动把政府机构和民主进程作为目标，其直接的意图常常是破坏稳定与安全，削弱对民主选举结果的信任。女性人权维护者和其他积极活动分子越来越多地依赖数字技术，这增加了他们遭受线上骚扰与攻击的风险。此外，人权与基本自由、包括表达与集会自由正越来越多地受到严格监控、关闭互联网和带宽调节的限制。与此同时，数字平台常常遭到利用，被用来散布虚假信息、错误信息以及仇恨言论，包括仇视女性和同性恋的内容以及激进的内容。

我们促进该领域稳定的集体努力必须立足于线上和线下的人权。网络政策必须做到对冲突和年龄有敏感认识，并且响应性别需求，以便识别和防止数字安全威胁的有害影响，比如因为技术而变得容易的性别暴力。妇女充分、平等、安全和切实参与网络决策并发挥领导作用举足轻重，特别是在冲突中和冲突后的背景下。

我们重申，国际法、尤其是《联合国宪章》适用于网络空间的活动，这一点已得到大会的承认。本着同样的精神，网络空间负责任国家行为框架为会员国提供了已商定的指导方针。所有会员国应坚持该框架，我们支持制订一项行动纲领，以确保继续对话并使对话制度化。此外，我们呼吁各国尽职尽责，根据网络空间负责任国家行为框架采取妥善措施，免于参加或者协助源自于其本土的恶意网络活动。

得到国家支持的恶意网络行为体利用勒索软件和数字盗窃来获取非法收入，这些行为包括攻击关键基础设施、金融机构以及加密货币公司。网络攻击与犯罪不分国界，任何国家都无法幸免。有报告估计称，仅2023年，由朝鲜民主主义人民共和国支持的黑客开

展的恶意网络活动就创造了相当于10亿美元的收入。该政权利用这些收入来资助其威胁朝鲜半岛内外和平与安全的非法的大规模毁灭性武器计划。这些活动在第1718（2006）号决议所设委员会专家小组的报告中有完备的记载，该小组在调查这些罪行方面发挥了宝贵作用。

最后，安全理事会可在处理网络安全问题方面发挥重要作用。安理会的努力能够而且必须同大会下设的其它网络安全论坛、包括其信息和通信技术安全和使用安全不限成员名额工作组相辅相成。安理会可充当一个有力的平台，强化已商定的原则，并推动进行更多的讨论。它应倡导一个开放、安全、便捷并且和平的网络空间。我们将继续支持安理会再次介入该议题。

山崎先生（日本）（*以英语发言*）：主席先生，我衷心感谢您领导召开这次重要而及时的公开辩论会，同时感谢秘书长和通报者提出宝贵见解。

首先，日本表示致力于促进自由、公平和安全的网络空间。近年来，我们目睹了一种令人担忧的趋势，恶意网络行动的质量和数量都有增加，涵盖了用勒索软件进行攻击、破坏重要基础设施、干扰民主选举和盗窃敏感数据。加密货币盗窃事件增长惊人，也对国际和平与安全构成了明显和现实的威胁，有可能为非法武器计划提供资金。特别是，北朝鲜众所周知地正在通过恶意网络行动资助其大规模毁灭性武器和弹道导弹计划，正如第1718 （2006）号决议所设委员会专家小组报告的，国际社会必须紧急应对这种威胁。此外，间谍软件等商业网络入侵工具扩散，令人深切关注它们对国家安全、人权以及国际和平与安全的影响。所牵涉的利害关系从未如此之大。

为了应对这些令人担忧的挑战，确保一个自由、公平和安全的网络空间，我们应该维护网络空间法治，进一步具体讨论现有国际法的适用问题，落实商定的负责任国家行为的规范、规则和原则。我们还特别要共享有关现有潜在威胁的信息，分享最佳做法，促进能力建设工作。我们应通过各级对话，促进信任，减少威胁，尤其是减少误判。在联合国框架下，日本将继续建设性地参与目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。日本还认为，在国际安全背景下促进使用信息和通信技术方面的负责任国家行为，这样的行动纲领作为一个注重行动的框架，应当成为一个未来的常设平台，支持执行商定的负责任国家行为的规范、规则和原则。

同时，日本完全同意，对维护和平与安全负有主要责任的安全理事会，应当在网络安全领域发挥更大的补充作用。安理会必须密切监测对国际和平与安全造成重大后果的严重网络事件，包括那些针对关键基础设施的事件。安理会的定期通报是非常有益的，能够跟踪信息和通信技术安全领域不断演变的威胁特征。此外，安理会需要应对全球军备控制和不扩散制度面临的日益严重的网络威胁，包括非国家行为体可能造成的扩散风险。

最后，日本重申坚定不移地致力于维护自由、公平和安全的网络空间。安全理事会必须高度警惕，防范新的信息和通信技术相关安全风险。主席先生，我们期待着在您今天提议举行的辩论会基础上，更深入地讨论安理会接下来应采取哪些措施来有效处理这一重要议题。

吴百纳女爵士（联合王国）（*以英语发言*）：我感谢大韩民国外长赵兑烈先生召开本次辩论会，并就我们如何能够推进这方面的工作向安全理事会提出了一些明确想法。我也感谢秘书长和今天的通报者阐述了网络威胁如何对国际和平与安全产生影响。

我将谈谈对联合王国具有重要意义的三个趋势。

首先，正如我们所听到的，勒索软件会扰乱政府职能和至关重要的公共服务。如果大规模或持续发生，将滋生条件，产生不稳定，而安理会知道，这会对和平与安全产生影响。任何国家都可能成为勒索软件的受害者。这就是为什么需要采取国际应对措施，限制助长勒索软件的生态系统，让所有国家都能提高复原力和应对能力。联合王国正与新加坡一道，作为反

勒索软件倡议政策支柱的共同主席发挥领导作用。我们敦促其他国家也加入这一倡议。

其次，随着社会越来越多的使用人工智能系统，我们需要了解网络威胁将如何变化，同时找到机会让人工智能支持我们实现网络安全目标。恶意和不负责任的行为者可能利用人工智能系统的漏洞，诱导产生特定的行为，或者操纵其决策过程。为了维护国际和平，人工智能系统必须刻意设计成安全的系统。这就是为什么联合王国去年在担任安理会主席期间举行了安理会有史以来第一次关于人工智能的辩论会（见S/PV.9381），这也是为什么我们与美国和一个由18个国家组成的跨区域集团一道公布了安全的人工智能系统开发准则。

第三，恶意和不负责任的行为体也能够利用先进网络入侵能力方面不断扩大的市场，导致产生更加不可预测的威胁特征，危及我们大家。在我们考虑如何解决这一共同关切之时，联合王国和法国邀请国际伙伴与我们一起参加帕尔·马尔多利益攸关方进程。

在此背景下，我们必须继续提高对网络威胁的认识。例如，我们非常关切朝鲜民主主义人民共和国利用恶意网络活动获取加密货币，为其非法武器计划提供资金。因此，我们必须加倍努力，确保有效执行对朝鲜民主主义人民共和国的制裁制度。

最后，网络威胁也增加了造谣的风险。这显然是我们工作的一大挑战。俄罗斯指责联合王国发动虚假信息战，十分令人吃惊，而与此同时它自己的虚假信息机构却被如此明显和清楚地揭露了出来，包括在联合国受到揭露。我们可不是那个在会议厅指责把蝙蝠和鸭子当成武器的阴谋并发布到互联网上的代表团。

网络威胁将给国际和平与安全带来越来越多的风险，各国政府需要不断提升，才能有效应对这些风险。作为其中的一部分，联合王国一直致力于维护联合国网络空间负责任国家行为框架，通过能力建设和启动公私伙伴关系与其他国家开展合作。

钱达夫人（瑞士）（*以法语发言*）：我感谢大韩民国组织本次关于网络安全威胁的重要辩论会。我也感谢秘书长、Nnenna Ifeanyi-Ajufo教授和日内瓦网络和平研究所首席执行官Stéphane Duguin先生的通报。

瑞士正在目睹网络空间的两个决定性进展，这也是我们所关注的。一方面，冲突日益数字化和武装冲突中的网络行动正在改变冲突的性质。另一方面，来自勒索软件的攻击和国家资助的针对重要基础设施的网络攻击日益加剧，这是瑞士的一大关切。不论是使用勒索软件勒索货币和加密货币，还是攻击重要基础设施，都有可能使我们社会的关键架构瘫痪。鉴于发展中国家更容易受到攻击，这些活动也影响到国际社会实现可持续发展目标的能力。它们可能对国际和平与安全构成威胁，因此属于安理会的职责范围。

大韩民国提供的概念说明（S/2024/446,附件）提出了安理会可在应对网络空间恶意活动所造成的威胁方面发挥何种作用的问题。请允许我就此提出若干备选答案。

第一，安理会应定期关注当前的网络安全事态发展和威胁。鉴于这一问题的多层面影响和地理范围，安理会宜定期举行通报会。通报会可包括联合国实体、私营部门、民间社会和学术界以及其他相关实体的代表的发言。这种提高认识的活动将使安理会能够作出充分知情的决定，特别是在涉及特定地域的问题和维持和平行动时。

第二，安理会应重申某些既有原则。我们特别重视国际法对网络空间的适用性，尤其是国际人道法对武装冲突背景下网络空间活动的适用性。安理会还应强调国家责任和尽职调查的重要性，并承认网络空间国家负责任行为11项准则。这些要素加上建立信任和能力建设措施，构成了网络空间负责任国家行为框架，这一框架已由全体会员国以协商一致方式通过。我们将支持安理会通过一份文件，肯定这一框架，从而为重建信任作出贡献。

最后，安理会的活动必须与其他机构的活动相辅相成。安理会不应制定行为规则或协议。这是大会及

其授权的专家进程的特权。安理会应专注于加深对风险和减轻风险的认识，包括在特定的情况下。

负责任地利用网络空间可为迎接明天的挑战提供了巨大机会，尽管存在各种公认的风险。秘书长在他提出的《新和平纲领》中鼓励我们寻找新的办法来保护自己免受这些新威胁之害。虽然关于《未来公约》的谈判为我们提供了在这方面形成共同认识的机会，但安理会也可以发挥关键作用。今天的辩论会就证明了这一点。

傅聪先生（中国）：我感谢你主持今天的会议，感谢古特雷斯秘书长所作通报，也感谢两位专家作的介绍。

当前，我们正身处一个前所未有的数字时代，信息技术革命日新月异，数字和网络经济蓬勃发展，国际社会加速融合为一个利益交融、休戚与共的命运共同体。与此同时，网络空间风险与挑战日趋严峻，网络攻击、网络窃密、网络犯罪、虚假信息有增无减，网络恐怖主义成为全球公害，网络军事化、阵营化、意识形态化愈演愈烈，国家和地区间的数字鸿沟不断扩大。

各国在网络空间既享有共同机遇、拥有共同利益，也面临共同挑战、承担共同责任。国际社会应深化交流，增进互信，携手合作，共同推进网络空间治理和国际规则制定。中方愿提出以下主张：

首先，要构建更加和平、安全的网络空间。网络空间和现实世界深度融合，是人类社会发展的重要依托，决不能成为新的战场。个别国家将网络空间定为“军事行动疆域”，发展进攻性网络军事力量，构建网络军事同盟，推动制定网络空间交战规则，只会削弱各国间互信，推高网络摩擦和冲突风险，威胁国际和平与安全。各方应摒弃零和博弈和冷战思维，树立共同、综合、合作、可持续的安全观，坚定维护网络空间和平属性，切实防止网络军事化和网络军备竞赛，通过对话合作解决网络安全威胁，致力于通过共同安全实现自身安全。

第二，要构建更加普惠、繁荣的网络空间。数字和网络经济已成为推动全球经济增长的重要引擎，各国应采取更加积极、开放、协调、普惠的政策，促进信息通信技术应用和普及，保障信息通信产业链开放、稳定、安全，让更多国家和人民享受互联网红利。发达国家应帮助发展中国家提高数字化、网络化、智能化水平，以及风险防范与应急能力，确保公平获取网络基础设施、技术、算力等关键资源，以缩小数字鸿沟，落实2030年可持续发展目标。以意识形态划线构建“小圈子”，泛化国家安全概念，拉起“数字铁幕”，谋求技术垄断和优势地位，甚至公然干扰、打压他国经济科技发展，只会阻碍国际社会推进网络治理的努力。

第三，要构建更加公平、有序的网络空间。制定各方普遍接受的网络空间国际规则，是维护网络空间长治久安的关键。各方应切实遵守《联合国宪章》宗旨和原则，特别是主权平等，不干涉内政、不使用或威胁使用武力、和平解决争端等原则，遵守并落实联合国网络空间负责任国家行为框架。同时，各方还应始终坚持联合国的主渠道作用，在平等、广泛参与基础上，将长期以来的国际共识转化为有法律约束力的网络空间行为准则。中方提出的《全球人工智能治理倡议》《全球数据安全倡议》等建设性解决方案，可作为未来网络空间规则制定的蓝本。

第四，要构建更加平等、包容的网络空间。多样性是世界的基本特征，也是人类进步的源泉。互联网以前所未有的方式联通所有国家、所有人民、所有文明，理应成为全人类展示多样文化、促进文明发展与传承的平台。要充分利用信息通信技术，加强网上交流对话，鼓励各国人民相知相亲，推动不同文明包容共生，更好弘扬全人类共同价值。应警惕少数国家将自身价值观作为“普世价值”强加于人，甚至干涉别国内政、扰乱别国发展和稳定。必须坚决反对利用网络传播极端主义、恐怖主义、虚假信息以及仇恨言论。

中国是互联网发展的见证者和受益者，如今已拥有近11亿网民，建成全球规模最大、技术领先的网络基础设施，形成完善的网络治理政策体系。近年来，中国积极同“全球南方”深化政策沟通和经验分享，推进基础设施、技术、执法、应急等方面能力建设的务实合作，深入参与联合国信息安全开放式工作组进

程, 以及二十国集团、亚太经合组织、金砖国家、上合组织、东盟地区论坛等框架下的网络安全进程, 为促进全球网络治理作出重要贡献。

信息革命的时代潮流浩荡前行, 网络空间承载着人类对美好未来的无限憧憬。中方愿同国际社会一道, 建设更加和平、安全、开放、合作、有序的网络空间, 携手构建网络空间命运共同体。

德拉加斯卡先生(厄瓜多尔)(*以西班牙语发言*): 我谨欢迎大韩民国外交部长官赵兑烈先生出席会议。我还感谢秘书长安东尼奥·古特雷斯提供的信息, 感谢通报人Stéphane Duguin先生和Nnenna Ifeanyi-Ajufo女士所作通报。

在一个日益相互联系和相互依存的世界中, 网络安全是一个全球性挑战, 需要整个国际社会采取协调合作的应对措施。

恶意使用信息和通信技术可使和平与安全面临的威胁倍增, 包括在以下方面。

第一, 影响如卫生系统、金融服务和能源网络等对社会运转至关重要的关键基础设施。

第二, 传播虚假信息和仇恨言论, 进一步分化社会, 助长冲突。

第三, 支持恐怖主义活动, 资助国家和非国家行为体的非法活动。

鉴于这些挑战, 安全理事会绝不能在应对不断演变的网络威胁方面滞后, 因为这种威胁与安理会若干议程项目, 包括不扩散和反恐问题都相互关联。在这方面, 安全理事会应考虑是否有可能在每个问题的工作中根据需要纳入网络安全相关内容。加强和平行动和特别政治任务中的战略沟通就是一个例子。

促进安全、开放与和平的网络空间需要建立使用信通技术的负责任行为标准。此外, 这一领域国际法的发展必须伴之以能力建设, 特别是在处于冲突局势中的国家, 因为这些国家最容易受到滥用信通技术的影响。信息和通信技术安全和使用安全不限成员名额工作组正在这方面取得进展。其工作成果可成为安理会工作指南。

最后, 我要回顾, 必须维护和促进负责任地利用网络空间, 以保障网络空间的稳定和安全, 从而减少网络空间给各国带来的巨大风险。

德里维埃先生(法国)(*以法语发言*): 我感谢秘书长、Duguin先生和Ifeanyi-Ajufo女士的通报, 主席先生, 我还感谢你召开本次辩论会。

信息和通信技术的传播有助于实现进步和可持续发展目标。然而, 它也对我们的集体安全构成了重大挑战。在高度依赖这些技术的社会中, 恶意网络活动越发频繁、严重和复杂。它们能够利用大量漏洞, 使用日益多样化的载体, 而现在多种行为体都可使用这类载体。侵入工具和服务正在市场上肆意蔓延, 不负责任地使用这些工具和服务致使网络威胁加剧。

网络攻击本身可对关键基础设施造成影响并带来升级风险, 从而对国际和平与安全构成威胁。据法国主管部门称, 勒索软件攻击在2023年增加了30%, 因此可能影响能源等重要部门, 破坏经济稳定, 甚至扰乱政府机构运作。现在, 网络攻击正被用于武装冲突中, 正如俄罗斯非法入侵乌克兰一开始对Viasat卫星网络发动的攻击。

恶意网络活动还会加剧对国际和平与安全的其他威胁, 包括扩散。第1718 (2006) 号决议所设委员会专家小组的最新报告 (S/2024/215) 表明, 朝鲜政权非法大规模毁灭性武器计划高达40%的资金通过非法网络手段获得, 如勒索软件或加密货币盗窃。

尽管如此, 联合国和安全理事会确实在履行职能上有办法对这些威胁采取协调一致的应对措施。首先, 让我们回顾一下, 网络空间既不是“蛮荒西部”, 也不是在规范方面一片空白。国际法, 包括《联合国宪章》、国际人道法和国际人权法, 完全适用。负责任国家行为规范是以协商一致方式制定的, 旨在推进合作、促进预防冲突、加强网络空间稳定。

法国支持大会第一委员会进一步发展这一规范性框架的工作。为了支持规范的落实，法国提出了一个雄心勃勃的未来网络空间行动纲领机制的架构。安全理事会必须将尊重网络空间负责任国家行为规范框架置于其应对网络威胁工作的核心，并鼓励各国履行促进网络空间安全与稳定的承诺。

除此之外，安全理事会必须继续努力将网络问题纳入到其职能的不同层面。安理会必须定期就网络威胁的演变及其对国际和平与安全的影响听取专家通报。今天的辩论会就是这方面的一个有益例证。

安理会还必须继续关注利用网络手段规避制裁的问题。在这方面，朝鲜政权为资助其大规模毁灭性武器计划而从事的恶意网络活动值得继续关注。法国将继续积极参与，确保安理会尽管未能延长1718委员会专家小组任务期限却仍继续严密监测这方面违反该决议的行为。

主席（*以英语发言*）：我现在请冈比亚共和国外交、国际合作和侨民事务部长马马杜·坦加拉先生阁下发言。

坦加拉先生（冈比亚）（*以英语发言*）：首先也最重要的是，我谨感谢各位通报人具有启发性的发言，并祝贺大韩民国举行本次辩论会。

今天，我们正处在一个十字路口。数字时代编织了一个联接、机遇与进步的网络。然而，就在这个架构中潜伏着一片威胁国际和平与安全的不断扩大的阴影。网络犯罪的威胁不断演变，不只是一个经济利益或者数据失窃的问题。新一波的网络威胁直接挑战了国际和平与安全，要求我们给予紧急关注。在这方面，我们感谢大韩民国提请我们注意安全理事会的另一种创新介入，就“维护国际和平与安全：应对网络空间不断演变的威胁”这个议程项目交换实质性见解。作为被责成维护国际和平与安全的机构，安全理事会不能保持沉默。我们赞扬它继续努力，在我们共同面临的这个重要问题上发出警示。我们需要一种全面的做法来处理这种不断演变的威胁。

在这方面，我谨建议以下三点意见，以支持我们的共同努力，遏制国际和平与安全面临的与网络有关的威胁。

首先，安全理事会必须充当表率，倡导网络空间负责任国家行为的榜样性规范。要做到这一点，我们可以通过定期提高认识以促进网络安全方面的讨论，从而拓展大会网络论坛的工作，还可以通过与会员国一道努力，把这些规范转化为行动，促进能力建设和信息共享，从而震慑恶意活动。

其次，安全理事会可倡导增强会员国的网络能力，以识别恶意行为体，并结成打击有罪不罚的统一战线，从而加强对与网络有关的安全威胁的问责。

第三，安全理事会可利用联合国实体、如裁军事务厅和反恐怖主义办公室的专长，以充分处理破坏可持续的国际和平、安全以及民主的威胁。与这些实体协作还可促成协调，从而 避免重叠，并且确保采取一种胜任使命的全面做法。

在安理会任务授权范围内采取的这些行动将不仅促进国际和平与安全，而且还提高认识，倡导问责，并且促进国家和相关机构间的有效协作，从而加强现有工作的力度。因此，安全理事会处于有利位置，在为各方建设一个更加安全和稳定的网络空间方面充当先导。

我们必须提升这些讨论的地位，定期把网络威胁纳入我们对地区冲突和专题问题的审议。这扩展了大会专门处理网络规范的论坛的工作。我们还必须鼓励会员国把这些规范转化为具体的行动。这包括建设网络防御能力，促进信息共享，以及震慑恶意活动。

最后，我必须再次赞扬大韩民国提出这个值得称赞的倡议，给会员国提供机会，参加本次关于一个共同关切问题的非常重要的具有现实意义的辩论。 安全理事会对于提供急需的关键支持以减少和阻止国际和平与安全面临的与网络有关的威胁举足轻重。

主席（*以英语发言*）：我现在请德国代表发言。

林德纳先生（德国）（*以英语发言*）：德国感谢大韩民国发挥领导作用，提请安全理事会注意网络安全问题。我还感谢秘书长和各位通报人具有启发性的发言。

国际社会受到越来越多的恶意网络活动事件的影响，其中既有得到国家支持的网络活动，也有私人网络活动。这些事件给维护国际和平与安全造成严重影响。网络罪犯的严重攻击、包括勒索软件的攻击表明，这些攻击有可能威胁国家机构的稳定。它们已经影响了整个社会。

近期的一个趋势是，在发生国际冲突的地区出现攻击主要的关键基础设施目标的黑客活动团体。这种趋势侵蚀了对提供公共服务的信任，在平民中散布恐惧。若干国家行为体同私营信息技术公司、黑客活动团体以及网络罪犯增加合作，进一步加剧了现有的风险。所有这些趋势导致威胁倍增，因为网络空间使传统战场深入延伸到平民领域之中。

有鉴于这种正在发生剧烈演变的威胁格局，德国提议，安全理事会应在以下四个方面积极开展工作。

首先，我们认为，安全理事会可在评估威胁方面发挥重要作用，这不仅是根据《联合国宪章》第34条，该条赋予安全理事会调查可能导致国际摩擦或者引发争端的任何情况的权威，而且也是从安理会应该更加深入地审查和分析网络攻击对国际和平与安全构成的风险这个总体角度而言。

其次，基于《联合国宪章》在网络空间的充分适用，安全理事会可发挥重要的解决争端作用。

第三，我们认为，安全理事会具有发挥建立信任和制订规范的有力作用的潜力。通过把国际网络冲突摆在其议事日程之上，调查网络冲突局势或者推动这些局势的和平解决，安理会将协助建设不断演变的网络空间负责任国家行为框架。这项工作必须基于国际法，并且由联合国的自愿规范与建立信任措施作为补充。

最后，德国欢迎安全理事会把网络安全威胁纳入其议事日程的主流。这应涵盖保护联合国、尤其是它在实地的存在如维和行动，使其免遭恶意网络攻击。

最后，我谨强调，德国将继续推动国际上对这个重要问题的讨论。仅强调一个例子：去年，我们就“冲突中的网络”启动了一场全球性对话。它专门寻求处理在国际冲突中使用网络工具对平民构成的更多风险，提高认识，并且制订减缓方案。该系列活动的下一次活动将于7月8日在纽约这里的德国大厦与日本、塞内加尔以及红十字国际委员会合作举办。

主席（*以英语发言*）：我现在请阿拉伯联合酋长国代表发言。

沙拉夫先生（阿拉伯联合酋长国）（*以英语发言*）：我感谢外长赵兑烈先生阁下主持本次公开辩论会，并赞扬大韩民国指导安全理事会本月工作。我也感谢秘书长和其他几位通报人富于见地的发言。

正如我们今天听到的那样，网络空间面临的威胁正在快速演变。恶意网络工具和技术如勒索软件、网络钓鱼和拒绝服务攻击正在被用来攻击政府和私营部门的网络，威胁关键基础设施和公共安全。这一点尤其令人担心，因为我们这些国家、包括阿拉伯联合酋长国正在经历数字转型，这使我们更加依赖安全的线上系统。教育机构也面临风险，数字教育基础设施和宝贵的信息资产正在被恶意行为体作为攻击的目标。此外，对信息和通信技术、包括但不限于新兴的人工智能技术的恶意使用在现有冲突中充当了成倍增加威胁的工具。

作为全球技术和创新中心，阿拉伯联合酋长国于2020年成立了网络安全委员会。该委员会旨在实现更安全的数字化转型，增进我国所有目标行业的网络安全。我们致力于同合作伙伴进行能力建设和信息共享，促进负责任的技术设计，利用人工智能做好事，以打击仇恨言论、错误信息和虚假信息的传播和扩大。根据这一承诺，我们与阿尔巴尼亚一起于2023年12月主办了阿里亚办法会议，以应对这些挑战。

考虑到这一点，我想提出四点看法供审议。

首先，国际法必须指导网络技术的使用。必须尊重《联合国宪章》、主权、不干涉国家内政、国家责任和武装冲突法，包括联合国关于网络空间负责任国家行为的准则。填补规范方面的漏洞需要就在网络领域如何捍卫和维护国际法继续达成共识。

其次，阿拉伯联合酋长国支持将网络关切作为安理会国际和平与安全工作的重要内容。这可以包括在通报、声明和优先问题中更频繁地提及与网络相关的问题、趋势和发展，以及与特定国家和其他专题相关的内容。例如，第2341（2017）号决议认识到保护关键基础设施免受恐怖袭击（包括网络安全）的必要性，强调需要更好地应对数字化和网络空间带来的广泛网络威胁。

第三，安理会应考虑就新出现的技术威胁及其对国际和平与安全的影响召开年度通报会。此外，秘书长发布的年度网络安全报告将对全球网络威胁形势进行全面评估，并为加强国际合作提出建议。该报告还应包括性别分析，以便更好地应对网络空间中针对妇女和女童的威胁。

第四，培养强有力的公私伙伴关系对于利用专业知识和资源有效应对网络威胁至关重要。阿拉伯联合酋长国致力于同私营部门合作开发强大的网络安全工具并建设国家和国际能力，同时支持私营部门确保安全、负责任地设计解决方案。

利用网络技术对我们的未来至关重要，但对其风险保持警惕也至关重要。国际合作和能力建设对于全球安全的韧性至关重要。阿拉伯联合酋长国将继续推动网络空间的负责任行为，并确保它反映我们对于和平与安全的集体愿望。

主席（*以英语发言*）：我现在请拉脱维亚代表发言。

梅尔巴德女士（拉脱维亚）（*以英语发言*）：拉脱维亚谨对大韩民国组织安全理事会本次高级别公开辩论会表示感谢。我们还要感谢秘书长以及网络和平研究所和利兹贝克特大学的通报人富有见地的介绍。

自二十多年前网络安全相关问题首次被列入联合国议程以来，数字技术的使用和依赖显著增长。今天，网络领域已成为全球经济社会发展的结缔组织。网络空间的扩张在提供巨大的进步机遇的同时，也带来了不断增加的风险和挑战。近年来，我们在国际和平与安全方面遇到了一些消极趋势。以下情况越来越多：关键基础设施（包括关键信息基础设施）成为网络攻击的目标，并可能对现实世界造成灾难性后果。此外，我们还看到网络攻击已成为俄罗斯全面侵略乌克兰的一个组成部分。网络威胁经常与其他敌对行为交织在一起，例如传播虚假信息和错误信息的传播以及恶意使用人工智能和其他新兴技术。网络犯罪也十分猖獗，勒索软件造成的支付金额在2023年创下历史新高。这些事态发展影响着全球和平与安全。国际社会必须协调应对措施，安全理事会也可以根据其职责发挥作用。

因此，拉脱维亚认为网络空间威胁和挑战值得安理会定期讨论。秘书长的定期报告可为此类讨论提供参考。安理会加大对网络安全的关注还可促进将网络相关问题纳入其他专题任务，例如维持和平以及妇女与和平与安全。安理会还应考虑加强其应对具有潜在国际安全影响的大规模网络攻击的能力。

显然，让安理会在处理网络安全问题方面发挥更强有力的作用不可能一蹴而就。这项工作需要循序渐进，像今天这样的会议在推动这一进程方面就发挥着关键作用。同样明确的是，安理会不应替代大会旗下联合国其它机构已经完成的工作。恰恰相反，安理会应该加强在这些机构中达成的谅解，特别是关于在网络空间适用整个国际法的问题。在实施网络空间负责任国家行为框架方面还有更多工作需要共同完成。我们期待建立一个处理网络安全问题的联合国常设机制，即《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》，认为安理会与大会在这方面有望实现新的协同增效。

最后，我想强调拉脱维亚致力于继续支持联合国内部努力应对日益增长的网络安全威胁和挑战。我们

一直积极参与联大各委员会就此议题的讨论，也将继续倡导安理会发挥更大作用。

主席（*以英语发言*）：我现在请埃及代表发言。

里兹克女士（埃及）（*以英语发言*）：埃及高度重视信息和通信技术（信通技术）的国际安全问题，并强烈呼吁联合国通过开展所有国家参与的包容性和公平进程，在促进和制定各国使用信通技术的规则和原则方面发挥核心和领导作用。

一些国家正在开发信通技术能力，用于可能的恶意目的和进攻性军事目的。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。新的军备竞赛对国际和平、安全与稳定产生深远影响，特别是在常规武器与非常规武器的界限继续受到侵蚀的情况下。

此外，各国开发的相关技术正在被恐怖分子和犯罪分子转让、拷贝和复制。恐怖分子和犯罪组织恶意使用信通技术对国际和平与安全构成严重威胁，特别是考虑到责任归属方面的难度。根据国际法和《联合国宪章》，所有会员国均应避免采取任何明知或故意损害或以其他方式损害其他国家关键基础设施的使用和运行或干涉其内政的行为。毫无疑问，信通技术的国际安全问题已经变得非常重要和具有战略意义，国际上不能没有具有约束力的明确规则。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和最有效途径。

联合国已经采取了一些步骤来建立一个补充国际法原则的规范性框架。随着大会第75/240号决议所设信息和通信技术的安全和使用安全不限成员名额工作组两份年度进展报告以及联合国相关进程其他协商一致报告以协商一致方式获得通过，联合国已确立了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息和通信技术时以第一委员会政府专家组历次报告中所载网络空间负责任国家行为不断演变的累积框架为指导。然而，由于这些规范属于自愿性质且无任何后续机制，它们的执行充其量也只是最低限度的。

虽然对大会第75/240号决议所设不限成员名额工作组在其任务不同方面取得进展予以认可，但工作组必须为今后建立联合国主持下的以行动为导向、基于协商一致的包容性单轨机制打下基础。工作组应当在联合国相关进程的商定成果上更进一步，把重点放在执行商定成果上，包括网络空间负责任国家行为框架及其进一步发展，促进与发展中国家的国际合作和对发展中国家的援助。

主要由大会主持的联合国内部包容性进程是在这一领域建立公平、全面和有效安排的最有效途径。就安全理事会而言，我们鼓励它在审议维和与反恐等议题时考虑到新兴技术提供的机会。然而，安理会不应被用作试图代表联合国会员国就必需包容和透明进程的事项制定规范和规则的立法机构。

大会以协商一致方式核可的建议可成为具有政治或法律约束力的规则的基础，特别是因为这些建议源自国际法和《联合国宪章》的原则。虽然我们认为国际法和《联合国宪章》原则确实适用于包括网络空间在内的所有领域，但我们也认为，亟须确定具体义务，使网络空间的国家行为符合国际法以及《联合国宪章》的目标和原则。

在一个联系日益紧密的世界中，任何国际网络安全机制的强大程度都取决于其最薄弱的环节。所幸，有一种共识，认为必须强化和加强能力建设努力，以防范对关键基础设施的潜在攻击，并培养发展中国家所需的能力和技能。联合国应领导旨在向发展中国家提供必要援助的协调努力。

最后，信通技术带来了巨大机遇和挑战，我们着重强调，亟须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，防止网络空间成为另一个冲突和军备竞赛场所。

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。

我现在请乌克兰代表发言。

哈约维申女士（乌克兰）（*以英语发言*）：我们感谢安全理事会主席国大韩民国召开本次高级别公开辩论会。我们还感谢秘书长和其他通报人的发言。

乌克兰赞同将以欧洲联盟（欧盟）名义所作的发言，并愿以本国身份发表几点意见。

我们坚信，安全理事会在应对包括网络空间在内的国际和平与安全威胁方面发挥着重要作用。网络威胁格局不断演变，比以往任何时候都更充满挑战。勒索软件对政府、企业和个人构成越来越普遍和重大的风险。此外，我们还看到针对关键基础设施和关键信息基础设施，包括能源部门、公共服务和选举进程的恶意网络行动日益增多。一些国家行为体继续通过开展恶意网络活动，破坏基于规则的国际秩序和负责任国家行为框架。

在这方面，朝鲜民主主义人民共和国一直在从事网络间谍和加密货币盗窃活动，目的是进一步发展其核武器计划和大规模毁灭性武器计划，违反了安全理事会有关决议。最近，俄罗斯网络间谍组织APT28对多个欧盟成员国进行了网络攻击。

乌克兰一直面临俄罗斯的侵略，包括在网络空间。自战争开始以来，俄罗斯的网络攻击越来越复杂，并以政府和安全机构、企业和金融机构为目标。莫斯科的网络犯罪分子一直在进行网络钓鱼攻击、网络间谍活动和针对关键基础设施的攻击，此外还散布虚假信息和宣传言论。

为有效预防、打击和减轻网络威胁，乌克兰积极与国际伙伴合作，开展有效的网络能力建设，这对于在网络空间行使自卫权必不可少。此外，乌克兰还开始将网络攻击作为战争罪进行调查和起诉。

各国必须履行其国际承诺和义务，包括在安全使用信通技术方面。正如我们曾在联合国这里重申的那样，包括《联合国宪章》在内的国际法适用于网络领域。因此，所有违反商定框架的国家行为体都应承担责任。

最后，我们鼓励联合国会员国继续共同努力，加强并执行网络空间负责任国家行为规范框架，提高认识，交流最佳做法，以应对网络领域现有和新出现的威胁。

主席（*以英语发言*）：我现在请爱沙尼亚代表发言。

坦姆萨尔先生（爱沙尼亚）（*以英语发言*）：我们欢迎今天的意见交流，感谢通报人，尤其是秘书长提供了十分宝贵的见解。

爱沙尼亚赞同欧洲联盟代表将要作的发言。请允许我以我国代表的身份发表几点意见。

不容忽视的是，国家和非国家行为体实施的恶意网络事件日益复杂化并造成巨大损害。由于受到攻击的目标十分重要，例如关键基础设施、金融机构和民主进程，攻击事件具有跨境性质且攻击能力不断加大，网络攻击能够造成的损害愈发严重。因此，网络安全显然是国家和国际安全挑战的一部分，防止和减轻这种威胁是我们共同的优先事项。

俄罗斯对乌克兰的侵略凸显出网络行动与热战如何相互交织。我们看到了俄罗斯如何违反国际人道法，将乌克兰的关键基础设施作为目标。俄罗斯的行动突出表明，必须注重对国防和国内安全采取全面方法。为加强乌克兰对网络攻击的防备和抵御能力，爱沙尼亚在网络领域通过双边方式以及塔林机制和信息技术联盟积极支持乌克兰。

我们还深感关切的是，来自平壤的最新消息表明，朝鲜民主主义人民共和国与俄罗斯的军事合作进一步加强，这严重违反了安全理事会有关决议。爱沙尼亚强烈谴责朝鲜民主主义人民共和国当前持续实施的恶意网络活动，这些活动旨在推动朝鲜民主主义人民共和国的武器计划，破坏区域安全稳定，威胁全球和平。

联合国网络空间负责任国家行为框架建立在现有国际法基础上。国际法——特别是《联合国宪章》、国家责任法、国际人权法和国际人道法——完全适用

于网络行动。我们要共同努力维护国际法，确保国际法在网络空间也得到遵守。为支持执行网络空间负责任国家行为框架，爱沙尼亚主张，在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于2025年结束工作后，建立一个包容各方且以行动为导向的行动方案，作为单一常设架构。

开放、安全、稳定、便捷与和平的信息和通信技术环境不会自己到来，也不能与现实世界割裂。俄罗斯对乌克兰的侵略展示了网络攻击和动能战争的交融性质，同时我们认为，这种模式也会用于未来的冲突。因此，安全理事会可发挥重要作用，充当分享现有和未来网络威胁信息的论坛，提高对网络安全战略影响的认识，爱沙尼亚在安全理事会成员任期内已经强调过这一点。

最后，正因如此，爱沙尼亚赞扬大韩民国在安理会会议厅召开本次讨论，真是再恰当不过。像这样关于网络安全的公开讨论，有助于网络冲突的预防和缓解，从而为强化国内、区域和全球的网络复原力提供支持，具有至关重要的意义。

主席（*以英语发言*）：我现在请捷克代表发言。

库尔哈内克先生（捷克）（*以英语发言*）：首先，我感谢大韩民国组织本次非常有意义的公开辩论会。我们欣见大家今天讨论安全理事会在网络安全领域的作用，特别是在执行商定的网络空间负责任国家行为框架方面的作用。

不用说，我们赞同会上表达的许多关切和警告。我们尤其关注对关键基础设施的攻击、网络间谍活动、针对包括医疗保健部门在内的公共和私营机构的勒索软件攻击、加密货币盗窃，以及试图持续渗透关键工业系统的努力。这种渗透不仅是为了刺探情报和盗窃知识产权，也是为了能够以公开和敌对的方式控制这些系统。武装冲突中越来越多地使用信息和通信技术，对平民造成有害影响，令人震惊。这些不负责任的行为危及国际和平与安全，安全理事会对此负有责任。同样，网络空间正越来越多地被用来传播虚假信息，加剧现有的社会冲突，甚至煽动恐怖主义行为。安理会应与处理网络议程的联合国相关论坛和其他国际组织一道，加大努力，寻找有效途径，处理网络空间中那些不太明显的恶意活动。安理会还应努力帮助人们更好地认识这些威胁的真正规模，帮助开展活动提高复原力。

5月份，捷克与德国和其他国家一道，公开谴责俄罗斯国家控制的行为体APT28的活动。该行为体一直在欧洲国家开展长期的网络间谍活动，并以捷克政府机构为目标。这些活动违反了联合国关于负责任国家网络空间行为准则。我们将继续与我们的伙伴一道，履行我们的国际义务，有力地应对这些活动。

捷克完全赞同建立一个以国际法为基础的国际秩序，推动营造一个开放、安全、稳定、无障碍且和平的信息和通信技术环境。我们重申，支持在目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于2025年完成工作之际，由联合国主持建立一个常设、单轨、包容和注重行动的机制。我们认为，在国际安全背景下促进使用信息和通信技术负责任国家行为的行动纲领，可以作为这样一个机制。

最后，我重申，我国一贯致力于积极参与真正的全球伙伴关系，应对当今和未来的网络安全威胁。这确实需要我们采取全员参与的办法。我们已经与非洲、印度洋-太平洋和拉丁美洲的一些国家进行了详细讨论，以明确不断变化的威胁形势，加强联合应对措施。例如，4月底，捷克在波哥大组织了一次研讨会，讨论当前网络空间犯罪活动领域的挑战。我们感谢来自哥伦比亚、哥斯达黎加、多米尼加共和国、厄瓜多尔、萨尔瓦多、危地马拉、洪都拉斯和巴拿马的专家出席这次活动，并与我们分享宝贵见解。

主席先生，我再次感谢你让我有机会分享我国对这一重要议题的看法。

主席（*以英语发言*）：现在请萨姆森夫人发言。

萨姆森夫人（*以英语发言*）：我荣幸地代表欧洲联盟（欧盟）及其成员国发言。候选国北马其顿、黑山、阿尔巴尼亚、乌克兰、摩尔多瓦共和国、波斯尼亚和黑塞哥维那、格鲁吉亚以及安道尔赞同这一发言。

主席先生，感谢你组织这次高级别公开辩论会。欧盟欣见今天的交流，讨论不断演变的网络威胁形势及其对维护国际和平与安全的影响。

刚才的发言反映了各种新出现和不断演变的威胁，既有影响较小的拒绝服务攻击，更有大规模的网络行动和对关键基础设施的攻击。除这些关切外，我们还关注恶意网络活动可能造成的潜在跨境影响。我们还注意到，犯罪活动与国家支持的利用雇佣网络犯罪分子发起的攻击之间，难以彼此区分，这使本已困难重重的归因工作变得更具挑战性。我们必须共同致力于加强集体复原力工具包，同时我们欢迎其他代表团分享他们的见解和经验。

欧盟及其成员国震惊地看到，针对政府机构和民主进程的恶意网络活动数量众多、高度复杂且规模宏大。上个月，德国分享了对与俄罗斯有关联的网络间谍团伙APT28活动的评估，认为其损害了德国社会民主党的电子邮件账户。捷克、波兰、立陶宛、斯洛伐克和瑞典等欧盟成员国的国家机构、部门和实体，之前都曾受到过同一威胁行为者的攻击。这些恶意活动必须停止。

联合国网络空间负责任国家行为准则提供了这方面的指导。其中主要的承诺简单明了：国际法适用于网络空间；各国应维护国家行为自愿准则；各国必须防止在其领土上滥用网络；需要采取切实可行的建立信任措施，帮助降低网络事件造成升级和冲突的风险。对欧盟而言，如果我们要履行与共同利益相称的共同责任、保护所有国家免受恶意网络活动风险，就必须着重发展和实施商定的网络空间负责任国家行为框架。各国可以澄清现有国际法的适用情况，讨论现有负责任行为准则的实施和遵守问题，从而取得有意义的进展。要使商定的负责任国家行为框架行之有效，我们就必须共同维护它。这就更加突出了有必要由联合国主持建立一个常设、包容和注重行动的机制。因此，我们支持制定一项行动纲领，在国际安全背景下促进使用信息和通信技术方面的负责任国家行为，并希望在今年夏天就具体步骤达成一致。

我们期待着进一步推动关于这一重要议题的讨论，并欢迎像本次会议这样的努力。这种努力就是要凸显网络领域所出现的独特而具体的国际威胁，突出安全理事会在履行《联合国宪章》规定的任务、应对国际和平与安全所面临威胁方面的重要作用。我们还希望继续探讨安理会今后的工作如何有效补充联合国在这方面的其他相关进程。

主席（*以英语发言*）：我现在请菲律宾代表发言。

拉达梅奥先生（菲律宾）（*以英语发言*）：菲律宾借此机会再次强调，应对信息和通信技术（信通技术）对国际安全的威胁至关重要。数字技术的迅速发展带来了新的挑战，需要立即采取协调一致的行动。在这方面，我们谨强调三个要点：信通技术威胁的趋势、网络威胁对国际和平与安全的影响以及网络攻击这一威胁倍增因素。

第一，关于信通技术威胁的趋势，人工智能操控的机器人电话的兴起被用于欺诈、深度伪造和错误信息的扩散以及勒索软件攻击带来了巨大的风险和复杂的挑战。全面的战略对于应对这些复杂的威胁至关重要。在网络空间恶意使用人工智能会构成巨大风险。我们必须优先评估这些威胁，以制定强有力的网络安全政策，并确保人工智能技术的安全应用。

第二，关于网络威胁对国家和平与安全的影响，菲律宾亲身遭受了网络攻击对国家安全和公众信任的严重影响。最近发生的事件，如政府网站被篡改、重要机构数据遭泄露和个人信息被大规模盗取，突出表明迫切需要加强网络安全措施。网络攻击会中断基本服务，破坏对机构的信任，并造成深远的社会经济后果。我们还特别关切意图干涉各国内政的恶意信通技术活动。我们看到，据报告，国家恶意利用信通技术秘密开展宣传活动以影响别国进程、系统和总体稳定的情况有所增多。这种使用损害信任，会导致事态升级，并可能危及国际和平与安全。另一个令人想来感到震惊的情况是，非国家行为体可以获得这些先进信通技术能力，而且有能力恶意利用这些技术谋取商业利益和逃避责任。

第三，关于网络攻击的威胁倍增效应，网络空间的犯罪活动加剧了对国际和平与安全的现有挑战。菲律宾就曾目睹网络攻击成为严重的威胁倍增因素，使维护和平与稳定的努力复杂化。网络空间的跨国性质意味着，任何国家都无法独善其身，我们集体安全的强度取决于其最薄弱的一环。鉴于网络威胁构成的严重风险，菲律宾强调安全理事会在应对这些威胁方面的关键作用。虽然信息和通信技术安全及使用问题不限成员名额工作组正在进行的讨论很有价值，但安全理事会也必须继续参与制定全球网络安全议程。

在这方面，菲律宾支持安理会采取在4月份举行的”阿里亚办法 “网络安全会议期间提出的以下集体措施来应对网络威胁： 第一，加强商定的网络空间负责 任国家行为规范性框架； 第二，每年召开会议讨论和审 查信通技术威胁状况，并在这方面请秘书长编写年度 趋势报告，为会员国的讨论提供信息； 第三，牵头收集 信息或研究具体威胁或事件，为会员国提供指导和参考。

菲律宾重申致力于加强网络抗攻击能力，倡导网络空间负责任行为。我们呼吁继续开展合作，努力建设能力，建立各种支助机制，包括设立一个经常信托基金，以协助发展中国家应对网络威胁。我们指望伙伴关系和技术转让帮助我们缩小数字鸿沟，加强我们的网络防御。

主席（以英语发言）： 我现在请印度尼西亚代表发言。

纳西尔先生（印度尼西亚）（以英语发言）： 印度尼西亚感谢大韩民国召开本次重要会议。我们也感谢秘书长和通报人介绍情况。

网络空间的威胁已成为国家和国际和平与安全面临的真切而现实的威胁。我们日益受到各种快速发展的新技术所带来的新威胁的影响。只有采取协调一致的应对措施，建立强有力的法律框架，国际社会才能增强网络抗攻击能力，并有效缓解这些风险。

有鉴于此，请允许我强调以下几点。

第一，我们必须优先减轻针对关键基础设施的网络攻击给人类造成的影响。我们必须确保网络空间的安全得到保障，使之成为一个没有冲突的领域，而不是冲突的场所。虽然人工智能——包括生成式人工智能和机器学习——的进步可以造福人类，但它们也可能带来危害，为网络攻击提供机会，给全球人口造成巨大负面影响。因此，在我们努力防止恶意网络行为体和不负责任的国家造成重大危害的过程中，必须保障关键基础设施的安全。

第二，联合国系统内在网络安全、信息和通信技术以及国际和平与安全领域的协同性和一致性至关重要。安全理事会肩负着维护国际和平与安全的重要使命，而联合国其他机构则在处理数字和信通技术安全及网络安全问题方面肩负着同样重要的使命。重要的是，安全理事会应确立有助于促进协作和协同作用的框架和机制，使人们更好地了解网络威胁对国际和平与安全构成的风险。因此，印度尼西亚重申，它致力于支持信息和通信技术安全及使用问题不限成员名额工作组以及在该领域开展的其他进程——包括未来峰会进程——的工作。

第三，我们必须加强区域合作，以加强全球网络安全。与区域组织的合作是必要的，因为它们在推动各国对网络安全采取强有力的全面办法方面发挥着重要作用。在我们区域，东南亚国家联盟（东盟）通过东盟区域论坛等渠道，在建立框架和制定举措以加强区域抵御网络威胁的能力方面发挥了重要作用。利用区域组织的这种专门知识，确实可以提供宝贵的见解，推动更全面的国际努力。

最后，我们必须弥合技术差距，以增强网络抗攻击能力。网络安全能力不足是发展中国家面临的一个重大挑战，使它们在各种不断升级的威胁面前脆弱不堪，稳定受到破坏。各层面的合作措施，包括与相关私营部门利益攸关方的合作措施，特别是能力建设、技术援助和技术转让，对于加强网络空间的稳定至关重要。只有共同努力，我们才能打造一个安全的网络空间，促进全球的和平与稳定。

主席（*以英语发言*）：我现在请新加坡代表发言。

谢先生（新加坡）（*以英语发言*）：我们感谢大韩民国召开今天的会议，讨论这一重要问题。

自2021年6月安理会首次就网络安全问题举行公开辩论会（见S/2021/621）以来，网络威胁状况继续以令人担忧的速度演变。在此背景下，在联合国开展国际合作对于应对网络威胁状况的全球性和跨界性至关重要，不可或缺。在这方面，大会和安全理事会必须携手合作，在适用国际法和尊重《联合国宪章》原则的基础上，加强对网络空间负责任国家行为规范性框架的遵守。作为一个小国，新加坡一贯支持基于法治的多边体系。在对许多小国和发展中国家至关重要的网络安全问题上，我国的态度也是如此。新加坡坚信，联合国作为讨论制定和实施管理网络空间的负责任国家行为规则、规范和原则的重要平台，具有重要意义。

新加坡很荣幸自2021年以来担任信息和通信技术安全和使用安全不限成员名额工作组主席。不限成员名额工作组以联合国二十多年的工作为基础，这些工作产生了一个关于网络空间负责任国家行为的累积而且不断发展的框架，它得到所有会员国的认可。令人鼓舞的是，过去三年来，不限成员名额工作组在进一步加强网络空间负责任国家行为规范框架方面取得了良好进展。

不限成员名额工作组本身也是一种宝贵的建立信任措施。除了不限成员名额工作组分别于2022年7月（见A/77/275）和2023年7月（见A/78/265）以协商一致方式商定的两份年度进度报告中达成的共同谅解之外,它还率先制定和实施了面向行动的具体举措，这在加强网络空间的国际和平与安全方面发挥了重要作用，最显著的是5月9日正式推出的全球联络点名录。同样在5月，不限成员名额工作组成功召开了关于信息和通信技术（信通技术）安全能力建设的实质性部长级会议。那次会议传达的主要信息是，迫切需要能力建设来帮助许多小国和发展中国家实现网络抵御力。同样重要的是，人们普遍认识到，能力建设可以成为国家间建立信心和信任的重要手段。

主席先生，在你的指导性问题中，你问了网络威胁如何与安全理事会其他议程项目相互关联，以及安全理事会在应对来自网络空间的国际和平与安全挑战时可以发挥什么具体作用。鉴于大会当前开展的工作，安全理事会必须避免重复已经在其他进程中进行的工作。然而，与此同时，我们必须承认，安全理事会有讨论维护国际和平与安全相关事务的明确授权。我们不能排除一种可能性，即网络事件可能造成国家间的误解，导致局势升级和潜在冲突，从而造成国际和平与安全事件。因此，我们不能排除安全理事会的作用，它承担着《宪章》赋予的维护国际和平与安全的责任。

因此，安理会应该兼容并包地看待何为国际和平与安全受到的威胁，并在开展行动时认识到网络威胁可能会产生涉及实物的现实后果。在这方面，我们对安全理事会继续举行今天这种公开辩论会的想法持开放态度，以此作为会员国之间交流信息和增进理解的手段。安理会的讨论有助于为大会工作提供信息，包括在能力建设和建立信任领域，并进一步有助于加强网络空间负责任国家行为框架，包括考虑如何以最佳方式针对现有和潜在的网络威胁适用规则、规范和原则。

最后我要强调，需要加强国际合作，从而加强我们在网络空间的集体抵御力。促进安全理事会和大会在国际和平与安全问题上加大合作，并以持续、全面和协同的方式共同努力，将使国际社会能够更好地维护网络空间领域的国际和平与安全。新加坡已准备好与所有会员国一道努力实现这一目标。

主席（*以英语发言*）：我现在请哥斯达黎加代表发言。

陈·巴尔韦德女士（哥斯达黎加）（*以西班牙语发言*）：我感谢大韩民国召开今天的公开辩论会。

两年前，哥斯达黎加成为大规模勒索软件攻击的受害者。我们仍然感受得到保健系统、社会保障、金融和其他关键部门所受破坏造成的影响。

在这方面，哥斯达黎加今天想提三点看法。

第一，哥斯达黎加坚信，保护平民议程应当扩大，将武装冲突期间影响平民的网络活动包括在内。各国必须加入日益壮大的协商一致意见，即认可民用数据与所有其他民用物体一样享有国际人道法保护，以及国际人道法禁止那些瘫痪或妨碍民用系统功能的网络操作。各国还必须避免将平民卷入军事网络活动，因为这可能会让他们身处险境。

第二，哥斯达黎加认为，现在是时候更新妇女与和平与安全议程了，以便应对妇女的数字安全问题。哥斯达黎加呼吁安全理事会成员考虑通过一项新的决议草案，规定保护妇女和女童免遭网络暴力、虐待和剥削的措施，尤其是在冲突和冲突后环境中。数字安全方面的考虑也必须被系统地纳入与该议程相关的所有新任务、目标和举措中。

第三，所有国家，无论是否是安理会成员，都有责任加强网络空间的国际法治。越来越多国家发表了关于在网络空间适用国际法的国家立场，哥斯达黎加自豪地成为其中一员。这些立场文件建立在全球共识的基础上，即国际法，包括国际人道法和国际人权法，适用于各国使用信息和通信技术问题，对于维护和平与稳定至关重要。我们鼓励其他国家制定这种立场文件，并赞扬现有的法律能力建设资源，如网络法律工具包，它可以指导该领域的努力。

随着我们的社会越来越容易受到网络和数字威胁，哥斯达黎加敦促安理会将这些关切纳入工作，同时要在和平和武装冲突时期加强对国际法的尊重。

主席（*以英语发言*）：本次会议名单上还剩下一些发言者。征得安理会成员同意，我打算暂停会议，今天下午3时复会。

下午1时10分会议暂停。