



## 安全理事会

第七十七年

第**九〇三九**次会议

2022年5月23日星期一上午10时举行

纽约

临时逐字记录

主席：	托马斯-格林菲尔德夫人.....	(美利坚合众国)
成员：	阿尔巴尼亚.....	霍查先生
	巴西.....	德奥利维拉·马尔克斯先生
	中国.....	张军先生
	法国.....	德里维埃先生
	加蓬.....	比昂女士
	加纳.....	阿吉曼先生
	印度.....	蒂鲁穆尔蒂先生
	爱尔兰.....	弗林先生
	肯尼亚.....	基博伊诺先生
	墨西哥.....	戈麦斯·罗夫莱多·韦尔杜兹科先生
	挪威.....	尤尔女士
	俄罗斯联邦.....	涅边贾先生
	阿拉伯联合酋长国.....	努赛贝夫人
	不列颠及北爱尔兰联合王国.....	罗斯科先生

## 议程项目

维护国际和平与安全

技术与安全

本记录包括中文发言的文本和其他语言发言的译文。定本将刊印在《安全理事会正式记录》。更正应只对原文提出。更正应作在印发的记录上,由有关的代表团成员一人署名,送交逐字记录处处长(U-0506) (verbatimrecords@un.org)。更正后的记录将以电子文本方式在联合国正式文件系统(<http://documents.un.org>)上重发。

22-35744 (C)



无障碍文件

请回收



上午10时05分开会。

## 通过议程

议程通过。

## 维护国际和平与安全

### 技术与安全

**主席** (以英语发言)：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：主管政治和建设和平事务副秘书长罗斯玛丽·迪卡洛女士；全球之声组织Advox数字权利项目主任南贾拉·尼亚博拉女士；麦吉尔大学国际和平与安全研究中心兼职教授、国际和平研究所非常驻研究员德克·德鲁特先生。

安全理事会现在开始审议其议程上的项目。

我请迪卡洛女士发言。

**迪卡洛女士** (以英语发言)：数字技术深刻改变了各国社会的方方面面。它们为可持续发展、教育和包容提供无限机会。例如, 社交媒体改变了人权和人道主义宣传的方式, 使我们能够围绕需要紧急关注的问题快速、高效地动员世界各地的民众。它们也为我们的和平与安全工作创造了新的可能性。技术发展提高了我们发现危机、更好地预先储备人道主义物资和设计数据驱动型建设和平方案的能力。

我们正在预防冲突、缔造和平和建设和平工作中使用数字技术。请允许我分享几个例子。

数字工具加强了我们的信息收集和预警能力。在也门, 联合国支助荷台达协议特派团利用各种制图、地理信息系统和卫星技术工具来加强对该省停火工作的监测。数字工具让我们为理解、分析和应对可能涉及数字层面的危机以及应对数字风险做好更充分的准备。例如, 我们与伙伴方一起建立了一个关于数字风险管理的电子学习平台。

新技术有助于支持政治进程, 特别是促进包容。在各种和平谈判中, 我们用人工智能辅助的数字对话来接触数千名对话者, 听取他们的观点和优先事项。

这是接触包括妇女在内传统上被排斥的群体的一个特别有用的方式。

在利比亚, 联合国特派团举行了五次数字对话, 每次都有1000多人参加。这一努力提高了这一进程的合法性, 因为各群体注意到自己的声音得到了倾听。在也门, 特使通过数字协商与来自各省的数百名妇女接触, 这使他对战争的性别层面有了更深入的了解。

使用数字技术还可以改善实地维和人员和文职人员的安全保障。启动《联合国维持和平行动数字化转型战略》是实现这一目标所不可或缺的步骤, 也有助于更有效地执行任务, 从而提高预警能力。

最后, 借助这些工具, 我们能够形成可视化信息并进行数据丰富的分析, 以支持安全理事会的决策。我们最近以虚拟现实方式向安全理事会介绍哥伦比亚的情况, 表明我们能够以新的方式提请本机构注意我们在实地的工作。

数字技术对维护国际和平与安全的好处是多方面的。然而, 技术进步也带来了新的重大风险, 并有可能影响冲突动态, 使之恶化。有几个方面令人担忧。

根据一些估计, 自2015年以来, 国家和非国家行为体支持的恶意使用数字技术实现政治或军事目标的事件数量几乎翻了两番。攻击卫生和人道主义机构等提供基本公共服务的基础设施的活动令人特别关切。与此同时, 致命自主武器引发了有关人类对使用武力承担责任的问题。

如秘书长明确指出的那样, 机器若拥有未经人类参与即可夺取生命的权力和酌处权, 在政治上就是不可接受的, 在道义上也令人深恶痛绝, 应该为国际法所禁止。此外, 非国家行为体正越来越善于利用成本低廉、唾手可得的数字技术实现其图谋。伊拉克和黎凡特伊斯兰国和基地组织等团体仍然活跃于社交媒体, 利用平台和短信应用程序与追随者分享信息、进行交流, 目的是进行招募、规划和募集经费。加密货币等数字支付方式的日益普及带来更多挑战。

此外, 数字技术在人权方面引起重大关切, 包括

人工智能系统可能具有歧视性，以及可针对特定社区或个人部署的监视技术唾手可得。我们也关切越来越多地采用关闭互联网的做法，包括在激烈冲突局势下这样做，从而使社区丧失通信、工作和参与政治事务的手段。

例如，在缅甸，自2021年2月1日军事政变以来，互联网和手机关停的次数和期限都有所增加，特别是在军事行动区。社交媒体可助长分化对立，有时还会挑起暴力。滥用社交媒体，以及社交媒体公司做出的反应有时不是有限就是不够充分，都在助长虚假信息、激进行为、种族主义和厌女症的蔓延。这可能加剧紧张局势，在有些情况下还可加剧冲突。正如安全理事会在2021年11月5日的新闻谈话(SC/14691)中确认的那样，在埃塞俄比亚，随着战斗升级，社交媒体传播煽动性言论的帖子惊人地增多，有些帖子甚至煽动种族暴力。

我们已经看到网上的虚假信息和仇恨言论如何导致线下伤害，包括暴力。我们知道，虚假信息可导致谎上加谎，助长分化对立，从而妨碍我们特派团执行任务的能力。在秘书长发起的《联合国消除仇恨言论战略和行动计划》以及“联合国认证信息”等倡议的推动下，我们正在采取许多行动减轻这些风险。例如在伊拉克，有报告称，在去年的选举中，女候选人在网上遭到的骚扰增多，其后，联合国伊拉克援助团与民间社会组织开展合作，以监测仇恨言论，发布公开报告，并加强选民教育。

我们必须充分利用数字技术提供的机会推动和平，但为了做到这一点，我们还必须减小此类技术构成的风险，促进所有行为体负责任地加以使用。会员国通过大会在建立规范性框架以确保网络空间负责任行为方面取得了重要进展。会员国还开展合作，制定和实施一系列建立信任措施，以防止冲突，避免误解和误会，减缓紧张局势。

然而，必须开展更多的工作推进、拟订和执行新的规范性框架。秘书长在题为“我们的共同议程”的报告(A/75/982)中要求达成一项全球数字契约，这

项契约将勾勒出为所有人建立一个开放、自由、安全的数字未来的共同原则。加上《我们的共同议程》的其他方面，如新的和平议程和拟议的促进新闻诚信的行为守则，我们就拥有重要机会，可借以就如何利用数字技术造福于民众和地球、同时应对其风险达成共识。但是，会员国的集体行动对于实现这一目标仍然至关重要。

主席(以英语发言)：我感谢迪卡洛女士的通报。

我现在请尼亚博拉女士发言。

尼亚博拉女士(以英语发言)：今天，我荣幸、高兴地在安全理事会就数字技术问题发言，因为它关系到和平与安全。正如成员们在开场白中听到的那样，我是一名研究人员，工作任务是研究技术、社会和政治相互交叉的问题，我特别关心如何加深我们对数字权利的共同认识。

过去20年，我们亲眼目睹数字技术在社会生活各个层面——个人、集体、国家和跨国层面——的使用范围骤然扩大。不幸的是，这种扩大并未辅之以如下做法：一是在防止我们自身受到其造成的危害方面进行类似投资，二是承诺在我们正在建设的体系内了解和捍卫人权。简而言之，我们对数字化的渴求过于强烈，对其影响的认识却不够；而且，越来越多的证据证明，没有章法的做法可带来危害，因此，现在已到关键时刻，应该进行评估，并决定我们是否必须改变或扭转自己的行动方针。

试图在分配给我的发言时限内概述数字时代对权利的所有影响是荒谬之举。因此，在本次通报中，我只强调数字化带来的一些全局性挑战，以及为维护和平与安全创造行动机会的三项关键原则。

作为开场白，我仅限于表示，谈论涉及和平与安全的数字技术，绝不能被解读为鼓励互联网军事化和安全化。毕竟，安理会的授权任务是维护和平与安全，重要的是要以一种精神为指导，这种精神是出于对安全的关注，同样也是出于对积极和平的渴望，而后者甚至可能超过前者。互联网一直是巨大创新、创意和机会的空间，在思考如何解决互联网今天面临的挑战

时,我谨敦促安理会致力于将因特网作为全球公益物加以维护,一如我们在思考南极或外层空间之类的空间时所秉持的合作精神。

尽管如此,在多年无节制的技术乐观主义之后,我们现在正处于一个日益玩世不恭的时刻,因为在我们努力加快进展时所忽视的各种威胁已开始真切呈现。在我与Advox牵头开展的研究中,我们运用一种简单的类型学帮助自己了解这些威胁,并且将数字技术领域分为四类:数据、访问、语音和信息。

关于专门针对数据栈的引发数据担忧的做法问题,如监视或越来越多地使用生物识别技术,全球监视经济一直惊人地增长,包括广泛使用“飞马”

(Pegasus)等技术监视政治领袖、新闻记者和民间社会成员。为了使这些做法成为可能而开发的技术是在富裕国家开发的,然后被部署或出口到穷国,没有从总体上考虑权利环节,使带头推进和平者陷于严重危险境地。

因此,我们与联合国人权事务高级专员办事处一道,敦促全球暂停开发和销售监视技术,并请安全理事会共同向私营公司施加压力,要求它们遵守这一暂停令。国家和非国家实体也越来越多地使用大规模数据采集技术,或将我们的生活数据化,却没有相应地努力保护甚或提高对数据隐私或数据保护等关键权利的认识。在冲突地区,难民生活的数据化程度骤增,包括更多地收集和储存并且在不透明的条件下保留寻求庇护者的生物鉴别数据,这些数据有时被用来剥夺难民的权利或限制其自由。

访问问题着眼于限制人们上网能力的主动和被动做法,包括关闭互联网和社交媒体、性别差距和蓄意减少基础设施投资,对资源匮乏的社区造成危害。2021年,全球数字权利组织——“立即普及组织”的记录显示,有34个国家关闭互联网182次——高于2020年29个国家关闭159次的备案数字。互联网关闭的最长期限持续了近三年。互联网关闭率最高的国家一年内曾高达109次。

除关闭互联网之外,带宽限制和社交媒体关闭等

相关做法也有所增加,尤其是在紧张的选举期间。这些干扰旨在吓阻公民言论和参与,是对民主与和平的直接攻击。

更广泛而言,一些国家的妇女仍然面临系统性障碍,没有机会上网——当世界各地的学校试图利用虚拟教育来应对2019冠状病毒病大流行时,这一事实变得尤为明显。在某些国家,这种转变没有妥善实现,年轻女孩首当其冲受到排斥,无法利用任何可用的技术,就因为她们是女孩。此外,在某些国家,包括一些富庶国家,虽然在公民生活中强制使用数字技术的趋势有所加强,包括出生、死亡和其他登记,但是为了使残疾人能够利用数字基础设施或者以土著语言和非主要语言利用数字基础设施而进行的投资极少。

言论问题着眼于表达、信息或意见自由所受的限制。在很多国家,数字平台和模拟平台一同运作,例如媒体和实体公共广场,民众可以在这里集会、商讨和分享关于如何改进社会的想法。利用立法来限制民众参与这类言论的做法急剧增多,包括利用法律来毫无道理地扩大刑事诽谤的定义,将几乎所有批评国家官员之举列为非法。联合国人权事务高级专员办事处指出,至少40项社交媒体法律于2020年至2021年之间获得通过,在同一时期,还有30项正在审议之中。

其中有很多法律载有非常宽泛的定义,界定它们本应处理的基本伤害,这些定义往往首先被用来对付新闻记者和批评国家的人。这些法律获得通过之后,针对新闻记者的民事或刑事案件通常会激增。在这一点上值得强调的是,这些做法常常涉及性别层面,专门针对例如玛丽亚·雷萨和Rana Ayyub等新闻记者,或者民间社会成员,甚至针对普通青年妇女,因其被指控违反公共道德,或者仅仅因其所从事的工作。

最后,信息方面涉及的做法是在公共领域操纵信息,以扭曲民众对现实的看法,因此也扭曲他们采取适当行动来应对社会或政治问题的能力。这包括散布错误信息、虚假信息或恶意信息等做法,以及采取协作虚假行为或者假草根行为,改变社交媒体平台上的公共议程。这些做法借助互联网才得以实施,在互联网



网上,广告推动流量,因此,受关注度是可以购买的。

在冲突区,敌对政府利用协作虚假行为消除批评声音,为此利用大量负面评论对其进行狂轰滥炸,使其社交媒体变得无法使用。一些国家的行政管理机构已经设立政府部门,专门操纵网上言论,或者建立貌似新闻类组织,歪曲对国家行为的看法,或者用大量噪音污染沟通渠道,使信号无法传播。这些做法共同发挥作用,使和平难以实现,因为它们使民众难以就冲突原因达成一致,因此无法就制止冲突的必要做法达成一致。

或许,令人忧惧的最大原因是,这些做法增多,未必限于特定类型的政府或者我们毫不迟疑地指斥其专制的政府。相反,我们的研究发现,人们越来越容忍对国家安全的关切压倒对人权和民主的关切。

重要的是,我必须提出对以下做法的忧惧:名义上的民主国家研发并向公开实行专制的国家出口促进数字专制主义的技术。这一切发生在我们解决技术自身蕴含的不公正之前,例如,包括对于人工智能蕴含的不公正的关切。

与此同时,将互联网当前面临的挑战单纯视为各国面临的挑战,导致在监管对策上各自为政,有损互联网作为连接器的价值。我们的研究发现,数字化产生的威胁是多边的——也就是说,在单一国家之内很少能够始终得到遏制;这种威胁是跨国的,因为它们通常涉及跨国境技术转让;它们是跨代的,因为我们正在为了当前认为的安全而抵押子孙后代使用自由互联网的可能。这些现实情况需要与之相称的应对措施。仅仅单独挑出个别国家还不够。我们需要做的是在数字专制主义文化落地生根并走遍世界之前对它们加以识别。

最后,我谨再次指出安全理事会在维护和平与安全方面的职责,并敦促采取一种多边、跨国和跨代做法来解决数字时代的人权挑战。为实现这样一种做法,我敦促安理会回顾三项原则。

第一,数字权利是人权,为应对这些挑战所作的任何努力,都必须首先防范国家和私营公司对人过渡

使用权力。

第二,尽管存在这些挑战以及更多挑战,互联网的力量仍然能够也必须得到利用,以促进更大的公益,因此我们必须将其作为一种全球公益加以塑造和保护,而不允许安全利益或利润压倒和平利益。

最后,无论安理会选择采取何种行动,都必须超越此时此刻,着眼于保护子孙后代的期冀。我们的行动有可能促成什么样的数字化共同未来?它们会框定什么样的未来?显然,这些原则之中包含着很多紧张和矛盾。我们需要加强还是减少管制?私营公司应当发挥何种作用?我们如何平衡我们对技术进步的渴望和我们对综合、公平利用的渴望?

我认为,如果铭记这些原则,为了保护数字权利并确保数字技术在国际和平与安全方面发挥积极作用,联合国可以采取的某些行动就显而易见了。联合国必须继续运用其无与伦比的号召力,为保护作为全球公益的互联网而促进审议并争取支持。联合国必须运用其设置议程的权力,确保以追溯性和前瞻性方式,把人权植入我们研发和利用的数字技术中。联合国必须运用其制定准则的权力,促进在人权标准上达成一致,从而有可能实现一个自由、安全和公正的数字化未来,这不仅是为了当代人,也是为了子孙后代。

最后,联合国必须为世界各地一直奋斗在这项工作第一线的人争取支持,他们常常面临巨大的个人风险,必须为Alaa Abd El-Fattah这样因为利用互联网推动民主理想而蒙受严重不公正的人公开声辩。

此时此刻,我们集体走上了一条通往不公正的数字化未来之路,但是也有可能走上一条更公正的不同道路,安全理事会会有机会推动我们走向这个更美好的未来。

**主席**(以英语发言):我感谢尼亚博拉女士的所作的通报。

我现在请德鲁埃特先生发言。

**德鲁埃特先生**(以英语发言):我感谢有此机会并有幸向安理会通报不断发展的数字技术如何影响

暴力冲突的性质,以及对联合国为预防暴力、保持和平和减少苦难与战争所作的努力产生的影响。

正如安理会主席所提到的那样,我多年来参与联合国的技术能力开发,尤其是从了解局势、分析及维和情报的角度出发。目前,我在麦吉尔大学研究这些问题,并就技术、冲突性质和国际和平与安全干预措施的交叉问题向不同利益攸关方提供建议。

今天,我谨就三个相互关联的议题提出我的看法。第一,数字技术如何改变安全理事会正在解决的冲突;第二,这些技术以及冲突各方乃至联合国自身对技术的利用如何影响本组织预防和解决暴力活动的努力;第三,我谨就在这些不断变化的情况下,联合国的和平与安全工具包、尤其是其和平行动如何更有效和更负责任地适应其工作提出一些建议。

关于第一个议题,即影响问题,安理会已经多次听取了数字技术如何充当团体内外的动态促进因素、迅速传播反信息或错误信息的平台,以及操纵民众的工具,包括国家、非国家和极端主义行为体的此种做法。例如在缅甸,有翔实记录表明,“脸书”上不受约束的煽动暴力之举以及提高极端思想受关注度的算法助长了对罗兴亚人实施的灭绝种族暴力。自那时以来,互联网和通信已被用作工具,用来控制考克斯巴扎尔的难民。最近,乌克兰冲突凸显了公共舆论在现代冲突大部分甚至所有当事方的战略中的重要性。

必须指出,在联合国介入的许多冲突和脆弱局势中,民众显然容易受到错误信息和虚假信息的影响。一些国家,如中非共和国,缺乏传统的新闻职业素养和媒体基础设施,使民众几乎完全依赖社交媒体获取消息。此外,尽管社交媒体公司非常重视在自身平台上打击虚假信息的工作,但2021年脸书披露的内部文件表明,内容审核资源严重偏向美国和西方,而一些脆弱和受冲突影响的环境几乎被忽视。在这方面,安全理事会有机会要求社交媒体公司在全球范围内平等履行其责任。

除影响冲突动态之外,数字技术正日益成为在冲突环境中保护或剥夺人权的重要平台。在阿富汗,平

民谈到了无人驾驶航空系统无处不在的嗡嗡声对他们精神健康的影响,而在缅甸,军政府利用其对互联网的控制来打击2021年政变的反对者,限制他们的联络和组织能力。在叙利亚冲突和最近乌克兰冲突引发的移民危机中,有关人道主义行为体等各方收集和管理生物识别数据时是否征得知情同意的严重问题越来越突出。

关于第二个议题,即对和平行动的影响,数字技术和舆论在战争逻辑中越来越重要,冲突各方难免会将联合国在这些冲突中采取的行动为己所用,试图达到对自身有利的结果。在中非共和国,一直有人蓄意针对联合国中非共和国多层面综合稳定团开展活动,试图破坏该特派团在民众心目中的公信力。这些活动的动机似乎因环境和参与者的不同而大相径庭。例如,在马里,当地一些权力掮客散布有关联合国马里多层面综合稳定团的虚假信息,这似乎是为了破坏该特派团扰乱非法经济网络的行动。还有一些情况是,造谣者似乎受意识形态目标的驱使,另一些情况则是,联合国似乎成了试图转移人们的注意力的东道国或其伙伴的有效靶子,使人们忽视其在为本国人民提供安全保障和服务方面的不良表现。无论出于什么动机,这些袭击严重减少了联合国接触当地困难民众的机会,破坏了联合国与东道国政府以及调解与和平进程当事方的关系,在某些情况下严重威胁到维和人员的安全保障。

但同样重要的是,必须承认数字技术在使联合国能够在现代冲突环境中有效执行任务方面发挥的作用。例如,联合国在索马里和马里的和平行动正在利用自然语言处理技术,快速、精准地了解当地的看法和国家政治言论。正在使用非武装无人驾驶航空系统等监测和监视技术,越来越有效地将其纳入全特派团的定性和定量数据收集工具和分析系统,以生成更高质量的维和情报,继而在掌握更多信息的基础上发现威胁并更加迅速地采取行动保护平民,当然还要确保联合国人员的安全和保障。

在这方面,我想就联合国可以如何适应数字技术对冲突的影响、减轻这些技术对其自身行动的负面影

响以及在这些局势中更加有效和负责任地使用数字技术提出一些想法，供安理会审议。在这方面，我特别注意到四个方面。

第一，在冲突环境中，联合国应该作为信息行为体，发挥更加明确、审慎的作用。在信息战的情况下，获得准确的信息日益被视为一项人权，联合国可以在说明真相和充当可靠信息渠道方面发挥作用。我应该指出，多年来联合国特派团已经在和平进程机制中发挥这一作用，例如为此实施停火监测。因此，有必要考虑如何通过这些机制形成的良好做法用于在冲突中更广泛地为社会提供信息。

然而，联合国要发挥这一作用，其行动就必须获得并保持各阶层民众的信任。当一些联合国活动，如保护平民或支持东道国当局，可能使特派团受到批评——这些批评有时有道理，有时没道理——时，这项任务不易完成，当这些特派团成为造谣运动的对象时更是如此。因此，第二个优先事项是，联合国和平行动必须大幅提高其监测和分析信息空间的能力，并有效应对传播恶意信息的情况。引用国际和平研究所最近的报告，特派团必须“预见危机并积极主动地重构舆论，进行双向而非单向的沟通”，并“根据特定受众调整其信息”。

第三，联合国自身将需要新技术和有效使用这些技术的能力，包括在通信领域，以及在态势感知和维和情报、用于战略规划的数据分析以及用于对话和调解的新技术等领域。联合国在这些领域推动了许多令人振奋的创新，包括迪卡洛女士强调的那些创新，同时我们必须认识到，这些工具带来重要、复杂的道德、法律和政治问题，对本已遭受冲突之苦的人民的权利产生了影响。采用会员国使用这些工具的说法和理论可能很诱人，但我要向安理会提出，在冲突环境中使用敏感技术时，联合国行动的利益和责任是不同的。

因此，作为第四项建议，我谨强调联合国获取和使用新技术的方式对这些特派团在实地的信誉和政治地位的重要性。经验表明，获取敏感的新技术以及这方面的伙伴关系在它们加强联合国的公正性并为

负责任的使用提供可信公开保证时最为有效。

因此，我敦促秘书处制定自己的系统性工具、政策和程序，要考虑到联合国作为这些技术使用者的独特性质。已经在为此开展宝贵工作，包括和平行动部正在努力丰富其跟踪和监视政策，以及联合国“全球脉搏”举措正在领导联合国全系统努力，在整个系统内推出数据隐私政策。我认为，如果做得好，对会员国和公众保持完全透明，这些努力具有重要的规范作用，就如何在涉及弱势群体的冲突局势中负责任地使用敏感技术制定标准。

这些努力应包括正视联合国保护敏感信息特别是个人信息免遭国家和非国家行为体入侵的能力的局限性，然后审查在人道主义行动过程中收集生物识别数据等做法。这一审查还应包括根据《联合国人权尽职政策》，就联合国如何与包括平行军事部队在内的非联合国部队、东道国当局和国际法治行为体分享信息制定进一步的指导意见。

最后，今天的讨论涉及两组截然不同但又密切相关的问题：第一，在联合国介入的局势中，数字技术如何改变冲突的性质；第二，联合国自身如何利用数字技术为其任务服务。需要这两组问题以及不同的政策和行动对策进行细致入微的考虑和辩论。正确处理这两组问题对我们当前和未来行动的成功至关重要。安理会可以在这方面发挥关键作用。

**主席** (以英语发言)：我感谢德鲁特先生的通报。

我谨提请各位发言者注意主席说明S/2017/507第22段，该段鼓励安理会会议的所有与会者按照安全理事会关于更有效利用公开会议的承诺，在五分钟内结束发言。

我现在以美国代表的身份发言。

我感谢迪卡洛副秘书长的通报。她的发言清楚表明，新技术已经在联合国维持和平努力中发挥重要作用，至关重要的是要以建设性方式使用这些技术。我感谢尼亚博拉女士就这些技术的潜在使用和滥用给人权活动人士和民间社会带来的利弊谈了她宝贵的看



法。我感谢德鲁特先生分享了如何利用数字技术支持我们的维和人员的工作,而滥用数字技术也会破坏他们的工作。我们一定要把前者最大化,把后者最小化。本次通报谈的是一个巨大的机遇和一个紧迫的挑战。

机遇在于安全理事会可以利用数字技术的力量来促进和平与安全,以便负责任地使用这些工具,在它们正在造成伤害的冲突和环境上做很多好事。毕竟,这些技术有巨大潜力来支持联合国系统在世界各地开展的良好工作。社交媒体工具和短信应用程序可以在冲突前和冲突期间帮助获取救生信息。卫星数据可以识别气候变化带来的风险,为维和人员提供重要信息,并改善冲突和自然灾害期间的应急通信。我们可以在饥荒开始前察觉并防止它们。我们可以为难民找到家园、住房和工作。我们可以更好地保护我们的维和人员和他们受命服务的人。

但我们也必须应对一个紧迫挑战,即数字技术如何被滥用来限制人权和助长冲突。在国家行为体手中,在非国家行为体手中,以及在某些情况下,这些技术被用来切断获取信息的渠道,压制言论自由和传播虚假信息,从而加剧冲突,破坏我们负责维护的《联合国宪章》的基本价值观。

在中非共和国和马里,针对联合国维和特派团的虚假信息威胁到维和人员的安全和安保,削弱了特派团保护平民的能力。在埃塞俄比亚,自2020年11月以来,由于埃塞俄比亚国防军和提格雷地区部队之间爆发冲突,当局切断了提格雷地区的互联网接入。这种行动妨碍了平民获得保健服务的能力,对记录暴行和侵犯人权行为造成拖延,扰乱了金融服务,也限制了家人亲人之间通过网络进行联系。

坐在这个会议桌旁的国家也在利用技术以前所未有的方式骚扰、任意监控、审查和压制民间社会和独立媒体。这一点在俄罗斯选择对乌克兰发动的战争中表现得最为明显。俄罗斯政府继续关闭和限制互联网连接,降低连接速度,审查内容,在网上传播虚假信息,恐吓和逮捕报道其入侵真相的记者。这些做法是错误的,同时很普遍。正如安理会从尼亚博拉

女士那里听到的那样,据非政府组织Access Now估计,2021年,在34个国家中发生过182次互联网断网。更令人不安的是,我们经常听到有人声称以保护和平与安全的名义采取这种行动。没有什么比这更偏离事实了。

我们还继续看到,包括恐怖分子和暴力极端分子在内的非国家行为体利用在线通信平台进行招募、煽动和动员暴力。我们所有致力于解决和预防全世界冲突的人都必须尽自己的一份力量,确保技术成为积极变革的力量,而不是被滥用为侵犯人权、煽动仇恨和加剧冲突的工具。

正因为这个原因,美国正在与民间社会、私营部门和其他利益攸关方合作,推进这一全球努力。就我们而言,我们明确批评部分和完全关闭互联网、使用审查等手法来阻止行使网上言论自由的做法。继民主峰会之后,我们将继续与我们的自由在线联盟合作伙伴携手保护互联网自由,并确保整个数字生态系统尊重国际人权框架。

我们知道,监控工具和其他两用技术可能被滥用于威胁人权维护者和其他人。所以,我们才使用出口管制来追究那些开发、交易或使用间谍软件及其他技术来帮助进行此类恶意活动的公司的责任。

我们正在通过联合国和其他论坛努力倡导网络空间负责任的国家行为框架,该公约明确指出国际法适用于各国的网络活动,并制定了一套自愿准则来指导各国在和平时期的行为。我们还与世界各国站在一起,防范和应对恶意网络活动。在全球范围内,男女有别的网上骚扰和虐待,包括针对妇女领袖的造谣活动,正在破坏妇女平等参与和平与安全事务决策。

我们必须共同努力,在全球范围内打击散布错误信息和虚假信息的做法。联合国已经在发挥关键作用,制作透明和易于获取的信息,为一线记者发声。

我们还必须抓住机遇,释放技术促进和平与安全的潜在潜力。因此,上个月,一个由60个全球合作伙伴组成的团体发布了《未来互联网宣言》,以重振全球互联网的民主愿景。我们吁请所有致力于维护《宣言》



原则的相关当局和联合国会员国加入我们的行列。

为了有效维护21世纪的和平与安全, 我们需要应对21世纪的威胁, 动用21世纪的工具。现在是联合国负责任地利用数字技术的力量来应对我们最紧迫的挑战和促进全世界和平与安全的时候了。

我现在恢复行使安理会主席职能。

**霍查先生(阿尔巴尼亚)(以英语发言):** 我们感谢美国组织本次及时的会议, 讨论这一复杂而重要的议题。我们也感谢迪卡洛副秘书长一贯深刻的见解。

我们感到高兴的是, 民间社会在这次会议上被摆在了突出的位置——这样做有充分理由, 因为我们听到了他们提出的意见和建议的广度。因此, 我感谢尼亚博拉女士和德鲁特先生。

技术的快速发展改变了世界运作的方式, 影响着现代生活的方方面面。技术已经在我们的日常生活中根深蒂固, 以至于我们很难记起以前的世界是什么样子。

不可否认, 现代技术为多个领域带来了诸多好处。个人、国家、政府、工业、保健、金融系统、区域和国际组织以及维持和平特派团都利用了数字技术的快速发展。

它们帮助人们提高生产力, 帮助公司和实体变得比以往任何时候都更具创新性、灵活性和适应性。

我们欣然接受了设备和系统的互联互通, 这显然使我们的生活和工作变得更容易了, 但这不可避免地带来了一项成本, 那就是面对邪恶力量构成的各种威胁。“新技术、新威胁”的关联无需解释。

正如我们今天听到的那样, 各方对国家和非国家行为体邪恶活动带来的巨大风险已有共识。滥用信息和通信技术的行为对国际和平与安全有着直接影响, 因为它破坏全球社会的完整、安全、经济增长和稳定, 引起争端和冲突。

鉴于人们日益关切技术的两用性及其对维护国际和平与安全的影响, 非常重要, 安全理事会在评

估这种风险和影响方面应发挥主导作用。因此, 我非常欢迎举行今天的会议。

人工智能正在包括农业和医学在内的许多领域创造奇迹——拯救生命、增加粮食产量、改善能源状况和管理生产流程。但是, 如果使用不当, 特别是如果不遵守道德准则, 它可能导致严重侵犯人权, 例如对特定群体和社区实施不当监视。由于技术发展速度通常快于各国能够充分了解其影响的速度, 我们必须确保公平、平等、包容、负责任、透明度和追究责任等核心原则和价值观不受负面影响。

不幸的是, 技术因被国家或非国家行为体滥用而严重影响社会凝聚力以及当然还有国际和平与安全的可能性正在显著增加。一些国家不断试图通过滥用数字技术, 故意提供误导性信息, 歪曲事实, 干涉其他国家的民主进程, 传播仇恨, 怂恿歧视, 煽动暴力或冲突。同样, 我们关切地看到关闭互联网以及限制或剥夺使用互联网方面人权和自由的行为。各位通报者提供了具体的例子。正如秘书长关于数字合作路线图的报告(A/74/821)所概述的那样, 我们应加倍努力减轻这些行为可能造成的伤害, 并认真审视他的建议。

我要强调阿尔巴尼亚的坚定立场, 那就是支持建立一个全球性、开放、自由、稳定和安全的网络空间, 在这个网络空间中, 各国将充分运用国际法, 包括尊重人权和基本自由, 来支持社会、政治和经济发展。

我们深感关切的是, 最近数月, 恶意网络和数字活动有所增加。我们知道, 2022年2月24日, 就在对乌克兰实施无端和无理入侵前一小时, 俄罗斯蓄意攻击卫讯公司的卫星, 导致通信中断, 包括关键基础设施的通信中断。

据报源自俄罗斯的网络攻击还企图干涉乌克兰选举, 将乌克兰电网作为目标, 破坏乌克兰政府网站, 并在这些网站系统中传播恶意软件, 造成破坏性影响。我来自西巴尔干, 干涉和信息操纵运动正系统性地把我们地区作为目标, 以便蓄意引发政治动荡并损害我们地区各国加入欧洲-大西洋体系的愿望。我们不会允许这种行为。我们会予以抵制。

其他臭名昭著的例子是朝鲜民主主义人民共和国政权一再开展的邪恶活动。该政权正试图收集情报、实施网络攻击和获取非法收入。除其他外，这些收入用于资助其军事化和扩散，违反国际法和安全理事会决议。除这些例子之外，还有缅甸关闭互联网的行为，今天人们也提到了此类行为。我们呼吁停止此类活动，维护网络空间现有规范和基于规则的国际秩序。互联网不是而且也不应成为一种武器，而应仍然是一种公共产品。

我们欢迎政府专家组以及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报告。借助这些报告，会员国商定了一个实质性的联合国框架，其中包括现有的国际法、11项自愿的非约束性准则、建立信任措施、能力建设以及多利益攸关方群体的专门知识。

最后，我要指出这一点：纵观历史，新的挑战为合作开辟了新的机会。今天情况并无不同，即使目前挑战非常复杂，瞬息万变，并在冲突和危机感上升之际出现。但是，我们别无选择，只能首先进行切实的对话，通过负责任的行为开展合作，然后就技术发展如何影响个人、国家和社会，以及造成最大干扰的技术使用和应用，特别是对和平与安全构成直接威胁的技术使用和应用等问题，建立规范性框架。至于许多其他方面，我们应决定是分享巨大的惠益还是承受巨大的成本。

**德里维埃先生（法国）（以法语发言）：**我感谢迪卡洛女士、尼亚博拉女士和德鲁特先生所作的通报。

我愿着重谈三点。

首先，数字技术对于国际和平与安全而言是一个机会。维和行动一直率先作出这些努力。去年8月在印度倡议下通过的主席声明(S/PRST/2021/17)评估了这一局势。这些技术有助于保障维和人员的安全并提高维和行动的运作水平，特别是能够改善对平民的保护。它们正在彻底改变战略性的维和通信。因此，法国将继续支持所有这些创新。

技术也是动员和包容民间社会的工具。在苏丹，

联合国苏丹特派团进行了一次在线协商，让民间社会所有方面使自己的声音被听到，包括在各区域。通过促进信息流通，技术也有助于打击有罪不罚现象，乌克兰冲突中的媒体报道和公开来源情报就说明了这一点。

然而，对技术的恶意使用正在扩散，并可能对国际和平与安全构成威胁。这是我要谈的第二点。

网络威胁的发展也是如此，乌克兰冲突再次说明了这一点。法国和欧洲联盟以及若干伙伴谴责了俄罗斯在入侵乌克兰前一小时对一个卫星网络实施网络攻击，目的是为其入侵提供便利。国际法完全适用于网络空间。我们还谴责朝鲜开展邪恶网络活动，窃取敏感信息和加密货币，以支持其核导计划。我们还对加密货币越来越多地被用来资助恐怖主义感到关切。我们谴责针对人道主义行为体和非政府组织的越来越多的袭击。

数字技术也在促进信息战。我们谴责在中非共和国和马里开展的大肆造谣运动以及支持俄罗斯对乌克兰战争的大肆造谣运动。在马里，法国最近挫败了瓦格纳集团雇佣军操纵信息的企图。这个例子说明寻求模糊国家与非国家行为体之间界限的混合战略构成的威胁。

关闭互联网的行为侵犯人权。我们斥责持续干扰埃塞俄比亚北部电信的行为。这使得收集侵犯人权行为的证据变得困难，而这些行为决不能不受惩罚。在中东，互联网关闭被用来削弱抗议运动，一些维权人士在社交网络上受到监控和骚扰。

面对这些不断增多的威胁，各国政府必须通过合作和法律予以应对。这是我要谈的第三点。

联合国为此提供一个不可替代的框架。法国将继续为此作出贡献，包括确保安全理事会决议考虑到这些挑战。我们正与60个国家一道，推动在联合国内制定一个行动纲领，以提高各国执行网络空间商定标准的能力，并加强网络的应对能力。

**蒂鲁穆尔蒂先生（印度）（以英语发言）：**我欢迎

美国倡议组织今天的重要通报会。我感谢副秘书长罗斯玛丽·迪卡洛女士和其他通报人，即尼亚博拉女士和德鲁埃先生的宝贵见解。

数字技术应用的增加加快了经济发展，改善了提供给公民的服务，提高了社会意识，使信息和知识直接掌握在个人手中。它们使治理更加包容、以公民为中心和透明。这个数字时代的大多数活动——政治、社会、经济、人道和发展活动——现在都不可避免地在线空间进行或与之相连。然而，鉴于数字技术有两用性，也容易被国家和非国家行为体用于有害目的，它们也可能对国际和平与安全产生负面影响。

几十年来，冲突的性质及其潜在工具发生了巨大变化。虽然国家间冲突仍在继续，但我们看到包括恐怖主义团体在内的非国家行为体构成越来越大的威胁。同样，战争和冲突的场所也扩大了。除了领土冲突之外，世界正面临着新的海洋和空间冲突——我所说的空间是指外层空间和网络空间。在这些冲突中，技术已经成为共同的潜在最低标准，也是改变规则的力量。因此，需要重新设定我们在国家和国际安全方面的传统方法。

我谨提出以下五个问题供安全理事会审议。首先，有必要处理恐怖主义团体滥用数字技术传播恐怖主义思想、激进化、煽动暴力和招募下一代恐怖主义人员的问题，它们利用了青年越来越多的上网机会。恐怖组织正利用在线工具建立网络、招募新成员、采购武器和获得后勤支持。这些团体使用的数字通信方法是有组织且复杂的。他们已变得善于利用游戏聊天室、暗网和其他限制访问的网站以及不受监管的在线空间来扩大宣传和煽动暴力。此前有过恐怖分子在各大平台上直播袭击以尽可能扩大宣传和影响的例子。网络空间的广泛延伸使恐怖主义团体能够利用我们这样的多元民主社会的开放性，助长社会分裂和教派仇恨，支持反民主运动和旨在破坏政府和国家机构稳定的激进思想。

恐怖分子能够通过数字平台联系、交流和分享信息，这更加凸显了越来越有必要监管这类线上煽动内

容。同样需要努力应对依法惩处这些罪行的实施者的法律挑战，这尤其是因为他们是从远距离参与恐怖活动的。虽然我们习惯于将恐怖主义视为犯罪者的直接人身攻击，但在数字领域，通过仇恨内容和激进思想煽动恐怖行为的犯罪者与实际实施恐怖行为的人员可能相隔甚远。煽动者应对这种恐怖行为负同等责任。他们的罪责不会轻于那些犯下恐怖行为的人。我们在考虑网络领域的恐怖主义时，这一点至关重要。

新的金融技术的出现，如新的支付方式、虚拟货币和在线筹资方式，包括直接捐赠、非同质化代币和众筹平台，以及它们带来的便捷性、匿名性和处理难度，使恐怖主义实体能够在逃避监测和执法单位的同时收集、转移资金。预付电话卡、线上支付服务和虚拟货币等新支付方式使恐怖组织能够将它们兑换成真金白银和其他金属，最近还用于移动电话支付，并资助恐怖活动。预付卡经常被当成现金替代品。使用比特币资助恐怖活动也是众所周知的。此外，恐怖分子出于各种恐怖主义目的滥用人工智能和3D打印，其影响遍及全球，这也需要我们立即关注。

会员国需要更具战略性地全面应对和处理恐怖分子利用数字技术的影响，这种需求从未像现在这样迫切。在这方面，我高兴地通知安全理事会，印度已提议尽快在印度举行一次安理会反恐怖主义委员会特别会议，专门关注这一问题，并试图提出前进的方向。

第二，一些国家正利用它们在数字领域的专门知识来实现其政治和安全相关目标，并执迷于当代形式的跨界恐怖主义，攻击包括卫生和能源设施在内的重要国家基础设施，并通过在网上空间宣扬激进主义来破坏社会和谐。开放的社会尤其易受这种威胁和虚假信息攻击。新兴数字技术——例如使用机器学习和大数据——有可能增强此类行为的致命性，从而对国际和平与安全构成重大威胁。在应对这些威胁时，国际社会不能采取选择性做法，需要避免双重标准。

第三，数字领域相互关联的性质要求人们不能孤立解决源自这一领域的复杂问题和威胁。有必要采取基于规则的协作方法，努力确保数字领域开放、稳定、



安全。促进公平获得数字技术及其惠益也应该成为这一方法的重要组成部分。日益扩大的数字鸿沟、数字性别鸿沟和数字知识差距在网络领域创造了一个不可持续的环境。在2019冠状病毒病后的时代，日益增长的数字依赖加剧了风险，暴露了数字不平等的裂痕。必须通过能力建设和技术转让来弥合这些差距。

第四，联合国维持和平特派团需要配备最新的数字技术，以对抗武装团体使用的技术。保护保护者应该和保护平民一样是我们的首要任务。我们在这方面采取了行动，在2021年8月担任安理会主席期间，与联合国合作推出了Unite Aware平台。这一技术方案为维和人员提供实时威胁评估，需要在所有联合国维和特派团中推广。我感谢法国代表提到2021年我国担任主席期间通过的关于技术与维和的主席声明（S/PRST/2021/17）。

第五，维护网络空间的国际和平与安全也有赖于各国就滥用数字技术实施犯罪问题交流信息。这种合作需要是有效、实时的，以便遏制、破坏和减轻这种滥用。因此，成立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是朝正确方向迈出的一步。

最后，我要重申，国际社会需要利用数字技术造福全人类，而不仅仅是少数人。我们的首要目标应该是利用这些技术来促进发展和繁荣以及增强所有人的权能，并促进国际和平与安全。印度已准备好作出这一共同努力，提供专业知识并分享经验。

**张军先生（中国）：**科学技术的迅猛发展带来新机遇和新挑战。去年5月，中国同肯尼亚、墨西哥、阿联酋等共同举办阿里亚模式会议，就新兴科技对国际和平与安全的影响深入交换意见。中方欢迎有机会在安理会继续关注技术与安全问题。为更好地开发和利用科学技术，造福全人类，中方有如下主张：

第一，积极鼓励科技创新。创新是引领发展的第一动力。历史上每一次科技和产业革命都深刻改变人类生产生活方式，极大促进人类进步和福祉。

当今世界面临前所未有的复杂挑战，数字技术、

人工智能、生物技术等科技快速发展，在疫情防控、应对气候变化、维护粮食安全、能源安全等领域发挥着重要的作用。无论是为世界经济增长提供新的动力，还是为解决人类重大难题寻找新的途径和方法，都离不开科技创新。

世界经济高度依存，全球产业链、供应链深度交融。各国要以开放思维和举措看待和促进国际科技交流合作，共同打造开放、公平、公正、非歧视的科技发展环境，积极开展联合研发，共同推动科技进步。

第二，让科技成果造福人类。技术无国界，是人类共同的财富。科技成果不应成为埋在山洞里的宝藏。当前，发达国家和发展中国家间的技术鸿沟、特别是数字鸿沟不断拉大，正在加剧新的不平等。

要积极利用联合国等多边平台支持发展中国家科技能力建设，加大技术转让，加快成果转化，让发展中国家共享科技红利，通过缩小数字鸿沟跨越发展鸿沟，加快落实2030年可持续发展议程。

要支持发展中国家运用现代科技产品和大数据方法，提升社会治理水平，有效预防和打击犯罪。

安理会在维和与建设和平工作中，也要积极运用新科技手段，加强信息收集、风险预警、应急响应、紧急救援等能力。

第三，合作管控技术风险。技术发展可能成为风险的源头，带来规则冲突、社会风险和伦理挑战。国际社会要秉持“科技向善”理念，发挥联合国主渠道作用，积极开展对话交流合作，坚持多边参与、多方参与，共同管控技术发展的风险，制定和完善普遍接受的规则规范。

要遏制信息技术滥用，反对网络监听和网络攻击，反对网络空间军备竞赛。要防止恐怖分子利用互联网招募成员、获取资金和策划实施恐怖袭击，防止互联网成为仇恨言论、种族主义、色情暴力的温床。各国政府要依法加强监管，规范技术应用，更好维护公共利益。技术平台企业和互联网公司要加强规范自律，履行社会责任。

第四,反对技术问题政治化。科学世界不是零和博弈的战场,技术创新不应只有一个冠军。但令人关切的是,一段时间以来,个别国家政府将科技问题政治化,泛化国家安全概念,滥用国家力量,变本加厉地打压别国高科技企业。他们为维护自身科技垄断地位,组成排他性的“小圈子”,搞所谓的“战略”或“框架”,对其他国家进行技术封锁,推行科技霸凌主义,干扰阻碍其他国家经贸科技合作。

这种带有陈旧冷战思维的做法违背国际合作精神和时代潮流,损害世界各国的共同利益,注定不会成功。我们敦促有关国家政府秉持理性开放心态,正确看待科技发展和国际科技合作,停止对他国科技企业的无理打压和限制。

面对全球挑战,团结合作方是正途。中方敦促有关国家停止在世界各地包括亚太制造分裂、搞地缘对抗,停止以意识形态划线、胁迫其他国家选边站队,停止制造经济科技脱钩、破坏全球产业链稳定和经济复苏。

中国高度重视科技创新,始终采取负责任态度防范技术风险,为推动各国深化共识、开展合作做出积极努力。中国于2020年提出《全球数据安全倡议》,呼吁维护全球供应链开放、安全和稳定,反对利用信息技术破坏关键基础设施、从事大规模监控,主张尊重各国主权、司法管辖权和对数据的管理权等。这项倡议为制定数字安全国际规则提供蓝本,期待各国政府、国际组织和多利益攸关方共同参与。

面对人工智能引发的巨大变革,中方基于联合国多年讨论的成果,于去年底提出《关于规范人工智能军事应用的立场文件》,为国际社会探讨应对人工智能军事应用在战略安全、治理规则、伦理道德等方面的影响提供可行的框架。

去年7月,20多个国家的科学家达成《科学家生物安全行为准则天津指南》,倡导负责任的生物科研,这反映了国际科学界的共同愿望。中方欢迎各国和相关利益攸关方自愿采纳并进一步推广天津指南,以利于防止生物科技滥用误用,降低生物安全风险,促进

生物科学造福人类。

为了和平目的利用科技并开展国际合作,是国际法赋予各国不可剥夺的权利。第76届联大通过中国和其他26个国家一道提出的“在国际安全领域促进和平利用国际合作”决议,敦促各国在履行防扩散国际义务的同时,取消对发展中国家和平利用科技权利的不合理限制。

中方欢迎在联大框架下持续开展包容对话,增进互信、凝聚共识,确保发展中国家充分享有和平利用科技的权利,更好实现可持续发展目标,更好维护国际和平与安全。

**基博伊诺先生(肯尼亚)(以英语发言):**我感谢迪卡洛副秘书长;我国同胞尼亚博拉女士;和德鲁埃特先生就今天审议的议题发表的见解和提出的建议。

当我们思考数字技术在这十年中所发挥的非凡作用、以及数字革命对我们时代和平与安全的空前影响,并鉴于数字技术的这种普遍、重要、基本不受政府管制的特性,显而易见的是,必须有一个由讨论者和行为体组成的群体,包括安全理事会,来探讨如何确保数字创新与解决国家和非国家行为体在和平与安全相关事项中恶意使用数字创新问题这两者之间的微妙平衡。

肯尼亚已在确保互联网无障碍接入方面取得重大进展,国家及其公民受到最大程度的保护,不会遭受数字领域破坏性和意外事件及威胁的影响。但我们认识到,网络安全不是也不可能是一个单独国家的努力。的确,多边体系寻求国际和平与安全的常态行为现在也必须在网络领域进行。

在这方面,我要强调五个要点供大家考虑。首先,必须认识到,联合国应支持各国应对数字革命对其公民和国家稳定的影响,包括滥用人工智能、大数据、社交媒体和其他数字前沿等。安全理事会有责任确保联合国具有能力和专门知识来发挥这一作用。

第二,数字技术与和平之间的关联,尤其是在政

治过渡时期。选举进程是一种民主承诺，但在数字平台上，选举进程往往面临更多的安全缺陷，对国家民众凝聚力和危机管理产生影响。2021年10月28日，在担任安全理事会主席期间，肯尼亚召开了一次关于应对和打击仇恨言论以及防止在社交媒体上煽动歧视、敌意和暴力的阿里亚模式会议。显然，在平衡言论自由与仇恨言论、平衡民主追责与保护私人专有信息方面，决策者经常面临两难境地。我们主张更多地关注并投入支持各国政府处理网络安全与国家选举安全之间的关联问题，特别是在冲突局势中。

第三，关于私营部门和政策监管者之间的伙伴关系，我刚才提到的阿里亚模式会议将来自脸书、推特、抖音和谷歌等主要技术公司以及民间社会的代表汇集在一起，他们表明建立这种伙伴关系是可能的。加强技术公司、政策监管者和联合国之间的伙伴关系，将使之有可能确立有效的机制和标准，以确保在网络空间的负责任行为，这些机制和标准基于涉及公共产品的原则，在不同群体之间和不同议题之间建立和平的桥梁。

第四，数字技术和恐怖主义之间的关联。新兴技术无处不在、可编程和数据驱动的性质尽管有益，但为武装团体和恐怖分子滥用这些技术打开了大门。他们利用简化的用户界面系统进行招募、鼓动激进化、调动资源，并计划和实施恐怖行为。必须确保各国有能力减缓网络恐怖主义威胁，提高调查技能，协作降低网络激进化和非法资金流动的速度，并识别和删除网络极端主义内容。

第五，包容性和保护参与。我们认为，政府对互联网无障碍接入的责任还包括保护数字平台访问者，包括社交媒体。具体而言，参与和平与安全进程的妇女的安全仍然至关重要。因此，各国必须加大力度，针对网络攻击实施者、恐吓行为、私营媒体发布信息、以及对参与和平议程的妇女实施人身暴力的行为进行追责和起诉。作为妇女与和平与安全议程的保护和参与支柱的一部分，安全理事会也应当采取具体步骤，特别是增加对在安理会通报情况的妇女进行各种形式网络恐吓的代价。

戈麦斯·罗夫莱多·韦尔杜兹科先生(墨西哥)(以西班牙语发言)：主席女士，首先，我们要感谢你召开本次会议，讨论一个几乎具有无限影响的议题，这要求我们除其他外，思考如何调整联合国的工作，以应对使用数字技术给维护国际和平与安全带来的各种挑战。我们也感谢今天上午的各位通报者——副秘书长迪卡洛、Advox项目主任以及麦吉尔大学的德鲁特教授——所作的出色分析以及所提出的建议。

如果正面看待问题，我们就要从这样一个原则出发，即数字技术的使用首先必须用于捍卫人权与民主。这两个方面密不可分。在这方面，墨西哥重申其多年来一直坚持的承诺，即致力于建设一个自由、开放、稳定与安全的网络空间，在这个空间里，国际法，包括国际人权法、国际人道法、国际刑法以及其他确立隐私权等的法律先例完全适用。我们回顾，通过从国际安全角度促进网络空间负责任国家行为政府专家组的报告、以及信息和通信技术安全和使用问题不限成员名额工作组的报告，我们在政府间一级，特别是在网络安全领域已经达成并正在执行各项相关协议。同样，我们应当回顾正在展开的其他进程，包括拟订一项关于打击为犯罪目的使用信息和通信技术的全面国际公约特设委员会。

正如今天早些时候在通报中提到的那样，必须寻求应对目前维和面临的创新办法，特别是通过加强和平行动与特别政治任务中的数字技术能力。使用这项技术极具建设性意义，可推动改进对新出现威胁的预警和判断，防止人道主义危机和侵犯人权行为，并加强保护和支持平民与民用基础设施的必要措施，包括打击武器贩运和扫雷活动。

新技术在医疗支助等领域显示出特别的前景，包括提供及时、常规和紧急的心理健康和社会心理照护服务。受人道主义危机影响的维和人员和平民都可以受益于远程医疗的灵活性和可及性。此外，我们已经看到，使用可再生能源技术可以加强联合国人员的安全和保障，并提高特派团的效力和可持续性。面对早些时候所强调日益严重的错误信息环境，使用社交网络是加强维和特派团与其行动所在社区两者之间关



系的关键。正因如此，第2589（2021）号决议的规定和主席声明S/PRST/2021/17至关重要，安全理事会在其中承认，技术可帮助维持和平特派团更好地了解其运作环境，这些规定应使我们能够更好地收集、分析和共享信息。

同样，我们注意到秘书长关于新技术和信息的《联合国维持和平行动数字化转型战略》以及对“以行动促维和+”倡议的跟进。该《战略》的执行要求加大联合国系统同实地利益攸关方之间的协调，还需要与区域组织、私营部门、民间社会当然还有学术界合作。

在最近的联合国维持和平部长级会议上，墨西哥赞同大韩民国提出的关于维和技术与医务能力建设的倡议。该倡议有三个目标——最大限度地利用可用的技术，以便更好地了解局势和提供预警；应对冲突局势下的虚假信息，改进网络安全方面的情报，以及促进数据和信息分析领域的能力建设。

最后，墨西哥在大会表示赞同的第75/316号决议强调了快速的技术变化对于实现《2030年可持续发展议程》进而对国际和平与稳定将产生的影响。我们强调《数字合作路线图》和《我们的共同议程》（A/75/982）报告所载信息的重要性。

阿吉曼先生（加纳）（以英语发言）：首先，我谨感谢美国召集今天关于在维护国际和平与安全工作中使用数字技术的通报会。

我也感谢迪卡洛副秘书长富于见地的通报，同时感谢全球声音数字权利项目Advox项目主任Nanjala Nyabola和麦吉尔大学国际和平与安全研究中心兼职教授Dirk Druet发表更多见解。

加纳承认数字技术在全球无孔不入的特点，并赞同这样的观点，即：这些技术可在维护国际和平方面发挥重要作用，因此必须利用它们来增进我们的集体安全。我们认为，在认识到国家主权与领土完整要求的同时，克服地域障碍的数字技术可被用来提高态势感知，从而更好地实现预防外交的目标，启动预警，识别新兴的威胁，并且随着各种不同的意见和立场被调

动起来，形成一个旨在强化和平目标的建设性的连贯整体，从而弥合社会分歧。

在处理冲突方面，我们看到，数字技术也可在分析风险、缩短保护平民和民用基础设施所需时间等方面带来好处，它还增加力度，更好地执行和平支助行动的任务，强化军警人员和其他工作人员的安保。数字技术还可有力支持建设和平努力，重建遭战争摧残的社会。

加纳认为，数字技术可在加大维护国际和平与安全工作的力度方面带来不可估量的裨益，这种利用已有的现代工具实现世界和平的更有力的补充性做法以规范性的框架为支撑，只有对此形成共识，这些裨益才能更好地累积。实际上，我们意识到，尽管数字技术是良性的，但是如果不负责任地使用，它们也可加剧全球的不安全。假如关系紧张的脆弱社会继续认为，外部力量正在左右民众的意愿，以使其接受可能被这些社会视为异类的价值观，这些技术也可加深不信任。

我们还注意到，在某些情况下，国家和非国家行为体恶意使用数字技术，为民众提供错误信息并进行操纵，威胁和骚扰活动分子和记者，并以一种颠覆国家统一和团结的方式助长歧视。这些技术被用来招募人员加入恐怖团体，对民众进行激进化，组织恐怖袭击，以及为恐怖活动提供资金，令人高度关切。

数字技术在加强现有的维护国际和平与安全的工具方面潜力巨大，但是我们注意到它的消极后果，有鉴于此，我们愿强调几点补充意见。正如先前已指出的那样，利用数字技术来维护国际和平与安全必须本着趋同的出发点，并且基于尊重国家主权和倡导普遍价值观的原则。在这方面，我们认为，联合国在加大数字技术对全球和平的积极影响方面要发挥不可或缺的作用。例如，秘书长的《维持和平行动数字化转型战略》旨在利用数字技术提供的机会，在该战略所做承诺的基础上更进一步，将使特派团能够适应不断变化的冲突动态，并且利用效率的提高。此外，政治和建设和平事务部在冠状病毒病大流行期间使用数

字技术开展调解工作方面吸取的经验教训可提供一条可接受的道路,为了和平,构建与广大民众开展此类协作的持久框架。

其次,各国政府改进其网络安全空间的能力应当被摆在搭建使用数字技术的有力框架的核心位置。根据非洲联盟的《非洲数字化转型战略2020-2030》,恐怖分子和极端团体恶意使用数字技术和网络战的趋势要求弱势国家、比如存在脆弱性的一些非洲国家获取所需的支持,以提高其数字能力。这些能力建设努力应包括收集、处理、使用以及分析新技术及其对安全的影响。在这方面,反恐怖主义委员会执行局发挥的支持作用值得称道,我们欢迎更多的此类努力。

第三,国家也要发挥关键作用,采取防止滥用网络空间的政策,其要素包括:鼓励对关键的国家基础设施进行投入,倡导负责任的媒体内容,为早期发现、调查以及起诉违法者提供便利等。国家应兑现其对《联合国宪章》的承诺,遵守国际人权法,确保对个人数据的收集、存储、处理、使用、转让以及披露做到维护和保护个人隐私。此外,我们欢迎那些鼓励公司根据《联合国工商企业与人权指导原则》遵守国际人权法和商业标准的措施。

第四,我们认识到,区域安排通过预警机制在防止冲突和冲突后建设和平方面卓有成效,因此大力敦促加强全球多边系统与区域机构之间的数字技术伙伴关系。我们鼓励为落实现有的条约、如《布达佩斯公约》和非洲联盟《关于网络安全和个人数据保护公约》暨《马拉博公约》提供支持,同时我们认为,各种预警机制、如中部非洲国家经济共同体和非洲联盟的预警机制可通过有力的全球支持得到进一步加强。

此外,支持区域性的情报和信息共享平台可更好地早期发现恐怖网络的扩张图谋,包括在西非的扩张及其线上活动。此外,必须继续采取行动并加大行动力度,切断恐怖主义的资金来源,包括在网络空间经济中,因为加密货币已成为恐怖活动筹资所选用的一种介质。尽管西非反洗钱政府间行动小组与西非各国金融情报中心之间的合作产生了重大成果,但其行动

仍需要深化。

在结束发言之前,我要提及,加纳致力于通过采取行动加强国内信息和通信技术生态系统,促进将技术用于和平目的。除已形成制度的旨在提高全社会对网络威胁的认识的国家网络安全意识月之外,国家通信管理局、中央银行和国家信息技术机构等关键机构的部门计算机应急小组已投入运作,增强了网络生态系统在线上服务、金融部门和政府业务各个领域的抵御能力。因此,我们主张在发展和平与安全关系中的复原力时采取全社会办法,包括与私营部门、民间社会组织和技术巨头建立伙伴关系,必须让它们发挥越来越大的作用,为公共利益服务。此外,妇女和青年是变革的关键力量,对于增强技术对全球安全的积极影响仍然至关重要。

加纳致力于加强所有可用工具的集体目标,认为多边和区域倡议能够有效利用技术实现全球和平与安全的目标。

**涅边贾先生(俄罗斯联邦)(以俄语发言):**我们愿感谢我们的通报人所作的通报。

数字技术已经改变了世界,并已成为经济、政治和社会进程的一个组成部分。人们希望它们将成为经济和社会进步的引擎,让通信变得简单,帮助人类过渡到新的数字化发展阶段。

在2019冠状病毒病疫情期间,多亏了信息和通信技术(信通技术),工作和被隔离隔离的世界的团结才得以保留。政府提供的公共服务,包括医院、银行和整个金融部门、学校以及其他对社会至关重要的机构的工作,几乎完全与信通技术联系在一起。毫不夸张地说,人类今天比历史上任何时候都更加依赖信息和通信技术。

但是,信通技术将成为明确的向善力量的希望并没有实现。罪魁祸首不是技术,而是技术被用来实现地缘政治目标和推行霸权的事实。不仅在物质环境中如此,在在线环境中也是如此。

近年来,对信息的操纵已达到了危险的程度。一

大批来自非政府组织的伪调查人员已经出现，他们在西方政府的授意下，正在炮制有偏见的所谓调查，事实上，这些调查正在制造和传播大量来自公开来源的虚假和未经证实的信息，目的是玷污那些让西方认为是麻烦的国家。一个臭名昭著的例子是白头盔和贝灵猫网。他们因在叙利亚化学武器问题、马来西亚航空公司MH-17航班事件以及许多其他备受瞩目的问题上大肆捏造事实，为西方宣传服务而闻名。可以说，专家们已经多次当场抓住他们，指出他们结论中的不一致之处，这些结论与专业、独立的调查性新闻报道毫不相干，是在违反所有最基本原则的情况下得出的。

我们对一个新趋势深感不安：现在正在进行一场信息战，不仅其方式完全脱离现实，而且以歪曲现实和完全取代现实为目标。真相正被源源不断的信息和充满意识形态色彩的垃圾邮件推到一边，不让受众有丝毫机会获得客观信息。

一个令人震惊的例子是西方媒体在其政府的指示下发布的关于布恰平民死亡的信息，在这种情况下，俄罗斯军方受到指责。所有的客观事实和证据都被掩盖起来，而彻头彻尾的谎言却被传播开来。在事实的压力下，甚至西方媒体最终也被迫承认，布恰的许多和平居民并非像乌克兰所称中弹死亡，而是死于乌克兰武装部队轰炸该市时使用的废弃炮弹。现在，他们正在使用新的“假消息”转移人们对乌克兰武装部队明显的挑衅责任的关注。同样，他们现在也对克拉马托尔斯克袭击保持沉默，此前的调查揭示出证据，清楚表明乌克兰武装部队参与了这一袭击。

最近几个月，西方真理部，或者更准确地说是谎言部集体的工作达到了登峰造极的地步。针对俄罗斯发动了一场范围和力度前所未有的造谣和操纵公众舆论运动。本来就不以客观性著称的西方媒体，最终变成了赤裸裸的国家宣传的喉舌和假新闻工厂。

垄断了社交网络和视频托管领域的信通技术巨头们的表现也好不到哪里去。数字平台终于扔掉了面具，不再试图隐藏自己的政治偏见。他们屏蔽了任何

内容与西方精英所支配的议程不一致的账户。Meta公司明确允许在其平台上发布针对俄罗斯人和讲俄语者的仇恨言论和暴力呼吁。

自称“民主社会”的国家实际上正在打造真正的网络极权主义。他们想要创造一个世界，在这个世界里，他们——只有他们——将完全控制信息流，决定什么是真实的，什么是观众需要读到和看到的。任何不同观点都会立即被打上虚假信息 and 宣传的烙印，令人不快的事实则被抛在一边。俄罗斯电视频道被关闭，俄罗斯记者被驱逐，俄罗斯网站被屏蔽。这就是所谓的获取信息的自由吗？我们希望，这是今天会议的组织者所说的以确保国家安全为借口滥用对使用互联网资源的限制。

恐俄信息攻击的发起者针对各种活动领域，包括与政治完全无关的领域，如教育、文化和体育。这公然违反了不允许以族裔为由进行歧视的基本原则。除了针对人们思想的信息攻击之外，还策划了一场运动，通过组织计算机攻击来破坏信通技术基础设施本身。在基辅，最近宣布建立了网络军队，并公开肯定对俄罗斯和白俄罗斯目标的这种网络攻击。此外，基辅政权的西方支持者不仅没有试图阻止，还故意培养黑客大军，完全不考虑后果。如我们所知，相关任务最近由北约推进，作为乌克兰武装部队参加的“锁定盾牌”网络安全演习的一部分。

今年4月，华盛顿宣布悬赏1000万美元，奖励任何能够证明俄罗斯情报机构涉嫌参与对美国的网络攻击的人。我们一再呼吁通过主管机构处理这些问题，但这些呼吁都被忽视了。

西方各国政府蓄意让黑客团体和普通用户参与发动网络攻击。在公共领域公布计算机攻击的工具和关于如何策划这种攻击的详细说明，并在社交网络上进行大肆煽动，鼓励对俄罗斯基础设施进行黑客攻击。

在此背景下，我们对以下情况并不感到惊讶：出生于乌克兰西部、以领导关于洗白乌克兰新纳粹主义的宣传运动和传播有关根本不存在的俄罗斯门信息



而闻名的尼娜·扬科维奇获得任命，自今年4月27日起领导美国国土安全部的所谓虚假信息治理委员会。最近变得很清楚的是，她曾直接接受特朗普的竞选对手希拉里·克林顿的指示。甚至在美国本国，这种公然的玩世不恭行为也引发了丑闻。扬科维奇不得不辞职，该项目也暂时中止了。然而，我们毫不怀疑，它将以某种方式恢复，因为我们的西方同事除了促进假消息和谣言外，已经几乎没有什么外交手段可用了。

在西方向乌克兰大量提供常规武器的同时，有人还受控制地分发网络武器及其使用技术。大量的人员正在获得实用技能。据泽连斯基说，他的所谓网络大军中有30多万作战人员。

一支无法控制的网络军队正在创建中。它在有关会员国驻乌克兰人员指挥下发展技能，同时攻击俄罗斯。此后，它不会停步。它不是正规军。专家们非常清楚，追踪黑客活动、查明其来源并加以抑制是多么困难。有关会员国动员的黑客将遍布世界各地，会产生各种后果，包括对西方国家的民众构成威胁。

西方进行的数字空间军事化大大增加了发生直接军事冲突的可能性，尤其因为基辅政权正利用西方技术在信息空间大肆进行挑衅。然而，这些挑衅的后果可能更加可怕。对关键基础设施进行的计算机攻击会造成真实的大规模人员伤亡，更不用说更不用说伪旗攻击情况中错误识别肇事者身份的风险了。与在真实生活相比，在虚拟空间组织伪旗攻击要容易得多。在这种情况下，意外升级和相互进行网络攻击的风险将成倍增加。

基辅政权的鲁莽行动会导致网络空间发生全面对抗，会把其他国家卷入进来。北约已将第5条规定的集体自卫权延伸至信息空间。这种升级的责任将完全落在西方国家身上，因为它们正在鼓动基辅领导层鲁莽行事。

面对这种威胁，我们肯定会反击任何企图危害俄罗斯信息安全的行为。但是，我再次敦促安理会成员思考把世界拖入网络空间对抗的危险。这一做法的危险性不亚于使用大规模毁灭性武器。二十多年来，我

们一直在试图防止这种情况发生。

我要回顾指出，俄罗斯早在1998年就率先在联合国提出国际信息安全问题，并将这个问题永久列入联合国议程。我们坚持认为，联合国应建立谈判平台，首先是专家平台，然后是向所有会员国开放的平台。在其中的每一个阶段，我们都不得不克服来自我们西方同事的最强烈的抵制，他们声称没有联合国他们也能管控这个问题。世人清楚地知道，没有联合国，他们是怎么做的。

我们正在寻求一项国际承诺，那就是，所有国家都应承诺不把信通技术用于军事目的。我们要求信息空间非军事化。这些年来，我们一直在提出具体的国际文书草案——确保国际信息安全的普遍概念——并以上海合作组织名义提出这一领域负责任行为守则草案。

我们的西方同事呢？这些年来，他们一直在公开建设攻击性网络潜力，并制定这一潜力的使用规则。回顾一下邪恶的《适用于网络战的国际法塔林手册》就足够了，该手册详细规定如何以所谓的人道方式进行网络战。

因此，这些年来，我们当中谁一直在为网络战做准备——是俄罗斯还是西方国家？俄罗斯呼吁禁止把信通技术用于政治和军事目的，并愿承担相应义务，而西方国家却一再拒绝所有这些倡议，以便能够在信息空间为所欲为。

绝不能允许数字领域成为地缘政治对抗的领域。这是一个关乎人类生存的问题。现在比以往任何时候都更有必要进行负责任的讨论，旨在制定切实可行的解决办法。不管政治气候如何，我们都有责任支持这一讨论。我们呼吁在大会主导的专门论坛——不限成员名额工作组——就确保国际信息安全的所有方面进行非政治化的讨论。我们相信，我们今天的会议并未以任何方式取代该工作组的活动。

**努塞贝赫夫人**（阿拉伯联合酋长国）（以英语发言）：阿拉伯联合酋长国要感谢美国召开本次会议，讨论一个越来越重要的问题。在阿拉伯联合酋长国

看来,安全理事会应共同超越具体冲突,完全以就事论事的态度处理这个问题。我们也感谢迪卡洛副秘书长、尼亚博拉女士和德鲁埃特先生今天所作的确实很有见地的通报。

数字技术正以令人眩晕的速度发展。让我们回想1989年的情况,那一年建立了万维网。到下一个十年结束时,拉里·佩奇和谢尔盖·布林发明了谷歌。当时我们几乎不知道,这个来自加利福尼亚一个车库的新想法将永远改变我们的生活。快进十年,谷歌出现在了大家的智能手机中,它是工作和生活的不可或缺的一部分,带来了巨大的进步和变化。

现在,让我们想象一下,正如我们听到的那样,今天,在我们注视下,技术的邪恶一面正在以同样的曲速发生。例如,数字技术的不断进步正在使无人机等装置能够做的事情成倍增加。在不久的将来,恐怖团体使用的无人机群会利用人工智能促成的面部识别技术和其他功能进行跨境袭击,而人们却无法认定这些袭击是一个国家还是一个非国家团体实施的。各国,包括在座各位所代表的国家,未来将如何根据国际人道法合法应对这种袭击?

为防止未来出现这种反乌托邦局面,我们现在需要在联合国、安全理事会和其他论坛采取紧急行动。显然,我们不应期望政治和伦理辩论会产生切实的答案。这些辩论已经持续二十多年,一直未跟上这些技术发展的步伐,而现在,这些技术无处不在,有可能被人以极具毁灭性的方式使用。

毫无疑问,数字技术带来了相当多的风险和挑战,特别是会让恐怖团体的力量倍增。但是,正如我们还听到的那样,这并不是故事的全部。

正如我们今天听到的那样,数字技术也可以促进和平。例如,依靠最新技术和数据的自然灾害预警系统,使我们能够预测极端天气事件,例如干旱、飓风和洪涝,并相应地预先布置援助。在索马里连续开展的预测行动方案帮助社区处理了严重的缺水和干旱问题。由于这种技术,人道主义事务协调厅和其他伙伴得以缓解生计损失和粮食消费下降的情况,确保人

们能够获得水,并让儿童继续上学,学校是儿童应该呆的地方。正确的信息能够帮助国际社会更好地应对气候安全威胁。它拯救生命,而且有助于防止脆弱性成为产生不稳定局势的触发因素。

当我们考虑数字技术的双重性质时,安理会不应该止于赞叹这一问题,而要讨论安理会如何利用技术创新促进可持续和平与安全的具体方式。今天,阿拉伯联合酋长国想谈五个具体问题。

首先,正如其他人提到的那样,绝不能允许达伊沙、基地组织和许多其他恐怖主义和极端主义团体利用互联网宣传其纲领,操纵社交媒体及其数十亿用户。科技公司越来越多地投资于基于人工智能和人力审核团队的检测工具,从其平台上删除此类内容。然而,一段时间以来,各国政府已经清楚地看到,采用惯常的做法是不够的,因为恐怖分子和极端分子继续在网上进行激进化宣传并招募人员。这个问题绝不仅限于发展中国家。最近欧洲和美国大部分地区发生的多起针对宗教和族裔少数群体的高调仇恨犯罪的肇事者就是通过这些在线平台成为激进分子的,达伊沙在世界各地招募到许多成员也是采用了这种方式。因此,尽管我们看到,近年来在加强监管和立法框架以保护用户免受恐怖主义和极端主义内容影响方面取得了进展,但我们显然需要加大这方面的力度,因为国际规范框架没有跟上。这不仅是科技公司的责任,也是政府的责任。

第二,我们必须解决使用社交媒体平台在网上散布虚假信息和错误信息运动的有害影响,包括对和平行动和人道主义活动的影响。这些行动和活动应该受到保护。我们已经看到,为了保护平民,维和人员和人道主义救济人员已经身处险境,却因针对他们的错误信息和虚假信息的传播而面临更大的危险。现在,需要在多个层面采取有效应对措施,打击虚假信息,包括通过规章制度、事实核查、信息标签和媒体扫盲运动,让私营部门参与进来。通报者今天提出的建议,即联合国应该扩大这方面的能力,应该受到欢迎。

第三,我们应该利用数字技术来加强保护平民,

使他们免受伤害。例如，在现实世界中，医疗行为体和某些人道主义行为体使用红十字或红新月标志，表明他们应受到国际人道主义法的具体保护。这些行为体的数字主干网受到攻击，正面临新的数字威胁，我们应该开始考虑是否可能有一个数字标志来明确表明，医疗和人道主义行为体，无论是在线上还是线下，都绝不能成为攻击目标。这一标志不仅应该强化这样一种理念，即这些网络不仅应该得到保护，而且应该对任何违法行为追究责任，国际法适用于这一领域。

第四，数字创新正在对物理世界产生影响，增加了无人机等设备的功能。我在发言的开头提到了这一点。商用无人机现在可以飞得更快、更远，携带更大的有效载荷，能够利用人工智能和其他工具在没有人工控制的情况下进行操作。无人机不只是在空中运作。2020年3月3日，正如我向安理会通报的那样，胡塞武装恐怖团体使用一艘装载炸药的遥控无人驾驶船，意图袭击也门沿海的一艘油轮。如果袭击成功，将会造成毁灭性影响——不仅对油轮及其船员，而且会对环境、全球补给线以及也门沿海依赖海洋为生的当地社区造成毁灭性影响。对于拥有超级力量的非国家行为体使用技术的现象，我们正处于霍布斯式的自然状态。无所作为是不可取的，如果不进行监管，就等于在鼓励扩散这种做法。

今天，所显示的证据和其他报告都清楚地表明，恐怖团体和非国家行为体越来越多地获得这种技术。我们强烈谴责违反国际法，利用这种技术进行跨界袭击，攻击平民或民用基础设施。但是，随着技术的进步，这种威胁必然会变得更加危险，这个问题必须在联合国内加以解决。各国政府应加强协调，支持能力建设措施，交流良好做法和指导准则，以应对这一威胁。

最后，我们谈到了数字技术对保护人道主义行为体的重要性。现在我们来谈谈这种技术在扩大人道主义行动中的作用。人工智能、预测分析、数字现金转移和区块链技术等数字创新可以改善人道主义行动。这些新兴技术不仅有助于人道主义行为体预测危机并做好准备，在发生危机时，还能使他们更快、更有效

地采取行动。

我们在考虑数字创新时，不能忘记还存在数字鸿沟。据估计，37%的世界人口——近30亿人——从未使用过互联网。这一差距仍然很大，对妇女和女孩的影响尤为严重。最不发达国家只有19%的妇女使用互联网，比男子少12%。物理世界的的不平等现象，显然正在数字世界复制。当我们思考创新如何帮助我们扩大影响力时，我们要优先考虑那些尚未看到技术发展红利的人，这些红利在世界其他地方已经司空见惯。

作为前沿技术的早期倡导者，阿拉伯联合酋长国正在利用我们在国内外的优势。这就是为什么四年前，我们倡导设立秘书长数字合作高级别小组，这反映了我们的信念，即数字技术能够为全球和平与安全做出积极贡献。我们积极支持落实执行，并深受鼓舞地看到秘书长的《我们的共同议程》(A/75/982)中提出了建立全球数字契约的想法。我们都必须进一步支持这项多边工作。

阿拉伯联合酋长国将继续与齐聚在这里的所有人和所有利益攸关方合作，确保世界受益于数字技术，因为这是建设更具复原力、更公平和更具包容性的社会的关键推动因素。

**De Oliveira Marques先生**(巴西)(以英语发言)：巴西感谢主席国美国召开今天关于数字技术对维护国际和平与安全的影响的通报会。我们也感谢副秘书长罗斯玛丽·迪卡洛、Nyabola女士和Druet先生富有洞察力的发言。

数字化转型进程为人类带来巨大的利益和机遇，包括建设和平和理解，以及增强代表性不足和弱势群体的权能方面的利益和机遇。

2019冠状病毒疾病疫情向社会展示了使用数字技术的巨大好处，数字技术已经证明，在受到病毒威胁的限制时，它是维持日常生活的有效工具。教育、贸易和银行系统，以及其他许多系统，已经能够使现有技术适应突如其来的新现实。安理会和联合国系统依靠这些技术继续举行会议，今天，我们甚至已经习惯了听取无法亲自出席会议的通报者发言的想法。当然，



由于在获取信息和通信技术方面持续存在不平等现象，这些益处并没有在所有地方平等享有。解决这一数字鸿沟仍然是国际社会的一项重要任务。

众所周知，通过产生、储存、传播和获取大量信息而彻底改变了我们生活的数字技术，经常被政府和非国家行为体滥用。今天的讨论触及了其中一些挑战，这些挑战性质各异，因此需要采用不同的国家应对方式。

大会认识到，国际法，特别是《联合国宪章》，适用于各国在网络空间的活动，对于维护和平与稳定、尊重人权以及促进开放、安全、和平和无障碍的数字环境至关重要。国际人权法和国际人道主义法在网上和网下都必须得到尊重。我们还强调，遵守大会认可的有关网络空间负责任国家行为的自愿、不具约束力的规范非常重要，包括保护用于支持为公众提供基本服务的关键信息基础设施。

要处理虚假信息的挑战，各国政府和社会必须采取广泛的战略。旨在提高认识的教育活动和公开辩论以及公私行为体、比如与社交媒体公司的合作可有助于处理滥用数字平台煽动暴力和恐怖主义的问题。

利用数字技术方面的国际合作已大幅增强我们识别共同威胁、包括来自如恐怖团体这样的非国家行为体的威胁的能力。随着技术的演化，我们还可更高效地利用它们来提高安全理事会的透明度和灵敏性。我们应鼓励利用新技术，拓宽妇女、青年以及民间社会参与和平进程和各种建设和平及维持和平举措的渠道。

联合国维和行动应利用现有的数字技术，充分发挥其潜力，以便更好地执行自己的授权任务。我谨强调新技术对于维和特派团内部战略沟通的重要性。战略沟通是一种使能因素，在各种授权领域、特别是保护平民和妇女与和平与安全议程方面具有倍增效应。此外，战略沟通对于处理可能阻碍执行授权任务、威胁维和人员安全与安保的错误信息和虚假信息至关重要。

**比昂先生（加蓬）（以法语发言）：**主席女士，我

感谢你倡议召开本次会议，为我们提供机会思考数字技术对维护国际和平与安全的影响。近来，这已成为国际和平与安全议程上的一个日益突出的问题。我谨感谢罗斯玛丽·迪卡洛副秘书长、Nyabola女士以及Druet先生具有启发性的通报。

我们今天讨论的核心主题比以往任何时候都让我们意识到，技术进步已把实体世界的极限推入数字和控制论的无限之中。这一方面意味着各方面、包括维护国际和平与安全方面的可能性增多，另一方面也意味着国际和平与安全面临的威胁发生重组与调整。

现在的维和比以往任何时候都更加依赖一个强有力的技术和创新生态系统，该系统不仅强化管理和预防冲突的工具，而且促进更好的态势感知，为特派团提供更好的支持，并且为常常在复杂环境下更有力地执行联合国维和任务提供便利。

技术进步还有助于加强维和人员和平民的安保，使我们能够更好地采取预防行动，特别是在人道主义领域。无人驾驶飞行器的使用和点分析系统正在日益成为在战场等难以到达地区进行观察和预见动向的首选手段，以便获取可靠信息，做出更及时和高效的应对。

显然，世界正处在我们各国社会、我们的治理——包括国内和全球治理——以及特别是我们的权利与义务变得机器人化和数字化的临界点。不幸的是，这种技术突变并非完全是有利的，与任何没有觉悟意识的科学一样，它伴随着各种后果与担忧。

技术进步常常被认为是一种战力倍增手段，但是也常常自暴为加剧冲突局势的一个因素。确实，仇恨言论、激进化、煽动歧视以及通过互联网和社交媒体散布各种形式的暴力——妇女和青年是易受其影响的主要目标——今天已成为散布恐怖和恐惧、延长危机的首选载体。

制造更强力、更精密并且经过技术进步淬炼的武器放大了滋扰和去人性化的能力，必须用一种严格的法律和道义框架加以约束，以免对人类构成真实的危险。在非洲多个地区，武装恐怖团体自由获取日益精

密的武器和新技术，以提高其破坏力，这种悲哀的现象再次表明，维和人员和当事国的正规部队也需要获取最新技术。

这些国家的生存岌岌可危，它们深陷于这些消极势力之中，有关民众的生存被夹在国家当局的颓废无能、与图谋恐怖与混乱的武装团体的折磨当中，处境险恶。至关重要的一点是，维和部队要能够获取与各种新兴威胁的规模相称、并且适应其必须面对的各种挑战的技术装备，特别是在打击恐怖团体的非对称性武装冲突中。

我们也坚信，有必要鼓励外勤地的技术创新与进步；最大限度地发挥现有技术和新技术的潜能，以提高我们的维和特派团有效执行任务的能力；使和平行动能够以一种及时和统筹的方式，识别、分析并且处理平民、维和人员以及人道主义和政治特派团面临的种种威胁；以及最后，确保和平行动更加负责任地使用数字技术，同时尊重人权，无论它们在何时何地面临风险。

我国支持《联合国维持和平行动数字化转型战略》，也支持《联合国消除仇恨言论战略和行动计划》。

加蓬继续坚定地致力于和平和负责任地利用技术来维护国际和平与安全，并呼吁加强三边合作，这特别是对于有关维和人员安全与安保的第2518（2020）号决议的执行至关重要。

最后，我谨强调，重要的是，要在国际、区域和国内各级动员起来，实现对数字空间和技术进步的最佳治理，使它成为促进联合国和平特派团执行任务的真正催化剂和实现国际和平与安全的主要工具。

**尤尔女士（挪威）（以英语发言）：**我谨感谢各位通报人饶有兴趣的发言。我也感谢美国协调安全理事会内部的这次重要讨论。

过去一年来，安理会以多种不同的方式就技术与安全问题展开讨论，包括2021年5月中国常驻代表团举行的有关新兴技术与安全的阿里亚模式会议，还有

6月份的公开辩论会，当时爱沙尼亚首次把网络安全问题摆在安理会的议事日程之上（见S/2021/621）。今天是对这些讨论的及时延续。

正在出现的不断演化的数字技术在多个领域带来重要机遇。确实，假如没有数字技术，安全理事会自身本无法在冠状病毒病疫情初期运作。与此同时，数字技术也会提出关切与挑战。当数字技术被用于险恶目的时，无疑它们可对国际和平与安全构成威胁。

因此，今天的讨论是安理会任务和责任的核心。

数字技术不仅仅是由国家创造和使用的。这突出各国和其他利益攸关方之间合作的重要性。我们必须与所有开发和使用技术者合作，包括与学术界和非政府组织合作。只有通过共同努力，我们才能确保新技术帮助我们朝着有利于所有人的方向前进。联合国为这种互动提供一个重要的全球平台。

数字技术的滥用，例如关闭互联网或大规模传播虚假信息的做法，会影响全球和平与安全。挪威感到关切的是，不断演变的数字领域滥用可能带来加剧紧张局势的后果，包括侵犯和践踏人权。故意限制全部或部分互联网访问只是滥用的一种形式。通过数字技术传播有针对性的虚假信息是另一种形式，这往往会限制人们在最需要的时候获得可靠信息。

然而，我们不应该低估数字技术的积极作用。数字技术可以让传统上被排除在外的群体，如妇女和少数群体，参与决策进程，包括在安全理事会以视频方式开会，协助更多不同的民间社会通报者的参与，从而帮助促进决策进程的包容性。

虚假信息也仍然是许多领域的一个挑战，包括对我们自己的联合国维持和平特派团构成风险，例如，在部署维和人员提供帮助的社区，虚假信息被传播以制造更加敌对的环境。然而，抵御虚假信息的最佳手段是自由、独立和专业的媒体部门。媒体必须能够自由传递重要信息，提出关键问题，并报道侵犯和践踏人权的行为。因此，支持独立和多元化的媒体并确保记者的安全也有助于缓解紧张局势和防止冲突。

主席女士，我再次感谢你将这个问题列入我们的议程。我期待着这成为一场持续的讨论，探讨我们如何能够防止和应对滥用数字技术造成的虚假信息和挑战，同时不忽视这种技术为维护国际和平与安全带来的巨大好处。

**罗斯科先生（联合王国）（以英语发言）：**主席女士，我感谢你组织今天的讨论。我们也非常感谢通报者所作的通报，因为他们展示了技术正在改变我们监测、了解和应对世界各地冲突和人道主义危机的方式。

显然，首先，技术可以在实际防止冲突爆发方面发挥作用。如果我们能够提前看到风险，那么我们就能够也应该在危机到来之前采取行动。更及时的决策有利于采取早期和预防行动，我认为这是安全理事会应该与秘书处一起进行更多探索的一个领域。这也是我国与其他国家以及行业合作开发人工智能驱动的冲突预防模型的原因。

第二，在冲突期间，执行任务的联合国维和人员准确了解局势至关重要。将远程监测等数字技术与改进的情报、监视和侦察程序相结合，可以帮助维和特派团和监察团更好地了解实地的威胁和脆弱性。如果我们能够让我们的阿拉伯联合酋长国同事描述的那些无人机帮助维和人员，而不是袭击民众，我们就能够取得进展。

第三，技术也能够加强追究责任。正如我们今天所听到，包括从我们出色的通报者那里听到的那样，社交媒体能够加强追究责任；它使人们能够在经历冲突时向世界讲述冲突，并确保世界从他们的角度了解正在发生的事情。这意味着真相，包括大规模暴行或违反国际人道法行为的证据，无法被那些想隐瞒真相的人所隐瞒。

正如我们今天也听到的那样，某些国家和其他行为体正在利用技术来压制人权、传播虚假信息，并将之作为冲突的工具。我们看到一些国家试图通过阻止访问社交媒体或独立媒体网站来隐藏真相。正如其他人指出的那样，我们去年看到这种情况：缅甸军政府关闭了互联网。我们还看到专制政权利用监视技术监

控和迫害自己的公民，剥夺他们的人权。技术也可能被那些寻求破坏稳定的人所利用，这一点在俄罗斯入侵乌克兰的背景下尤其明显，俄罗斯在那里进行了网络攻击，正如我们所报告的那样，俄罗斯利用网络巨魔工厂传播虚假信息，操纵关于其非法战争的舆论。

幸运的是，技术也可以帮助我们打击虚假信息。俄罗斯今天再次试图声称，躺在布恰街头的受害者尸体是乌克兰“有意安排的挑衅行动”。他们暗示，乌克兰部队在夺回该镇后实施了这场有意安排的挑衅行动。但卫星图像证明，布恰街头的尸体已经存在了几个星期，这表明他们是在俄罗斯部队占领该镇期间被杀害的。

今天，我们听到的不是“有意安排的挑衅行动”，而是一些新编造的关于过时火炮的无稽之谈。这是俄罗斯试图转移我们注意力、迷惑我们、混淆视听的又一种策略。一层又一层相互矛盾的谎言被批量生产，以至于人们感到困惑，不知道该相信什么。但是任何人都应该被这种策略所愚弄。我们期待国际刑事法院进行全面调查，以便我们能够根据真实证据了解在布恰所发生事情的真相。希望起诉将由此提出。

打击虚假信息以及捍卫致力于在线报道真相的媒体对于国际体系的正常运作至关重要。因此，当俄罗斯代表团哀叹其在社交媒体上受到制裁或其国家宣传渠道被封锁时，它不应该这样做。在数字空间，就像在所有空间一样，我们必须努力保护真相不受这种新型欺人之谈的影响。

最后，我们必须共同努力，包括与民间社会组织、私营部门和其他群体合作，以实现数字技术的好处，并应对与之相关的风险。这将包括调整机构和维护植根于高标准、人权和民主价值观的准则。在我们这样做的时候，安理会必须确保现有框架和国际法仍然是我们的指导原则。如果我们成功做到这一点，我们就能确保数字技术成为一股向善的力量、成为维持和平与发展的变革机会。

**弗林先生（爱尔兰）（以英语发言）：**我感谢各位通报者。



正如我们今天所听到，技术是我们生活中的积极力量，但也可能是煽动暴力和冲突的强大武器。网络攻击、网络犯罪以及滥用技术传播虚假信息的行为正在严重破坏信任，而现代技术的进步正在推动冲突性质的改变。仇恨言论可以在几分钟内传播和扩大，从而造成族群对立，破坏民主，并助长全球的不容忍和暴力。

这种风险的例子数不胜数。俄罗斯国家控制的媒体发布造谣言论，企图为其在乌克兰的非法、无理战争制造借口。战争持续进行。与此同时，俄罗斯联邦也继续企图歪曲现实，否认其在当地的野蛮侵略。

正如我们从其他人那里听到的那样，在缅甸，政变前限制访问互联网预示着其后要破坏基本自由，实施镇压、监视和野蛮暴力。在埃塞俄比亚，我们看到有人滥用技术压制人权卫士，对活动家实施监视，并通过社交媒体散布仇恨言论和煽动紧张关系。在其他许多情形下，有人正在滥用新技术威胁国家安全和完整，攻击要害基础设施，干涉民主进程和限制人权。

数字技术的扩散虽然带来新的风险和挑战，但在支持和平方面也有可能发挥重要作用。无论是在哥伦比亚还是在利比亚，我们都看到数字技术如何支持更大的包容性，如何促进对和平进程的参与，又如何对面对面的互动起到辅助作用。这些技术能够而且应该促进和扩大妇女、青年和少数族裔的参与。爱尔兰欢迎政治和建设和平事务部调解支助股和创新小组在这方面开展的工作。然而，这些努力必须注意到这些群体在网络空间面临的特殊风险，以及全球性别数字鸿沟。我们促请在座各位更加坦诚地看待技术可在预防冲突和应对气候变化等全球性挑战方面发挥的积极作用。能力建设、建立信任的措施和举措，包括爱尔兰自豪地联署的《促进网络空间负责任国家行为行动纲领》，都是这些努力的核心所在。

技术也可在维和任务中充当增强战斗力的手段，提高我们维和人员对形势的认识，并增强数据分析能力。这些至关重要的手段提高了安全、安保和行动效率，从而加强任务执行工作。正因为如此，实施《联合国维持和平行动数字化转型战略》非常重要。

恰恰是在武装冲突时期，我们必须大力捍卫网上网下的言论自由和获取信息的权利——这些自由对于促进持久和平、了解冲突的性质和确保追责必不可少。今天，我向乌克兰公民、新闻记者和人权卫士致敬，他们经常冒着巨大人身风险，利用数字技术分享前线发生的悲惨故事。他们正孜孜不倦地收集、核实和保存袭击行为的数字证据，希望这些证据能够用来追究责任人的责任。

毋庸置疑，国际法，包括国际人道法和国际人权法，均适用于网络空间。我们对数字技术的运用必须立足于人权、法治和民主价值观。

爱尔兰支持自由、安全无虞、包容和便捷的网络空间。我们知道，数字技术并非凭空存在。显然，非国家行为体在推动技术创新方面发挥着主导作用。包括人权卫士、妇女团体、技术专家、学术界和私营部门在内的民间社会必须积极和切实参与我们的工作，寻找应对共同挑战的办法。爱尔兰还大力鼓励建设和平委员会在其讨论和建议中考虑数字技术的积极和消极影响。

最后，致力于发挥数字技术的潜力就是致力于和平。就数字技术的使用而论，爱尔兰坚信，多边主义、负责任的国家行为、透明度以及追究人的责任，是建立和维护国际和平与安全所需基本信任的关键所在。

**主席**（以英语发言）：我现在以美国代表的身份再次发言。

首先，我要感谢各位同事今天参加一次颇具建设性的对话，讨论数字技术在促进国际和平与安全方面的作用。不幸的是，俄罗斯决意采取不具建设性的做法，发起无端攻击，蓄意散布那种我们今天在此要在一定程度上讨论如何预防和应对的虚假信息。

我不会掉进俄罗斯阴谋论的“兔子洞”。相反，我们今后将与安理会其他成员一道努力，在接下来的数周和数月继续进行这些重要讨论。我要再次感谢通报者今天所作的通报。我还要感谢全体同仁。

我现在恢复行使安理会主席职责。

中午12时35分散会。