联合国 S/PV.9779

安全理事会

第七十九年

临时逐字记录

第九七七九次会议

2024年11月8日星期五上午10时举行

纽约

主席：	卡里乌基先生	（大不列颠及北爱尔兰联合王国）
成员：	阿尔及利亚	库德里先生
	中国	耿爽先生
	厄瓜多尔	蒙塔尔沃·索萨先生
	法国	达尔马迪卡里先生
	圭亚那	佩尔绍德女士
	日本	御巫先生
	马耳他	卡米莱里先生
	莫桑比克	阿丰索先生
	大韩民国	黄先生
	俄罗斯联邦	涅边贾先生
	塞拉利昂	卡努先生
	斯洛文尼亚	布洛卡尔·德罗比奇夫人
	瑞士	豪里先生
	美利坚合众国	纽伯格女士

议程项目

对国际和平与安全的威胁

24-33610 (C)

上午10时05分开会。

通过议程

议程通过。

对国际和平与安全的威胁

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：世界卫生组织总干事谭德塞博士和阿森松保健公司总裁爱德华多·康拉多先生。

根据安理会暂行议事规则第39条，我还邀欧洲联盟驻联合国代表团团长斯塔夫罗斯·兰布里尼蒂斯先生阁下参加本次会议。

安全理事会现在开始审议其议程上的项目。

我请谭德塞博士发言。

谭德塞博士（以英语发言）：我感谢法国、日本、马耳他、大韩民国、斯洛文尼亚、联合王国和美国召开今天的讨论会，感谢有机会向安理会通报这个日益重要且令人不安的议题。

2020年3月，捷克布尔诺大学医院遭受勒索软件攻击，被迫关闭网络，将病人转至邻近机构，推迟预定手术，并恢复纸质流程。这次攻击发生时，恰逢捷克因大流行病而进入紧急状态。2021年5月，Conti勒索软件团伙入侵了爱尔兰卫生服务执行局。攻击从一封包含电子表格附件的钓鱼邮件开始，打开后会下载恶意软件。恶意软件在两个月内扩散到卫生服务执行局的整个网络，加密了约80%的数据，使国家诊断成像平台无法访问，并导致五个主要中心的放射治疗服务暂停。结果，半数以上的急症医院推迟了门诊预约以及择期临床调查和干预，临床工作人员采用纸质流程来维持基本服务。

我们首先要明确指出，针对医院和其他医疗设施的勒索软件和其他网络攻击不仅仅是安全和保密问题，还可能是生死攸关的问题。在最好的情况下，此类攻击会造成混乱和经济损失。最坏的情况是，它们会破坏人们对其所依赖的医疗系统的信任，甚至给病人造成伤害和死亡。

卫生系统的数字化转型、卫生数据的宝贵价值、对卫生系统日益增长的需求以及经费拮据，所有这些因素都致使医疗设施成为勒索软件攻击的目标。这些攻击以医疗设施的数字基础设施为目标，导致它们中断或关闭。犯罪者要求支付费用或赎金，才能恢复访问。

网络犯罪集团的运作逻辑是，对患者安全、保密性和服务中断造成的威胁越大，他们可以索要的赎金就越多。如果医疗设施不支付赎金，其后果就不仅仅是财务和运营方面的，还有可能危及患者。为了尽快恢复系统和找回数据，医疗设施通常愿意支付巨额赎金，即使不能保证数据会被解密或攻击者不会再次尝试。

调查显示，针对医疗保健部门的攻击在规模和频率上都有所增加。这是因为黑客对医院和医疗设施的攻击得逞。在2021年的一项全球调查中，超过三分之一的受访者表示在上一年至少遭受过一次勒索软件攻击，其中三分之一表示支付了赎金。然而，即使支付了赎金，仍有31%的受访者无法重新访问加密数据。

尽管勒索软件攻击的主要重点是医院和其他卫生服务提供商，但是在疫情期间，广大生物医学供应链也成为攻击目标。安全研究人员在至少17家参与生产冠状病毒病疫苗和开发疗法的生物医学公司中发现了漏洞。据报告，临床试验软件供应商、实验室和制药公司也受到攻击。

2021-2025年信息和通信技术安全和使用安全不限成员名额工作组的报告（见A/79/214）就会员国如何采取措施，通过负责任国家行为规则、准则和原则、国际法、建立信任措施、能力建设以及机构对话来加强网络安全提出了许多建议。世界卫生组织（世卫组织）和我们的合作伙伴正在努力落实其中许多适用于卫生领域的建议。

去年12月，世卫组织在日内瓦召集专家，制定应对网络安全威胁的战略和做法，特别是在资源有限的

情况下。他们确定了几项关键挑战，其中包括：未能向决策者明确传达勒索软件的威胁和投资于网络安全的价值；缺乏明确的网络安全治理框架；复杂的基础设施难以变得更加安全；以及全球网络安全技能和专家的供需之间存在巨大差距。

为了弥合这些差距，世卫组织和其他联合国机构正在积极支持会员国，为之提供技术援助、准则、标准和指导，以加强卫生基础设施抵御勒索软件等网络犯罪的能力。1月，世卫组织与国际刑警组织、联合国毒品和犯罪问题办公室和其他伙伴合作，就如何加强网络安全和打击虚假信息发表了两份报告。世卫组织还在制定关于实施和投资于数字卫生干预措施的网络安全和隐私保护的指南，该指南将于明年发布。

网络安全是整个政府的责任，但卫生部门当局、资助者和产品所有者仍须对卫生信息系统的安全负责。会员国可以采取许多措施来提高其网络成熟度，即其应对网络攻击的准备程度。这意味着投资于技术，并确保数字卫生项目的预算包括基本网络安全控制的成本。各组织应避免使用不受支持的软件，因为这些软件更容易受到攻击。具体而言，投资于早期识别攻击的系统至关重要，因为大多数攻击在发生几个月后才被发现，到那时损害已经造成。

然而，尽管用于识别、保护、检测、响应和恢复的技术至关重要，但它们还不够，尤其是随着人工智能的使用越来越广泛，更是这样。我们必须彻底改变观念，认识到我们不能仅仅依靠信息技术系统来保护我们免受网络攻击。因此，提高网络成熟度也意味着投资于人。实施勒索软件攻击的是人，能够阻止勒索软件攻击的也是人。培训工作人员识别和应对网络攻击以及演练事件应对计划至关重要。人类既是网络安全最薄弱的环节，也是最强大的环节。

这不是任何一个国家能够单独做到的。病毒不分国界，网络攻击也是如此。因此，国际合作至关重要。我们为应对其他威胁而采取的许多措施在这方面也同样适用，无论是在联合调查和执法方面开展合作，还是分享情报或建立区域网络。世卫组织主办了两个新的国际对话全球平台：全球数字卫生保健倡议以及全球人工智能促进健康倡议——一个与国际电信联盟和世界知识产权组织共建的三方平台。

我再次感谢安全理事会提请注意这一非常重要的问题。正如安理会成员所知，《联合国宪章》赋予安理会的任务是维护国际和平与安全。包括勒索软件在内的网络犯罪对国际安全构成严重威胁。正如安理会成员利用这一授权就实体安全问题通过决议和决定一样，我们也请安理会成员考虑利用这一授权加强全球网络安全和追究责任机制。世卫组织致力于支持所有会员国最大限度地发挥数字技术对卫生保健的作用，并最大限度地降低其风险。

主席（*以英语发言*）：我感谢谭德塞博士所作的通报。

我现在请孔拉多先生发言。

孔拉多先生（*以英语发言*）：主席先生，我感谢你允许我参加今天的会议。我叫爱德华多·康拉多，是美国第三大卫生保健系统阿森松的总裁。

阿森松是一家非营利的天主教医疗系统。我们拥有约33万名员工——包括约3.3万名附属医疗服务提供者——在我们遍布17个州和哥伦比亚特区的120家医院、2000个非住院医疗点以及75个非住院手术中心工作。每年，我们为600多万人提供护理，其中急诊就诊人次超过300万，手术近60万例。阿森松每年接生的婴儿约占美国新生儿总数的五十分之一——相当于每年72000到78000名新生儿。我们的使命是为所有人提供特别关注的服务，并为美国贫困和弱势人群提供富有同情心的全面护理。

各位安理会成员可能知道，卫生保健行业因其规模、对技术的依赖性以及我们需要保护和维护的敏感数据，特别容易受到网络和勒索软件的攻击。5月8日，阿森松遭到勒索软件攻击。这次攻击加密了我们数千个计算机系统，对我们为患者和社区提供服务的能力构成重大挑战。系统被加密的直接后果是，我们无法访问我们的电子健康记录。我们的其他几个技术系统也无法使用，包括患者用来与医生沟通和下载数

据的系统。勒索软件攻击还使我们更难访问用于预订和执行某些关键诊断测试——如实验室检测、磁共振成像、计算机断层扫描和X光检查——以及为患者配药的各种系统。

发现勒索软件攻击后，我们的医疗团队立即启动了停机程序，这是所有医疗机构在系统或网络故障时都要遵循的预定步骤。其中一个步骤包括在电子记录无法使用期间改用纸质记录。各位成员可以想象，这给我们敬业的工作人员和临床医生带来了巨大的负担。让我描述一下我们的工作人员在这段时间里的情况。

一夜之间，护士们无法从电脑工作站快速查找患者记录，不得不翻阅纸质备份来查找病人的病史或用药情况。影像团队无法迅速将最新的扫描结果发送给在手术室等待的外科医生。事实上，我们不得不依靠传递人员将扫描结果的打印件送到手术团队手中。我们在试图增加人手来减轻护士的负担时，也因为配置系统处于离线状态而受阻。由于这次恶意攻击，我们的医疗团队和患者从每天使用所有令人难以置信的技术，变成了使用纸质文件、传真和手工递送。简而言之，我们的现代医疗系统被迫回到了过去。

在遭到攻击期间，我们的几家医院也被迫进行紧急医疗服务分流，这意味着救护车被引导到其他医院的急诊室，而不是阿森松医院。分流的影响可能各不相同，但可能会由于行程时间增加而导致服务延迟，并可能给患者带来不良后果。这还会产生连锁反应，使接收医院不堪重负，也被迫分流患者。除了谨慎起见而分流救护车外，一些非紧急的择期手术、检查和预约在我们努力恢复电子系统期间也暂时中止。

现代卫生保健依赖于许多第三方数字解决方案。我们发现，让这些系统重新上线并说服数百家供应商中的每一家重新连接到Ascension是一项艰巨的任务。直到6月14日，即勒索软件攻击发起37天后，我们才恢复了所有电子健康记录的连接和访问，并使最后一家医院重新上线。

今天，我们仍在继续处理这次攻击的后果。现在，我们的电子病历系统已经恢复运行，我们正在对系统瘫痪的37天内创建和收集的所有纸质病历数据进行数字化处理，这是一个漫长的过程。形象地说，如果将在此期间产生的所有纸张堆叠起来，高度将超过1.5千米。我们很可能要到本日历年年底才能将这些纸质记录数字化，也就是说，从我们的系统重新运行开始，需要整整六个月。

虽然我主要关注的是勒索软件攻击对我们系统和服务的影响，但我想强调的是此类攻击对人的巨大影响。我们的医疗服务提供者和员工奋起应对技术限制和工作流程中断带来的巨大挑战，帮助为患者提供所需的安全有效的医疗服务。他们在这样做的同时，还承担了更长的工作时间、更大的压力，在某些情况下还加剧了职业倦怠。此外，当病人被转到其他医疗机构或在其他医疗机构寻求治疗时，由于病人数量增加、从Ascension获取医疗记录的途径有限以及压力增大，这些其他医疗机构的医疗服务提供者和工作人员也不得不承担额外的负担。我们赞扬这些医疗服务提供者所承担的工作，我想感谢他们愿意并努力这样做。

我们的组织只是每天被网络犯罪分子盯上的众多医疗机构之一。与许多可能没有Ascension那么多资源的小型医疗机构不同，我们很幸运能够迅速聘请内部和外部网络安全专家及法律顾问进行调查、控制问题并确保系统安全。我们还与联邦调查局和网络安全与基础设施安全署密切合作，共同应对此次攻击。尽管如此，2024年5月的勒索软件攻击仍对我们造成了巨大的财务影响；截至本财年末，Ascension为应对此次攻击花费了约1.3亿美元，损失了9亿美元的营业收入。

遭受网络攻击重大财务影响的不止Ascension一家。最近的估计表明，自2019年以来，美国医疗机构的宕机成本、恢复工作和收入损失累计已超过700亿美元，仅今年10月就损失了近150亿美元。针对医疗保健系统的勒索软件攻击一直在增加，根据美国卫生与公众服务部的数据，2024年迄今为止，美国共报告

了386起医疗保健网络攻击事件，而我们Ascension内部的卓越技术和网络安全团队几乎每天都在阻止攻击我们系统的企图。

针对医疗保健行业的勒索软件攻击不仅仅是网络威胁，还会对全球公共卫生和安全构成直接和系统性的风险。此类攻击并非由流氓分子所为，而是由技术高超、资源充足的专业网络犯罪分子所为。要打击勒索软件攻击和保护全球医疗保健系统，需要国际协调与合作。

我们感谢安全理事会对保护我们的医疗保健系统，并最终保护我们的患者和社区的关注。我感谢安理会成员今天上午花时间听我的通报。

主席（*以英语发言*）：我感谢孔拉多先生的通报。

我现在请希望发言的安理会成员发言。

纽伯格夫人（美利坚合众国）（*以英语发言*）：我叫安妮·纽伯格，自2021年以来，我有幸负责协调美国在网络和新兴技术方面的国家安全政策。我很荣幸今天能代表拜登总统谈谈勒索软件的威胁。

我要感谢联合王国将其担任安全理事会主席期间的部分时间用于今天的会议，并持续在促进网络空间负责任的国家行为方面发挥领导作用。我还要感谢世界卫生组织总干事谭德塞博士和Ascension医疗集团总裁爱德华多·孔拉多参加我们的会议。我们赞赏他们在通报中提供的专业知识和见解。

今天，我想向安理会谈三个话题：首先，勒索软件攻击所构成威胁的性质，特别是对医疗保健系统所构成威胁的性质；其次，美国正在全球和国内采取哪些措施来应对这一威胁；最后，每个国家在应对这一挑战方面可以而且必须发挥的关键作用。

现实情况是，对医院和医疗保健系统的勒索软件攻击是对国际和平与安全的严重威胁。它们危及生命。它们破坏社会稳定。因此，安全理事会在应对这种对和平的威胁和促使各国采取行动方面可以发挥作用。就在几个月前，安东尼奥·古特雷斯秘书长在大韩民国召开的安理会关于网络空间不断演变的威胁的高级别公开辩论会上，呼吁我们反思数字技术给我们社会带来的巨大好处（见S/PV.9662）。然而，正如秘书长所告诫的那样，把我们联系在一起的这种连通性也使世界各国面临重大的网络威胁。勒索软件是这些威胁中最普遍和最具破坏性的威胁之一。仅2023年一年，美国政府就了解到1 500多起与勒索软件相关的事件，产生的赎金超过11亿美元。这比2022年有了大幅增长，当时我们看到的赎金支付额只有2023年的一半多一点。事实上，2023年的数字比2018年增长了10倍，比2014年增长了100倍。

美国并不是个例。2023年7月，日本的商业航运港口名古屋港遭到LockBit团伙的勒索软件攻击，港口被迫停止处理很大一部分进港集装箱。同年，联合王国一家病理合作机构遭到勒索软件攻击，导致全国血液供应面临重大风险。南非国家卫生实验室服务局遭受了勒索软件攻击，影响了实验室结果的传播，阻碍了国家应对猴痘爆发的工作。

根据美国情报界2024年6月的分析，今年上半年全球51%的勒索软件攻击是针对美国受害者的。剩下的49%则遍布全球。这确实是一个全球性威胁。医疗保健和紧急服务是勒索软件攻击最多的四大目标部门之一，仅今年上半年，全球就发生了至少191起攻击事件。在美国，联邦调查局去年报告了249起针对医疗保健部门的勒索软件事件。

勒索软件攻击对医院意味着什么？正如我们刚才在通报中听到的，它意味着救护车改道和其他急救延误、手术取消、重要治疗延误以及极其敏感的医疗记录外泄。针对血库的勒索软件攻击会阻止人们获得救生用品。针对这些设施的勒索软件会导致严重的中断，危及病人护理和药物获取，延长病人住院时间，迫使病人转院，并造成生命损失。我要再次强调最后一句话。据卫生专家估计，2016年至2021年间，勒索软件攻击导致了美国医疗保险系统中数十名患者死亡。最近的数据证实，当医院受到网络攻击的破坏时，医院的死亡率会上升。

我们该如何应对这一危险的犯罪狂潮? 我们首先有一个前提, 就是人多力量大。面对这一威胁, 我们并不是孤军奋战； 想要维护国际规范, 全方面禁止这种行为, 我们也不是孤立无援。我们认为, 我们可以超越我们各部分相加之和。正是这种信念激励我们在2021年发起了由68个成员组成的国际反勒索软件倡议, 其中包括今天与我一起在座的一些国家。该倡议的重点是破坏勒索软件攻击, 加强重要基础设施的安全, 共同提高我们合作伙伴的实力和事件应对能力。

我们还利用自身的执法能力来瓦解这些犯罪浪潮。为了降低勒索软件攻击的吸引力, 我们正在与网络保险公司和私营部门密切合作, 以减少勒索软件造成的支付并改进事件报告。我们还与其他 40 个国家一起承诺, 不允许我们的政府或其任何机构支付勒索软件赎金。

除了减少赎金支付外, 我们还与公共和私营部门实体合作, 阻止勒索软件勒索的赎金的非法流动, 这些赎金通过虚拟资产服务提供商洗钱以加密货币支付。展望未来, 美国国际开发署正在努力建立一个基金, 以建设应对勒索软件攻击的长期网络安全能力, 并帮助各国应对勒索软件攻击并从中恢复。

但是, 我们大家都做得不够。只要有人支付赎金, 犯罪分子能逃避追捕, 特别是越境逃跑, 勒索软件攻击就会继续, 犯罪分子就会猖獗。

这就引出了我的第三个也是最后一个话题--每个国家可以且应该做些什么来结束这种受害、掠夺和有罪不罚的循环? 为什么安全理事会应根据其独特的任务授权支持各种努力应对这一对和平与安全的不断演变的威胁?

勒索软件攻击之所以对网络犯罪分子有吸引力, 是因为个人支付大笔赎金。对于像BlackCat这样的组织来说, 这是一门兴旺的生意, 自2019年以来, 该组织已收到超过4.2亿美元的赎金。事实上, 去年BlackCat和LockBit占全球据称发生的医疗保健勒索软件攻击的30%以上。2024年, 除其他攻击外, LockBit还宣称对克罗地亚最大的医院发动了网络攻击, 并公布了从法国医院系统窃取的患者机密数据。

首先, 每个国家都应按照大会多次以协商一致方式核可的网络空间负责任国家行为框架行事。通过确认这一框架, 我们已经承诺处理来自我们领土的恶意网络活动。根据该框架, 各国不应故意允许其领土被用于利用信息和通信技术（信通技术） 实施国际不法行为, 并应响应适当请求, 减少从其领土针对另一国关键基础设施的恶意信通技术活动。

因此, 当一个国家的勒索软件行为体以另一个国家的医院等关键基础设施为目标时, 第一个国家有责任采取行动, 根据框架规范调查并减少这种活动, 特别是在被要求这样做时。然而, 一些国家—尤其是俄罗斯--继续允许勒索软件行为体在其领土上肆无忌惮地开展活动, 即使在被要求约束此类活动之后也是如此。网络犯罪团伙LockBit的开发者和管理者是俄罗斯人德米特里·霍罗舍夫, 我国司法部已指控他犯有黑客罪。

我们根据成员的国籍、地理位置以及声称效忠或与已知俄罗斯网络行为体有关联的情况, 评估出与影响最大的勒索软件变体（如对阿森松保健公司实施攻击的变体）有关联的网络犯罪分子与俄罗斯有联系。这些顶级勒索软件行为体的一些洗钱者以俄罗斯为基地, 并利用俄罗斯银行或加密货币交易所来洗白其不义之财。

2021年, 拜登总统会见了普京总统, 要求他控制勒索软件对美国目标的攻击。拜登总统在会晤中明确表示, 当勒索软件行动来自俄罗斯领土时, 即使该行动不是由国家发起, 美国也希望俄罗斯政府采取行动。俄罗斯没有遵守其联合国承诺, 继续窝藏这些罪犯。美国恳求各国不要效仿俄罗斯保护国际网络罪犯的做法, 并重申我们要求各国遵循网络空间负责任国家行为框架, 以维护国际和平与安全。

我们今天发出行动呼吁——遭受针对医院的勒索软件攻击的国家应将攻击情况通知来源国, 并要求

它们按照联合国关于网络空间负责任国家行为的承诺采取行动。

总之，只要我们共同行动，遵守我们的共同原则，拒绝向犯罪团伙付款，并相互帮助，逮捕那些自以为能胜过我们系统的网络犯罪分子，我们就能够共同铲除这一祸害。我感谢各位成员的关注，并期待着在今后的日子里继续扩大合作。

达尔马迪卡里先生（法国）（*以法语发言*）：首先，我要感谢世界卫生组织总干事谭德塞博士和爱德华多·康拉多先生的通报，他们的通报明确强调了安全理事会今天会议的关键议题。

今年6月，在主席国韩国的倡议下，安全理事会就网络威胁的演变举行了一次公开辩论（见S/PV.9662）。许多国家强调，滥用信息和通信技术对国际和平与安全的影响日益严重。最严重的威胁之一是勒索软件攻击。勒索软件威胁继续增长，不断恶化。2023年，在法国，这类攻击比上一年增加了30%。这种增长是由于源代码和网络入侵工具进入市场，使众多犯罪分子得以实施网络攻击。

在经济动机的驱动下，勒索软件攻击影响到个人、公司和基本公共服务的运行，从而影响到国家的稳定。法国当局在2023年发现的勒索软件攻击中约有10%以医疗机构为目标，对重要医疗服务的提供造成了严重后果。许多攻击以战略部门的企业、研究机构、高等教育机构和公共行政部门为目标。

我们知道，勒索软件攻击有助于为大规模毁灭性武器的扩散提供资金。安全理事会第1874（2009）号决议所设委员会专家小组的最新报告（见S/2024/215）指出，朝鲜非法核计划和弹道导弹计划资金的40%源于网络犯罪活动。

为了应对这些威胁，我们必须首先重申我们对保障网络空间安全与稳定的准则的承诺。大会多次重申，包括《联合国宪章》在内的国际法适用于网络空间。各国以协商一致的方式确定了一系列网络空间负责任国家行为准则，以改善网络事件的预防和管理。这一规范框架敦促各国采取一切合理措施，防止其领土被恶意网络行为体用来实施国际不法行为。在大会，法国将继续支持旨在促进这一规范性框架的工作，促进对这一框架的共同理解，并支持各国执行这一框架。法国将在未来一年积极参加关于建立常设行动纲领机制的讨论，以实现这些目标。

法国支持并参与美国于2021年发起的国际反勒索软件倡议。该倡议促进分享最佳做法，以便制定共同应对勒索软件对我们社会和民主所构成威胁的办法。

正如一些国家在6月份韩国担任主席期间举行的公开辩论会上强调的那样（见S/PV.9662），安全理事会也必须在其任务框架内加强对网络安全威胁的控制。像今天这样的会议让安理会能够及时了解不断变化的网络威胁局面。法国随时准备努力提高安理会附属机构对网络挑战所代表利害关系的认识，特别是在规避制裁制度方面。

御巫先生（日本）（*以英语发言*）：主席先生，首先，我感谢你应包括日本在内的七个安全理事会成员的请求召开本次会议。我也感谢今天通报者带来的真知灼见。

重要的是，在阿里亚模式会议以及分别于4月和6月举行的公开辩论会（见S/PV.9662）之后，安全理事会继续处理网络攻击所构成的威胁。今天，我们正在目睹通过日益复杂手段进行网络攻击的风险越来越大。针对关键基础设施的网络攻击呈上升趋势，针对医疗保健设施的勒索软件攻击也是如此。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2021年的报告（见A/76/135）指出，信息和通信技术（信通技术）的复杂和尖端使用破坏信任，有可能升级，并可能威胁国际和平与安全。该报告还提到冠状病毒病疫情期间恶意信通技术活动的风险和后果。日本继续与牛津大学合作，通过牛津网络空间国际法保护进程以及去年发表的一份关于针对医疗保健部门的网络行动的报告，在法律层面对这些问题进行研究。信通技术的脆弱性是整个世界的一个风险因素。没有一个

国家能够单独应对这一威胁，我们必须带着紧迫感共同努力。

勒索软件是最具破坏性的网络威胁之一，它破坏社会关键基础设施，包括医院和发电厂的运行。鉴于其整体影响和后果，勒索软件肯定会对国际和平与安全构成直接威胁。日本一些医院也经历过勒索软件攻击所导致急诊病人护理和预定手术方面的重大障碍。至关重要的是，防止勒索软件攻击，并且在受到攻击的情况下，最大限度地减少社会和经济方面的破坏。为此，日本重视会员国当局之间的信息共享和密切合作，包括执法机构提高对勒索软件攻击潜在目标的认识、增强网络安全复原力、以及能力建设。同样，建设集体复原力依然至关重要，有助于防止各种行为体利用勒索软件攻击的任何漏洞。日本重视并赞赏美国主导的反勒索软件倡议，并表示坚定致力于在政策和行动层面作出共同努力，以打击勒索软件威胁。推动加强网络安全的能力建设方案也至关重要，可以确保网络基础设施的安全性和复原力。为此，日本一直在向印度-太平洋国家提供能力建设支持，并将继续与志同道合的国家、国际组织、工业界和学术界进行合作。

日本重申网络空间法治的重要性。在联合国框架内，我们一直在就适用现有国际法以及执行商定的负责任国家行为准则、规则和原则进行具体讨论。虽然我们同意现有国际法适用于网络行动，但我们也发现，对于关键问题，包括侵犯主权以及适用尽职调查原则，并没有达成一致意见。为了维护和平与安全，同时通过互联网依靠跨境数据流动，我们必须尽快在数据自由流动与领土主权之间寻求适当的平衡。我们认为，目前在这些问题上缺乏一致意见不利于维护国际和平与安全。因此，我们必须加紧努力，寻找适用现有国际法的共同点。为此，安全理事会也可以发挥作用。安理会可能很难确定单一网络事件是否对国际和平与安全构成威胁，但考虑到恶意网络行动不断增加的令人担忧的趋势，如对医疗保健部门的勒索软件攻击，安全理事会或许可以确定恶意网络行动的某些趋势对国际和平与安全构成威胁。

在我们继续工作的时候，日本期待着为信息和通信技术安全和使用安全不限成员名额工作组（不限成员名额工作组）即将举行的会议作出贡献。日本还认为，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应成为确保2025年后从不限成员名额工作组顺利过渡的未来常设平台。最后，日本将继续努力打击网络威胁，追求自由、公平与安全的网络空间。

卡米莱里先生（马耳他）（*以英语发言*）：我们感谢谭德塞博士和康拉多先生所表达的深刻见解。

勒索软件战术的演变代表着网络安全威胁局面的严重升级。这种攻击已经变得越来越具有破坏性，致使在不屈服于恶意行为体要求的情况下实现复苏变得更加困难。因此，马耳他加入要求召开本次会议的呼吁。世界卫生组织已将勒索软件确定为对医疗保健的主要数字威胁，这种情况因冠状病毒病疫情驱动的数字转型而恶化，这些攻击不仅危及获得基本医疗服务的机会，而且还侵犯个人的基本隐私权，并威胁到公民的整体福祉和安全及其基本人权。

信息和通信技术安全和使用安全不限成员名额工作组（不限成员名额工作组）7月份的年度进展报告强调各国对勒索软件日益增长的关切，指出攻击的频率和严重性有所增加。勒索软件作为一种服务的兴起扩大恶意参与者的范围。该报告强调指出，必须采取综合办法来应对勒索软件威胁，包括应对非法资助这些活动的行为。在6月份大韩民国担任主席期间举行的安全理事会关于网络威胁的高级别辩论会上（见S/PV.9662），若干代表团确认勒索软件有可能颠覆政府并扰乱基本公共服务。它们还强调指出，针对关键基础设施的勒索软件以及国家支持的网络攻击日益增多。

第1718（2006）号决议所设委员会专家小组的最后报告（见S/2024/215）也强调这些关切，该报告通报了对2017年至2023年期间58起涉嫌网络攻击事件的调查，涉案金额约达30亿美元。据报道，这些事件帮助朝鲜民主主义人民共和国规避制裁，继续研发大

规模毁灭性武器。马耳他确认由技术所驱动威胁的迅速演变性质，并强调必须采取全面的应对措施。至关重要的是，会员国要确保信通技术人员，特别是医疗保健人员，掌握最新的网络安全技能。此外，网络攻击可能成为公共卫生紧急事件，提高行政部门对这一点的认识至关重要。

人力资本投入、建立健全的事件应对流程、以及培训临床医务人员在网络攻击期间保持服务质量，这些都至关重要。同样重要的是，在医疗机构内部建立强大的沟通渠道，以协调应对措施，有可能要跨境行动。单靠国家努力只能到此为止。国家努力也必须得到国际合作的补充，以确保遵守国际法。跨境勒索软件攻击给公共卫生带来越来越大的风险，其影响远远超出单纯的技术中断。网上勒索软件的存在降低攻击的门槛，跨国有组织犯罪团伙的攻击也是如此，致使恶意行为体更容易在全球运作。

必须将性别平等纳入网络规范执行工作以及对性别问题有敏感认识的能力建设的主流。让妇女参与网络决策至关重要，特别是在冲突和冲突后环境里。确保我们的网络安全战略对性别问题有敏感认识，这对于制定全面有效的解决方案至关重要。

最后，我们期待着继续讨论网络安全问题，并赞扬为突出安全理事会的重要作用所作的努力。我们重申支持联合国指导的行动纲领。我们认为，商定的网络空间负责任国家行为框架对于履行我们的共同责任和协调我们的共同利益至关重要。

黄先生（大韩民国）（*以英语发言*）：我感谢世界卫生组织总干事和康拉多先生提出宝贵见解。

大韩民国欢迎今天召开及时会议，讨论勒索软件这一最严重的网络攻击类型之一。我们感到鼓舞的是，在大韩民国担任安全理事会主席期间主持的4月份“阿里亚办法”会议和6月份标志性活动公开辩论会（见S/PV.9662）的基础上，安全理事会今年的网络安全讨论出现了持续势头。在这些会议上，许多国家强调，勒索软件与其它类型的网络威胁一起已成为对国际和平与安全的重大挑战。许多国家一直强调，安全理事会必须根据《联合国宪章》赋予的主要责任应对网络威胁。在这方面，我要强调以下几点。

第一，包括勒索软件攻击在内的恶意网络活动是威胁倍增因素，加剧了现有挑战，扩大了冲突。它们扰乱基本的社会或公共服务，从而引发社会不稳定并破坏国家安全。在乌克兰，对电网和电信系统等关键基础设施的一些网络攻击正在造成大面积停电和网络中断。这些攻击不仅造成人道主义灾难，而且还使战争进一步升级。

第二，网络攻击严重损害安理会的制裁制度。例如，根据第1718（2006）号决议所设委员会专家小组的年度报告（见S/2024/215），朝鲜民主主义人民共和国约50%的外汇收入来自恶意网络活动。这清楚地表明，网络攻击已成为规避和取消安全理事会制裁的主要工具。此外，受制裁的武装团体正在利用非法网络活动筹集资金、隐藏资产和进行武器贸易，使资产冻结和武器禁运的执行工作复杂化。

第三，这种非法收入与大规模毁灭性武器的扩散有关，而大规模毁灭性武器的扩散属于安全理事会的直接管辖范围。事实上，正如专家小组最近的报告所指出的那样，朝鲜民主主义人民共和国通过恶意网络活动为其非法大规模毁灭性武器和导弹发展计划提供40%的资金。上周，朝鲜民主主义人民共和国发射了一系列弹道导弹，包括一种新型洲际弹道导弹。不用说，朝鲜信息技术工作者也一直在从事严重犯罪活动，例如从全球众多国防公司窃取知识产权，目的是提高其大规模杀伤性武器的能力。

为应对包括勒索软件在内的网络攻击带来的迫在眉睫的威胁，我们认为迫切需要加强安全理事会的作用，并加强国际合作。在安全理事会一级，我们应考虑请秘书长定期报告不断演变的网络威胁，将网络安全纳入安理会议程主流，并像处理其他议程项目一样定期举行安全理事会会议。从中长期来看，我们可以采取行动，在安全理事会追究责任，处理违反国际法和危害国际和平与安全的网络活动。

至于国际合作的需要，我们要强调，网络威胁是全球性的。过去几年哥斯达黎加和特立尼达和多巴哥最近发生的勒索软件攻击事件就证明了这一点。勒索软件攻击事件导致这些国家宣布进入紧急状态。

大韩民国也继续受到网络攻击。就在本周，国防部遭到分布式拒绝服务攻击。我国政府几小时前宣布，在朝鲜向俄罗斯部署部队之后，亲俄罗斯黑客团体的网络攻击有所增加。

鉴于网络空间的跨国性质，我们的网络安全强度取决于其最薄弱的环节。因此，国际合作和能力建设，特别是与发展中国家的合作和能力建设，对于应对网络威胁至关重要。为此，我国政府目前正在参加由美国牵头的反勒索软件倡议，该倡议旨在提高全球意识，建立集体抵御勒索软件的能力。

大韩民国坚信，为了保持相关性，安全理事会应当更多地关注网络和人工智能等新兴技术带来的威胁。除了我们正在进行的努力，例如本周在第一委员会通过了大会关于军事领域人工智能的决议草案（A/C.1/79/L.77），并在首尔举行了2024年军事领域负责任人工智能峰会，大韩民国将继续在安全理事会中发挥应有的作用。

布洛喀·德罗比奇夫人（斯洛文尼亚）（*以英语发言*）：我要感谢谭德塞总干事和康拉多先生为今天的通报所作的宝贵贡献。

斯洛文尼亚是反勒索软件倡议成员。正是以这一身份，我们首先要提请安理会注意2021-2025年信息和通信技术安全和使用安全不限成员名额工作组最近的年度进展报告（见A/79/214）。在该报告中，联合国会员国对扰乱包括医疗保健部门在内的基本服务的勒索软件攻击的规模和严重性日益增加表示关切，而对医疗保健部门的这种攻击尤其危险和令人担忧。会员国还强调，此类攻击可能对国际和平与安全产生影响，需要采取全面的应对措施。

安理会维护国际和平与安全的首要责任将继续指导我们在安理会会议厅讨论网络相关问题时的立场。由于网络空间的独特性，这一问题是国际性的，很少受国界限制。因此，这是一个只有通过高度国际合作才能解决的问题。为履行这一责任，安理会必须积极参与应对勒索软件攻击造成的威胁，包括对医院和其它医疗设施和服务的威胁。

继冠状病毒病大流行和全球医疗保健组织快速数字化转型之后，勒索软件攻击越来越多地针对这些实体。国家和非国家行为体都有动机利用关键的医疗保健信息技术系统或破坏个人数据和健康数据的保密性。在许多情况下，非国家行为体受到政府的庇护，或甚至为其提供便利。对医疗设施和机构的勒索软件攻击直接威胁到公众健康、安全和安保。

由于此类攻击，诊断成像、病理学、急诊科、救护车服务和癌症护理都一直受到干扰。这不是一种没有受害者的犯罪；人的生命受到威胁。此类攻击当然也造成了经济损失，据估计，一个会员国医疗系统遭受的勒索软件攻击造成了约1亿美元的损失。这笔钱可以用来资助其它犯罪，甚至可能是恐怖主义。

人工智能的迅猛发展进一步加速了勒索软件攻击的实施，使国家和非国家行为体无需高超的技术就能实施此类攻击，有鉴于此，国际社会需要采取果断的应对措施，防止和减轻勒索软件攻击的影响。能力建设，特别是技术层面的能力建设，对于增强网络抵御能力至关重要。在这方面，斯洛文尼亚共同创建了西巴尔干区域网络能力中心及其培训员培训方案，该方案在过去一年半中成功地在西巴尔干开展了区域培训。

由于大多数勒索软件攻击具有跨界性质，安理会应在缓和紧张局势和促进追究责任方面发挥决定性作用，特别是在此类攻击危及安全甚至生命的情况下。我们还认为，安理会可以考虑将网络犯罪分子列入制裁制度。

最后，请允许我向安理会其他成员保证，我国坚定不移地致力于与它们以及联合国广大会员国协作，继续讨论勒索软件威胁的问题，这是国际和平与安全方面的一个共同关切。我们还坚定不移地致力于继续

执行旨在减轻这些风险的措施，包括执行现有的网络空间负责任国家行为规范。

涅边贾先生（俄罗斯联邦）（*以俄语发言*）：我们谨感谢世界卫生组织总干事谭德塞博士的通报。我们认真听取了非营利组织Ascension主席爱德华多·孔拉多先生的发言。

国际社会所有成员都清楚知道，俄罗斯联邦非常重视与使用信息和通信技术（信通技术）有关的安全问题。25年前，正是我国在联合国内发起了关于这一问题的讨论。俄罗斯是在联合国内建立专门谈判模式这一想法的推动者，其中包括目前成功的2021-2025年信息和通信技术安全和使用安全不限成员名额工作组。我们还启动了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，并于8月成功商定了一份文件草案（见A/AC.291/22/Rev.2）。

有各种包容性的专题机制来讨论与信息安全有关的问题，包括该领域现有和潜在的广泛威胁。因此，我们仍然不清楚是什么让我们有必要将讨论进一步扩大到安全理事会。我们今天还没有听到对这个问题的具体答复。此外，鉴于今天的活动是在很短的时间内提出的，我们还无法从发起者的发言中了解到是什么构成了对国际和平与安全的直接和具体威胁。安全理事会必须根据其授权优先处理的正是此类局势。

鉴于今天会议的重点是勒索软件问题，我们要指出，我提到的《联合国打击网络犯罪公约》草案旨在用与打击其他类型的信通技术相关罪行相同的力度打击使用此类恶意软件的行为，这些罪行都对公共和个人安全造成严重影响。我们敦促所有的同事把重点放在促进这一重要而实用的国际条约迅速生效上。此外，鉴于网络犯罪威胁的范围不断扩大，我们应该已经要考虑通过附加议定书来进一步发展《公约》。

关于确保保护包括医疗设施在内的关键基础设施免遭恶意使用信通技术的行为，俄罗斯完全了解此类风险。我国经常面临对医疗设施的网络攻击。自2022年初以来，我们一再经历了不同性质和规模的事件——从窃取患者的个人数据和计算机断层扫描仪瘫痪到黑客攻击儿童医院网站导致其崩溃。在许多情况下，乌克兰团体——特别是北约支持的乌克兰信息技术军——对此类攻击负有责任。

我们谨回顾，在政府专家组和不限成员名额工作组关于国际信通技术安全的工作框架内，已多次确认了关于必须确保为民众提供重要服务的设施安全的共识。相关规范也是在该框架内制定的。我们深信，对加强重要基础设施安全的最大贡献将是编纂相关安排，目前这些安排是自愿的，不具约束力。

为此，我们赞成迅速制定一项国际法律文书，涵盖确保信通技术使用安全的所有方面。在这一领域开展努力的最适当平台将是联合国主持下的常设谈判机制，该机制将在目前的不限成员名额工作组于2025年任期结束时设立。事实上，就在前天，大会第一委员会以协商一致方式通过了一项由新加坡提出的决议草案（A/C.1/79/L.13），该决议草案体现了这一共识。

回到我们对今天会议的附加价值的质疑上来，我们认为，重要的是要铭记，安全理事会对恶意使用信通技术问题的审议，特别是对具体事件的审议，因网络空间的具体特点而变得复杂。我们谈论的首先是网络空间的匿名性，这使得几乎不可能可靠地确定恶意活动的来源。在此背景下，任何诉诸所谓政治归因的企图都是极不具建设性的，甚至是危险的——实际上，这掩盖了一种陈腐的愿望，即保留对不利国家进行毫无根据且政治化指控的权利，当然，这是在没有提供任何证据的情况下进行的。

遗憾的是，今天的会议也不例外。美国再次决定利用安全理事会的平台来宣传其脱离现实的说法。关于所谓俄罗斯黑客的猜测和对我国涉嫌鼓励使用信通技术进行恶意活动的影射长期以来听起来像一个笑话，任何明智的人都只会一笑置之。

然而，华盛顿坚持诉诸这样的言辞，显然主要是为了吸引国内受众。甚至在周二的美国总统选举期间，臭名昭著的俄罗斯干涉理论也不时被抛到公共空间，尽管美国自己的网络安全和基础设施安全局表示没有

人试图恶意影响选举结果。然而，美国及其盟友继续积极利用关于假想的政治对手网络威胁的言论。我们已在相关论坛上多次澄清这种含沙射影的无稽之谈。

我们要回顾，在大会主持的讨论框架内，已经制定了切实可行的措施，以加强联合国会员国在信息安全领域的非政治化合作，包括在应对网络攻击方面的合作。我首先指的是在俄罗斯联邦倡议下于5月份推出的全球政府间联络点名录。该机制旨在预防和解决网络空间的严重事件，并减少危机情况下的紧张局势。如果发生恶意使用信通技术的严重事件，任何国家都可以使用这一工具。我们没有收到那些热衷于指责俄罗斯进行网络攻击的国家通过登记册提出的任何请求，这一点很说明问题。这再次表明，美国及其盟友没有技术证据来支持其调查结果。

与此同时，华盛顿自己也毫不犹豫地承认其利用信通技术对俄罗斯开展行动的事实，以及其在该领域增强进攻能力的事实。此外，美国情报机构正在广泛实施所谓的假旗行动。它们甚至针对其最亲密的盟友也在这样做，而这些盟友却如此积极地支持美国推行其侵略政策。

鉴于上述考虑，我们认为，今天的会议很难被视为对安理会时间和资源的合理利用。我们的讨论基本上可以归结为摆出众所周知的国家立场，重复在大会主持下开展的工作。如果我们的西方同事希望讨论医疗保健设施的安全问题，难道他们不认为我们首先应该讨论的不是来自网络空间的威胁，而是安全理事会需要商定具体步骤，以制止以色列对加沙地带医院的可怕、毫无意义的袭击，这些袭击正在造成数千人死亡？直到在现实世界实现这一目标之前，把安理会的注意力转移到虚拟世界似乎会适得其反，甚至是玩世不恭的。

我们呼吁所有具有建设性思维的国家继续积极参与关于国际信息和通信技术安全的全球讨论。我国仍然坚定致力于继续与整个国际社会对话，以期创造一个和平与安全的网络空间，包括通过在大会主持下，在专门的包容性机制框架内制定这一领域具有法律约束力的协议。我们希望，这种合作将使我们所有人能够对该领域的任何威胁作出有效的集体反应。

耿爽先生（中国）：我感谢世界卫生组织谭德塞总干事以及康拉德先生的通报。

我们身处一个日新月异的网络时代，在充分享受网络空间带来的发展机遇的同时，也面临复杂多样的网络安全挑战。网络攻击、网络犯罪和网络恐怖主义日益成为全球公害，勒索软件就是其中的一个突出问题。

勒索软件问题专业性强、技术性强，本质是网络犯罪问题，中方并不赞同有关成员仓促推动安理会讨论这一问题的作法，希望各方能在其他更为合适的平台开展更为专业、务实、深入的讨论。刚才通报人及一些成员在发言中列举了勒索软件攻击事例，中方主张国际社会从勒索软件产生的源头、传播的途径、变现的渠道等多个维度分析和处理这一问题，主张各国加强信息共享以及技术、执法、司法合作，共同努力加以应对。

勒索软件只是众多网络安全挑战之一。网络钓鱼、云系统入侵、个人数据窃取、分布式拒绝服务攻击等各种其他类型网络攻击也在快速增多，网络犯罪手法更趋多元化、系统化。中方主张加强网络安全治理、维护网络空间长治久安，呼吁各方从以下几个方面作出努力：

一是坚定维护网络空间和平属性，反对将网络空间定义为军事行动疆域、制定网络交战规则、构建网络军事同盟、将他国关键基础设施列为网络打击目标等错误作法，抵制网络军事化和网络军备竞赛，从根本上遏制包括勒索软件在内的进攻性网络技术的发展及扩散。

二是坚持以联合国为主渠道，在广泛、平等参与基础上，制定各方普遍接受的网络空间国际规则，摒弃以意识形态划线的“小圈子”，打造多边、透明、民主的全球治理体系，共同维护各国的网络安全。

三是坚持通过双多边合作打击网络犯罪和网络恐怖主义，对有关非法行为开展全方位、全链条打击，进一步健全各国执法司法协助合作机制。在此方面，中方欢迎今年8月达成的《联合国打击网络犯罪公约》。

四是加大对发展中国家维护网络安全能力建设的援助，积极开展人才培养、技术创新、预警防范、应急响应国际合作，补齐全球网络安全短板，不让任何一个国家掉队，不让任何一处网络空间成为法外之地。

网络空间关乎和平安全与民生福祉，中方愿同国际社会一道，共同探讨网络安全威胁与挑战的应对之策，为维护全球网络空间繁荣与稳定、构建网络空间命运共同体作出不懈努力。

阿丰索先生（莫桑比克）（*以英语发言*）：莫桑比克赞扬主席国联合王国提请安全理事会注意这样一个及时和重要的议题。我们感谢今天的通报人，即世界卫生组织总干事谭德塞博士和阿森松医保公司总裁爱德华多·康拉多先生所作的非常重要和富有洞察力的通报。

勒索软件已成为网络犯罪分子和恐怖主义网络的首选工具。这是一种犯罪活动，给缺乏先进网络安全资源的国家带来尤其严重的后果。正如我们从通报人那里听到的那样，医疗保健部门特别容易受到此类攻击，特别是在发展中国家，这些国家正日益依赖数字系统提供电子健康记录和诊断等基本服务，但往往没有必要的安全措施。在我们这些国家，像我们今天听到的这种扰乱可能是灾难性的，不仅威胁患者的安全，而且危及人的生命。对那些应对资源较少的国家来说，影响成倍增加。在发展中国家，勒索软件对我们的国家安全、基本公共服务的稳定性、经济复原力以及公众对治理的信任构成明显和现实的威胁。此外，跨境袭击加剧了地缘政治紧张局势，使发展中国家面临风险。这些袭击可能会在更广泛的网络冲突中造成附带损害。

人工智能和量子计算等新兴技术加剧了这一威胁。它们加剧了那些无法获得先进网络防御能力的国家面临的挑战，并在正在将世界推向数字军备竞赛。在这方面，莫桑比克等发展中国家面临着特殊的脆弱性。这是由于网络安全基础设施有限，监管框架不完善以及缺乏高质量的数字安全培训。当勒索软件攻击破坏医疗保健等关键部门时，恢复工作需要大量财政资源用于专家干预、系统升级，有时还需要支付赎金。对于预算已经十分紧张的国家来说，这些需求几乎是不可能完成的挑战。

出于这些原因，我们认为，在发展中国家应对勒索软件需要采取全面和有针对性的策略。这种方法必须首先强调预防。它还必须包括防备和响应，包括培训信息技术人员、更新过时的系统以及建立健全的监管政策和合作伙伴关系。预防措施——如定期软件更新、网络分段、零信任架构和员工网络钓鱼意识培训——至关重要，但这些措施往往需要能力建设支持。

考虑到勒索软件对各国经济的负面影响，莫桑比克一直在制定一个监管框架，以解决这一问题和整个网络犯罪问题。作为这些行动的一部分，我们可以强调网络犯罪法、数据保护法和网络安全法的起草工作。除立法方面外，莫桑比克一直在执行加强网络安全和复原力的机制，重点是在各级开展宣传和培训工作。

在全球层面，我们呼吁重点制定统一的网络安全标准并改进执法工作。任何国家都不应成为网络犯罪分子的避风港。更重要的是，我们认为迫切需要一个全球性的、强有力的法律框架，它应完全符合《联合国宪章》的宗旨和原则。

我们希望，今天的对话将成为加强国际合作和外交参与的一个步骤，以遏制和应对网络威胁。加强这些努力至关重要，有助于维护全球和平与安全，确保在这个数字时代没有任何国家落在后面、得不到保护。如同在威胁国际和平与安全的其他局势中一样，

我们也必须共同努力, 使网络空间变得安全和具有复原力。

豪里先生(瑞士)(*以法语发言*): 我要感谢世界卫生组织总干事谭德塞博士以及孔拉多先生所作的详细发言。

瑞士欢迎安全理事会重新关注网络安全这一重要问题。正如《未来契约》(大会第79/1号决议)所确认的, 网络空间的威胁, 特别是来自国家行为体或得到国家默许的威胁, 可能危及国际和平与安全。

信息和通信技术的发展带来了许多机遇, 这是不可否认的。利用系统漏洞进行恶意网络攻击的危险以及国家和非国家行为体五花八门, 也是众所周知的。其中, 针对医疗保健系统的勒索软件攻击是一个极其令人担忧的趋势, 自2020年以来在全球范围内不断增加。

医疗保健系统的数字化使医疗保健系统在造福民众方面取得了巨大进步, 但其网络基础设施正变得越来越复杂, 因此需要付出更高的安全成本。由于需要始终保持运行状态, 医疗保健提供机构本身以及公共机构的压力也随之增加。因此, 此类攻击是对国家关键基础设施和主权的一种特别卑劣的攻击。

最近有报道称, 一个由朝鲜民主主义人民共和国赞助的团体与Play勒索软件网络合作, 这引起了人们对安全问题的严重关切, 因为这可能导致全球范围内更广泛、更具破坏性的攻击。

让我强调三个方面。

首先, 我们重申, 国际法, 包括《联合国宪章》、关于人权的国际公约以及在武装冲突情况下的国际人道主义法, 也适用于网络空间并必须得到尊重。特别是, 瑞士认为经过长期发展的尽职调查原则已成为习惯国际法的一部分, 这一原则要求所有国家不得在知情的情况下允许其领土被用于违反其他国家权利的行动。这既适用于现实世界, 也适用于网络空间。呼吁各国尽职尽责, 防止犯罪团伙利用其信息和通信技术基础设施, 并开展国家和国际合作, 阻止此类团伙的活动。以协商一致方式通过的网络空间负责任国家行为框架也承认了这一原则。这些标准还要求各国不得在知情的情况下开展或支持针对卫生服务等关键基础设施的网络行动。

其次, 打击活跃在网络空间的犯罪团伙非常重要。最近的警察行动对这些团伙产生了相当大的影响, 但仅靠镇压并不能根除这一现象。各国必须行动起来, 采取适当措施, 防止其关键基础设施受到攻击。我们特别重视加强医疗保健部门在网络安全领域的复原力和安全性。

第三, 在这种常常是跨国性的背景下, 我们只有共同努力才能取得成功。必须鼓励所有国家开展国际合作和能力建设, 以提高全球网络生态系统的复原力和安全性。瑞士作为成员之一的国际反勒索软件倡议, 是这方面的一个重要论坛。各国还必须更充分地履行其在处理司法协助请求方面的国际义务, 以便在查明犯罪人的任何地方都能提起刑事诉讼。

在多边层面, 我要强调从国际安全角度看信息和电信领域的发展不限成员名额工作组的重要性。明年, 该工作组必须能够建议在大会内设立一个单一机制, 以便在近年来所取得成就的基础上继续开展工作。

“应对变局, 弘扬人道”是第三十四届红十字与红新月国际大会的主题。在这一主题下通过的决议之一强调了国际人道主义法在数字世界武装冲突背景下保护平民及其财产的重要性。

安全理事会也可以发挥作用。它必须促进尊重国际法和执行网络空间负责任的国家行为框架, 以便我们的人民能够受益于网络空间提供的巨大机会, 特别是受益于卫生领域的机会。

库德里先生(阿尔及利亚)(*以阿拉伯语发言*): 首先, 我要感谢谭德塞博士的宝贵通报。我也认真听取了孔拉多先生的通报。

黑客软件和人工智能的迅速出现和越来越快的发展，使得针对医疗设施的勒索软件攻击加倍激增。由于这一领域缺乏国际监管规范，风险正在放大。

最近，在阿尔及利亚的牵头下，成功缔结了《联合国打击为犯罪目的使用信息和通信技术行为公约》，表明了我们可以通过真正的多边合作能取得怎样的成果。

有两项关键原则至关重要。

首先，当前的网络安全做法，包括医疗网络安全做法，继续使全球不平等现象长期存在，并加剧了在人工智能所加持威胁面前的脆弱性。

其次，解决方案必须来自尊重所有国家主权和主权平等性的包容性多边进程。

因此，有必要应对五大基本挑战。

首先，我们必须解决技术霸权问题，因为发达国家、私营公司甚至个人垄断了网络安全能力和人工智能技术，使发展中国家的医疗保健系统不堪一击。

第二，我们必须应对单边行动的挑战，因为网络空间的主导权和人工智能的发展，通过设置技术壁垒，继续破坏国际合作。

第三，我们必须应对资源差异的挑战，因为在难以获得技术和专业知识的情况下，发展中国家必须竭力保护其医疗保健基础设施。

第四，我们必须应对不确定性的挑战，因为人工智能工具在为发展、国防和安全提供巨大潜力的同时，也可能被滥用，使针对医疗设施等目标的攻击更加复杂和普遍，而不是保护这些设施。

第五，我们必须应对重叠威胁的挑战，因为勒索软件攻击并不是针对个人数据的唯一危险，不透明和复杂的数据业务同样威胁着个人数据和隐私权。

上述霸权、非包容性、差异性、不确定性和人工智能混乱局面的表现模式都是相互关联的。

在这方面，我们强调三项具体措施。

首先，我们必须建立技术转让和能力建设的国际机制，确保民用设施普遍获得网络安全解决方案。

第二，我们必须制定标准化但可调整的网络安全协议，适用于处于不同发展阶段的国家，因为认识到“一刀切”的方法是无效的。

第三，我们必须针对发展中国家医疗保健系统的需求，制定负担得起的安全解决方案。国际社会必须在人工智能发展中优先考虑道德至上问题。

此外，我们必须致力于安全性和可控性。人工智能相关技术的开发和应用存在诸多不确定性，安全是必须坚守的底线。国际社会需要增强风险意识，建立有效的风险预警和应对机制，消除可控风险。

我们强调，南方国家的关切必须成为国际网络安全和人工智能框架的核心，而不是边缘事项。这不仅关乎公平，还关乎有效性。发展中国家的医疗保健系统往往面临独特的网络安全挑战，这需要量身定制的解决方案，而不是强加的标准。

总之，正如《网络犯罪公约》的成功所证明的那样，这一领域的前进道路需要通过包容性的多边进程采取近期和长期措施，所有行为体在平等的基础上共同努力。

世界应朝着技术更加平等、能力更加共享、多边合作更多、单边行动更少、强加的解决方案更少、包容性更强的方向发展。世界应朝着服务于人类而非危害人类的人工智能发展方向迈进。

我们医疗系统的安全不是富裕国家的特权。它是一项基本权利，必须得到保护并提供给所有国家的所有人。我们应共同努力，确保医疗保健网络安全和人工智能方面的技术进步不会成为扩大全球不平等的另一个因素。

卡努先生（塞拉利昂）（*以英语发言*）：我感谢世界卫生组织总干事谭德塞博士内容翔实的通报，并感谢Ascension总裁爱德华多·孔拉多先生提供的信息。

塞拉利昂在担任安全理事会成员期间，一直把应对国际和平与安全面临的新威胁和正在出现的威胁作为优先事项。因此，我们很高兴有机会讨论针对医院、医疗设施和服务的勒索软件攻击威胁不断上升这一重要问题，因为这种威胁有可能损害基本健康权，并威胁到全球应对公共卫生危机的斗争。

塞拉利昂坚定地认识到，包括勒索软件攻击在内的网络攻击对国际和平与安全构成日益严重的挑战，特别是当这些攻击针对医疗保健系统等关键基础设施时更是如此。这些攻击不仅造成广泛的破坏，而且危及生命，影响到最脆弱的群体，其危害在冲突地区、资源不足的环境中以及在大流行病等卫生紧急情况期间尤为严重。

对医疗保健系统的网络攻击，特别是勒索软件，无论是否出于经济利益和（或）社会政治破坏目的，都伺机利用我们对数字医疗干预措施的依赖，包括对与互联网连接的远程医疗、电子保健、虚拟通信平台和医疗系统管理仪表板的依赖。这种情况自冠状病毒疾病大流行提高了对医疗保健系统的需求以来，变得更加严重。对医疗保健系统的攻击还会损害人们更好利用保健和保健系统的机会。虽然依靠联网的电脑化医疗保健系统可以提高医疗保健管理的效率和成效，但这更容易遭受犯罪组织的网络攻击。这类犯罪组织对那些提供救生服务，但同时也存储了大量敏感数据和个人数据的医疗机构加以利用，从中牟利。

虽然勒索软件攻击的勒索金额在全世界各行各业都有所增加，但是世界卫生组织、国际刑警组织和一些会员国情报部门的报告显示，对医疗保健行业的攻击尤其狡诈。据报道，2024年上半年发生了数起对医疗保健网络的攻击事件。国际刑警组织的《2024年非洲网络威胁评估报告》指出，在接受调查的非洲国家中，近半数国家报告了针对其关键基础设施（包括医院）的勒索软件攻击。此外，近年来有多个国家报告，其医疗保健基础设施遭到攻击，导致患者数据丢失、基本医疗服务受到干扰，甚至造成死亡。这些攻击不仅具有犯罪性质，而且对公共卫生构成了明显和现实的危险，而公共卫生与国际和平与安全息息相关。

与非洲联盟的努力和区域努力相一致，塞拉利昂强烈主张必须采取协调一致的国际办法来打击网络犯罪，并加强我们卫生系统的抗御力。2020年的非洲联盟《网络安全和个人数据保护公约》强调，成员国之间必须开展协作、进行能力建设和知识共享，以防范和应对网络威胁。塞拉利昂承诺与这一框架保持一致，并与非洲联盟和广大国际社会一道努力，以提高非洲国家的网络安全能力。

我们还必须认识到，以多边参与方式来应对这些挑战很重要。联合国应通过所属各机构，包括通过反恐怖主义办公室和国际电信联盟发挥重要作用，提供合作平台、促进技术援助和推动制定负责任的国家网络空间行为国际规范。《全球数字契约》（见大会第79/1号决议）最近呼吁，必须把确保一个安全、包容和可持续的数字未来视为一个重要机会，藉此促进全球网络安全合作。塞拉利昂支持《契约》规定的原则，其中包括确保获得安全和有抗御力的数字基础设施，保障关键服务，以及促使所有行为体负责任地利用技术，其中包括私人和非国家行为体，他们往往在这些攻击中发挥作用。

有鉴于勒索软件对世界各地医疗保健业务和设施的攻击越来越猖獗，我们强调三个要点。

第一，如前所述，塞拉利昂认识到，利用勒索软件攻击医院和其他医疗业务是对国家安全乃至国际和平、安全与发展的威胁。获得优质医疗保健服务是全世界人民的基本需求，网络攻击扰乱这些服务，危及公众健康，使数百万人的生命和生计面临风险，并可能加剧不安全和冲突。最近，勒索软件攻击在世界各地造成混乱，令人揪心，我们已经听取了康拉多先生的通报。

在这个世界上，大多数三级医疗保健设施已经部分或完全数字化，如果这些系统蒙受损失，就会严重影响对病人的有效护理。如果我们考虑到对全球医疗机构和医学研究中心实施的攻击，全球健康和安全所

受的影响就更严重，因为这些机构和中心为世界上很大一部分人口的医疗保健服务提供支持，并从事生物毒素或感染源的医学研究，它们很容易遭到恐怖组织和犯罪组织的不当利用。

第二，包括勒索软件攻击在内的网络攻击具有跨界性质，其实施者往往没有国界、没有面孔、隐匿姓名，而受害者则分布在不同地域，这就需要在国际一级进行协作和协调。在区域一级，我们紧急呼吁提供支助，以落实非洲联盟的网络安全倡议，同时推行区域办法，确保非洲大陆的卫生基础设施免遭数字化威胁。

随着网络犯罪分子变得更有组织，使用更复杂的恶意软件，实施更有针对性的攻击，如攻击医疗设备而不是医疗网络和系统，我们打击这种威胁的努力必须结合可行和适当的立法、情报及执法措施。在国家一级采取有力行动必须依仗全球条约、法律和法规，这些条约、法律和法规不仅要建立行为规范，还要让违反者承担切实后果，从而确保将针对医院和医疗设施的网络安全威胁作为关乎国际和平与安全的严重问题来对待，并强调集体行动、问责和威慑。

塞拉利昂作为“国际反勒索软件倡议”的成员，继续通过我们于2021年颁布的《网络安全和犯罪法》等立法，致力于加强我们打击网络犯罪的国家应对系统。我们作为《欧洲委员会网络犯罪公约》签署国，欢迎大会设立的特设委员会在今年8月批准了《联合国打击网络犯罪公约》，据联合国毒品和犯罪问题办公室称，这是“具有里程碑意义的一步，是20多年来第一个打击犯罪的多边条约，也是网络空间威胁快速增长时期的第一个《联合国打击网络犯罪公约》”。

第三，也是最后一点，近年来，安全理事会发挥有益作用，支持各国和各机构制订措施来应对这一威胁，包括曝光这一威胁和扩大全球社会的知识库，以便作出知情决策。应当共享关于威胁和肇事者的信息，同时制定和利用预防性安全措施，包括酌情与私营部门合作，这是保护公众健康和安全的关键。同样重要的是，安理会必须确保遵守关于负责任地使用网络空间的既定规则、规范和原则。

鉴于各国在利用必要的财政、后勤和人力资源能力来充分应对网络攻击方面存在巨大差距，全球和区域合作机制必须包括在能力建设方面加强合作，其中包括分享技术和专门知识，特别是针对小国和发展中国家，以加深它们对这些威胁的认识，并采取措施打击这些威胁。

最后，塞拉利昂坚定地认为，由一个团结一致并且强有力的安理会来应对勒索软件攻击医院、医疗保健业务和设施所造成的威胁，是建立一个和平而安全的网络空间的关键。我们重申，我们主张在负责任国家行为、人权和《联合国宪章》基本原则的既定规范和原则范围内采取这方面的举措。

佩尔绍德女士（圭亚那）（*以英语发言*）：首先，我感谢世界卫生组织总干事谭德塞和康拉多先生的通报。

最近的统计数字显示，全世界勒索软件攻击的频率和规模都有惊人增加。针对关键基础设施，特别是医院和医疗保健设施的攻击，正在对公共卫生和国家安全造成严重影响。随着全球越来越多的医疗系统利用数字化转型来提高临床质量和服务成本效益，这类攻击的风险也在不断增加。

由于全世界的勒索软件越来越容易获得，威胁行为体也越来越多，我们看到针对医疗机构的勒索软件攻击规模不断扩大，除了导致机密数据被盗之外，还对医疗机构的运营和医疗服务供给产生不利影响。除了干扰医疗服务的提供和因网络中断造成的财务影响外，在某些情况下，当紧急治疗受到影响时，勒索软件的攻击还导致生命损失。

鉴于勒索软件的攻击可能对国家医疗系统的稳定性造成破坏性影响，因此必须优先制定强有力的框架来抗御此类攻击。各国必须更加紧迫地行动起来，采取积极主动的整体方法来应对此类攻击，同时认识到这些攻击超越国界，任何国家都不能幸免。

在这方面，我要强调以下几点。

首先，各国必须投资于能力建设举措，并制定应对事件计划。许多发展中国家缺乏必要的资源和专业知识，难以保护自己免受勒索软件攻击等网络威胁以及打击此种威胁。因此，在这些国家建设能力至关重要。这应包括提供技术援助、资金支持和培训，以提高脆弱国家的应对能力，包括制定应对事件计划，有效应对这些袭击。

第二，鉴于勒索软件攻击的规模不断扩大，后果日益严重，圭亚那强调，必须促进国家间的合作，分享最佳做法和挑战方面的知识，交流信息，并开展技术转让。在这方面，至关重要的是，必须建立一个国际信息共享系统，向各国提供信息，说明它们可以如何加强和保护重要的卫生基础设施，使其免受勒索软件的攻击，以便能够及时发现和解决这些问题。此外，必须建立一个全球框架，在各国和相关利益攸关方之间共享关于潜在网络威胁的此类情报。

第三，必须对勒索软件攻击的肇事者追究责任。必须优先重视开展合作和建立伙伴关系，以调查和起诉网络犯罪，包括跨国家和跨区域的勒索软件攻击。这应该包括摧毁勒索软件网络，并监控涉嫌勒索软件的支付交易。最近通过的《联合国打击网络犯罪公约》为处理此类犯罪提供了监管和合作框架，从而为这一努力做出了贡献。此外，圭亚那确认国际法适用于网络空间。

医院、医疗保健设施和服务应被视为是神圣不可侵犯的，必须尽一切努力保护它们免受勒索软件的攻击。国际社会必须联合起来，防止对重要国家基础设施的一切形式的网络攻击。圭亚那仍然致力于寻求提高对这一威胁的认识和应对这一威胁的全球倡议，并确保这一威胁不会破坏国际和平与安全。

蒙塔尔沃·索萨先生（厄瓜多尔）（*以西班牙语发言*）：我感谢世界卫生组织总干事谭德塞博士的重要通报。我国代表团还要感谢Eduardo Conrado先生，我们认真听取了他的通报。

针对卫生部门的勒索软件攻击不仅使卫生系统的完整性面临风险，还威胁到人的生命。这些袭击破坏关键服务，限制获得基本医疗服务的机会，影响了公共健康，因此对国际和平与安全构成威胁。2024年7月信息和通信技术安全和使用安全不限成员名额工作组第三次年度进展报告强调指出，各国日益关注这种攻击日益增加的频率、规模和严重性。正如我国代表团在大韩民国倡议下于今年6月举行的公开辩论中指出的那样（见S/PV.9662），安全理事会在应对不断变化的网络威胁方面绝不能落后。

厄瓜多尔多次指出，我们认为预防是建设和平的基石。同样，安全理事会的产品中，也应该包括利用技术和战略打击恶意使用网络的能力建设，以补充全球努力。

如果一个会员国不安全，就没有一个会员国会是安全的。今天我们面临的威胁在很大程度上具有跨国性质，在实体领域和网络空间应对这些威胁的唯一途径是开展国际合作。网络安全是一项全球性挑战，需要整个国际社会采取全面、协调和合作的对策。因此，我国代表团支持任何有利于加强国际合作的机制，以减少各国执行负责任行为规则能力不对称的现象，并采取措施加强各国保护重要基础设施的能力。现有的规范必须得到加强，以考虑到技术的快速发展。

厄瓜多尔重申，我们致力于建设一个安全、开放与和平的网络空间，让技术成为发展的工具。所有国家都有义务加强多边主义，必须促进国际和平与安全，建立一个尊重人的尊严的数字环境。国际法和国际人道主义法适用于网络空间。

最后，我要指出，必须维护和促进负责任地使用信息和通信技术的做法，这是确保网络空间稳定和安全的关键。

主席（*以英语发言*）：我现在将以联合王国代表的身份发言。

我感谢谭德塞博士和Conrado先生今天向我们通报情况。

今年早些时候，在大会信息和通信技术安全和使用安全不限成员名额工作组中，所有国家都认识到勒索软件攻击可能对国际和平与安全产生影响。勒索软件行为体一直在攻击重要的国家基础设施、地方政府和医院，以牟取个人经济利益。大多数此种团伙存在于允许它们不受惩罚地活动的管辖区。我们呼吁这些国家采取进一步行动，打击以其领土为基地或利用其领土的犯罪团伙。

与今天在座的许多国家一样，联合王国继续遭受勒索软件事件侵害。2017年，我们的国民医疗服务体系受到Wannacry勒索软件病毒的感染，恢复工作花费了1.18亿美元。这笔钱本可用以拯救生命。今年，伦敦医院的一家关键供应商受到了勒索病毒事件的影响，该事件导致推迟了10000多个保健预约和1700多个医疗手术。我国各个关键部门都发生过此种破坏事件。因此，我们认为勒索软件是对国家安全最重大的网络威胁之一。为了应对这一问题，联合王国正在努力打破勒索软件的商业模式，并劝阻受害者向罪犯付费。联合王国与国际伙伴一道，对参与此类活动的行为体实施了36项制裁。然而，我们需要对这一全球威胁采取全球应对措施。

首先，我们敦促其他国家加入联合王国政府的行列，不要支付赎金。10月份，联合王国和国际反勒索软件倡议其他49个成员签署了一份公开声明，承诺政府不支付赎金。

第二，协调将是我们最好的防御。最近，联合王国执法部门领导了一个全球执法机构联盟，以瓦解2024年最活跃的Lockbit勒索软件集团。

第三，我们必须分享信息，说明各种威胁并建立集体理解，从而提高对这些攻击的抵御能力。我们将继续与国际合作伙伴和行业合作，打击勒索软件，摧毁网络犯罪生态系统。

我现在恢复行使安理会主席的职能。

我现在请兰布里尼蒂斯先生发言。

兰布里尼蒂斯先生（*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、塞尔维亚、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和格鲁吉亚赞同这一发言。

当医院、实验室和急救服务因勒索软件而瘫痪时，其影响不仅仅局限于任何单一国家，会使患者的生命面临危险，破坏医疗保健系统的稳定，并削弱人们对基本公共服务的信任。每11秒钟就有一次勒索软件攻击发生，预计到2031年，这一速度将上升到每2秒钟一次。勒索软件的全球性及其对国际和平与安全的潜在影响要求我们采取果断的集体应对措施，以防止今后的伤害。

为了防止这一威胁，欧洲联盟正在采取强有力的行动来保护包括医疗保健在内的关键基础设施和基本服务。我们正在加强防御，增加应对措施，并加强国际伙伴关系，以应对勒索软件数量不断上升的问题。2022年12月通过的欧盟网络和信息安全指令规定了欧盟各关键部门的网络安全风险管理和事件报告要求，并确认卫生是“高度关键部门”。这确保了卫生设施的网络安全要求。这些措施旨在保护我们的医疗保健，确保敏感医疗数据的安全，并确保基本服务在遭受网络攻击的情况下仍能正常运行。换句话说，我们认识到勒索软件是一个严重威胁，并重申了这一问题在欧盟政治议程上的紧迫性。

除了预防之外，我们还加强了对恶意网络活动，特别是勒索软件攻击的应对措施。今年6月，欧盟对与勒索软件活动有关的个人实施了限制措施。此外，2月，欧盟网络犯罪中心与国际合作伙伴共同发起了一项行动，以瓦解全球最猖獗的勒索软件运营商之一LockBit勒索软件集团。我们正在采取行动，利用我们所掌握的一切手段来对付那些蓄意破坏关键服务的人。我们还强烈呼吁所有国家根据联合国负责任国家行为框架，不要允许其领土被用于此类恶意活动，并对减少此类活动的适当请求作出回应。

最后，我们将继续加强伙伴关系，通过支持制定国家网络安全战略和改善危机管理等欧盟能力建设举措，来应对勒索软件的威胁。建立一个联合国常设机制——一个联合国网络行动纲领——将使我们能够提高集体能力，应对勒索软件等对我们社会和经济的威胁。欧洲联盟随时准备继续与国际社会以及私营部门合作，保护关键基础设施，特别是医疗保健，使其免受网络威胁。我们可以通过团结、协调一致的全球办法，共同有效应对勒索软件不断升级的威胁。

中午12时05分散会。