JIU/REP/2021/3

联合国

联合国系统各组织的网络安全

联合检查组的报告

撰写人：豪尔赫·弗洛雷斯·卡列哈斯、艾莎·阿菲菲和尼古拉·洛津斯基

GE.21-14702 (C) 090322 110422

JIU/REP/2021/3

Chinese
Original: English

联合国系统各组织的网络安全

联合检查组的报告

撰写人：豪尔赫·弗洛雷斯·卡列哈斯、艾莎·阿菲菲和尼古拉·洛津斯基

联合国 • 日内瓦，**2021** 年

项目团队：

检查专员豪尔赫·弗洛雷斯·卡列哈斯、艾莎·阿菲菲、尼古拉·洛津斯基

评价和检查干事 Vincent Hermie

协理评价和检查干事 Szilvia Petkov

研究助理 Hervé Baudat

咨询顾问 Dejan Dincic

实习生 Charlotte Claveau、Alina Datsii、Bianca Canevari

执行摘要

联合国系统各组织的网络安全

在当今的数字化世界，网络安全已经成为各国际组织的重要事项，联合国也不例外。数字化转型，对信通技术和借助网络的解决方案的依赖日益增强，网络威胁的复杂程度和破坏潜力不断增加，导致联合国系统面临的网络安全风险空前增大。尽管网络安全问题最初出现在信通技术领域，但鉴于信息管理系统深深植根于大多数业务活动，威胁格局也发生了很大变化，从而需要超越单纯的技术驱动的防御，仅从信通技术的局限角度审视网络安全似乎已不再可行。在本报告中，检查专员主张将网络安全考量纳入更广泛的组织框架，譬如企业风险管理、业务连续性规划、安全和安保，并主张将网络安全问题纳入整个组织的主流。

近年来，联合国系统越来越深入地认识到网络安全需要关注。的确，网络安全态势薄弱的潜在后果不仅限于信通技术基础设施和系统受到破坏，或者数据量最终遭到泄漏。联合国系统各组织履行任务的能力以及对于成员和受益者的信誉都会岌岌可危。此外，联合国系统各组织掌握着与许多类型的个人有关的数据，一旦数据泄露，当事人可能会面临严重的不利后果。网络攻击对任务和结构各异的组织产生的影响可能并不相同，但威胁是真实的、共同的。无论准备多么充分，无论多么警惕，任何组织都不能奢望永远不会经历网络安全事件。此外，如果忽视这些风险，可能会在声誉、运作、法律和财务方面产生相当大的影响。

本次审查的目标和报告的结构

本次审查的主要目标是：(a) 查明和分析联合国系统各组织作为个体所面临的共同网络安全挑战和风险，以及这些组织各自的应对，同时考虑到各组织在具体情况下的要求(纵向视角)；(b) 考察目前促进以全系统办法处理网络安全的机构间动态，以便改善联合国系统各组织之间的协调、协作和信息共享，并酌情考察共享解决方案的可能性(横向视角)。

检查专员以参加组织提供的自我评估为基础，首先在第二章中概述了联合国系统面临的网络安全格局，描述了最普遍的威胁类型和攻击手段，并说明了据报告这些威胁和攻击的影响，同时提请注意供进一步审议的选定技术问题。在第三章中，检查专员参照审查过程中确定的促进组织网络复原力的一系列关键要素，考察联合国系统各组织的体制安排和相关做法，并酌情强调良好做法。第四章侧重讨论旨在促进联合国系统各组织之间协调和协作的机构间机制，以及在共享网络安全解决方案具有合理性的情况下，促成制定和实施这种解决方案的业务能力。专家们一致认为，应对措施必须基于各组织自身的特点和要求(取决于组织的任务、拥有或管理的信息、风险暴露、资源等)。与此同时，联合国系统各组织并不是孤立运作，而是在许多方面相互联系，包括联合拟订方案，在任务和活动方面也有一定程度的相互依赖。因此，至关重要的是认识到哪些领域面临共同风险，并探索哪些领域适合采取协同办法。

联合国系统内的网络安全

联合国系统各组织不论大小，没有一个组织可以声称从未遭受过某种形式的网络攻击。针对信息系统用户的恶意行为(通过“网络钓鱼”、盗用身份、“中间人”骗局等)或针对基础设施的恶意行为(恶意软件、分布式拒绝服务攻击等)是到目前为止报告的最普遍的威胁来源。虽然网络安全威胁通常与复杂的技术操作有关，但专家界看到一种明显的转变，即黑客从攻击服务器、网络和终端设备转向攻击人，这些黑客为追求欺诈和其他非法目的，使用旨在操纵个人，使之泄露敏感信息的社会工程手段。2019 冠状病毒病(COVID-19)大流行进一步加剧了与社会工程相关的风险：超过三分之二的参加组织报告，全球封锁导致许多用户与集中管理的网络安全资源断开联系，在此期间，网络安全威胁和漏洞急剧增加。

与此同时，据报告，参加组织经历的事件影响有限，这可能导致过早得出结论认为网络安全不致引起严重关切。而这并不是检查专员得出的结论。首先，收集的数据必然隐含一些盲点，原因包括对于暴露已知脆弱性的可以理解的疑虑，更普遍的原因是网络活动的不透明性质，这表明，威胁的确切规模和相关后果可能根本不为人知。大多数时候，特别是在实施较复杂攻击的情况下，对手无意透露自己的存在或利用的漏洞，这表明，系统入侵和数据泄露的数量可能比所报告的数量高得多。与已知的网络安全威胁规模相比，“已知的未知”比例很大，但“未知的未知”比例之高可能更令人关切。因此，根据以往发生的已知程度来判断威胁的严重性会受到误导。造成损害的可能性仍然很高，需要持续关注并确定优先顺序。

各组织在成熟度和技术准备的特定方面存在差异

本次审查不是要全面评估各个参加组织的运作安排或技术基础设施的稳健性，而是要了解现有的一般能力，并找出一些可能值得特别关注的共同问题。由于与本次审查的主题有关的显而易见的原因，检查专员选择不披露具体的组织安排，那样做有可能损害有关实体的安全。联合检查组铭记，主要通过自我评估收集的资料存在固有的局限性，而且答复者提供的资料在详细程度上差别很大，它观察到，参加组织各自采取的应对网络安全威胁的办法有显著差异，因此，这些组织网络安全态势的成熟度也有显著差异。这些差异可以参照以下方面解释：每个组织的运作环境；所持有的数据类型产生的要求；领导层对网络安全的理解程度和重视程度；各组织自身的既往观点；资源的可用性；整个联合国系统使用的信通技术系统、工具和软件解决方案多种多样。

参加组织认为自己已充分了解网络安全的核心技术方面，并根据各自的能力进行了投资。关于技术和业务能力，检查专员的分析仅限于强调一系列可能值得给予更集中关注的问题，譬如：终端设备管理和便利远程工作的工具，特别是在 COVID-19 大流行的情况下；与过去采购的或在内部逐步搭建的旧系统的残留部分相关的风险，新的安全扫描和修复可能不再支持这些系统；云计算的使用继续扩大；漏洞管理的组织安排；影子信息技术(影子 IT)做法，涉及到使用和实施组织信通技术框架之外的技术工具。应当指出，尽管遇到了许多挑战，但大流行的暴发也促进了一些积极的事态发展。联合国各实体被迫更加仔细地审视其安全管理框架，并在迫切需求的推动下，开始落实所规划的组织信通技术项目。可以

说，在非常短的时间里大规模转向远程工作，导致许多组织加快了改善远程访问安全性的努力，而且可能提供了激励这方面行动所亟需的动力。

有助于提高网络复原力的要素

检查专员考察了一系列可能改善联合国系统各组织整体网络安全态势的要素，并考察了联合国系统各组织识别、预防和检测网络威胁以及应对并从事件中恢复的能力。需要采取多元做法，并使组织的所有层级参与进来，包括：立法和理事机构；监督机制；行政管理层；行政、实务或业务单位的中层管理人员；以及一般工作人员。此外，该领域的交叉性质要求将视野扩展到信通技术之外，将网络安全牢固嵌入企业风险管理，并力求使实体安保与网络安全进一步趋同。最后但也同样重要的是，专门的内部人力资源能力辅以外部供应商提供的服务，以处理特定的临时需求，加上与各组织需求相称的财政资源分配，构成稳固的网络安全态势的支柱。总而言之，这些要素在多大程度上反映在组织的网络安全方法中，直接影响组织的网络复原力。因此，检查专员建议各行政首长启动一次全组织审查，以考察下文进一步详细说明的各项要素在多大程度上纳入了组织的政策和实践，并向立法和理事机构报告结果，以期获得关于如何进一步加强网络复原力的指导，同时考虑到在这一过程中查明的强点和弱点(建议 1 和建议 2)。

立法和理事机构提供战略指导和资源

在联合国系统，网络安全仍然主要被视为技术问题，这或许可以解释，为什么在大多数组织，立法和理事机构被要求参与或者本身呼吁参与该议题的程度到目前为止是有限的。鉴于本报告确定的网络安全的更广泛层面，检查专员认为，立法和理事机构应进一步参与这一事项，并提供高级别战略指导，包括通过拟定明确的风险偏好陈述书和确定相应的资源分配，以促进达到理想的保护水平。更广泛地说，行政管理层应当思考，如何在认为必要和充分的范围内，并在不损害有关组织的防御的情况下，定期向立法和理事机构报告网络安全事项，并利用定期报告促进与这些机构的互动。考虑到网络安全事件的突发性和潜在的重大影响，检查专员还建议各组织预先设想将事件的升级呈报立法和理事机构的必要性以及在需要呈报的情况下须遵循的程序，各组织内部以及立法和理事机构的成员都应这样做。

监督机构的关注有助于加强网络安全措施

审查发现，联合国系统各组织的内部和外部监督机制一直关注网络安全事项，即使在这些机制的任务授权中没有具体提及网络安全事项的情况下也是如此。检查专员发现，有几个实例表明，一些从整体上加强参加组织网络安全框架的举措源自监督建议(例如设立首席信息安全干事职位，建议开展培训，制定可行的路线图等)。事实上，各个审计和监督委员会处理网络安全问题时，不是将其置于信通技术治理的范围内，而是将其作为涵盖整体企业风险管理任务的一部分。这些委员会接纳网络安全议题值得称许，这不仅有助于为管理层提供支持，而且可以通过这种方式向立法和理事机构通报相关的网络安全风险，使立法和理事机构推动减轻组织风险。为确保所有监督机构在网络安全方面最大限度地增加

价值，必须利用组织内部网络安全专家的知识和经验，为监督职能的工作提供信息和投入。

监管框架、合规和问责

各参加组织参考一系列广泛的与网络安全有关的行业标准，有时不止参考一项标准，其中大多数组织要么已经取得 ISO 27001 认证，要么计划取得认证，或者选择在不寻求正式认证的情况下自愿使组织框架与该标准保持一致。检查专员不主张在这方面采用单一的行业标准或统一的全系统办法，因为不同的标准可以有效地服务于不同的目的，并提供对应不同成熟度水平的适当选择。尽管如此，在建立和管理自己的监管框架时，有充分的理由以正式或非正式的方式从相关的行业标准中汲取灵感。因此，各参加组织必须进行适当的、针对具体组织的网络安全风险评估，根据这种评估查明的要求和风险，并基于与自身情况相匹配的所需保护水平，确定适当的标准，并在该标准的范围内，确定最切合实际的控制。

几项主要的行业标准要求有具体的网络安全政策和形成文件的程序，作为支撑实体网络安全方法的各项控制的重要支柱。除少数组织以外，参加组织可以说已经认识到，必须建立明确的参照框架来指导处理网络安全的办法。高级别的信通技术战略一般包括网络安全考虑，尽管详尽程度不一。超过三分之二的参加组织制定了具体针对网络安全的文书，其中三个组织目前正在修订框架，四个组织正在制定专门的政策。与此同时，四个参加组织的网络安全职能，包括相关的监管框架，被认为至多算是刚刚起步。遵从现有指南，尤其是如果出现不遵从的情况如何实施强制执行，这一问题令人不太确信整个联合国系统存在组织网络安全文化。检查专员认为，有必要更加仔细地审视这一问题，并采取更加细致的办法，以强化对违规行为的问责，并更加广泛地保护各组织。

网络安全文化从领导层向下渗透

灌输网络安全文化的第一步是高级领导层自身意识到相关风险，并理解不良网络卫生产生的影响。这要求高级管理人员采取更积极的立场，确保建立内部治理机制，使之为高级管理人员提供所需的信息和证据基础。行政管理层在这方面的作用不仅限于就资源分配作决策。一项关键因素是鼓励一种内部文化，在这种文化中，承认事件的发生和主动跟踪发生的情况不被视为承认失败，而被视为联手处理共同问题和更好地保护组织及其资产的起点。行政管理层还可以通过以下具体方式，自上而下地激励行动和影响思维模式，即树立推荐的行为模式，确保在整个组织实现管理层问责，参与提高认识方案，在整体网络安全事项上表现出参与式的领导风格。联合国系统需要文化转变，高级管理人员在自上而下确定基调方面的贡献对于实现这种转变至关重要。

将网络安全作为全组织努力纳入主流

对于网络安全责任不能仅由信通技术部门承担的认识逐渐加深，在这种趋势下，大多数参加组织以某种方式承认，行政部门和实务部门都应发挥作用。然而，本次审查期间收集的资料表明，各组织单位可能仍然不能充分接受，在设计和执行项目和活动时，将网络安全和复原力要求纳入其中。在一些组织单位，网

络安全政策和程序据说被视为业务灵活性和效率的障碍，而不是被视为组织声誉和资产的护盾。尤为重要的是，行政首长应积极反对这种看法。更加明确方案和行政职能的网络安全层面，能够减少对不同部门互补作用和责任的误解，并能够处理在本次审查期间发现的一些利益攸关方缺乏自主性的问题。将网络安全考虑纳入指导所有部门工作的政策和实践的主流，本身就是承认一个组织的每一项职能都可以为实现以全组织办法处理网络安全事项作出贡献。

工作人员作为第一道防线

教育每一名工作人员了解自己在保护组织的信息和数字资产方面发挥的作用，并了解恪守网络安全政策、程序和最佳做法的重要性，这是一个持续存在的挑战。人的因素不仅在整体网络安全威胁格局中越发重要(对于攻击越来越多地指向个人最终用户的全球关切便反映了这一点)，而且是参加组织防御结构中一项重要因素，前提是这些用户接受适当的教育。尽管资源有限，用户对培训感到疲惫，而且难以跟上主题事项的不断演变，但认识到网络安全保护的责任始于知情而警惕的用户，催生了在培训和提高认识举措方面所作的重大努力。尽管如此，大量的方案和具体的举措似乎没有以一致、系统或基于风险的方式推进。因此，检查专员建议各组织设法制定全面的培训和提高认识方案，将这些方案作为改变内部文化的积极工具，途径是根据各类利益攸关方可能对组织构成的风险，确定针对各类利益攸关方的明确目标，而不是在没有战略远景指导的情况下向每个人提供单独的模块。关注偶尔使用组织信通技术系统的用户，包括会议代表、实习生、访客和其他非工作人员类别的人员至关重要，因为这些用户通常使用个人设备登录机构基础设施。此外，这些用户不经常使用相关系统，不太可能熟练掌握如何根据适用的组织政策和做法，正确和安全地使用这些系统。

优化网络安全支出和投资

对目前专门用于网络安全的资源进行估计并非易事，原因在于联合国系统各组织财务和预算框架的特点以及各组织管理和核算这类资源的做法。不言而喻，可提供良好保护的网络安全框架需要投资。尽管分配给网络安全的资源据报有所增加，但联合国系统的从业人员仍然认为，资源短缺对各组织涵盖网络复原力的所有方面构成障碍。需要考虑的重要问题是，网络安全支出的金额并不能自动反映保护水平。关键不在于争论金额的多少，而在于决定资源应当如何分配，以产生最积极的影响。无论可用资金的金额有多少，所收集的信息表明联合国系统各组织在确定网络支出方面的优先顺序时并未采取一致的办法，因而增加了低效利用本已稀缺的资源的风险。为优化网络安全支出以及相关投资，全面的网络风险评估是争取立法和理事机构的支持并获得水平充足的资源分配的先决条件，该评估最终应形成一项业务论证，详细说明成本、效益、风险和预计节省的费用，并与不投资所造成的潜在财务影响相对照。

网络安全方面的内部专业能力

一半以上的参加组织在内部建立了专门和专用的人力资源能力，从一名信息安全专家(有时仅为非全职)，到由首席信息安全干事领导的较大的组织单位，规模不等。而在 10 个参加组织中，网络安全任务主要由信通技术干事处理，信通技术干事同时还履行其他职责。在网络安全领域，由于技术性质复杂，使用外

部知识专长的情况很常见，该领域不断演进，所需的专业化程度相当高，使专业能力长期保持可用和不落伍具有挑战性，而且费用高昂。为对网络空间的快速发展保持灵敏反应，借助外部提供者提升和补充内部能力不可避免，甚至是可取的。在多大程度上借助外部能力，可由各个组织根据自身的需要和环境酌情判断。然而，检查专员认为，各组织必须在内部保持适当程度的控制、监督和技术能力，以有效管理外部提供者贡献的能力并与之对接。在这方面，如果能够依靠专门的首席信息安全干事职能，可以为网络安全目的提供所需的集中性和保证。首席信息安全干事职责范围内的核心职能不仅限于在业务层级制定控制措施，还默认包括管理层面，以确保尽可能充分反映出网络安全考量属于组织风险和复原力管理事项。

检查专员注意到各参加组织的内部设置存在差异，这种差异更多可能是表明所面临的制约，而不是深思熟虑或战略性的选择，因此检查专员认为，内部有专用和专门的网络安全知识专长可用，有助于加强该组织以及整个系统的网络安全态势，是一项值得考虑的投资。此外，各组织应审慎评估寻求建立安全行动中心(即使是最基本的形式)是否可以使组织获益，这种评估应基于针对具体组织的成本效益分析，所涉参数包括相关组织信通技术基础设施设置的复杂性，所管理的关键资产和流程的数量和类型，总体数据流量，由此决定的威胁发生频率以及其他因素。正式的安全行动中心不论规模和能力如何，其重要方面之一都是充当日常监测行动，发挥关键的协调和同步作用以及提高组织认识的聚焦点，这可能对内部资源和能力的有效分配产生重大影响。

网络安全——全系统优先事项？

会员国和行政管理层多年来作为优先事项强调，应通过在战略层面加深各组织之间的协调与合作，并通过加强全系统业务能力，强化联合国系统的网络安全态势。然而，尽管系统内有一些可用的重要资源、机制和倡议，包括明显的政治意愿，但在将这些豪言壮语变为现实方面，取得的进展并不太明显。迄今为止，没有一个实体正式负责推动与统一的网络安全方法有关的议程，全系统的网络安全努力从体制上说集中于联合国系统行政首长协调理事会之下的各项机构间协调机制，从业务上说，在一定程度上由联合国国际电子计算中心支持，该中心为联合国系统的一些组织提供共享网络安全服务。检查专员在本次审查中发现，全系统战略方向与业务能力之间的联系不足，影响了这些结构之间的互动，可能会使系统错失开展更直接合作的机会，从而付出无法实现增效的沉重代价。

需要确定基本的保护水平和商定的最低防御要求

人们普遍承认，一个组织对网络威胁的防御不力，会使整个系统更加脆弱。因此可以说，联合国系统的强大程度受其最薄弱的环节制约。然而，以往旨在在各组织之间引入共同基准或相对成熟度评估的举措未得到充分支持，批评者指出，结构设置的多样性以及各组织运作的背景是一种障碍，限制了这种集体或累积办法的价值。此外，由于保密原因和担心暴露漏洞，哪怕是在组织之间暴露漏洞，参加组织的高层人员对于共享内部网络安全信息兴趣寥寥。这些关切可以通过可提供适当保障的信息共享协议缓解。然而，为预防、检测和应对网络威胁而建立全系统业务能力的尝试尚未取得切实成果。联合国国际电子计算中心填补了这方面的一些空白，该中心的网络安全服务组合吸引了相当大的客户群，但是

否使用服务由各组织自行选择，因此该中心只能部分满足联合国系统的需要。无论在概念方面还是在业务方面，全系统采取共同或协同办法的努力迄今为止都收效有限，但检查专员认为，为联合国各组织，从而为整个系统确定基本保护水平和最低防御要求，仍然是值得继续追求的合理目标。

处理网络安全的机构间机制

审查发现，处理网络安全的机构间机制设立已久，大体上能够发挥作用，在该机制的推动下，信息共享和全系统专业交流已经达到坚实的水平，但除此以外，该机制为自己设定的一些雄心勃勃的目标尚未转化为切实的成果。数字和技术网及管理问题高级别委员会的记录证明，在至少 30 年的时间里，网络安全在全系统议程中占据较为突出的地位。自 2011 年以来，在数字和技术网下运作的信息安全特别利益小组一直是促进机构间合作与协作以优化成员组织内信息安全的主要机制。根据信息安全特别利益小组的职权范围，该小组的主要宗旨是知识共享，不过，这些职权范围在 2018 年修订后，也强调该小组在开展合办项目方面的作用——在数字和技术网呼吁信息安全特别利益小组更加积极地设计和交付共享解决方案和创新之后，这一愿景进一步放大。检查专员肯定该小组的专业信誉和多年来产生的大量成果，但认为联合国系统的大规模共享解决方案没有按规定实现。信息安全特别利益小组作为协调机构，在这方面面临与任何其他机构间机制相同的挑战，该小组没有决策权，无法在系统一级直接要求采取行动，这就是为何期望在该论坛内实现落实是不现实的。信息安全特别利益小组的影响在一定程度上受到以下因素制约：该小组依赖其召集的组织的个体参与和后续行动；小组成员在各自的体制架构内被赋予的权能不均衡；该小组不具有执行所达成协议或所提出建议的业务能力。此外，该小组隶属数字和通信技术网，因而体现了在大多数组织内观察到的普遍设置，即首席信息安全干事向各自的信通技术部门主管报告工作，同时具有这种设置所包含的种种优势和局限性。

联合国国际电子计算中心作为联合国系统网络安全服务的主要提供者

联合国国际电子计算中心多年来一直在向联合国系统约三分之二的组织提供网络安全服务，尽管该中心 13 项相关服务的各自客户群千差万别。该中心服务目录中的网络安全服务领域出现了显著和多元的增长，尽管按预算计算，这一领域仍然仅占该中心业务的一小部分。各参加组织对联合国国际电子计算中心网络安全服务的评估结果不一，共同安全威胁情报服务被认为是该中心的旗舰服务。联检组 2019 年就已倡导更好地利用该中心尚未发挥的潜力，特别是在网络安全服务方面的潜力。鼓励联合国系统各组织与该中心寻找更多共同点，以更多的共享服务补充各组织现有的内部能力。本着这种精神，请各参加组织的行政首长重新考虑现有的组织安排，并重新审视利用该中心网络安全服务的机会。联合国国际电子计算中心作为在世界卫生组织规则和行政框架下运作的机构间设施，业务模式基于成本回收和共享服务模式。事实证明，这种结合对该中心成为联合国系统网络安全枢纽既起到推动作用又构成了阻碍。由此造成的情况是，该中心提供的服务依赖客户提供种子资金来预先支付开发新服务以满足需求所需的费用，而许多客户仅有能力购买在已订购用户数量足够多时才会开发的服务。考虑到网络安全带来的挑战和各组织面临的风险，尝试利用自愿捐款作为补充供资机制，以便为维护联合国系统的整体网络安全态势提供更直接的资源被认为是及时

之举。检查专员认为，可以设立一个信托基金，在现有筹资机制之外辅以自愿捐款，专门用于使全系统受益的共享网络安全解决方案，这种做法可能改变游戏规则，清除这方面的一些绊脚石。该信托基金不仅允许希望为加强全系统网络安全直接捐款的会员国捐款，而且还将通过治理机制提供机会，使相关利益攸关方能够设计该基金，以改善信息安全特别利益小组能够提供的战略方向与联合国国际电子计算中心提供的业务能力之间的联系(建议 3)。请大会注意该建议并邀请捐助方向信托基金捐款(建议 4)。

使实体安保与网络安全考虑更加协调一致

众所周知，安全和安保部承担一项全系统任务，即在全球各实体的实体安全和安保领域制定政策并指导运作安排。尽管物理空间与网络空间在保护人员和组织资产方面趋同，但大会赋予安全和安保部的任务侧重于其职权范围内的特定安全和安保威胁，因此没有明确提及网络安全或者风险和威胁的网络层面。多年来，使实体安保与网络安全更加一致的必要性显然在一些机构间实体引发了辩论，但这尚未发展成为适用于全系统的可采取行动的结论。为帮助澄清将联合国安全管理系统普遍依据的基于风险的方法和以问责为中心的结构化应对扩展到网络领域所伴随的机会和风险，检查专员建议秘书长向大会提交一份报告，报告应着重说明如何利用更具整体性的方法保护联合国的人员和资产，还应说明须采取哪些必要措施相应地强化现有结构，同时特别注意安全和安保部在这方面的作用。报告应参考处理网络安全的相关机构间协调机制与机构间安保管理网之间的协商结果，并酌情参考联合国国际电子计算中心的投入(建议 5)。

建议

建议 1

联合国系统各组织的行政首长应当作为优先事项，至迟于 2022 年编写一份关于其组织网络安全框架的全面报告，并尽早提交给各自的立法和理事机构，报告中应涵盖本报告审视的有助于提高网络复原力的要素。

建议 2

联合国系统各组织的立法和理事机构应审议行政首长编写的关于有助于提高网络复原力的要素的报告，并在必要时对将在各自组织实施的进一步改进提供战略指导。

建议 3

联合国国际电子计算中心主任应争取至迟于 2022 年底设立一个信托基金接受捐助方捐款，信托基金将补充该中心设计、开发和提供共享服务和解决方案的能力，以加强联合国系统各组织的网络安全态势。

建议 4

联合国大会至迟应在其第七十七届会议上注意到向联合国国际电子计算中心主任提出的关于设立共享网络安全解决方案信托基金的建议，并邀请希望加强联合国系统各组织网络安全态势的会员国向该信托基金捐款。

建议 5

秘书长至迟应向联合国大会第七十八届会议提交一份报告，探索更多利用实体安保与网络安全之间趋同趋势的机会，以便确保以更具整体性的方法保护联合国人员和资产，并说明相应加强现有结构的必要措施，同时特别注意安全和安保部在这方面的潜在作用。

除上述正式建议以外，还有 35 项作为补充的非正式或软性建议，在本报告正文中以粗体显示，检查专员认为，这些建议作为补充意见，可以加强联合国系统的网络安全态势。

目录

附件

简称和缩略语

首协会	联合国系统行政首长协调理事会
粮农组织	联合国粮食及农业组织
原子能机构	国际原子能机构
国际民航组织	国际民用航空组织
信通技术	信息和通信技术
劳工组织	国际劳工组织
海事组织	国际海事组织
标准化组织	国际标准化组织
国贸中心	国际贸易中心
国际电联	国际电信联盟
联检组	联合检查组
影子 IT	影子信息技术
艾滋病署	联合国艾滋病毒/艾滋病联合规划署
贸发会议	联合国贸易和发展会议
开发署	联合国开发计划署
环境署	联合国环境规划署
教科文组织	联合国教育、科学及文化组织
人口基金	联合国人口基金
人居署	联合国人类住区规划署
难民署	联合国难民事务高级专员公署
儿基会	联合国儿童基金会
工发组织	联合国工业发展组织
毒品和犯罪问题办公室	联合国毒品和犯罪问题办公室
项目署	联合国项目事务署
近东救济工程处	联合国近东巴勒斯坦难民救济和工程处
妇女署	联合国促进性别平等和增强妇女权能署
世旅组织	世界旅游组织
万国邮联	万国邮政联盟
粮食署	世界粮食计划署
世卫组织	世界卫生组织
知识产权组织	世界知识产权组织
气象组织	世界气象组织

一. 导言

A. 背景

1. **数字时代网络安全的重要性。**在当今的数字化世界，网络安全已经成为国际组织的重要事项，联合国系统各组织也不例外。数字化转型，对信通技术和借助网络的解决方案的依赖日益增强，网络威胁的复杂程度和破坏潜力不断增加，导致联合国系统各组织面临的网络安全风险空前增大。曾经被认为非常规的事件变得更加频繁和普遍。检查专员回顾，在 2017 年致秘书长的一封信中，参加首次联席会议的联合国系统各监督委员会的代表指出，在联合国系统各组织的三项核心关切中，查明管理层需要适当考虑新风险和正在出现的风险，尤其是对网络安全构成的全球和关键业务威胁，以及随数字化转型步伐加快而出现的新工作方式所带来的风险。[1] 在这种背景下，联合检查组(联检组)参加组织支持联检组审查联合国系统现有的网络安全政策和实践，该审查被联检组作为 2020 年工作方案的组成部分，是与信通技术治理、互联网站管理和云计算服务使用等事项有关的一系列技术专题审查中的最新一项。[2]

2. **作为网络攻击目标的联合国系统。**联合国系统各组织面临的网络安全威胁格局与影响其他实体网络安全威胁格局并无不同，因为攻击的教唆者、手段和目标(从获取金钱到追求象征性目的)都是相同的。如果有任何区别，则在于联合国与其他私营和公共部门实体相比，可能被视为首选目标。首先，吸引力可能在于，联合国各实体具有高能见度和全球影响力，因此，对追求名声的黑客而言，联合国实体是更加突出的目标，攻击联合国所获的关注大于攻击任何一个国家政府或公共部门实体所获的关注。此外，与许多私营部门目标相比，联合国各实体可能更吸引遵循意识形态动机，抗议或反对联合国系统各组织所主张或宣传的价值观的“黑客活动家”。由于各组织在政府间环境中运作，还有一个不可否认的政治层面，对此各组织本身仅作出了暗示，但无一例外，都承认该层面确实存在。总之，尽管攻击方法相同，但动机可能不同。显然，在过去五年中，针对联检组参加组织的大大小小的攻击呈指数增加，检查专员从各种来源查阅的数字均证明了这一点。

3. **网络安全事件不仅会破坏系统，还可能对执行任务造成影响。**对联合国系统各组织来说，网络安全态势薄弱的潜在后果不仅限于行政处理能力以及信通技术基础设施和系统受到破坏，衡量时不应仅参照最终遭到泄漏的信息和数据量。如果泄露影响到敏感数据，譬如可辨别个人身份的信息、员工医疗记录、知识产权数据、历史和政治档案或类似档案，一次泄露就可能对组织造成毁灭性影响。此外，各组织履行任务的能力以及在其成员国和受益者眼中的信誉都会岌岌可危。在这些组织运作的领域，即使是技术上的微小事件也可能产生连锁反应，这些连锁反应可能干扰外交和政府间进程、人道主义干预，在最坏的情况下，甚至可能影响国际和平与安全。虽然网络攻击对任务和结构各异的联合国系统各组织产生

[1] 致秘书长的信，2017 年 1 月 26 日。

[2] JIU/REP/2008/5；JIU/REP/2008/6；JIU/REP/2011/9 和 JIU/REP/2019/5.

的影响可能并不相同，但威胁是真实的、共同的。[3] 无论准备多么充分，无论多么警惕，任何组织都不能奢望永远不会经历网络安全事件。此外，如果忽视这些风险，可能会在声誉、运作、法律和财务方面产生相当大的影响。

4. **国际社会和联合国认识到网络安全的重要性。**至少自 1990 年代初以来，人们就认识到网络空间的敌对活动对国际社会以及更具体而言对联合国各组织构成威胁，在相关立法和理事机构以及内部协调机制的决议和报告中对此均有记录。与这一问题有关的实质性辩论一直在并行不悖地进行。一方面，各国政府作为联合国立法和理事机构的成员，在针对网络犯罪和网络威胁的出现制定全球应对方案时进行这种辩论(联合国网络安全工作的“外向”层面，在这方面，联合国系统行政首长协调理事会方案问题高级别委员会具有全系统协调能力)；另一方面，联合国系统各组织在寻求强化内部的整体准备充分程度以及集体和单独应对相关挑战的能力时进行这种辩论(“内向”层面，属于管理问题高级别委员会的职权范围)。秘书长最近在 2019 年首协会届会上发表的结论声明，证明联合国系统在这方面的双重作用得到承认，该声明指出：“联合国系统需要在网络安全和抵御相关威胁方面发挥领导作用，建立统一的立场，同时作为召集平台，供会员国和其他利益攸关方从各个层面讨论网络安全。”[4]

5. **各国对保护包括网络空间数字资产在内的联合国资产所负的责任。**就与网络安全有关的法律保护而言，联合国系统各组织依赖的是适用于其财产、资产、档案、文件以及更广泛地说通信的特权与豁免。[5] 这种特权与豁免的存在，使得各缔约国有义务根据各自的法律提供必要的保护和保障，以使拥有这种特权与豁免的实体实现其宗旨，并特别确保房地、档案和文件“不论其位于何处，亦不论为何人持有”，均不可侵犯。换言之，各国，特别是东道国，有义务保护各组织不受敌意攻击，无论是在实体领域还是在数字领域。法律事务厅向检查专员确认了这种解释，解决了现有法律规定是否涵盖电子数据和数字资产的问题。事实上，在各组织与接纳它们的东道国双边缔结的较新的总部与东道国协定中，法律事务厅表示，“档案”一语已被明确界定为包括电子邮件和计算机记录，以及属于有关组织或由有关组织持有，以促进组织职能的任何此类类似材料。受保护的通信也被认为包括电子数据通信，而其他协定则更广泛地规定，通信无论采用何种手段都不受侵犯。从最广泛的意义上说，这意味着根据国际法，各国有责任保护联合国的资产，包括网络空间的资产。

6. **从信通技术演进到更广阔的视角。**传统上，网络安全考虑首先出现在信通技术领域，并在该领域加以处理，在计算技术的早期，信通技术在组织活动中的作用没有今天那么突出。这种将网络安全作为一个学科，侧重于信通技术的理解是一个时代合乎逻辑的产物，当时威胁主要局限于计算基础设施，对信息资产和业务流程的影响范围要小得多。然而，如今信通技术深深植根于大多数业务活动，威胁格局已发生演变，大大超出了只需要较简单的修复和由技术驱动的防御的单纯技术破坏，因此仅从信通技术的局限视角看待网络安全似乎不再可行。**事实**

[3] 关于联合国系统各组织所面临挑战的背景资料，见联合国信息和通信技术厅编写的联合国数字蓝盔小组小册子。

[4] CEB/2019/2, 第 39 段。

[5] 《联合国宪章》第一百零五条；1946 年 2 月 13 日《联合国特权和豁免公约》；1947 年 11 月 21 日《专门机构特权和豁免公约》；1959 年 8 月 17 日《国际原子能机构特权和豁免协定》。

上，检查专员认为，界定网络安全应采用更广泛的视角，涉及一些组织领域和职能，包括企业风险管理、实体安全和安保、数据保护和隐私、法律专长以及更广泛的信息和知识管理背景下的信息安全。

7. **业务连续性规划是基于风险的网络安全方法的关键。**一些组织已经开始接受组织复原力管理的概念，这一概念涵盖许多方面，其中之一是网络安全。组织复原力领域的中心任务是充分评估网络风险，以期一方面采取预防性的减轻风险措施并防范威胁，另一方面引入适当的规程，在这类风险和威胁真正发生的情况下指导行动并保持业务连续性。在网络安全领域，减轻风险从来不是绝对的，而是一个程度问题，要判断减轻风险的有效性，不能仅看能否成功避免威胁，还要看在发生成功的攻击之后，能在多大程度上帮助恢复运行。因此，在发生严重事件时，具备针对所有信息系统并经过充分测试的灾后恢复程序至关重要。要实现这一点，必须将恢复规程作为日常业务连续性规划的一部分，进行定期和严格的测试，最好运用渗透测试这一强大的风险管理工具。虽然灾后恢复程序具有很强的技术层面，但应在相关组织领导层设定的战略参数(包括风险承受能力和风险偏好、可利用的资源等)和既定的业务制约(譬如可接受的恢复时间)范围内制定，才能行之有效。因此，业务连续性规划与风险管理一并成为面临物理威胁和网络威胁时不可或缺的组织复原力支柱。[6]

B. 目标、范围和方法

目标

8. 开展本次审查的主要目标是：

(a) 查明和分析联合国系统各组织面临的共同网络安全挑战和风险以及这些组织各自的应对措施，同时考虑到各组织在具体情况下的要求的相关共性和差异，以及各组织在保持履行任务的能力的同时保护重要资产的能力；

(b) 摸清目前的机构间安排，考察这些安排是否能够有效促进对网络安全采取全系统办法，并查明酌情改善联合国系统各组织之间协调、协作和信息共享的机会。

范围

9. **覆盖全系统。**本次审查在全系统范围内进行，包括所有联检组参加组织，即联合国秘书处、秘书处各部厅、联合国各基金和方案、其他联合国机构和实体、联合国各专门机构以及国际原子能机构(原子能机构)。国际贸易中心(国贸中心)没有参与审查程序，因此没有计入本报告所列的总数。此外，考虑到联合国国际电子计算中心在向联合国系统几个组织提供网络安全服务方面发挥的作用，联检组对该中心进行了审查。

10. **侧重于内部网络安全安排。**本报告侧重于与联合国系统各组织内部网络安全框架管理有关的组织安排，这些安排旨在保护各组织在网络空间的资产，并使各

[6] 联检组 2021 年工作方案包括专门针对业务连续性的审查。

组织能够开展已获授权的活动(网络安全的“内向”层面)。[7] 附件一概述了联合国系统为支持会员国而开展的政府间工作，包括通过技术援助建设国家网络安全能力或应对网络犯罪，相关情况是作为背景介绍，而不是本次审查的重点。附件一中对该问题在大会和其他政府间机构的各种工作流之下如何发展，作了简要的历史回顾。

11. **未对技术方面进行详细评估。**网络安全虽然不是纯粹的技术问题，但不参照信通技术层面就无法处理。不过，检查专员未试图深入分析各组织在技术针对性或稳健性方面采取的措施。为考察这些经证明对完成本报告不可或缺的技术因素，检查专员利用了外部专长，并仅限于强调供审议和可能进一步考察的选定领域。特别是，检查专员无意在本报告中通过比较或以其他方式，对联合国系统每个组织的成熟度进行全面评估。这种评估被认为超出了本报告的范围，而且不论从集体还是从个体上看，对有关组织的效用也有限。

12. **与网络安全相关但超出本研究范围的以数据为中心的相关领域。**各种知识和信息管理领域以及数据保护、隐私和相关领域与网络安全相互交叉，但超出了本研究的范围。一些领域已经成为联检组报告的主题(例如信息分类，作为记录和档案管理的分专题)，[8] 另一些领域则是根据全系统指导方针在单个组织层面阐述(例如，将首协会 2018 年通过的《个人数据保护和隐私原则》转化为组织政策和行政通知)。此外，同一年引入了《欧洲一般数据保护条例》，并尝试在联合国系统各组织执行该条例，与此有关的挑战和复杂性提出了一套单独的问题，这些问题对网络安全的影响超出了本研究的范围。这些问题无法详尽无遗地列述，但它们表明网络安全作为贯穿各领域的问题，覆盖面很广，本报告只能点到为止。**然而，检查专员希望特别指出，数据保护和个人信息隐私领域是非常令人关切的热点问题，对联合国系统各组织在这方面的政策和实践进行专门的严格审查是适时和必要的。**

方法

13. 检查专员根据联检组内部标准和工作程序，使用了一系列定性和定量数据收集方法从不同的来源获取数据，以确保调查结果的一致性、有效性和可靠性。编写本报告所使用的资料是截至 2021 年 5 月的最新资料。

- **问卷调查和书面材料审评。**联检组通过向其参加组织发出两份调查问卷来收集资料。检查专员审查了适用的监管框架的相关组成部分(与信息安全和网络安全有关的现有理事机构决议、组织信通技术战略、具体政策和程序指导文件)，并查阅了内部和外部监督机构的报告。对联合国国际电子计算中心进行了几轮询问，检查专员因此能够对该中心在网络安全领域的任务、服务目录以及体制和业务能力进行严格审查。法律事务厅就一系列法律问题作了书面澄清。对首协会各委员会和网络(主要是数字和技术网及其信息安全特别利益小组)的报告进行了分析，有助于进一步洞察机构间动态以及当前和过去的全系统举措。

[7] 一封写给联检组参加组织行政首长的致管理当局函对本报告形成补充，该函侧重于与保障和保护各组织的法律、规范、行政、政治、历史文件和数据有关的风险(JIU/ML/2021/1)。

[8] JIU/REP/2013/2.

检查专员还查阅了相关的行业标准和与网络安全有关的文献，作为背景文件。

- **访谈**。检查专员参照对调查问卷的答复进行了 45 次访谈，访谈对象包括负责信通技术和更具体地负责网络安全的官员，为提供更广泛的组织视角，还对高级官员作了访谈。随后对监督机构、安全和安保部以及选定的非参加组织的代表进行了访谈。对信息安全特别利益小组主席和首协会秘书处代表的访谈就机构间网络安全举措提供了更多洞见。对联合国国际电子计算中心代表的访谈提供了与该中心所提供网络安全能力有关的详情。检查专员还参加了由联合国国际电子计算中心主办的 2020 年共同安全会议，以了解该中心此项服务的订户讨论的最新事态发展和挑战。受当前的冠状病毒病(COVID-19)大流行影响，会议以虚拟形式举行。此外，检查专员通过焦点小组，受益于几名首席信息安全干事的意见和经验，这些首席信息安全干事参加的一个非正式全球网络由面临类似挑战的城市政府组成，通过该网络了解到这些城市政府的政策、实践和经验教训，可以为联合国各实体提供来自公共部门的参照。

14. **与信息的可用性和保密性有关的限制**。检查专员遇到的限制主要涉及：(a) 信息的可用性(因为没有系统地记录与网络安全事件有关的指标，或者在记录时没有遵循共同商定的方法，也限制了数据的可比性)；(b) 与威胁、事件，特别是应对措施有关的数据的保密性，因为各组织认为，分享此类信息会造成不必要的暴露，造成安全基础设施中的漏洞被识别和揭示，这就是为何在本报告的叙述中，主要以汇总形式提供信息，除非有理由逐案陈述，否则不指明特定的实体；(c) COVID-19 大流行对数据收集进程的影响，这种影响造成延误，导致必须完全通过视频会议进行访谈，这可能影响到与一些对话者的接触以及对话者分享敏感信息的意愿，而这些敏感信息本可通过面对面的互动取得。此外，尽管检查专员试图研究和思考各参加组织应对大流行的举措如何影响网络安全考虑，但在大流行背景下实施的一些安排和措施可能出现了进一步演变，因此在审查过程中可能没有得到充分考虑。

15. **致谢**。检查专员谨向协助编写本报告的联合国系统各组织的所有官员和其他组织的代表表示感谢，特别是向参加访谈并欣然分享知识和专长的各位表示感谢。为保证质量，采用了内部同行审评方法，以征求联检组各位检查专员对报告草稿的意见，报告草稿随后分发给有关组织，以征求对调查结果、结论和建议的实质性意见，并纠正任何事实错误。

16. **建议**。本报告载有五项正式建议，其中一项向大会提出，一项向各立法和理事机构提出，一项向联检组各参加组织的行政首长提出，一项向秘书长提出，一项向联合国国际电子计算中心主任提出。为便于处理本报告，执行其中的建议并对执行情况进行监测，附件十载有一个表格，说明本报告提交给相关机构是供采取行动还是供参考，并具体说明建议需要由相关组织的立法和理事机构还是行政首长采取行动。除正式建议以外，还有 35 项作为补充的非正式建议，以粗体显示，检查专员认为，非正式建议作为补充意见，可以加强联合国系统的网络安全态势。

C. 定义

17. **缺乏普遍接受的网络安全定义。**与信息安全有关的国际和国家行业标准通常包括网络安全的定义。然而，并没有普遍接受的定义，也没有对该用语的确切含义形成全球共识。就联合国而言，检查专员指出，相关的机构间论坛没有制定任何全系统指导方针，向联合国系统一致建议一项具体的权威定义，[9] 各组织自己的监管框架也没有系统地尝试为网络安全下定义。在本报告中，检查专员决定使用国际电信联盟(电信联盟)制定的网络安全定义，该定义载于方框 1。绝大多数联检组参加组织确认，该定义可反映它们处理网络安全事项的办法，除此之外，这些组织还经常参照相关的行业标准作为补充。

方框 1: 国际电信联盟对网络安全的定义

“网络安全涉及用以保护网络环境以及组织和用户资产的各种工具、政策、安全理念、安全保障、指导方针、风险管理方法、行动、培训、最佳做法、保证和技术。组织和用户的资产包括相互连接的计算装置、人员、基础设施、应用、服务、电信系统以及在网络环境中传送和/或存储的全部信息。网络安全力求确保实现和维护组织及用户资产的安全属性，防范网络环境中的相关安全风险。网络安全的总体目标包括以下方面：可用性；完整性，其中可能包括真实性和不可否认性；保密性。”

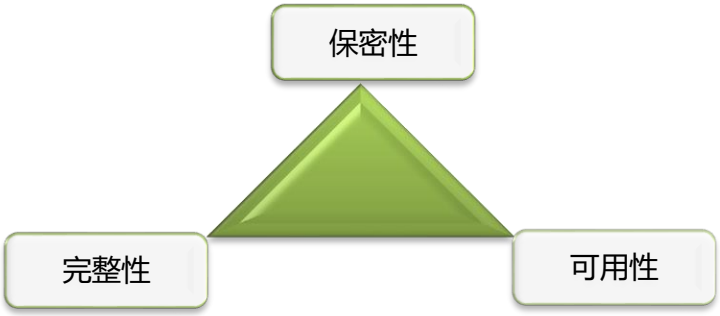
国际电信联盟(电信联盟)电信标准化部门 X.1205 建议书，《网络安全综述》。

18. **信息安全与网络安全。**许多组织使用“信息安全”这一术语，“信息安全”涉及一切形式、处于一切存储地点的信息的安全，而不仅限于数字领域的电子数据。相比之下，如国际电联的定义所示，网络安全可能与纯粹数字形式的信息以及保护与网络空间有关或受网络空间影响的更广泛的资产联系更加密切。尽管这两个术语之间在概念上略有差异，但在很大程度上相互重叠，特别是在保护信息的可用性、完整性和保密性(如图一所示，也被称为“信息安全三要素”)的核心目标方面。一些组织将“网络安全”与“信息安全”完全互换使用。另一些组织认为“网络安全”取代了较传统的“信息安全”，不过，“网络安全”丧失了一些较广泛的与知识和信息管理有关的内涵，而是具有更多以信通技术为中心的属性，还有一些组织将“网络安全”作为总括术语使用，涵盖“信息安全”和较狭义(也较少使用)的术语“信通技术安全”，后者专指信通技术基础设施(如硬件、软件、网络和技术流程)的安全。

[9] 联合国全系统网络安全和网络犯罪框架(见 CEB/2013/2)和联合国系统网络安全和网络犯罪内部协调计划(2014 年，附件)包含定义，以建立对网络犯罪和网络安全这两个术语的共识，但告诫说，这些是功能性的工作定义，本身没有得到联合国系统的核可。

图一

信息安全三要素模型[10]



资料来源：美利坚合众国国家标准和技术研究所。

19. 术语上类似的模棱两可，也见于与领导职能(在这些职能下，网络安全往往被置于组织背景中)有关的术语。例如，“首席信息安全干事”可能向“首席信息技术干事”或“首席信息干事”报告工作，而“首席信息技术干事”或“首席信息干事”被作为近义词使用，两者均可表示信通技术部门主管，或者首席信息干事还承担知识和记录管理或传播和公共关系职能。就界定每个术语所附职能范围之间的差异而言，无法识别出表明在概念上保持审慎或严谨的一贯模式。

20. 检查专员在报告中通篇使用上文定义的“网络安全”这一术语。提及“信息安全”时都是有意为之，目的是在直接引用时忠实于原始文件，或者为确保正确使用技术术语，譬如“首席信息安全干事”或“信息安全管理系统”。尽管如此，检查专员认为，没有必要对术语进行修订或统一术语的使用，因其并不妨碍各组织之间沟通或交流相关的信息。

[10] 根据互联网安全中心的定义，“保密性－完整性－可用性”三要素模型是信息安全的基准模型，旨在对组织如何应对数据的存储、传输或处理进行控制和评估。如下所述，三要素中的每个属性都代表信息安全的关键组成部分。保密性意味着未经授权不得访问或读取数据。保密性确保只有经授权的当事方才能访问。针对保密性的攻击是“泄露攻击”。完整性意味着数据不应以任何方式被修改或泄漏。相关假定是数据保持在预想状态，只能由经授权的当事方编辑。针对完整性的攻击是“更改攻击”。可用性是指在提出合法请求的情况下应当可以访问数据。可用性确保经授权的当事方在需要时可以不受阻碍地访问数据。针对可用性的攻击是“破坏攻击”。

二. 联合国系统内的网络安全状况概览

A. 对网络安全的关注渐增，但系统内各组织的成熟度水平不同

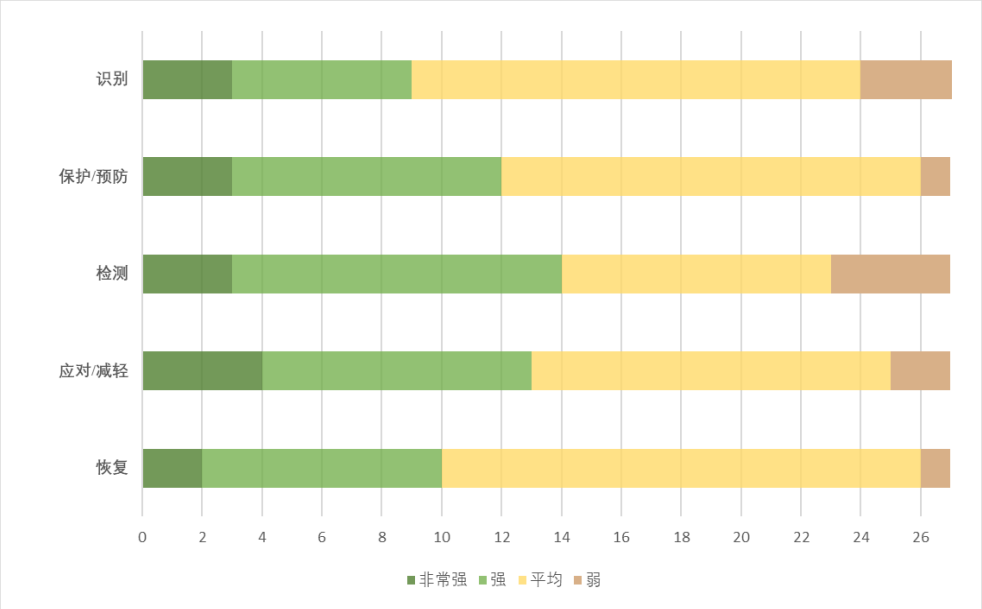
21. **日益认识到需要关注网络安全。**近年来，联合国系统各组织内部越来越深入地认识到需要关注网络安全，尽管认识程度不一。联合国系统各组织作为网络攻击者的目标，曝光度和吸引力是无可争议的，尽管可能因各组织的任务或知名度而异。可以说，各组织将网络安全确认为重要事项的快慢，受到其任务或业务模式以及拥有或管理的信息的影响。处理对国际安全或者国家或经济利益构成影响的政治敏感数据的组织，以及管理大量法律敏感数据，包括最弱势受益人口的个人数据的组织，似乎较早地着手升级网络安全准备水平，而任务相对无争议的组织也加入进来，以较和缓的速度建立网络防御。此外，一些因任务的话题性而成为公众关注焦点的组织不得不在短时间内大幅加紧努力(如世界卫生组织(世卫组织))，因大规模或高能见度的网络攻击而急需迅速采取行动和加强网络复原力的组织(譬如国际民用航空组织(国际民航组织))也是如此。然而，总体而言，没有一个联检组参加组织未以某种方式认识到，必须保持与业务要求相称的坚实网络安全态势。

22. **联合国各组织的成熟度水平不同。**虽然并未发现任何联检组参加组织忽视对网络安全进行投资的必要性，但注意到不同的组织所采取的应对网络威胁的办法存在显著差异。尽管缺乏有助于进行方法上可靠、有据可依的比较的共同基准或统一使用的标准，但审查发现，联合国系统各组织的网络安全框架在成熟度水平方面差异很大。这些差异可以参照以下各方面解释：每个组织的运作环境；所持有数据的类型所决定的要求；领导层对网络安全的理解程度和重视程度；资源的可用性；所使用的信息技术系统、工具和软件解决方案的差异，通常反映出整个系统的投资决策和供应商选择多年来未经协调。尽管联检组审查的大多数组织(如果不是所有组织)在结构上和其他方面无疑存在共同点，但如果试图对整个联合国系统的总体网络安全成熟度进行一锤定音的评估，将无法公正地反映成员的多样性特征。这种方法的实际价值也被认为有限，因为一个组织自身的保护水平难以通过与其他组织或全系统的“平均”成熟度相比较来反映。

23. **所收集的答复表明尚有改进的余地。**为介绍与现状有关的概况，图二说明了各参加组织如何参照联检组调查问卷所界定的各大类职能领域，对其总体网络安全框架进行自我评估。注意到由于缺乏共同参考框架或比较基准，在解释所收到的答复方面存在明显的挑战，但总体情况并不表明全系统的安全态势稳健，即使按照主观标准也是一样。联合国国际电子计算中心针对相同的问题，对联合国系统各组织的总体表现进行了自己的评估，因为该中心也有能力就客户的情况提供洞见。该中心在这一评估中给出从“一般”到“薄弱”不等的评级，这进一步证实了在全系统层面仍有改进余地。

图二

对多个网络安全领域的表现进行的自我评估，按控制类型和联检组参加组织的数目分列



资料来源：2020 年联检组调查问卷。

注：自我评估的类别在概念上受到网络安全领域经认可的参考框架和标准启发。联检组调查问卷中提及的网络安全领域细分如下：识别(关键流程、资产、资源、风险等)；保护/预防(访问管理、提高认识、培训、程序、技术等)；检测(异常和事件、持续监测、检测过程等)；应对/减轻(规划、沟通、分析、减轻等)；恢复(规划、复原、沟通、改进等)。

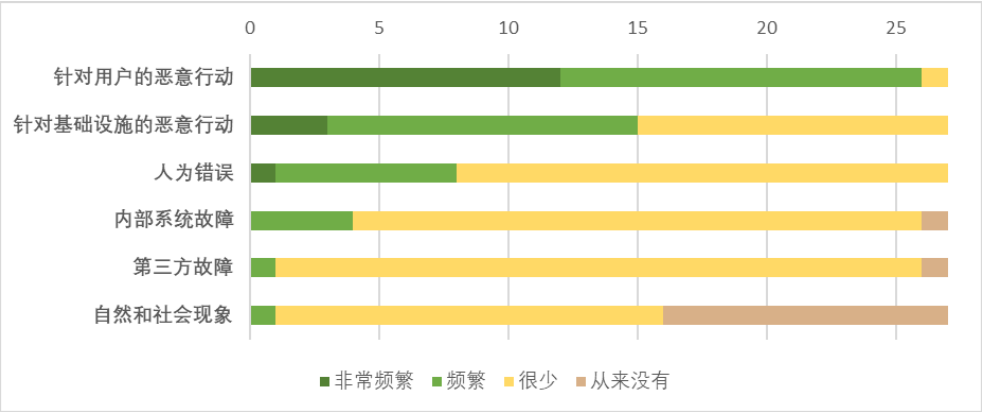
24. **个别组织的薄弱态势加剧了全系统的风险。**适当的网络安全准备程度这一问题不仅限于各组织各自的风险暴露。在访谈中，网络安全专家证实了这样一种观点，即一个组织防御脆弱或薄弱，对系统其他实体构成风险。攻击者一旦获得管理权限，得以对一个组织的信息系统进行更深入的访问，就可以利用这种访问渗透到另一个实体的数字领地。从一个组织到另一组织的恶意横向流动(称为“跳板攻击”)可能也更难检测和应对，因为这种流动可能表现为正常流量。黑客可以基于在一个组织的基础设施中收集的信息，进一步调整攻击方法，并部署一套更有针对性的手段和工具来实现目标。因此，单独自我评估为“薄弱”的组织构成一个集体问题。所以可以说联合国系统受其最薄弱的环节制约。本报告第四章进一步探讨这一层面。

B. 网络安全威胁格局

25. **最普遍的威胁来源和攻击手段。**图三概述了目前易受的网络安全威胁，反映出联检组参加组织就过去五年对它们构成影响的事件的发生频率所作的答复，按威胁来源分类。针对信息系统用户的恶意行为(通过“网络钓鱼”、盗用身份、“中间人”骗局等)或针对基础设施的恶意行为(恶意软件、分布式拒绝服务攻击等)是到目前为止报告的最普遍的威胁类型。受访官员证实，针对最终用户的恶意行为是近期最常见、增长最快的攻击类型。这种攻击因疫情大流行而加剧，大流行迫使许多最终用户远程工作，通常使用私人设备，这在许多情况下，在不同程度上为组织网络安全保护措施带来额外的压力(第 39-41 段)。

图三

过去五年面临的网络安全威胁，按威胁来源类别和联检组参加组织数目分列



资料来源：2020 年联检组调查问卷。

注：威胁来源进一步说明如下：针对用户的恶意行动(“网络钓鱼”、盗用身份、“中间人”骗局等)；针对基础设施的恶意行动(恶意软件、分布式拒绝服务攻击、其他技术行动等)；人为错误(配置错误、操作错误、未遵守程序、设备丢失等)；内部系统故障(设备或系统功能失常，或者硬件故障、供电故障、通信链路故障等)；第三方(互联网服务提供者、电力网、远程设备管理等)故障；自然和社会现象(洪水、地震、轰炸、内乱、火灾等)。

26. **社会工程攻击增加，特别是在 COVID-19 大流行期间。**虽然网络安全威胁通常与针对基础设施的复杂技术操作有关，但联合国网络安全人员报告了一种明显的转变，即黑客从攻击服务器、网络和终端设备转向攻击人，这些黑客为追求欺诈目的，使用旨在操纵个人，使之泄露敏感信息的社会工程手段。COVID-19 大流行加剧了与社会工程相关的风险。超过三分之二的参加组织报告，在全球封锁期间，网络安全威胁和漏洞急剧增加，全球封锁实际上切断了许多用户与集中管理的网络安全资源的联系，由于突然转向远程工作，用户不太能够直接与训练有素的专业人员联系，就可疑电子邮件和网站征求意见。据联合国国际电子计算中心称，网络罪犯和对手还利用了这种混乱以及人们对疫情大流行相关内容兴趣的增加，发送以 COVID-19 为主题的“网络钓鱼”电子邮件并创建虚假网站，这些网站声称提供与 COVID-19 有关的信息，实则加载恶意软件。疫情大流行期间的另一特点是不实信息以前所未有的水平传播，有时伴有剥削意图，“网络钓鱼”攻击在大流行期间特别成功。

27. **与社会工程手段有关的具体挑战。**与侧重于基础设施的攻击(直接针对数量有限的计算资源，可能较易防范)不同，社会工程被认为在几个方面具有挑战性。这些手段在技术上易于应用，其设计意在同时接触大量用户，从而最大限度地提高泄露的可能性。此外，尽管社会工程针对最终用户，但这些用户往往只是提供通往其他关键资产的通路的入口。由工作人员在不知情的情况下促成的入侵可能持续多年不被发现，从而使对手能够更多地访问内部安全基础设施和保密信息，这反过来又提供了更多攻击机会。这其中可能包括“跳板攻击”，使用这种手段是为了利用共享或相连接的基础设施，在最初渗透之后从一个组织的网络环境横向移动到另一组织的网络环境。对联合国系统各组织(其中许多组织共享共同的房地、数据中心或服务器)而言，“跳板攻击”策略尤其令人关切，因为它导致即使是最先进、保护水平最好的组织，其防御也与链条中最薄弱的环节一样脆弱。因此，特别重要的是确保所有用户接受充分的培训并有充分认识，以加强健康的做法。

28. **其他威胁**。各组织还确定了人为错误是不可忽视的漏洞来源，其中涉及配置错误、操作错误、未遵守程序、丢失设备，或者更广泛的由认识不足造成的意外损害。第三方故障据报告很少发生，这令人鼓舞，因为这表明各组织在选择商业伙伴时似乎进行了充分的尽职调查。据报告，自然灾害以及其他危害，包括冲突或恐怖活动造成破坏的情况最不普遍，但这些构成一个重要领域，在该领域，实体安保和网络安全考虑必须齐头并进，以减轻影响。

29. **威胁的来源**。在联合国范围内以及一般而言，网络安全事件可能源自广泛的威胁行为体(方框 2)，这些行为体可能在实体的内部或外部，可能自愿(蓄意攻击)或非自愿地实施行为(通过无意的作为或不作为，或者在不知情的情况下被

方框 2: 网络环境中威胁行为体的主要类型

- **黑客**。侵入网络造成破坏、伤害或混乱的个人或团体，大多是为了名声或者追求挑战带来的刺激。
- **黑客活动家**。抱有特定动机的黑客，将自己的活动视为一种公民抗命的形式，或者作为政治或意识形态自我表达的手段。
- **网络罪犯**。这类行为体参与借助网络实施的犯罪活动(欺诈、盗窃、勒索等普通犯罪，借助计算机化手段实施)或者依赖网络的犯罪活动(例如部署病毒或恶意软件，以及开展只能通过计算机化手段实施的其他活动)。根据技术复杂程度和组织能力的不同，所涉行为体从小型机构到大型有组织犯罪网络，不一而足。
- **行业间谍**。行业间谍有时被视为犯罪集团的一个子类别，这些行为体的具体目标是获取商业秘密，为经济利益进行勒索，或者破坏竞争，行业间谍大多在企业界活动。
- **国家或国家资助的团体**。这类行为体高度老练、资源充足，其活动往往难以检测、追踪或识别，它们可能以秘密方式追求复杂且通常为间接和不明显的目标，直接受雇于政府或军事机构，或者由政府或军事机构间接资助。过去，国家主要发展调查能力，但近年来，一些国家还取得了攻击能力，这已成为广泛接受的事实。
- **内部人员**。这类行为体因与所涉组织存在合同关系，不被视为外部行为体，而是从内部危及实体。其中可能包括心怀不满的雇员，缺乏培训的工作人员或订约服务提供者等。

利用)。一些犯罪集团以租用方式将能力提供给其他行为体，这实际上是通过可被称为“网络犯罪即服务”的做法将攻击外包。因此，谁是特定攻击的幕后推手这一问题(威胁归责)难以回答，尤其是因为存在无数掩盖攻击实际来源的机制(例如通过网络欺骗、“僵尸放牧”等)。事实上，一些受访官员承认，联合国系统各组织不仅缺乏可靠地确定攻击来源的能力，而且不愿意追责，因为试图追责所涉的成本远超查明入侵幕后指使者所带来的效益或效用。许多官员表示，他们将工作重点放在预防、检测和应对上，而不是投入时间和资源追查对手，因为这样做需要付出相当大的努力，即使成功地阻止了对手，也无法解决问题，因为各组

织将继续面临新对手。进阶持续渗透威胁现象也是如此，各组织证实，进阶持续渗透威胁是不可忽视的事件，往往采取入侵、监控和缓慢行动的形式，需要一定程度的资源和复杂性，通常与国家支持的攻击有关。

C. 网络安全事件的已知和未知影响

30. **所报告的影响有限。**为更好地了解风险在多大程度上转化为影响联检组参加组织的网络安全事件，联检组请这些组织按严重程度(从不严重到严重)和影响类别(财务、业务、数字、政治或声誉、物质或实体，或者与生产率有关)，对既往事件的影响进行评级。有趣而且也许令人惊讶的是，各参加组织在答复中均报告称，所遇到的网络安全事件无论影响类型如何，影响都微小或不显著。与此同时，各组织承认，所避免的网络安全事件数量大、频率高，每月达数千起，而且近年来成倍增长。这说明了各组织及其基础设施当今所面临的网络威胁之多。但从表面上看，同时考虑到这方面相对缺乏系统的数据收集，这似乎表明总体影响比较有限。

31. **受影响最大的领域。**各组织报告说，受网络攻击影响最大的领域(这种影响被数量相对较多但仍然有限的组织评为“中等”，被一两个组织评为“重大”，但未被任何组织评为“严重”)是数字领域(主要是数据泄露)，其次是政治和声誉损害(不实信息、不利的媒体关注、不当干涉政府间进程等)。即使在财务方面，直接损失(譬如欺诈性资金转移)也只涉及很小的数额，这在一定程度上表明，控制措施在这方面有效。然而，检查专员希望强调网络攻击的其他相关财务后果(例如：调查发生的情况和确定造成的损害程度所需的工作人员工作时间和费用，追回资产或设备的费用，解决泄露问题所需的外部能力的咨询费，系统停机期间的生产力损失，或者用于预防今后问题的投资成本)，这些后果量化起来可能复杂得多，但无疑值得关注。总体而言，尽管大多数参加组织对网络安全应对能力的自我评估为“一般”(仅有三分之一认为“强”或“非常强”)，但据报告，联合国系统目前经历的网络安全事件的影响本身不致引起严重关切。

32. **现实情况不明。**然而，若干因素表明，有必要优先关注网络安全。首先，收集的数据隐含一些盲点，这证实了威胁的确切规模和相关后果可能并不清楚，一些组织在答复中承认了这一点。大多数时候，特别是在实施较复杂的攻击的情况下，对手没有动力透露自己的存在或利用的漏洞，这表明，未检测到的系统漏洞和数据泄露的数量可能比所报告的水平高得多。在这方面，一些对话者指出，与已知的网络安全威胁规模相比，“已知的未知”比例很大，但“未知的未知”比例之高可能更令人关切。第二，这些答复可能(有意或无意地)尽量淡化影响，因为驱动组织文化的是与绩效有关的报告，以及严重依赖与这种报告挂钩的资源，在这种文化中，如实承认弱点尚未成为组织文化的一种规范。这可能会相应地扭曲调查结果。例如，11 个参加组织在对联检组调查问卷的答复中正式确认，近期至少经历了一次对业务产生影响的重大网络攻击。然而，一些(根据公开记录)已知遭受过这种攻击的实体，却未在与联检组的互动中披露这些情况。因此，可以假定实际威胁及其影响既超出已知水平，又超出各组织可能准备透露的范围。

33. **既往威胁无法预示未来事件。**尽管如此，专家们似乎一致认为，如果根据已知的威胁以往发生的程度来判断威胁的严重性，则会受到误导。造成损害的可能性仍然很高，应当预先制定应对策略以便随时调用。例如，不断增加的勒索软件

威胁(部署勒索软件是为了窃取数据，以勒索金钱)到目前为止似乎未对联合国系统各组织构成影响，但有一些例外。媒体报道证实，一些知名实体，包括私营部门的大型公司，甚至地方政府实体被迫支付了赎金，以重新获得对其数据与信息系统的访问权。检查专员注意到，各参加组织目前采取的明确立场，是反对向罪犯支付任何赎金。同样，值得注意是，联合国系统各组织目前没有报告经历过针对电梯、通风系统、无人驾驶汽车或类似的遥控设备等联网设备的任何网络攻击。针对联网设备的攻击是新出现的网络安全风险领域，但各实体应予以关注，因为行业专家预测，未来这类威胁将大幅增加。这两个例子表明，必须对迄今为止在联合国范围内先例可能有限的风险进行预测，并积极主动地将网络安全考虑纳入各组织的总体风险管理进程。

34. **网络安全保险。**为对新出现的威胁加强主动防范，一种选择是购买网络安全保险，以弥补网络攻击造成的损失，也可以说以避免被迫应对是否支付赎金这一问题的道德层面。客户可能会根据具体情况要求商业供应商提供网络安全保险。在审查期间，联合国系统没有任何组织表示选择了这种覆盖网络相关风险的保险，尽管一些组织表示一直在考虑。检查专员肯定联合国各实体的普遍立场，认为网络安全保险在大多数业务背景下并不是积极应对相关风险的有效工具，特别是因为，网络安全保险只是一种部分减轻战略，有助于尽量减少网络攻击可能造成的财务损失，而在处理业务或声誉损害方面收效甚微。然而，**检查专员认为，行政管理层最好为可能发生这种威胁做好准备，这种威胁今后可能会增加**。

D. 与国家主管部门的接触与合作

35. **在向国家主管部门报告方面，做法不一且意愿有限。**在向可能有能力就网络攻击进行调查并采取行政或司法行动的国家主管部门报告网络安全漏洞时，各参加组织采取不同的做法。约三分之一的参加组织表示向国家执法机关报告过事件，但很少有组织进行系统或例行的报告。在表示过去曾就网络安全事项与国家当局接触的组织中，大多数组织确认，这种接触是逐案进行的，而不是根据组织政策或惯例采取行动。许多组织尽可能不使用正式渠道，而是使用非正式工作层面的关系，且仅在发生重大攻击，可能导致东道国受到影响或者对组织造成重大声誉风险的情况下才使用这种关系。即使在国家层面的调查能力超过追查可疑攻击者的内部能力，并因此可以有益地补充内部能力的情况下(通常非常有限)，也很少有组织表示希望或需要将与国家主管部门就网络安全漏洞进行的互动正式化，或者增加系统性互动。总体情况表明，与国家主管部门接触的意愿有限，倾向于保持非正式和“视必要性而定”的互动。

36. **影响各组织做法的因素。**有各种因素可能导致各组织在与国家主管部门联系之前犹豫不决。一项因素是各组织作为特权与豁免享有者的法律地位，特别是在其数据的保密性和不受侵犯性方面，这些数据不得受到任何立法、行政或司法性质的干预。网络安全从业人员往往不太了解这一领域法律义务的边界。事实上，虽然国家负有提供保护的法律义务，但各组织只有在与国家主管部门的合作不会对其独立履行职能的能力构成干扰的情况下，才有责任进行这种合作。因此，这种合作始终是自愿的。这种办法在实践中可能确实难以拿捏，但不应阻碍在必要时以及在充分评估合作可能产生的风险之后进行自愿合作。无论如何，各组织没有义务向国家主管部门报告事件或者披露任何认为敏感的数据。法律部门最适合在这方面向决策者提供建议。在决定是否与国家主管部门联络时，另一个考虑因

素可能涉及各国自身的网络安全机构的成熟度，以及各国如何处理移交国家司法管辖机构的网络罪犯。在各组织自己的工作人员涉嫌危害组织网络安全的情况下(内部人员威胁)，这种关切可能会加剧。在这种情况下，标准程序的设想是取消特权与豁免，并将有关人员移交国籍国，进行进一步调查和可能的起诉。然而，这仍然是相对罕见的情况，特别是对网络不当行为而言。自 2007 年开始汇编和公布相关统计数据以来，在通过法律事务厅移交国家主管部门进一步调查的工作人员不当行为案件中，只有一起涉及违反信息安全规定。[11] 除上述考虑因素以外，在决定是否与国家主管部门联络时，事件的严重性，将攻击责任成功归于特定实施者的效用和可能性，不当暴露机密或敏感信息的可能性，以及开展调查对业务活动可能产生的影响，所有这些都是最常援用的考量因素。一些官员还承认，通常根本不会考虑向国家主管部门报告这一选项。

37. **向国家对口单位报告的决策过程。**如上所示，要决定是否开始与国家主管部门联络，涉及的层面超出网络安全专家的职权范围。须综合考虑政治、法律、证据和实际因素，因此，这种决定应涉及一系列利益攸关方。检查专员发现，有证据表明一些组织采取了较为既定的办法与国家主管部门接触，在这些组织中，职责分配反映了所涉及的各种考虑，这被认为是一种良好做法。更具体地说，受影响的方案办公室或实务单位将评估入侵的严重程度，同时权衡与国家主管部门联络为方案带来的风险和效益。鉴于各组织及其工作人员在有关管辖区的特殊地位，法律办公室将就可能产生的具有法律性质的影响进行评估并提出建议，包括可能需要取消特权与豁免以及酌情将受指控的工作人员移交国籍国。信通技术部门或网络安全专家的作用是尽可能地提供违规行为的法证证据。是否继续向东道国提出有关事项，将由行政管理层参照上述所有利益攸关方提供的投入作出决定。一旦决定就某一事件与国家主管部门接触，这种接触机制通常是联合国各组织有关办事处、有关国家常驻代表团与所涉东道国有关主管部门之间的既定联络渠道。鉴于对既定程序的有效性提出了一些批评意见，或许可以研究一些替代或补充途径，其中一些途径在本报告的其他部分进行了说明(第 161-163 段)。

E. 技术准备——需要关注的特定问题

38. **基础技术能力发展良好，需要进一步关注的领域受到了重视。**检查专员向各参加组织提出了一系列问题，目的是审查这些组织抵御网络威胁的总体技术准备情况。审查的意图不是要全面评估参加组织的运作安排或技术基础设施的稳健性，而是要了解现有的一般能力，并找出一些可能值得特别关注的共同问题。答复表明，各参加组织认为已经充分了解网络安全的核心技术方面，并根据自身的能力对此进行了投资；检查专员同时铭记，主要通过自我评估收集的资料存在固有局限性，而且与检查专员分享的信息在详细程度上差别很大。例如，三分之二的参加组织表示已有网络监测工具。此外，大多数组织表示已建立防火墙或其他入侵预防系统，而 13 个组织报告称已实施安全信息和事件管理系统。在最近出现更加活跃的技术发展的领域，情况似乎更加微妙，各参加组织可能有必要给予一些关注。出于安全原因，本节中没有指明具体的组织安排，以避免得出可能危及有关实体安全的结论。

[11] A/75/217，附件一。

终端设备管理和便利远程工作的工具

39. COVID-19 **大流行使终端设备的管理成为关注焦点**。大流行迫使各组织实施替代和弹性工作安排，实施范围远大于以往，涉及总部和外地的几乎所有职组。在这种背景下，由于实际进出房地和访问连接中央系统的计算设备的机会受限，各组织的异地运作能力受到前所未有的压力考验，便利远程工作的工具从网络安全角度受到更多审视。一方面，异地运作能力包括员工安全地远程访问计算资源的能力，三分之二的组织表示正在通过使用虚拟专用网络来促进这种能力，其余的组织使用基于云的服务，这些服务可通过公共网络上的加密互联网协议访问，而不需要虚拟专用网络。另一方面，异地运作能力涉及对终端设备(台式计算机、移动计算机以及其他移动设备)的管理，相关答复表明，对终端设备的管理覆盖水平差别较大。

40. **终端设备管理滞后**。虽然大多数组织提到某种程度的集中式设备管理，但其中一些组织似乎没有提供全面覆盖。在一些情况下，覆盖范围仅限于位于总部的设备，七个组织指出，外地办事处采用单独的设备管理做法，在另一些情况下，仅有永久连接的计算机得到集中覆盖，而约三分之一的参加组织既不集中管理也不集中保护移动设备，尽管有一些组织正在为此目的推出平台，或者计划在不久的将来这样做。只有两项答复提到终端设备加密，而终端设备加密是防止数据被盗和泄漏的重要措施，特别是在一般更容易丢失和被盗的最终用户便携式设备层面。这些答复证明各组织意识到机构设备管理的必要性，但表明移动设备管理滞后。使用个人、非机构的移动设备，譬如私人笔记本电脑(这种做法在大流行期间大幅增加)，使得这方面的现有漏洞更加严重。

41. **重要的网络安全措施出台或者加快推进**。尽管遇到了许多挑战，但大流行的暴发也促进了一些积极的事态发展。联合国各实体被迫更加仔细地审视安全管理框架，受迫切需求推动，所规划的组织信通技术项目开始实施。可以说，在非常短的时间里大规模转向远程工作，导致许多组织加快了改善远程访问安全性的努力，从对联检组调查问卷的答复判断，大流行可能提供了激励这方面行动所亟需的动力。事实上，大多数实体为远程访问目的建立了多因素身份验证系统，以前所未有的水平推出了在线协作和数据共享工具，使电子签名的使用进一步制度化，并提供了更多信息安全培训机会。从某种意义上说，大流行成为联合国一些实体信通技术转型的催化剂，并推动这些实体进一步实现数字化和采用先进的数字工作方法——这项因素不仅影响网络安全领域，从更广泛的角度看，也影响到各组织的工作方式以及资产和房地的管理方式。

旧系统

42. **旧系统产生的特定漏洞**。一些参加组织指出，最先进的应用程序可能不再支持老化的旧系统，这些系统的升级或淘汰构成重大的网络安全挑战。这种旧系统的持续存在据称是漏洞的主要来源，因为根据设计，其中许多系统仅在(局域或广域)专用网络局部使用，这些网络曾被视为安全环境。主要由于远程访问的发展和云计算使用的增加，这些应用现在因全球范围系统和数据的互联性增强而暴露在更多的风险之下，而这些应用在开发时并没有考虑到要抵御更加同步的攻击形式。由此产生的一些漏洞可能会被漏洞管理系统登记并发出信号，但一些专有的旧版应用仍有可能无法被自动检测出。漏洞即使被检测到，也不一定能够立即修复，这可能导致有关实体的风险暴露时间过长。这些漏洞除为旧版应用本身带

来风险以外，还对可能共享相同基础设施的其他应用和数据构成风险，因为旧版应用一旦遭到入侵，可能被用于跨系统和跨应用的横向流动。

43. **需要仔细审查旧系统。**因此，联合国系统各组织必须对旧系统进行追踪，并积极努力升级或更换这些系统。考虑其中有一些旧系统大且复杂(譬如企业资源规划系统)，并且有许多是历经很长时间在内部定制的，对许多旧系统而言，上述任务可能很复杂，需要投入更多资金并付出更多努力，才能获得和维持当初投资开发现在认为不安全的定制解决方案的业务单位的接受。**检查专员建议行政首长与信通技术和网络安全专家以及受影响的业务单位密切合作，对组织内的旧系统问题启动认真审查，除非已经开始进行审查。**在相关分析中应突出网络安全考虑，同时战略性和及时地考虑所涉及的资源投入以及此类系统停止运行对业务产生的短期和长期影响，应通过适当规划，在可能的情况下采取临时缓解措施处理这一问题。

云安全

44. **网络安全专家界认为，外部云计算服务提供商提供的保护大大加强。**自 2019 年联检组发布关于云计算的报告以来，[12] 联检组参加组织对基于云的服务的使用大幅增加，这类服务的范围和成熟度也大幅增加。基于云的服务具有普遍性、灵活性(使计算资源的分配与实际资源需求不断实时匹配的能力)和成本效益，技术水平不断提高，这激发了用户对这类服务的稳健性和安全性的信任，进一步增加了这类服务对联合国系统的吸引力。各组织继续将现有的应用迁移到基于云的服务，迁移决定仍然取决于各组织的具体情况。在这方面，检查专员承认，网络安全专家界日益认识到，商业界领先企业今天提供的云计算能力和保障超过这些企业仅仅一两年前能够提供的数据安全、保密性和网络复原力水平。据专家称，这些提供商目前提供的保护可能也超过任何一个组织使用内部开发的解决方案达到同等安全程度的能力。在本次审查期间，仅发现一个参加组织选择完全脱离基于云的解决方案来处理其管理的数据中一个特别敏感的独立部分，这是审查期间遇到的唯一例子。然而，值得注意的是，这一选择是针对有限的数据集作出的，取决于该组织提供可行替代办法的能力(包括财务能力)，未必适用于大多数组织。

45. **使用外部云计算服务时应继续保持警惕。**即使在近年来云计算安全方面取得重大进展的背景下，所参考的联检组报告中向行政首长提出的建议在以下方面仍然有效：需要使云计算服务与业务需求保持一致，以提供投资价值；在聘任外部云服务提供商时，进行全面的风险评估和谨慎的供应商管理；采取策略，以减轻供应商可能无法提供订约服务的风险。与联合国数据被垄断和过度集中在相对较少的技术巨头手中的风险有关的关切也继续存在。因此，在使用基于云的应用或在云中部署应用和数据时，各组织不能放松警惕，特别是考虑到未经授权访问保密或敏感数据的风险。各组织在依靠云计算服务时，必须继续加以应有的注意，并保持健全的网络安全做法，特别是要求提供商提供遵守独立审计要求的证据，并出示相关证书，譬如系统和组织控制报告，特别是所谓的“SOC 2 报告”，或者被行业专家广泛认可的类似保证。在使用外部提供商时，内部审计和其他组织监督机制的管辖权可能会停止，考虑到这一情况，要求这种外部独立保证变得很

[12] JIU/REP/2019/5.

重要。因此，建议在签订这类服务合同时征求内部审计部门的意见，以确保纳入相关规定，为遵守与收集、储存和使用所提供信息有关的适当内部控制标准提供合理保证。还建议咨询法律办公室。因此，各组织必须找到可接受的替代办法，以确立认为适当的一定程度的控制，例如在与外部云服务提供商的合同安排中纳入允许相关实体对合规情况进行监督和控制的条款。此外，基于云的商业设施可能发生所有权变更，甚至跨国变更，在某些情况下，如果试图在相应的国家司法管辖机构提起诉讼，可能进一步加剧这类设施持有或管理的数据被暴露的风险。在这种情况下，将为代表联合国系统各组织持有的所有数据主张和维持特权与豁免。然而，各组织必须保持警惕，并采取必要的预防措施，尽可能地管理此类风险。

46. **零风险无法实现，需要细致分析。**检查专员回顾，无论将获得何种成本效率和安全效益，基于云的解决方案和传统的数据中心方法都面临网络安全威胁，永远不能声称不可渗透。因此，在任何一种环境中，寻求完全消除风险都是不现实的。无论这种风险是否在一定程度上转移到管理相关计算环境的外部实体，组织内部仍然要为网络攻击的后果承担责任。因此，建议各组织先进行细致分析，再确定是否为委托第三方保护组织信息做好了准备，如果是，保护哪些方面的信息。本着这一精神，数据保护评估应确保云计算服务的保障措施符合各组织的要求，并与有关数据资产的类型和敏感性相称。类似的考虑适用于有关外包的任何决定，因此不仅限于使用云安全的环境。

漏洞管理

47. **各参加组织的做法不一致。**漏洞管理被认为是当今国际组织面临的主要网络安全挑战之一。在广泛使用的软件，包括联合国系统各组织使用的软件中，几乎每天都会发现新漏洞。虽然设备和软件供应商不断开发并提供相应的补丁，但这些补丁转化为大量需要处理的信息，在复杂的技术环境中应用补丁还涉及很大的工作量。一半以上的参加组织报告，为应对这项挑战，已经实施了某种形式的漏洞管理解决方案。例如，一些组织通过订阅多个情报馈送服务持续了解(和防御)新威胁，包括新漏洞，另一些组织则选择部署从商业提供商处采购的集成安全解决方案，其中包括漏洞管理方案。一些组织强调，检测漏洞和修补漏洞是要求很高的网络安全活动。一些组织注意到，企图发现网络和系统漏洞的恶意行为随时间推移而增加，而这些组织信通技术网络的分布式性质导致难以集中管理漏洞修补过程，特别是在多个外地工作地点。几个组织还报告说，漏洞修补费用是与网络安全方案有关的最大成本之一。

48. **持续进行漏洞管理。**检查专员提请注意，在有效性方面，临时性的(例如年度)漏洞评估与持续的漏洞管理和修补进程之间差异显著。如果不能定期应用补丁程序，信通技术系统就会在过长的时间里一直受到恶意利用，受到损害的风险大大增加。从参加组织收集的相关资料不能让人充分相信，这一挑战正以适当和一致的方式得到处理。几个组织对联检组调查问卷的答复表明，这些组织采取较为临时性的办法进行漏洞评估(每年一次，甚至频度更低)，而另一些组织，譬如联合国近东巴勒斯坦难民救济和工程处(近东救济工程处)、世界粮食计划署(粮食署)、国际民航组织和联合国教育、科学及文化组织(教科文组织)则将有效、持续的漏洞管理列为组织的良好做法。**在这一领域有改进的余地，检查专员敦促行政**

首长给予足够的重视和充足的资源，以便能够进行定期的漏洞评估，以期将漏洞管理作为联合国系统各组织的一项系统工作。

影子信息技术(影子 IT)

49. **利用影子 IT 的原因。**“影子 IT”这一术语是指在组织内部，但在通常集中管理的组织正式信通技术框架之外，开发或采用的信通技术应用或解决方案。在大多数情况下，造成影子 IT 的原因，是用户认为通过既定渠道和结构性信通技术能力提供的解决方案可能无法满足其在及时性、成本或定制方面的需要，因此试图使用在市场上容易获得的低成本或免费工具解决实际问题。利用影子 IT 也可能是因为希望根据不断演变的需要迅速创新，或者确保与执行伙伴使用的工具保持一致或兼容，而这些工具可能与组织整体批准的选择不一致。相关例子包括，在提供数据存储、文件传输、网页设计或内容管理解决方案的服务提供商处开设免费账户，或在内部开发应用程序，供单独的部门或外地办事处使用，或在项目环境中使用。这些解决方案通常不会或者不一定会受到审查，以确定是否符合在组织层面由官方中央主管部门制定的网络安全政策和程序，因此可以被视为在未经授权的“影子”环境中运作。

50. **与使用影子 IT 相关的风险。**在一些组织，这种现象据说已经扩散开来，特别是在外地办事处或以其他方式进一步脱离中央控制的部门。中央信通技术和网络安全部门对个别的信通技术开发活动了解有限，这往往会放大这些环境下的风险。同样，COVID-19 大流行突然催生了远程履行许多职能的需要，从而进一步加剧了这一挑战，因为许多用户开始使用通过机构软件包提供的解决方案以外的在线协作工具，包括会议工具。然而，用户作为潜在替代方案使用的许多服务未经各组织的网络安全专家评估或未被批准大规模使用，可能使有关组织面临风险(例如，在认证或保密性方面，替代方案遵守的标准与实体一级建议的标准不同)。例如，信息安全特别利益小组在大流行暴发初期研究了一个常用在线视频会议平台的使用情况，以评估该平台是否适合联合国系统各组织使用，但网络安全专家无法得出可认为对整个系统有效的确定和明确的(肯定或否定)建议。他们转而拟定了一系列选项，以及在特定环境下使用在线平台时要考虑的注意事项和预防措施。

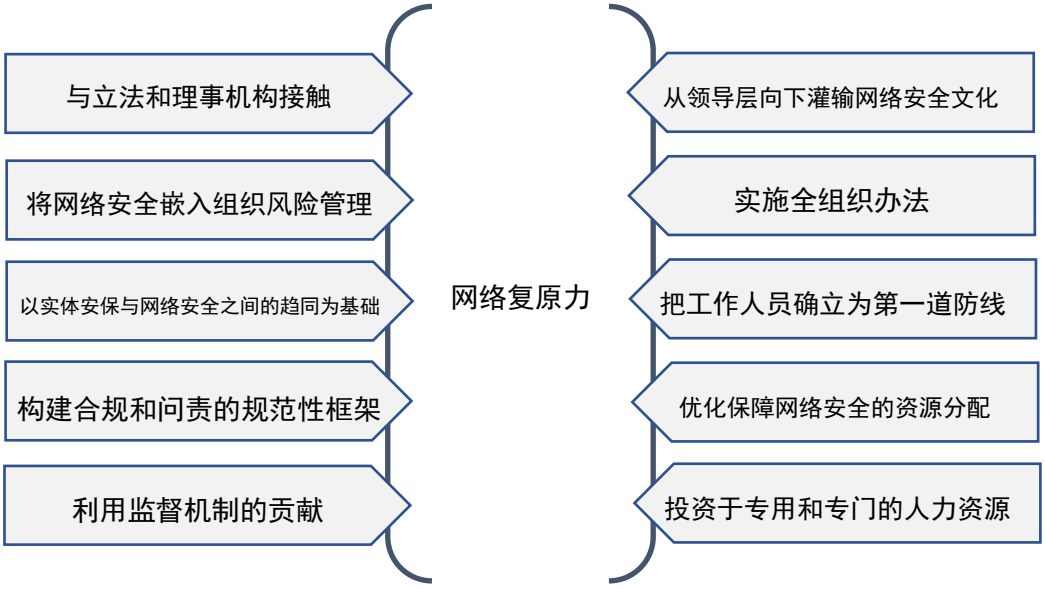
51. **关于进一步关注影子 IT 管理的一些建议。检查专员认为，与影子 IT 做法有关的网络安全挑战需要得到更多关注，既要顾及在容易面临网络风险的环境中进行控制的需要，又要顾及用户创新和利用可用的替代解决方案的合理需要和建设性动机。**事实上，有人认为，不应把一些用户寻求利用影子 IT 解决方案的做法理所当然地视为不可取的行为，因为这被认为是为创新做好准备的健康迹象，一般应允许业务单位在这方面拥有一些空间和能力，最好是在安全和受保护的计算环境中。在这方面可以利用的设想包括：为数字创新创造或扩展安全环境；通过本地信通技术协调人，提高在较分散的环境中发生的分布式信通技术开发的能见度；加强最终用户培训和提高认识措施，纳入可靠、明确的信息，说明在标准程序和做法之外使用第三方服务的安全和风险问题，并纳入与已批准的机构替代方案有关的信息以及关于更安全地使用此类解决方案的建议。

三. 有助于提高网络复原力的要素

52. **网络复原力是网络安全文化的必然结果。**要实现强健的网络安全态势，除须做好涉及确定数字解决方案和识别数据源的技术准备，以保护组织资源以外，还须采取涉及组织各个层级的多元做法，这些层级包括立法和理事机构、监督机制、行政管理层、实务或业务单位、方案主管、一般工作人员以及执行伙伴和外部服务提供者。换言之，要为提高网络复原力创造条件，必须采取全组织办法。此外，网络安全贯穿一些组织领域和职能，包括信通技术、风险管理、实体安全和安保以及更广泛的信息和知识管理。多种多样的考虑因素以及所有利益攸关方认识到它们对成功提高各组织网络安全标准的作用和贡献，可被视为网络安全文化的组成部分，这一文化一旦创建和实施，有助于实现组织的网络复原力。在本章中，检查专员就参加组织的框架和做法在多大程度上反映出图四所概述的有助于提高网络复原力的要素(纵向角度)，介绍了其审查结果，并提出可能的改进建议。

图四

有助于提高网络复原力的要素



资料来源：联检组编写。

注：一项主要的行业标准将网络复原力定义为，对利用或借助网络资源给系统造成的不利条件、压力、攻击和损害进行预测、承受、恢复和适应的能力。

A. 与立法和理事机构接触

立法和理事机构提供战略指导和资源

53. **网络安全值得立法和理事机构关注。**联检组一贯指出，政府间组织的立法和理事机构可发挥决定性作用，提供战略指导和适当的资源配置，使任何组织有能力开展已获授权的活动。如联检组最近关于企业风险管理的报告[13] 所述，立法和理事机构必须参与进来，至少应了解组织所面临的主要战略风险以及管理这些风险的现有战略和框架。**检查专员认为，这应包括在网络安全领域的参与和指**

[13] JIU/REP/2020/5.

导，因为网络安全具有至关重要的性质，既是风险管理问题，又是各组织履行任务的关键推动因素。方框 3 提出了各立法和理事机构进一步参与和支持这一领域组织努力的具体方式。然而，由于网络安全仍然主要被视为技术问题，因而被作为业务问题而非战略问题，所以在大多数组织，要求立法和理事机构参与或者其本身呼吁参与该议题的程度到目前为止非常有限。

方框 3: 立法和理事机构参与网络安全事项的机会

- 就组织在网络安全事项方面的风险承受能力和风险偏好拟定明确的陈述书，阐明在组织的具体环境下被认为可接受的风险水平。没有什么证据表明各参加组织普遍存在这种陈述书，例外情况是联合国开发计划署(开发署)和世界知识产权组织(知识产权组织)，这两个组织采用了精心设计的复杂方法来阐明风险偏好。
- 就网络安全优先领域提供高级别战略指导。这种指导的一个好例子是联合国秘书处信息和通信技术战略中关于“信息安全”的章节，该战略于 2014 年得到大会的核可(A/69/517)。
- 根据行政管理层提出的合理业务理由分配充足的财政资源，将有助于根据风险偏好执行立法和理事机构提供的战略指南中拟定的目标。

54. **立法和理事机构参与实践。**在网络安全方面，与立法和理事机构接触的深度和程度并不相同，在很大程度上取决于组织的任务和业务要求。很少有组织认识到就网络安全事项与立法和理事机构积极接触的潜力，更不用说利用这种潜力，在已经认识到并利用这种潜力的组织当中，大多数是在遭受重大攻击，使得在政治层面增加关注和互动势在必行之后才这样做的。虽然这种接触形式各异，也不存在“正确”的互动水平或程度，但人们已经在一定程度上认识到，组织内部负责网络安全者与组织的立法成员之间进行某种信息交流不仅有益，而且可能是必要的。在下文中，检查专员将网络安全定期报告机制与向立法和理事机构呈报事件所应遵循的程序加以区分。

报告和呈报机制

55. **现有的报告机制。**检查专员发现，少数组织就网络安全事项定期向自己的立法和理事机构进行某种形式的报告。在存在此种机制的组织，报告采取不同的形式：(a) 一些组织可能把相关信息纳入方案预算和绩效报告(通常作为信通技术相关章节的一部分，可能明确涵盖网络安全，也可能不明确涵盖)；(b) 另一些组织应立法和理事机构的要求提交专门的报告，譬如提交报告以展示在执行经核可或通过的战略或路线图方面取得的进展；(c) 还有一些组织依靠内部和外部监督机构的年度报告，将其作为主张对网络安全问题加强关注的主要渠道。

56. **既没有系统地收集也没有系统地提出网络安全指标。**向立法和理事机构所作的这种报告在内容上也存在差异，很少有组织分享在内部收集和分析的与其网络安全风险暴露和绩效有关的指标的特定方面。一方面，这种在报告上不一致的做法可能是由于许多组织抱有合理疑虑，这些组织不愿建立公开甚至保密的网络安全指标记录，这些记录可能会揭示漏洞，从而增加风险暴露。另一方面，这种做法可能反映出，各组织仍在努力确定报告的适当详细程度和选择最相关的指标，

并确定首先要收集的最有意义的一套指标。大多数参加组织制定的指标主要与一段时间内网络安全事件的频率、严重程度或数量有关，为内部目的而收集，而一些组织尚未在这一领域开展数据收集，或者尚未将较为临时性的数据收集形式正规化。然而，各组织收集和分析的数据类型差别很大，许多组织尚未确定以何种方式处理这些数据，以在内部或立法和理事机构层面指导决策。由于这些指标是据以阐明组织风险偏好的关键要素之一，**检查专员认为，谨慎的做法是继续在相关的论坛研究不同的网络安全指标组合，并制定一种可根据每个组织的情况酌情调整的基本方法。**

57. **向立法和理事机构呈报以及提高透明度的好处。**在发生网络安全事件时，立法和理事机构并不会系统地得到通知，这明确反映在参加组织提交的对联检组调查问卷的答复中。此外，检查专员发现，鲜有证据表明预先确定了发生网络安全事件时向立法和理事机构呈报的程序。呈报决定通常逐案处理。一些组织有机会(通常是为重大网络事件所迫)测试呈报和与理事机构联络的渠道，这些组织的经验表明，就是否呈报而言，需要考虑以下主要因素：(a) 事件的严重程度；(b) 对业务的影响；(c) 对政府间进程的影响；(d) 事件是否可能成为公开事件。其他决定性的考虑因素是呈报的时机和防范措施，以防透露可能使目标引起更多关注的具体漏洞或涉及有关组织应对能力的详情。受访的网络安全专家普遍认为，呈报的合适时机是在事件完全解决之前，或者说是在对正在处理的事件有充分了解后。发现入侵后立即呈报可能为时过早，有可能削弱正在进行的解决问题的努力，从而在无意中增加风险暴露。同时，将呈报推迟到事件完全解决时进行，可能会让人怀疑行政管理层以透明的方式行事并为可能的网络安全漏洞承担责任的可信度或意愿。一些参加组织向立法和理事机构“公开”了网络防御中的事件和缺陷，这些组织发出的总体讯息是，不要害怕沟通，因为声誉上的代价(也体现为捐助国政府丧失信心)到这时已超过攻击可能带来的难堪和破坏性影响，包括间接的财务影响。

58. **组织内部以及立法和理事机构预先设想呈报规程的必要性。检查专员认为，必须事先确定通过何种机制呈报重大网络攻击，提请立法和理事机构注意。**由于这种攻击的可能性可以预测，因此呈报规程也可以预先设想。具体而言，标准(触发呈报的理由)和机制(需要由谁，以何种顺序，采取何种步骤，以及由谁提供投入)不必受制于被动决策。如果只能在发生严重危机时临机决策，则这种决策更有可能因面临被迫采取临时补救措施的压力而受到影响，致使决策者无法大体遵循既定的规程，同时自由地专注于管理不可避免的与具体情况有关的变量。此外，如果不得不在危机模式下制定这种步骤，将使决策过程更容易在已经复杂和可能政治化的环境中受到不当影响，而这在很大程度上可以通过积极主动的办法避免。最后，在不妨碍各组织内部制定的呈报规程的情况下，谨慎的做法可能是，立法和理事机构预见到会有严重的案件提交其审议和采取行动，考虑就自身介入这类事项的规则进行辩论。这种前瞻性办法可能有助于为立法和理事机构采取的行动设定一些经过慎重考虑的商定界限，从而在这一可能具有敏感性的领域促进非政治化和合理决策。

B. 将网络安全嵌入组织风险管理

59. **以风险管理办法对待网络安全的好处。**联检组最近的一份报告将企业风险管理定性为在全组织范围内，以实现组织各项目标为目的，对风险进行条理化、一

体化和系统化的识别、分析、评估、处理和监测的进程。[14] 与网络安全相关的核心职能(通常是识别、预防、检测、应对和恢复的各种变体)反映风险管理的关键阶段和目标。将网络安全作为组织层面的风险管理问题对待也有具体的实际好处。首先，网络安全被认为是全组织的战略关切，成为关系到所有业务单位和所有员工的事项，这就鼓励和支持采取全组织办法以及通过分散的风险责任承担接纳网络安全事项。**此外，检查专员申明，将网络安全正式嵌入组织的企业风险管理框架，有助于提升网络安全问题，使其跻身于各种组织优先事项，并提供正式的基准点，在此基础上，立法和理事机构以及高级管理层可以共同规划妥善管理关键风险的路径。**由于这种框架往往被构想为动态文件，它也为根据迅速演变的组织需要，系统和经常性地重新审议、调整和定制风险减轻措施提供了机会。

60. **风险管理范式已在一定程度上得到认可。**各种论坛已经认识到将风险管理视角应用于网络安全领域的效用，不过，在实践中，以这种方式看待网络安全所产生的影响尚未被系统的许多部分充分理解和接受。例如，有网络安全专家参加了信息安全特别利益小组最近的专题讨论会，会议记录纳入了几个触及风险管理的议程项目，其中包括促请信息安全特别利益小组成员与在管理问题高级别委员会风险管理论坛任职的各自组织的代表接触，以确保将网络安全风险纳入有助于完善该论坛风险管理成熟度模型的观点。[15] 一些组织的审计和监督委员会还强调，需要将网络安全考虑因素纳入各组织更广泛的企业风险管理和业务连续性框架。事实上，大多数组织将网络安全作为整体企业风险管理任务的一部分，并强调需要加强信通技术职能与风险管理职能之间的融合。此外，最先进的网络安全标准，包括 ISO 27001、信息和相关技术控制目标以及美国国家标准和技术研究所的框架，将网络安全风险作为经营风险对待，远远超出计算基础设施的范围，这些标准还强调改善各组织网络安全态势的战略层面，认为网络安全态势如与组织层面的风险管理充分关联，可以最大限度地改善网络安全态势。

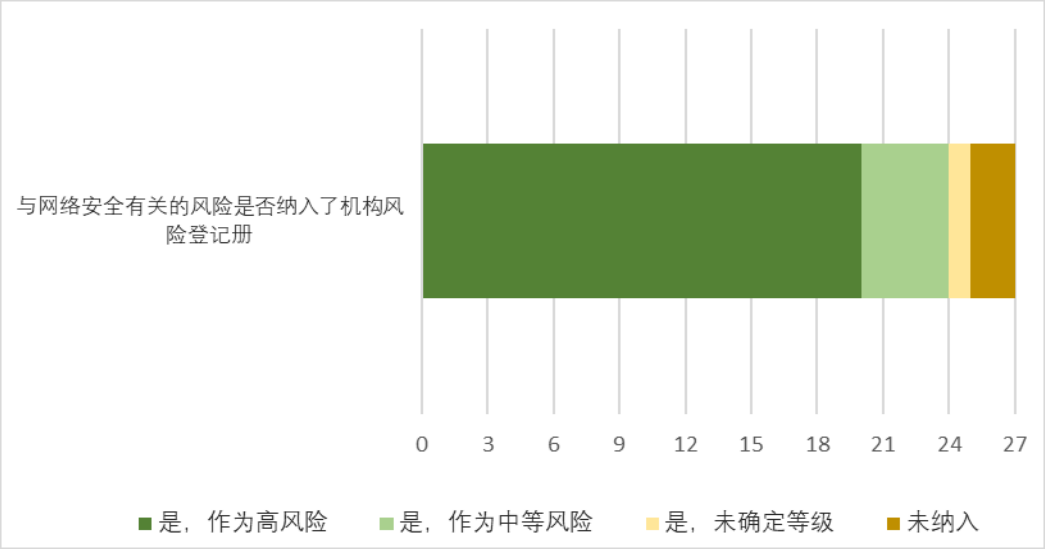
61. **参加组织对风险管理的关注。**接受联检组调查的各参加组织将网络安全融入风险管理问题的程度不尽相同。绝大多数参加组织(27 个组织中的 24 个)在答复中称，与网络安全有关的风险已正式纳入机构风险登记册。其中，20 个组织确认所指定的风险水平为“高”(图五)，19 个组织在机构风险登记册中纳入了具体的网络安全风险减轻措施。仅有 11 个参加组织向检查专员提供了内部风险管理文件，这些组织以保密方式分享了风险登记册的摘选。鉴于数据集不完整，得出的结论只能视为初步结论。然而，通过比较所提供的一些风险登记册样本，可以看到在网络安全风险的评估、分类和规划方面存在某些差异。一方面，一些组织强调战略方面，譬如网络安全事件对组织的声誉、生产力和财务的潜在影响。另一方面，一些事例表明，风险登记册几乎完全侧重于信通技术安全，主要强调保持信息的可用性，而不是信息的保密性和完整性。要保持信息的保密性和完整性，需要采取的措施往往比仅旨在避免技术中断和“停机”的措施更复杂，这可以解释，为什么所审查的文件中较少处理这些方面。主要将网络安全的技术方面置于关注中心的风险登记册的一个缺点是，可能无法在这些要素与对组织造成的更广泛后果之间建立联系。

[14] JIU/REP/2020/5.

[15] CEB/2019/HLCM/DTN/02.

图五

是否将网络安全纳入了机构风险登记册，按参加组织数目



资料来源：2020 年联检组调查问卷。

62. **减轻风险措施需要得到进一步关注。**虽然检查专员可用的数据有限，但一个值得注意的领域是网络安全风险减轻措施的明确程度，不论这些措施是作为风险管理框架的一部分，还是在风险管理框架之外。正如各审计和监督委员会指出的那样，减轻措施通常是描述现状(例如，详细说明已经采取的措施，而不是以未雨绸缪的方式预测特定风险并设想相应的行动)，这导致一种自利的进程：列举已经实现的目标，以粉饰报告，而不是认真努力制定有意义的减轻措施，并以此为基准逐步执行。意识到一些组织可能有意选择以笼统的措辞陈述减轻措施，以保护有关实体的防御，**检查专员认为，今后的重点应当是以具有前瞻性并持续反映现有制约和弱点的方式拟定减轻措施，同时承认，这可能需要更多努力，以实现新确立的目标，还可能需要设定报告的过渡期，在过渡期内，目标可能无法完全实现。**

63. **路线图。**网络安全风险评估促使一些组织采纳了组织路线图，以提高组织的网络复原力，路线图由管理层编写，由所有相关的内部利益攸关方提供反馈，并在许多情况下提交立法或理事机构核准。检查专员认为，当路线图被设计为多年期计划，与阶段性目标和绩效指标挂钩，同时改变资源分配，以确保减轻措施能够在实践中执行时，这种路线图最为有效。起草本报告时，制定这种路线图的进程在一些组织(国际民航组织、联合国粮食及农业组织(粮农组织)、联合国人口基金(人口基金)、联合国难民事务高级专员公署(难民署)、联合国项目事务署(项目署)和世界知识产权组织(知识产权组织))已经完成或正在进行，这被认为是优化整个组织的改进工作的良好做法。

64. **从风险意识到积极主动的风险管理。**最后，虽然许多参加组织已认识到网络安全考虑的重要性，并试图以不同程度的明确方式将其纳入更广泛的风险管理框架，但全系统的整体情况仍然不均衡，需要进一步关注，以便从仅仅认识到网络安全风险，转向根据各实体的要求真正管理这些风险，同时承认在网络安全领域不可能实现零风险。**因此，检查专员同意并重申网络安全专家所要求的谨慎态度：风险很大，呼吁采取基于风险的方法(附件二)。**今后的重点应该是制定有效和具体的减轻风险措施，同时制定有力的业务连续性规划。网络安全专家促进和

充分参与内部风险管理进程(从设计到实施和监测)，对于实现这些目标至关重要。

C. 以实体安保与网络安全之间的趋同为基础

65. **实体安保与网络安全之间的界限模糊**。将网络安全主要视为“网络”问题，即技术驱动的问题，还是安全问题(相当于实体安全和安保，但被移置到数字领域)，这一具有哲学意味的问题早已出现，甚至在本审查的构想阶段就已出现，在接受检查专员访谈的利益攸关方中引发了大量辩论。尽管联合国系统各组织传统上将实体安全和安保与网络安全作为不同的领域对待，但两者都涉及保护各组织的人员和保全各组织的资产。因此，这两项职能的任务都是，通过预测、防范和了解面对攻击时该做什么来管理不确定性或风险，从而使风险管理成为连接这两个领域的共同特征。在实体安保和网络安全方面也有一项共识：即使是最好的保护措施，也无法完全防止攻击突破一个组织的防御，无论这一防御是多么详尽或稳固。最后，当我们设想与网络安全和实体安保各自的起始边界有关的情形时，很快就会清楚地发现，实体领域与数字领域可能并不像乍看之下那样容易分离。

66. **实体安保和网络安全在实践中相互交叉**。目前，支持安全和安保职能的系统普遍依靠使用某种形式的信通技术，不依靠信通技术是例外情况。因此，对这类系统构成影响的网络安全漏洞，其后果可能在物理世界中显现，有时甚至会达到使人们的生命或人身健全面临重大危险的程度。有不少事例可以说明网络安全与实体安保以何种方式在实践中相互交叉。例如，黑客可能会控制安全门，利用安全规程中的弱点在电子设备上植入间谍软件或将保密信息下载至便携式设备，取得对办公室平面布置图的在线访问权限，以期研究武装攻击的最佳目标，或者参与虚拟身份盗用，以诱使他人陷入以下境地，即依赖被网络罪犯伪装为可信来源的信息，最终在不知不觉中危及自己的安全。此外，安全措施漏洞百出，无法充分保护房地、数据中心、服务器机房或数字接入点免受未经授权的进入或者由物理危险(自然或人为)引起的其他形式的不当干扰，可能会对数字领域产生直接的不利影响。这两个世界的趋同在外地工作地点可能更加明显，这些地点往往更加远离中央网络安全控制机制和监测，同时可能也是更有吸引力的目标，因为所持有的信息直接关系到生命和人身安全。这方面的一个例子是在保护水平较低的区域，人员的去向或调动数据。

67. **实体安保与网络安全之间的制度化联系仍然是零散的**。对联检组调查问卷的答复和随后对官员的访谈显示，各参加组织实现实体领域与网络领域之间相互联系的程度不一。仅有两个组织的整体架构反映了实体安全和安保与网络安全管理框架的实际融合，要么将这两项职能放在同一部门，共同向负责总体组织安全任务的副执行主管职级报告(知识产权组织)；要么对这两项职能进行战略性阐述，将它们作为更广泛的“组织复原力管理框架”(该框架将针对各种威胁的防御结合起来，不论是实体、数字、政治、自然威胁还是其他威胁)中多项贡献因素中的两项(国际电联)。其他组织已经认识到需要取得共同点和协同增效，并在一定程度上正式确立了这两项职能之间的协调和信息交流，例如通过虚线汇报关系，向高级管理层联合通报情况或交叉参加会议，或者通过让这两项职能在平等基础上促进机构进程，譬如风险管理、业务连续性规划，或者临时性参与需要两项职能均提供投入的突发事件应对。此外，已在开展与业务方面的具体措施有关的合作(例如，整合与网络和物理威胁有关的信息，用于发布任务差旅警报，或者为

人员身份识别和进入房地的出入卡联合设计先进的技术解决方案)，这为有关组织的安全态势带来一些切实的好处。即使在系统中那些认为实体安全和安保不同于网络空间且与网络空间基本无关的部分，各组织也提供了证据，表明这两个领域之间偶尔有非正式接触。尽管如此，就这一点接受调查的大多数组织认为，现实情况仍然是，实体安保与网络安全之间的联系被低估，或者只得到很少的承认，全系统层面的情况也是如此(第 159-164 段)。

68. **提高实体安全和安保职能内部的网络安全能力**。检查专员认为，有可能利用实体安保与网络安全之间的趋同，使这两个领域，更广泛地说，使组织复原力受益。一种选择是探索建设内部能力的可能性，途径是让数量充足的安全和安保专业人员掌握多技能并扩展职能范围，将网络安全方面纳入其今后的技能组合，特别是重新考虑目前对职责范围的界定方式(例如，在职责范围中增加网络威胁情报处理、威胁建模等要素和类似的分析能力)。认为网络安全本质上与这类专业人员的职责无关或者相分离的看法，部分原因可能是长期以来一直采取主要从警察和军事部队中征聘安保专业人员的做法——这种看法未能认识到，警察和军事部队自身已经在所需的领域发展出了现代能力。这种专门能力是存在的，随时可供联合国系统各组织从中征聘。这种额外能力一旦建立，将补充而不是取代现有这种由秉持传统安全思维的工作人员构成的运转顺畅的先进机制，并使该机制更有效地与联合国系统各组织内的专门网络安全能力进行互动。检查专员认识到，这两个领域具有相互区别和高度专业化的能力，这些能力为服务各自的保护目标而精心打造，因此，如果不开展进一步研究就试图将两者合并为一个结构或者将一方纳入另一方，似乎是不谨慎的。然而，努力拓展现有能力，以改善这两个领域之间的联系可能是需要探讨的要素之一，这是为了像建议 5 设想的那样，采取更具整体性的方法保护组织的工作人员和资产。

D. 构建合规和问责的监管框架

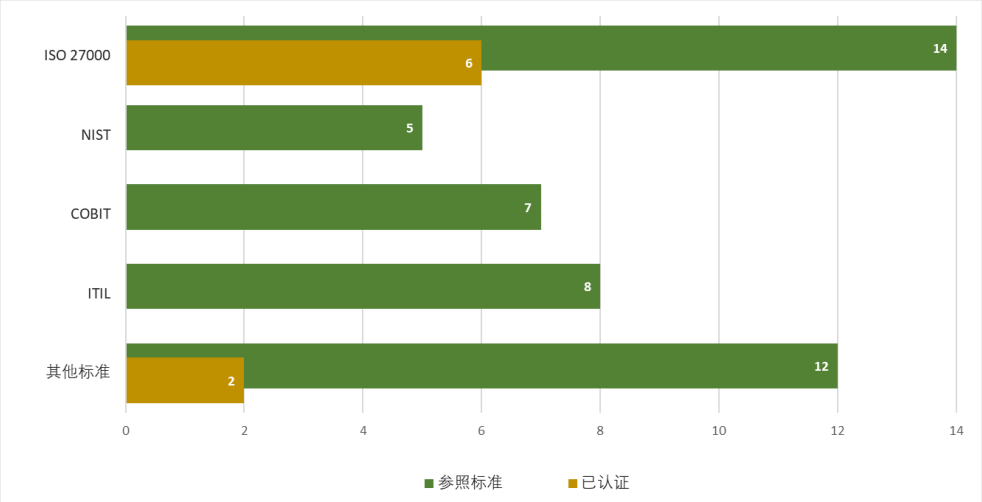
与信息安全有关的行业标准

69. **参加组织使用的主要行业标准**。在网络安全领域，已制定了一些国家和国际行业标准来提供指导和基准，以期建立具有复原力的信息安全管理系统。网络安全这一术语由国际标准化组织创造，是指反映实体网络安全方法的管理、规范和技术措施的总和。网络安全包括一套复杂的控制，从规则和政策文件到管理工具和流程、安全概念和风险管理战略，不一而足。参加组织提及范围广泛的行业标准，有时不止一项，它们表示，是根据这些标准与各组织具体环境和要求的相关性而进行选择的，并通过在有针对性的“适用性声明”中记入某一特定标准下最为相关的控制而进一步完善。检查专员回顾，早在十年前的 2011 年，信息和通信技术网就核可联合国系统各机构采用 ISO 27001 标准，[16] 2017 年，信息安全特别利益小组重申了这一立场。本次审查确认，联合国系统大多数组织要么已经获得 ISO 27001 认证，或者计划获得认证，要么选择自愿使其框架与 ISO 27001 保持一致，而不寻求正式认证。除 ISO 27001 以外，联合国系统各组织还使用其他几项标准，见下文图六，附件三中作了进一步说明。只有三个组织没有参照任何标准，或者没有通报这方面的信息。

[16] CEB/2011/HLCM/ICT/16.

图六

联检组参加组织使用的主要行业标准



资料来源：联检组调查问卷(2020 年)和访谈。

缩写：NIST, 美国国家标准和技术研究所；COBIT, 信息及相关技术控制目标；ITIL, 信息技术基础设施库。

70. **正式认证与参照标准。**检查专员发现，关于正式认证与各种软性的自愿合规方式，效用孰大孰小，专家们意见不一。事实上，管理层决定寻求认证，是以此作为向立法和理事机构以及外部伙伴提供可靠保证的手段，这种保证基于认证程序和认证证书的正规性以及要求每年进行独立审计以维持认证的严格性。鉴于需要证明网络安全不断加强，认证也可以作为反复触发创新的因素。与此同时，一些组织认为，认证可能过于昂贵和复杂，无法证明投资的合理性。这些组织还批评说，认证严重依赖形式合规，这可能会鼓励有意作出对自身有利的报告，而不是如实报告。检查专员承认，认证和与标准保持一致都是有用的选择，特别是在逐步加强网络防御的不同阶段。这一点尤其正确，因为可以不同的方式使用标准，包括将其作为基准或框架用于审计目的，作为内部路线图以寻求自我改进，作为对遵守控制的额外激励，或者作为采用有针对性办法的一种启发或参考工具。

71. **参照标准的好处。**检查专员不想主张在这方面采用某种特定的行业标准或统一的全系统办法，因为不同的标准可以有效地服务于不同的目的，并提供对应不同成熟程度的适当选择。因此，在网络安全方面并没有唯一正确的标准，也没有唯一正确的方法，但在建立和管理自己的监管框架时，有充分的理由以正式或非正式的方式从相关的行业标准中汲取灵感。因此，各参加组织必须根据在适当的、针对具体组织的网络安全风险评估中查明的要求和风险，确定适当的标准，并在该标准的范围内，根据与自身情况相匹配的所需保护水平，确定最切合实际的控制。检查专员不加评判地指出，这方面的组织决定可能也会在全系统层面产生影响，在全系统层面，使用相同的框架或标准可能更容易进行比较，并提供所有各方之间共通的表述。相反，在机构间机制的背景下，多种多样的办法可以提供更多机会，促进跨组织辩论，检验假设，使各组织对照其他组织的选择，更具批判性地审视自己的选择，并更加广泛地促进相互学习，最终使各个组织受益。

政策框架和程序

72. **构建适当监管框架的特权属于每个实体。**除上文提到的各种行业标准以外，并没有现成的普遍适用的权威指南来指导如何规范网络安全事项。网络安全领域缺乏国际法律文书或框架的原因可以归结为，该领域本身涉及多方面，难以界定，因此在规制方面情况复杂，即使仅在任何一个国家的国内法范围内也是如此。这种复杂性提升到国际层面，就更难确定共同框架，以管辖在网络空间活动的国家之间以及与其他公共和私营部门利益攸关方之间的关系。目前，对联合国系统各组织而言，既没有具有法律约束力的国际法文书，也没有单独的规范框架来专门管制网络安全。因此，对网络空间国际治理框架最恰当的描述是，该框架由交叉和重叠的技术标准、合同、法律和政府间决定组成的正式和非正式体制和规范拼凑而成。在缺乏可作为范例的一致框架的情况下，每个实体都保留特权(在其基本文书以及相关立法和理事机构的决定规定的参数范围内)，可以相对自主地制定自己的规则，并选择自己的网络安全蓝图。

73. **信通技术战略中经常提到网络安全。**现有的监管框架，或者说组织职能运作的规范环境以不同的方式涵盖网络安全，这往往反映了源于信通技术领域，并由此发展成为独立学科的网络安全领域的历史演变。有几个组织完全独立于信通技术阐述网络安全，将网络安全本身作为独立事项，与实体安保同等对待(知识产权组织)，或者作为更广泛的组织复原力管理愿景的组成部分(国际电联)，但这类办法仍然是例外。大多数参加组织拟定了组织多年期战略文件，概述在信通技术领域的愿景，而这些信通技术战略中的绝大多数纳入了网络安全考虑。但尽管如此，一些文件仅载有基本的参照标准，有时辅以较详细的低级别指南，而另一些文件则包含专门讨论网络安全主题的整个章节。**检查专员认为，不论各组织更广泛的信通技术战略中网络安全指南的详尽程度如何，在这类信通技术战略中纳入网络安全事项的参照标准都是积极的第一步。**

74. **许多参加组织已有或正在制定具体的网络安全政策。**几项主要行业标准的核心文件要求有具体的网络安全政策和形成文件的程序，作为为实体的信息安全管理系统提供支撑的控制的重要支柱。[17] 本次审查发现，许多组织已经制定了这种专门指南，尚未这样做的组织则处于制定指南的过程中，仅有少数组织例外。更具体地说，有证据表明，17 个组织制定了专门针对网络安全的规范性文书(其中三项目前正在修订)，4 个组织确认正在制定新政策。仅有 3 个组织报告称，既没有制定也没有开始制定具体的网络安全政策或条例，并表示依靠信通技术政策和程序处理网络安全问题。因此，参加组织可以说已经认识到必须建立明确的参照框架来指导网络安全办法，仅有少数组织例外。附件四列出了各参加组织监管框架内管理网络安全的主要文书。

75. **框架通常是复杂的、不同种类的和多层的。**不论有关组织是否已经制定了较详细的网络安全监管框架，也不论有关组织是否参照较为普遍地适用于信通技术的框架，检查专员遇到的框架往往分散在一系列战略、政策、程序和技术指导文件中。与这些文件有关的术语因参加组织而异，从战略到使命陈述，从政策到行

[17] ISO 27001 中包括规范性的控制目标列表，从控制要求附录 A.5“信息安全政策”开始，规定应当创建一套政策并将政策传达给员工和相关的外部当事方。美国国家标准和技术研究所在其核心文件《改善关键基础设施网络安全的框架》中，作为治理类别的一部分，具体规定“政策、程序和流程”将为“网络安全风险管理”提供信息。

政指示，从标准作业程序到指导方针，从“手册”到规程，不一而足，这些术语往往在概念上重叠，甚至互换使用。联合国国际电子计算中心建立了一个模型，分层表示信息安全管理系统中不同的规范性要素，顶层反映最高的抽象级别，底层反映最广泛的详细程度，该中心还为联合国系统几个组织评估和改进现有的规范和治理框架提供了支持。附件四以该模型为基础，概述检查专员审查的组织网络安全和信通技术文件所涉的目标、样式和典型内容，同时承认，对所有参加组织进行详细的定性内容分析将超出本次审查的范围。

76. **情境适应和定期审查。**若要确保政策体现出组织的特殊性，可能需要对政策进行调整，以酌情反映组织选择遵循的行业标准所要求的具体控制。这方面的例子见于粮食署和联合国开发计划署(开发署)，对于组织选择纳入其“适用性声明”的每一项 ISO 27001 技术控制，在监管框架中都有相应的政策声明。这可能还需要规范与一些组织更为相关的特别关切领域，譬如就内部网站、数据库或应用程序开发的安全做法提供指导。因此，所观察到的各种政策和监管框架设置方面的差异，至少可以在一定程度上有效地解释为是对组织现实情境的适应，而不是表明缺乏系统的规范方法。此外，在快速演进的网络安全领域，更重要的是，规范性指导要保持适应并切合实际，一些组织试图通过定期审查指导办法来实现这一点。在这方面，以下做法可被视为良好做法，即在这类指导文件和政策中纳入应当进行正式审查和酌情修订的明确时限，并说明由谁负责启动这一进程。

77. **指南的存在很重要，无论范围、详尽程度或组织环境如何。**鉴于可加以规范的网络安全相关事项种类繁多，难以摸清具体有哪些类型的政策或程序能够最有效地支持稳健的网络安全框架，更不用说对此作出规定。可以说，在通常具有很强技术性并涉及多方面的网络安全领域，即使仅存在基本的指南，对于确保安全措施适用的一致性和统一性也很重要，而不论组织的规模或所掌握的资源如何。

网络安全主流化

78. **主流化。**在制定增强组织网络复原力的监管框架时，仅制定针对信通技术和网络安全的特定政策是短视的。维护一个组织的网络防御是许多部门的共同责任，主流化可以大大促进实现全组织办法的有机采用而非强制采用(第 92-95 段)。一些组织显示出已经开始将网络安全考虑贯穿于不同政策的迹象。然而，要评估网络安全在多大程度上被纳入参加组织总体监管框架的主流，需要进行更广泛的分析和更深入的研究，这超出本次审查所允许的范围。检查专员在方框 4 中提出了几项供审议的建议。

方框 4: 将网络安全纳入组织监管框架主流的建议

- 与网络安全有关的要素可以直接纳入指导人力资源、采购、传播或法律事务等各部门工作的政策、流程和做法。将网络安全纳入指导各部门工作的做法的两个例子包括，在采购手册中列入使用外部服务提供者的具体审核要求，以及将在整个项目生命周期管理网络风险应遵循的步骤纳入项目文件模板，或者纳入业务单位在日常工作中使用的方案指导文件。
- 除直接处理信通技术或网络安全的部门或职能以外，其他部门或职能的作用和责任可在现有的主要规范性文书中得到分配和明确反映。例如，粮食署的组织信息技术安全政策详细规定了信息所有者、信息保管者、信息使用者、主管和工作人员等不同类别的个人的作用和责任。还有一个例子是知识产权组织。
- 可以确立一些途径，要求所有相关利益攸关方，而不仅限于信通技术和网络安全工作人员通过这些途径，定期推动这些文书的制定和执行(例如，让这些利益攸关方的代表成为相关内部治理机构的成员，或者构想政策审批程序，要求批准最后案文之前向某些利益攸关方征求意见)。

资料来源：联检组编写。

合规和问责

79. **可及性作为合规的先决条件。**即使是阐述得最明确的监管框架，其有效性也取决于有关各方的遵守程度。合规性可能受到几项因素的影响，包括能否便利地获得明确规定对每个利益攸关方和员工的要求以及相关理由的材料。接受检查专员访谈的一名首席信息安全干事强调应当阐述理由，这名干事指出，问题主要不在于缺乏书面指南，而在于用户不了解为何制定这种指南、指南的保护对象，以及未能熟悉和应用指南对个人和组织可能产生何种影响。这种认识的重要性在本报告其他部分作了进一步阐述(第 97-103 段)，包括需要使用简明、非技术性和生动的语言及信息传递方式，侧重于让个人体会到高风险网络行为的后果。审查发现，联合国秘书处树立了结构合理、全面的网络安全指导材料库的范例，材料库中包含通俗易懂的视频、海报、关于“如何操作”的短文、常见问题以及按专题分类并辅以解释性说明的全套适用条例和政策，可从信息和通信技术厅内联网主页直接一键访问。

80. **目前应对网络安全方面违规行为的措施可能不充分。**很可能对合规产生影响的一项重要因素是，是否存在可以在不合规的情况下适用的有效的强制执行措施，最好还应通过让人们了解和预见不合规行为将受到惩罚来强化这些措施。检查专员审查的政策很少包含具体措辞，说明如何惩罚违反网络安全规定的行为。所收集的关于实际执行情况的信息表明，即使在相关政策中提到具体惩罚的情况下，惩罚措施也很少得到执行，因此，参与高风险做法的雇员一般不会被追究责任。对大多数参加组织而言，可接受的信通技术资源使用政策中可能包含一些与信通技术相关不当行为(一般包括违反网络安全规定的行为)有关的具体惩罚规定。一般来说，针对这种违规行为的纪律措施与违反任何其他工作人员细则或条例的行为所附的纪律措施类型相同。然而，众所周知，标准程序即使能够成功援

引和完成，也缓慢、繁琐、耗费资源，往往只在特别严重的信通技术相关不当行为案件中启动。

81. **需要考虑更细致的惩罚制度。**就违反网络安全规定的行为(通常只是由无知或大意而导致)而言，**检查专员认为，能够较易部署、不那么正式和侵入性较小的惩罚可能是更有希望的办法。**这种惩罚将以与违规行为的严重程度相称的更直接、更迅速的方式处理问题。然而，需要取得平衡，以确保有过错的各方仍能充分感受到违规行为的后果，从而鼓励改善网络卫生和更负责任的行为。在一些组织的做法中，可以发现对上述事实的默认，这些组织在相关的网络安全政策中区分轻微和较严重的违规行为。然而，不太清楚的是，这些组织是否将这种区分成功转化为更适用于轻微违法行为同时又仍然有效的惩罚。例如，一些政策规定通知业务主管或信通技术部门主管，这可能是合规方面唯一可用的“软”压力，但这种措施除了可能造成难堪以外，并不会产生任何其他后果。原子能机构提供了一个反例，在政策中纳入了明确的非纪律惩罚，形式是取消不遵守规定的个人访问信息系统的权利，由于该反例具有针对性，会对用户产生直接的不利影响，又没有过度的惩罚，因此值得注意。还值得注意的是，该政策确认了相称性的必要性，将当事人了解规定作为因不当行为而接受惩罚的先决条件，该政策还兼顾有效保护组织资产和确保执行行动不含有管制工作人员的意味。在实践中，取消访问权是暂时的，在多次警告后实施。检查专员希望强调，没有行政首长的明确支持，就无法实施任何有效的惩罚机制，在所举的例子中，行政首长的支持是促成成功的一项因素。**检查专员认为，行政首长还应当探讨是否可能对报告事件采取鼓励措施，并鼓励个人对自己的不安全或存在风险的做法承担责任。**这样做时，必须设法兼顾通过更细致的惩罚措施进行威慑的目标和在不担心后果的情况下鼓励报告的目标。

E. 利用监督机制的贡献

82. **各个层级的审计和监督机制均关注网络安全。**检查专员审查了监督机构如何在各自的重点领域处理网络安全问题，无论是在内部审计职能层级(主要目的是评估政策和程序的遵守情况)、外部审计层级(主要涉及财务和合规性审计，有时涉及行政和管理领域的绩效审计)，还是在审计和监督委员会层级(主要就更广泛的组织问题提供咨询意见，供高级管理层以及立法和理事机构优先关注和采取行动)。检查专员欣见在上述每一层级，网络安全都是过去五年引起关注的主题，在一些组织，这种关注甚至持续了更长时间。

监督机构处理网络安全事项

83. **内部和外部审计主要侧重于信通技术，在一定程度上包括网络安全。**与信通技术相关的问题一般已很好地纳入基于风险的内部审计规划。然而，联检组在研究期间发现，过去五年中，专门侧重于网络安全的审计任务数量有限。就执行这类任务的能力而言，只有少数组织保有内部信通技术审计专门能力，大多数组织依靠外部聘请的专家。这种办法在大多数情况下似乎是令人满意的。多年来，信通技术也是许多参加组织的外聘审计师关注的一个领域，这些审计师处理了业务连续性、风险评估和风险管理、信通技术政策和信通技术资产管理等事项。总体而言，检查专员征求的管理层答复表明由此提出的建议得到接受，并表明为执行这些建议采取了措施。

84. 审计和监督委员会持续关注网络安全。2016 年，联合国系统 19 个实体的监督委员会的代表“除其他外，将数字化环境中的网络安全风险确定为一个重点领域，并同意检验管理当局的认识和准备情况”。[18] 事实上，对这些委员会报告的内容分析表明，加强网络安全的治理和风险管理方面是持续关注的重点，不过，这些委员会都没有在职权范围中具体提到网络安全，只有四个委员会提到信通技术。各委员会大都将此类问题作为整体企业风险管理任务的组成部分，或者在跟踪与信通技术有关的内部或外部审计建议的执行情况时酌情处理。本次审查发现，审计和监督委员会成员内部并没有系统性地具备专门知识，似乎只有四个委员会受益于这种专门知识，而大多数委员会依靠临时性的外部咨询意见，这与内部审计职能的普遍安排类似。这些委员会接纳网络安全议题的做法值得称许，因为这不仅有助于支持管理层采取基于风险的网络安全方法，而且可以通过这种方式向立法和理事机构通报相关的网络安全风险，从而使立法和理事机构推动减轻组织风险。

监督建议对加强各组织网络安全态势的价值

85. **监督建议正推动积极的结构改革。**参加组织报告称，网络安全方法的重大结构性变化源自监督机构的意见，从而突出了监督机制的额外价值。在访谈期间，负责信通技术和网络安全的官员普遍认为监督报告是变革的驱动因素，使高级管理层进一步认识到需要更加重视强健的网络安全态势。检查专员确实发现，有实例表明内部审计建议直接促进了有关组织内部网络安全的加强，譬如在知识产权组织。在国际民航组织和人口基金发现了其他例子，在这两个机构，一项审计建议推动制定了多年期路线图；在教科文组织，设立了一个首席信息安全干事职位；在联合国秘书处，信息安全培训的遵守情况大大加强。在过去五年中，外聘审计师还就与网络安全有关的事项向 16 个参加组织提出了建议，特别涉及信息安全培训的遵守情况、数据恢复、用户访问控制和专门用于网络安全的资源。如果审计建议不仅限于处理业务和技术方面的合规性，而是提出战略改进建议，同时承认仅仅遵守监管框架并不等同于保护，此时审计建议的效用似乎得到了更好的承认。与此同时，许多组织表示关切的是，这些建议有时没有充分考虑到资源限制和业务的实际情况，这使得其中一些建议不太可能得到执行。

86. **网络安全专业人员以系统的方式为监督职能提供信息。**要确保监督机构从网络安全角度提供最大价值，这些机构必须能够获得和充分了解涉及组织内部相关风险、能力和制约的所有相关信息。要做到这一点，最有效的办法是确保一个组织内网络安全专家的知识和经验能够为监督职能的工作提供信息和投入。在这方面有各种选择，其中一些选择已经单独或与其他选择相结合，扎根于参加组织的做法甚至监管框架，并可被视为良好做法。这些选择包括：(a) 强制要求在制定基于风险的审计计划时征求首席信息安全干事或相关单位的意见，并让其充分参与确定相关的控制和指标；(b) 根据监督机构各自任务的需要，通过事件指标报告、临时或定期简报或其他手段，向监督机构通报网络安全信息；(c) 涉及网络安全的任何审计报告或建议，在定稿前先提交首席信息安全干事或相关单位征求意见，以减轻对于建议没有充分依据组织现实，因而无法执行的关切。

[18] 见 A/72/295, 第 40-43 段。

F. 从领导层向下灌输网络安全文化

87. **领导层需要鼓励承认错误和弱点。**如上所述，组织的网络安全态势也事关强健的内部文化，这种文化始于行政管理层对网络安全问题的关注和重视，即最高层基调。然而，不能止步于此，需要向下渗透到每一名工作人员。为此，需要组织高级领导层的持续承诺和参与，不应仅限于发表将网络安全描述为组织优先事项的声明。一项关键因素是鼓励一种内部文化，在这种文化中，不会把承认事件的发生视为失败，而是视为一个起点，通过展现集体和个人对错误和弱点的承担和责任，处理共同问题以及更好地保护组织及其资产。在这方面，可以从实体安全和安保领域的执法文化中学到一些东西，在这种文化中，事件的发生被认为是理所当然的，所抱的期望是事件理应得到报告和处理，而无须评判。**检查专员认为，行政首长有责任向组织的所有职能和组织所在的所有地点灌输这种文化，因为信息系统是相互联系和相互依存的，任何地点发生的攻击或入侵都可能导致整个系统受到损害**。

88. **以行政管理层的认识和问责为出发点。**要灌输新的思维模式和文化，第一步是高级领导层本身认识到与网络安全有关的风险，并通过更多地关注这一问题，了解不作为和网络卫生状况差所产生的影响。要做到这一点，可以要求网络安全专家、风险管理干事等各组织内部的相关工作人员以及监督机构的代表定期通报情况，并实施专门针对高级官员的培训和提高认识举措。自 2020 年以来，在联合国秘书处，秘书长与高级官员之间签订的契约载有促进网络安全领域认识和问责的规定。这些契约及其所载业绩指标的一致性和有效性超出本次审查的范围，但将网络安全目标纳入高级官员的考绩，是朝着改善问责和在高层确定正确基调迈出的可喜一步。此外，应当对一些举措加以鼓励，包括在各个参加组织内加以鼓励，譬如在管理问题高级别委员会介绍情况，以提醒高级管理层注意网络安全风险对业务产生的持续影响，这种影响不仅涉及扰乱行政系统、网络和基础设施，而且涉及破坏实质性任务的交付。[19]

89. **仅靠金钱买不到网络安全文化。**行政管理层可以通过许多方式，以具体措施自上而下地激励行动和影响思维模式。首先，对网络安全的重视可以通过适当的资源分配来体现。同时，仅靠金钱无法解决网络安全准备问题，也买不到网络安全文化。具体而言，资金支助并不能免除行政管理层对网络安全事项进行参与式领导的责任，知名网络安全智库 Gartner 最近的一份报告便强调了这一点。[20] 如果支持仅体现在资金方面，行政管理层的责任实际上可能转移到下一较低层级，在这一层级，支出可能会在缺乏总体战略远景的情况下发生。资源分配和相关投资必须结合业务背景决定，而不是从纯粹的技术或风险管理角度出发，行政管理层最有能力适当权衡所有考虑因素，从而作出知情决定(第 108-109 段)。

90. **体现行政管理层支持的非金钱方式。**在高级管理层提供有意义的非金钱支助方面，参加组织的一些良好做法包括行政首长采取下列行动：公开参与提高认识方案，譬如通过录制视频发言表示支持；在员工大会上向工作人员宣讲网络安全事项；与工作人员分享网络安全攻击方面的个人经验；就所推荐的行为公开树立榜样；支持针对各级工作人员，包括高级管理人员经常和定期开展模拟“网络钓

[19] 见 CEB/2017/HLCM/ICT/9.

[20] Gartner, *The Urgency to Treat Cybersecurity as a Business Decision*, February 2020.

鱼”活动；确保责任逐级向下延伸，为此对高级管理人员施加压力，以促使这些管理人员参加培训并要求自己的团队为遵守政策和表现出适当的行为承担责任；支持实施相称的处罚，特别是对继续违反网络安全规则和程序的“惯犯”实施处罚。如上所述，起点是承认错误的发生，从中吸取教训，以及整个组织共同应对错误的后果。

91. **转变思维模式需要时间、前后一致的讯息传递和高层支持。**这类措施若要扎根于各级工作人员的态度，从而形成组织网络安全文化，必须反复实施，需要时间才能显现成效。经验表明，如果组织的高层发出前后一致讯息，表明网络安全很重要，不能一蹴而就，成功的机会就会增加，成功的速度也会加快。正如 2019 年举行的信息安全特别利益小组第八次专题讨论会所指出的那样，“改变人的行为很难，需要反复和持续地接触传递新信息的讯息，定期重新学习，了解技术带来的潜在风险和不良计算行为的后果”。[21]

G. 实施全组织办法

92. **行政部门的角色。**对于网络安全责任不能仅由信通技术部门承担的认识逐渐加深，在这种趋势下，大多数参加组织以某种方式承认，行政部门和实务部门都可以发挥作用。对联检组调查问卷的答复表明，在大多数组织，对于行政部门所发挥作用的认识似乎更加清晰。事实上，无论行政部门的角色是否正式列入了组织的监管框架，一系列行政部门都经常为维持组织的整体网络安全保护提供协助。这包括：人力资源部门，促进网络安全培训方案；采购事务部门，处理与外部服务提供商之间的供应商关系，包括从网络安全角度对外部服务提供商进行审查；法律服务部门，就规范、合同或合规问题提供咨询；传播部门，管理与外部利益攸关方之间的公共关系。除了提供基于具体职能的协助以外，还自然而然地期待这些部门中的大多数预先就有意向将网络安全考虑纳入其日常活动，因为这些部门的核心业务涉及处理敏感信息，包括个人和财务数据。从联检组研究的材料中无法明显看出，这种情况在实践中发生的程度是否充分，可否认为反映出这些部门真正认识到作为敏感信息保管者的特殊角色。该领域可能值得这些部门的主管和内部审计师进一步关注，并可酌情纳入外部提供者进行的网络安全评估。

93. **实务部门的角色。**在编写本审查报告期间收集的资料表明，与行政部门相反，实务部门的管理人员通常视网络安全为行政负担和业务制约，只有那些任务规定将严格的数据保密要求作为工作核心方面的参加组织例外。据报告，对于在项目和活动的设计和执行中纳入网络安全和复原力要求的必要性，各方案办事处没有充分接受。用一位受访的首席信息安全干事的话说：“网络安全政策和程序往往被视为拖慢执行速度的障碍，而不是保护各组织的声誉和资产以及维持运行效率的护盾。”在这种背景下，行政首长应积极消除加强网络安全措施妨碍业务灵活性或阻碍实现授权目标的看法，这一点特别重要。

94. **将角色和责任纳入主流以及承担角色和责任，是全组织办法的关键。**如上文(第 78 段)所述，将网络安全考虑纳入指导相关部门工作的政策和做法的主流，本身就是承认一个组织的每项职能都可以为实现全组织办法作出贡献。鉴于在许多组织中观察到权力下放和授权进一步向下延伸至中层管理人员的新趋势，主流化

[21] CEB/2019/HLCM/DTN/02.

还将有助于阐明相关责任，从而使各司其职的各个利益攸关方更容易加以参考，确保更加直接的全组织责任承担和问责制。通过主流化使方案和行政职能的网络安全层面更加明确，这可以减少误解和缺乏责任承担的情况。例如，检查专员注意到，网络安全专家与其他组织单位的代表之间存在一些矛盾，原因来自双方对自身在确保强健网络安全态势方面的作用的认知。**在这方面，检查专员强调，具体而言，实务部门需要对其工作的网络安全层面承担更大的责任。**然而，业务单位的参与不应意味着将责任完全转移给业务单位，将其作为风险责任人。也不能仅由网络安全专家负责保护组织资产，业务单位也应分担很大一部分责任。实现适当的平衡很重要，将网络安全考虑纳入各组织领域的主流，可以为不同部门之间设定正确的相互期望以及确定各自在这方面的角色奠定基础。

95. **基于角色的培训应进一步扩大。**审查发现，几个参加组织采取了一种令人鼓舞的做法，即提供基于角色的网络安全培训机会和提高认识措施，这些机会和措施应进一步扩大，以最大限度地使所有利益攸关方具备能力，为组织网络复原力作出各自应有的贡献。在全系统层面，信息和通信技术网已经鼓励根据用户组的职责，譬如企业资源规划干事、财务和会计专家、采购干事和行政管理人员，针对具体的用户组进行培训。一些组织还设计了有针对性的课程，面向执行敏感任务的工作人员或面临某些与地点或基础设施有关的特定风险的派驻外地工作人员。在这些特殊受众中，行政和高级管理人员以及方案管理人员可能值得优先考虑，因为他们自身对网络安全的认识和态度可能会在各自的组织或单位逐级向下渗透，并对网络安全文化的出现(或不出现)产生重大影响。

H. 把工作人员确立为第一道防线

96. **“人的因素”——威胁、防御以及网络安全文化和复原力的支柱。**联合国系统大多数组织采取了重大的技术和业务措施，以帮助防范和减轻网络攻击风险(第 38 段)。然而网络安全专家界一致认为，以下挑战依然存在，即教育每一名工作人员了解自己在保护组织的信息和数字资产方面的作用，并了解恪守网络安全政策、程序和最佳做法的重要性。在许多方面，“人的因素”在全球网络安全威胁格局中变得越来越重要，各参加组织日益关切个人最终用户越来越多地成为社会工程手法的目标便反映了这一点(第 26-27 段)。事实证明，“人的因素”也是特别难以管理的风险来源。每一名员工是其所在组织数字安全网的第一道防线和最薄弱环节，除此之外，也是组织网络安全文化和复原力的重要支柱。不良网络安全做法的不利后果是多方面的，往往表现为重大的内部威胁。这些威胁可能由以下因素造成：疏忽或大意的用户所犯的错误；意识或警觉性不足(“网络钓鱼”攻击通常利用这一点)；不良的数据保护做法，譬如选择弱密码，或者几个用户之间共享访问凭证；使用未经授权或过时的软件；在组织管理的信通技术环境之外开发应用程序；系统漏洞未加修补或疏于维护。这些行为很可能一直是各组织日常遇到的最普遍的威胁形式。因此，显然必须增强用户的能力，使用户在提高组织网络复原力方面发挥积极作用。

97. **数字素养是不容商榷的起点。**每一名工作人员的基本数字素养作为其了解自己的网络安全做法如何影响组织的前提条件，是不容商榷的起点。在二十一世纪，任何人不论以任何方式与联合国及其工作发生关联，都必须能够在数字环境中开展工作。必须为组织数字基础设施的任何和所有用户提供标准电子设备和应用的便利导航，无论是工作人员、关联人员、特派专家、会议代表，还是连接或

利用内部网络资源的任何其他人。只有在满足这一基本要求之后，才能提醒员工，保护组织信息和资产的保密性、完整性和可用性是每个人的工作和职责的组成部分。然而，更具挑战性的跨越可能是从提高对网络安全规则、责任和工具的认识以及关于健康网络做法的指导，演进到实现可持续的行为改变以及个人和集体态度的转变。

98. **培训的重要性得到承认**。要渗透思维模式的转变，使工作人员认识到网络风险，培养健康的网络安全态度，途径之一是推行有力的培训和提高认识方案。专业文献以及联合国系统几个组织的审计和监督委员会向行政管理层提交的报告都强调了这一点。这其中存在某种悖论；据受访的官员称，通常已经针对基础设施和系统建立了广泛的分层技术保护机制，但全体工作人员的能力似乎落在后面，并没有掌握与这些机制的使用和能力有关的可胜任实务工作的知识，至少在一些组织是这样。系统越稳健，风险就越多地转向用户，其中网络卫生状况差的用户是最大的风险。正如联合国秘书处独立审计咨询委员会所指出的那样，“缺乏安全意识可能导致信息和通信技术系统以及信息的保密性和完整性受到损害”。[22]

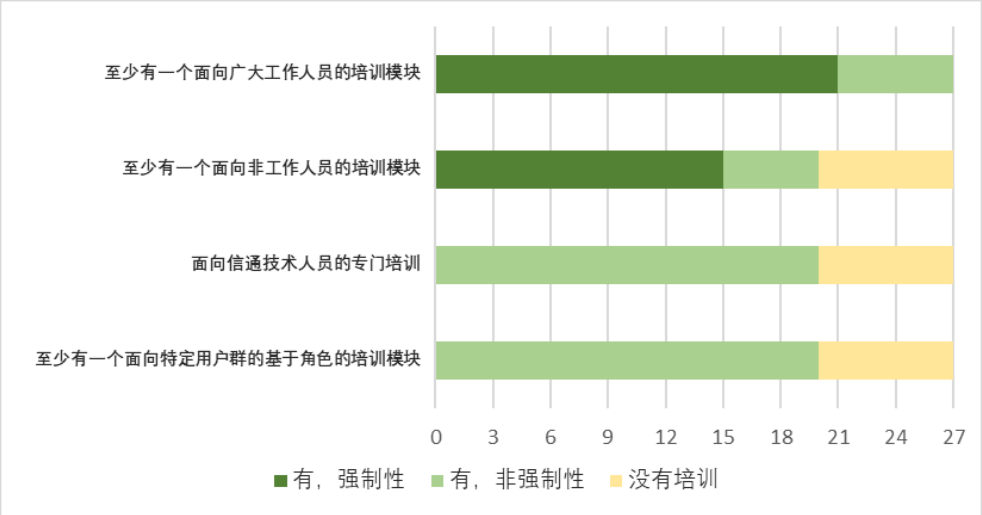
99. **对工作人员培训机会的调查显示，情况令人鼓舞**。多年来，信息和通信技术网一直指出信息安全意识培训对联合国大家庭的重要性，各参加组织也努力加强这方面的工作。[23] 图七载有所收集的关于四类目标受众的信息，这证实大多数组织有面向工作人员的强制性培训课程，但也表明在一些组织，这种培训课程仍然是非强制的。这类培训的内容通常侧重于如何适当地使用电子邮件账户处理业务与个人事务，打开来源不明的附件的风险，就密码的选择和管理提供指导，或者访问外部网站时的安全做法。近年来，审计和监督委员会提醒参加组织注意，需要提高强制性培训课程的遵守率，大体而言，这是可喜的事态。然而，检查专员希望强调，仅看强制性培训的遵守率，难以有效反映认识程度，也无法为实现实际的行为改变提供充分的保证。更切合实际的指标，可能是对一段时间内，特别是对在启动培训或提高认识干预措施前后参与不受鼓励行为(例如点击“网络钓鱼”电子邮件中的链接或附件)的用户人数进行比较，不过该指标可能较复杂，难以跟踪和分析。在强制性培训方面观察到的一些良好做法包括对新入职人员规定完成日期，以限制因缺乏认识而增加风险的时间段，以及要求工作人员每年参加复习课程，以长期保持学习效果。

[22] A/73/304, 第 51 段。

[23] 例如见 CEB/2011/3 和 CEB/2018/HLCM/ICT/10.

图七

2020 年信息安全认识培训，按培训模块和联检组参加组织的数目分列



资料来源：2020 年联检组调查问卷。

100. **需要特别注意其他类别的工作人员和偶尔使用的用户。**约半数的参加组织还规定其他类别的工作人员必须接受信息安全培训，而另一半的参加组织将这类培训作为可选模块提供，或者根本不提供这类培训机会。对编外人员类别予以关注确实至关重要。由于资源制约，这些类别的人员通常不得不使用个人设备登录组织基础设施。此外，不经常使用组织系统和基础设施的用户不太可能熟练掌握如何根据适用的组织政策和做法正确和安全地使用。对于非直接聘用，因而处于各组织完全纪律管辖范围之外的人员，缺乏有效的执行机制，这可能进一步抑制和削弱已经薄弱的遵守情况。在咨询人、承包人和短期人员在工作人员构成中占据很大比例的组织，这些挑战可能会更加突出。**检查专员回顾，培训和提高认识举措需要涵盖全体员工。威胁不会区分不同类型的用户。因此，检查专员建议尚未将这些模块作为强制性模块的组织的行政首长采取适当行动。**

101. **与培训有关的挑战。**参加组织向检查专员通报了所面临的一系列可能对执行有效的网络安全培训方案构成影响的挑战。一些组织指出，财务制约对创造或提供培训机会的能力构成限制，令人担忧的是，其中一些组织被迫优先选择某些类别的用户接受培训。主题事项具有快速演进的性质，可能使课程内容很快过时，从而需要更新和扩充，往往费用高昂，这使得财务问题更加突出。另一项挑战在于用户的培训疲劳，这可能影响方案的有效性。工作人员更替率高以及对某些类别的人员缺乏管理权，让情况变得更加复杂。外地部署的实体可能会面临一系列特殊困难，这与任何其他学习机会的情况大体相同。然而，这一层面在本次审查中无法充分探讨。最后，网络安全干事指出，对于不遵守培训要求的情况，普遍缺乏强制执行措施，许多培训方案可能没有效果，这加上缺乏惩罚措施，使得强制性培训事实上并无强制力可言。**为确保更好地执行，检查专员建议行政首长考虑在完成信息安全培训与其他的组织审查程序之间建立正式联系。**这可能涉及将外地部署的安全审查以及授予或扩大信通技术系统访问权与已经完成培训(包括“复习”课程)的证据挂钩。这种办法在出差前的人身安全考虑方面已有先例，是否批准进行这种旅行，取决于是否完成了基本的外勤安全培训，如果没有完成，将拒绝批准。

102. **整个联合国系统的提高认识举措。**联合国系统有多项与网络安全风险和所建议措施有关的提高网络安全意识举措。其中一个例子是十月的信息安全周，全球有几个组织参与了该举措，内容包括互动课程、游戏和信息说明会。国际劳工组织(劳工组织)和知识产权组织的方案被认为特别新颖和有效，其中一些方案的创新性和有效性已在外部审计中得到承认。值得探讨的其他设想包括，让提高认识课程侧重于影响私人领域的网络风险(例如窃取儿童或家庭照片并索取赎金的风险)，以期引起更多兴趣，并将取得的经验自然地推广到工作中的专业领域。一些组织由首席信息安全干事为新工作人员组织现场简报会，另一些组织向遭受过网络攻击的工作人员分发简短的视频讯息，以加强取得的经验教训。模拟“网络钓鱼”活动是最受欢迎的提高认识手段之一，据报告取得了成果(方框 5)。

方框 5: 模拟“网络钓鱼”活动取得了成果

“网络钓鱼”是指发送声称来自可信来源的欺诈电子邮件，以诱使个人透露敏感信息。随后，攻击者利用这些信息，在未经授权的情况下访问相关组织的系统，以便为经济利益或出于其他破坏性动机欺骗该组织。

模拟“网络钓鱼”活动对现实生活中黑客的策略进行模拟，有助于识别较易受骗点击恶意链接或打开受感染附件的用户。这些模拟活动也被用来检验通过培训获得的技能。为实现最佳效果，这些模拟活动应同时提供面向用户的服务，譬如明确的联络点和简单、广为人知的程序，以供工作人员报告可疑信息。例如，一些参加组织采用了直接点击员工使用的电子通信应用以报告“网络钓鱼”讯息的机制。

与检查专员分享的数据表明，这种模拟“网络钓鱼”活动是有效的，因为信息安全干事普遍发现，由于连续开展这类活动，打开可疑邮件和附件的用户的百分比有所下降。就背景而言，一些网络安全干事称，对更广泛的用户群体来说，不遵守规定的内部用户在员工中所占比例约为百分之五，这一比例是普遍接受的水平。

模拟“网络钓鱼”活动经常作为更全面的渗透测试工作的组成部分进行。这种工作通常简称为“pen”(渗透)测试，包括针对组织的网络、系统和人力资源的一系列实际操作，以查明漏洞，衡量政策和程序的遵守程度，并评估防御和恢复程序的有效性。

103. **从培训模块转向一致的提高认识方案。检查专员建议**，各组织不应继续在没有战略远景指导的情况下向每个人提供单个模块，**而应着眼于制定全面的培训和提高认识方案，根据利益攸关方可能对组织构成的风险，为各类利益攸关方确定明确的目标。**各组织通过遵循这种模式，将能够摆脱将完成率作为合规指标的做法，转而把培训作为积极主动地改变内部网络安全文化的工具。理想的情况是，实施相关方案时应当运用创新的执行方法，结合多种办法以及适合每个受众的讯息传递方式。为增强责任承担意识并促进这一领域学习内容的吸收，各组织还可以考虑创建一个同行支助系统，并在所有部门中查明哪些人可在接受培训后成为执行方案的资源，在需要时向其他工作人员提供手把手的帮助。

I. 优化保障网络安全的资金分配

估算专门用于网络安全的资源的现时水平

104. **联合国系统内部可用的网络安全资源普遍低于外部，但难以量化。**与公共和私营部门规模相当的实体相比，联合国系统各组织可以分配给整个信通技术领域，具体到网络安全领域的资源较少，这几乎是明摆的事实。然而，绝对和相对意义上的差距都难以量化。例如，据估计，“联合国不到百分之一的支出用于信通技术，信通技术支出中不到百分之一用于信息安全，而产业界的平均水平约为百分之七”。[24] 为提供有据可依的情况概览，联检组就信通技术和网络安全的资源分配问题对参加组织进行了调查。也许并不令人意外的是，检查专员得出的结论与 2018 年信息安全特别利益小组专题讨论会会议记录中所示的结论相同，即整个系统的数据仍然不清楚。

105. **估算网络安全支出的复杂性和效用。**几项因素导致可用于网络安全的资源难以确定。一般不把网络安全费用(方框 6)作为单独的预算项目或支出类别跟踪。与网络安全有关的资金可能被归入一个或几个预算项目(如业务费用，人员费用，基础设施或设备费用)或专题领域(如信通技术范围以内或以外的领域)。在预算文件和财务报表中查找与网络安全资源和支出水平有关的信息因预算结构多样而变得更加困难，这种多样性体现为经常预算与自愿(预算外)捐款并存，其中一些捐款可能包括用于大型组织基础设施项目的独立资本投资基金。几个组织还区分(一次性)投资费用和(经常性)业务费用，从而增加了更多的细微差别。审查甚至发现，有一个组织将很大一部分信通技术资源合并纳入了维持信通技术能力的各个业务单位的方案预算。在这种情况下，几乎不可能就可用于网络安全的总资源作出任何可靠的陈述。无论如何，这种估算过于复杂，与其效用不相称：一个组织分配给网络安全的资源水平的指示性价值有限，并不能很好地反映出组织所提供的保护水平。

方框 6: 网络安全费用

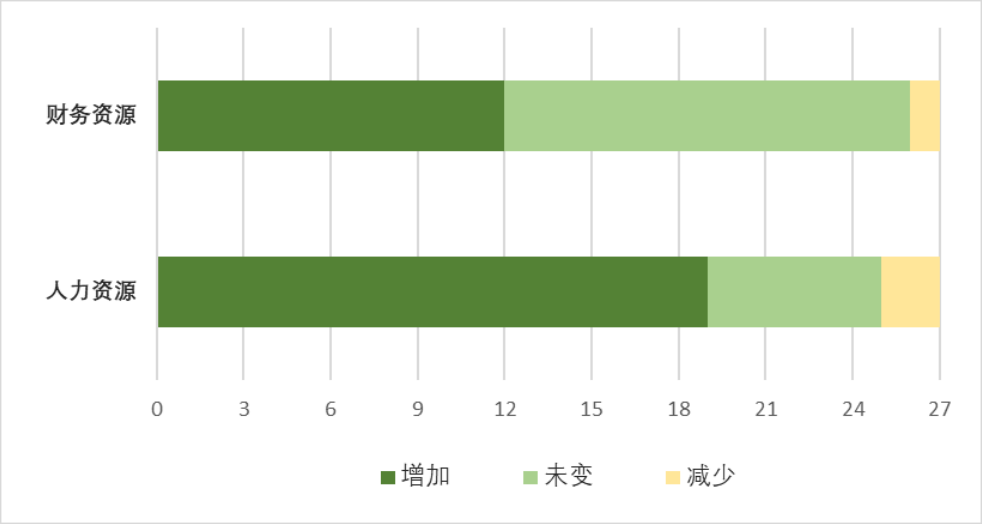
- **直接费用。**网络安全的显性(直接)费用包括人事支出(工作人员和承包人)，硬件和软件采购支出等与基础设施有关的费用(投资和管理费用以及许可证收费)，服务费用(如订阅威胁情报以及商业提供商或联合国国际电子计算中心的外包服务)等。这些费用的比例分配各不相同，反映了各个组织在平衡内部能力与外包方面的选择。
- **间接费用。**此外，估算网络安全费用时还要考虑其他(间接)费用。事实上，重大的财务影响往往与事件发生后采取的补救措施有关，其中包括调动临时能力以恢复中断的服务；修补新发现的漏洞；在系统停机时损失的生产力；培训工作人员，以更好地预防和应对入侵；保持现有的专门能力(人力和技术)不落伍。

[24] CEB/2018/HLCM/ICT/4.

106. **最新趋势：资金增加，但能力制约依然存在。**检查专员注意到，大多数参加组织表示，近年来分配给网络安全的资源有所增加(图八)。这乍看似乎是令人鼓舞的趋势。然而，从图中可以明显看出，所报告的资金的增加似乎没有自动转化为人力资源能力的增加。事实上，绝大多数参加组织警告说，目前可用的资源水平仍然阻碍创建有效的网络安全框架，一个组织甚至指出，在过去两个双年期内，确保和保护组织免受日益严重的网络威胁的费用增加了两倍。在各组织自己的评估中，发现资源制约对以下方面产生了最严重的影响，即人力资源能力和内部专门知识的可用性，对信通技术基础设施进行适当投资的能力，以及更换过时应用程序的能力。此外，在面临严重资源制约或预算零增长的组织中，新分配给网络安全的资源可能是内部重新部署的结果，可能以牺牲其他投资为代价，其中主要但不仅仅是信通技术投资。从长远来看，这可能是不可持续的，因此，检查专员感到关切的是，现有资源即使有所增加，增速可能也赶不上攻击者技术复杂性的增加速度以及信通技术在联合国系统各组织工作中的普及速度。正如信息安全特别利益小组恰当指出的那样，为信息安全职能提供的资源虽然增加，但抵不过日益增加的对网络服务的依赖。[25]

图八

联检组参加组织报告的网络安全资源演变情况(2015 年-2020 年)



资料来源：联检组 2020 年调查问卷。

107. **资金来源。**根据所收集的资料，大多数参加组织的网络安全资源主要来自经常预算。一些参加组织同时依赖经常资源和预算外资源，而只依赖预算外资源的组织很少。经常预算资源的可预测性相对较强，可能有助于促进网络安全能力的可持续性，但这种办法需要进行战略规划，以确保在需要时可以提供所需资源。与此同时，预算外资源可能具有较大的灵活性，对希望将此类资源指定用于网络安全的捐助者更具吸引力。一些组织保有特别基金，或者专门用于信通技术基础设施(世卫组织)，或者可以调动来实施重大的组织项目(知识产权组织和原子能机构)。正如改进各组织网络安全框架的长期路线图所提到的那样，这一领域的投资往往具有历时多年的性质。因此，目前的预算周期可能过短，无法落实长期战略考虑，但又不够灵活，无法迅速部署资金，以应对在网络安全这种快节奏

[25] 同上。

的技术领域和威胁格局中可能出现的临时短期需求。特别基金可以填补这方面的空白，前提是立法和理事机构商定的这些基金的治理原则以及条款和条件使其能够这样做。

追求网络安全投资的最优化

108. **需要进行业务论证，以向理事机构证明提出资源请求的必要性。**显然，如果没有证明网络安全投资应优先于其他组织支出的适当理由，各组织就不能指望向理事机构提出的资源分配请求获得成功。**作为起点，检查专员建议使资源请求立足于全面的风险评估和业务论证，业务论证应详细说明成本、效益、风险和预期的节省，并参考不进行投资造成的潜在财务影响。**这种办法在与拟议的执行计划和时间表(例如，如本报告其他部分所述，采取路线图的形式)相结合，并定期报告进展情况时最有效。检查专员注意到，当行政管理层提交令人信服的业务论证，说明明确的改进目标和参数，并证明投资的重要性时，理事机构一般更愿意以专门的资源分配来支持这一努力。近年来，国际民航组织、劳工组织、难民署、知识产权组织和其他组织都采取了这种做法，这是令人鼓舞的做法，因为网络安全威胁日益复杂，可能继续需要更多而不是更少的资源。

109. **可以且应该对网络安全支出的规模进行优化。**不言而喻，强大、可提供良好保护的网络安全框架需要投资，如果联合国系统各组织要认真保护信息、系统和数字资产，就必须为网络安全框架提供适当的资源。有人试图按网络安全相关资源在组织信通技术预算中所占百分比，来确定网络安全相关资源的适当水平，这并没有产生有意义的成果。不应迷信以金钱表示资源充足程度的想法，因为仅靠金钱不能解决问题。Gartner 一针见血地指出：网络安全支出的金额并不能反映保护水平。[26] 与网络安全支出应为多少这一问题相比，更重要的问题是应将资源分配到哪里，以期产生最积极的影响。对联检组调查问卷的答复表明，各组织优先安排网络安全支出的办法不一致，这增加了低效利用本已稀缺的资源的风险。要优化网络安全投资的规模，很有说服力(尽管有些复杂，而且时常需要定制)的选择是遵循严格的方法，譬如基于双向可追溯性概念的舍伍德应用业务安全架构(或等效工具)。也就是说，根据这种办法设立的企业安全架构使得每项业务需求由至少一项相应的安全控制处理，并且每项安全控制可以映射回所述的业务安全需求。[27] 知识产权组织已经在使用这种方法，信息安全特别利益小组也进行了讨论，**检查专员认为，这种方法值得进一步探讨，考虑以此作为手段，使网络安全投资牢固立足于业务要求和健全的风险管理做法并与之挂钩，从而避免对一项关键的业务连续性职能投资过度或投资不足。**

[26] Gartner, *The Urgency to Treat Cybersecurity as a Business Decision*, February 2020.

[27] 有关舍伍德应用业务安全架构的更多信息，可查阅 https//sabsa.org/sabsa-executive-summary.

方框 7: 开源解决方案可能提供具有成本效益的替代方案

开源软件是一种软件开发和分发模式，已成为信通技术产业的组成部分。一些基于开源软件的工具广泛用于网络安全领域，包括威胁情报共享、身份和访问管理、网络分析和入侵检测和预防、事件应对和法证等。一些开源软件甚至被认为是各自类别中的领先资源。

对联检组调查问卷的答复表明，一些参加组织已经将开源软件作为商业采购和内部开发解决方案的补充，但联合国各实体可能有机会更多地利用这些选择。开源软件可以提供适当的解决方案，特别是对在资源匮乏的情况下运作的组织来说。

开源解决方案与任何专有产品一样，应当根据其本身的优劣对其进行评价，但维护良好的开源软件产品通常具有某些普遍的优势，譬如透明度，安全性，较低的许可证成本和费用，使用开放标准，供应商锁定的危险有限。

尽管使用开源软件通常不涉及许可费，但这并不意味着完全没有任何费用。开源软件的安装、配置和维护以及所需掌握的相关技术意味着工作人员需要投入工作时间，因此会产生费用。对于部署这类应用的技术资源和经验有限的组织而言，拥有这类平台的全部成本可能不那么一目了然，但这种限制通常也在不同程度上适用于商业产品。

各组织不需要只考虑纯粹的专有模式或纯粹的开源模式。有些产品基于混合模式，旨在结合两者的优势，即开源方式的自由度和透明度以及敏捷的供应商提供的结构化支持。另一种选择是将专有工具和开源软件用于组织内的不同职能和目的。

J. 投资于专用和专门的人力资源

并非所有参加组织都具备信息安全职能

110. **与网络安全相关的职责不仅限于技术知识。**大多数参加组织为聘用专业人员进行了投资，以涵盖网络安全的不同层面，这些人员有时由一名专门的首席信息安全干事领导。属于相关职能职责范围内的核心方面既包括在业务方面制定控制措施，又包括在战略方面提供管理指导，目的是实现本报告提及的定义所列的网络安全保护目标。因此，该职能的范围超出数字领域，不仅限于提供技术专门技能。该职能涉及多种任务，譬如：制定和宣传组织监管框架(政策制定和传播)；就如何识别和管理风险提供咨询意见(风险管理)；与业务单位合作进行风险评估和业务影响分析(协调和分析作用)；调查重大违规行为(调查和分析能力)；建议和实施适当的控制改进措施(业务和技术专业知识)。[28] 对任务的这种说明意味着，这一角色包括信通技术环境内外的管理层面，需要与广泛的利益攸关方，特别是该组织的业务单位密切合作。因此，赋予首席信息安全干事(以及更广泛的网络安全专家)在整个组织传达信息和强制采取行动的职权变得至关重要。

[28] 见 SFIA Foundation, *Skills Framework for the Information Age (SFIA) 7*, 2018。

111. **内部能力存在差异**。根据联检组的研究，至少有 16 个参加组织在内部建立了专门和专用的人力资源能力，从一名信息安全干事(有时仅为非全职岗位)到由首席信息安全干事领导的较大的组织单位，规模不等，首席信息安全干事一般为 P4 或 P5 职等(附件五)。而在 10 个参加组织中，网络安全任务主要由信通技术干事处理，信通技术干事同时还履行其他职责。由于网络安全领域的技术性质复杂，使用外部知识专长的情况很常见，该领域不断发展，所需的专业化程度相当高，使专业能力长期保持可用和不落伍具有挑战性，而且费用高昂。因此，这种知识专长往往通过聘用咨询人和承包人等临时资源，或者订购商业提供商或联合国国际电子计算中心的服务来补充。一些对话者指出，全球范围都缺乏有经验的网络安全从业人员，这是联合国系统各组织在创建、维护和管理网络安全方案时面临的最大挑战之一。为了给无法立即设立专门职能的实体提供备选办法，检查专员希望强调，联合国国际电子计算中心提供一项名为“安全治理”的服务(有时也称为“首席信息安全干事即服务”)，目前有六个参加组织订购了这项服务，另有四个参加组织过去使用过这项服务。**检查专员认为，联合国系统各组织需要通过适当的人力资源规划，满足今后的网络安全知识专长需求，这尤其是因为，应对网络安全风险和挑战需要专门的知识、技能和能力，而这些知识、技能和能力可能不容易吸引和保留。**

112. **对专用能力的投资值得考虑**。在理想的情况下，组织安排应反映出组织的规模及其具体要求，这种要求的依据是所进行的风险评估和实体运作的网络环境，而现实是，其他因素可能更具决定性。具体而言，检查专员观察到的各参加组织内部设置的差异，可能更多是表明各个组织所面临的制约，而不是深思熟虑或战略性的选择。事实上，在四个参加组织中，网络安全职能至多被认为是新生的职能，这可能间接地使整个系统处于危险之中。**检查专员认为，每个组织内部具备专用和专门的网络安全知识专长，不仅有助于加强该组织的网络安全态势，而且有助于加强整个系统的网络安全态势，因此是一项有价值的投资**。如同与各组织核心业务有关的其他职能，一般倾向于尽可能地建立持久的内部人力资源能力以保护信息和网络资产，而不是依赖连续的临时资源，这特别是因为，存在与使用临时资源相关的额外风险，而且各组织对关联人员的执法能力有限(第 100 段)。此外，**设立首席信息安全干事常设职位来监督和管理这种知识专长，可能会在方法上带来必要的集中和一致，检查专员认为，这将有助于加强有关组织的网络复原力**。

113. **对于网络安全，没有普遍接受的组织定位**。网络安全在统属关系方面最适当的定位是联合国系统内外一直在辩论的问题，对于这个问题，没有明确、普遍适用的答案。国际标准无法提供权威指导，每个组织要根据需要和架构决定最合适的定位。在联合国系统各组织中，网络安全职能大多数情况下置于信通技术部门内，一般体现为直接向信通技术部门主管或同等人员报告。这种占主导地位的结构安排可被视为过去的遗留，但反映的现实是，鉴于管理相关信息系统和其他保护性基础设施所需的技术意识和知识专长，网络安全往往自然地倾向于与信通技术结合。此外，在发生网络攻击时，信通技术部门通常是设计和实施业务应对措施的部门，如果两者脱钩，可能导致效率上的损失。

114. **对信通技术职能与网络安全职能之间不同的组织优先事项进行管理**。尽管如此，将负责网络安全的干事或小组置于信通技术部门主管的领导之下，可能会在每项职能各自追求的主要目标之间造成紧张关系，风险管理和信息安全是首席

信息安全干事的主要关切，而信通技术主管的主要关切是业务和成本效益以及执行速度。潜在的利益冲突显而易见，但解决利益冲突绝非易事。当早些时候可能被忽视的网络风险开始显现时，过于注重业务的网络安全方法(譬如认为信通技术专业人员遵循的方法)可能会进一步加剧对执行构成的负面影响。与此同时，过于规避风险的态度(譬如认为是网络安全专业人员的态度)可能会不当地削弱业务灵活性，并以其他方式阻碍任务的执行。管理和化解不同组织目标之间，特别是所涉及的资源投入之间的紧张关系，是每个管理人员日常任务的一部分，行政领导最适合承担在这方面取得平衡的任务。

115. **增强网络安全职能的权能。检查专员强调，**不论网络安全在组织中处于何种位置，**都必须确保负有责任的决策者有机会不受限制地表达和听取网络安全考虑。**网络安全职能所处的位置应如本报告通篇所述的那样，使其能够独立与行政管理层对话，并有效地促进其他机构框架，譬如企业风险管理、信息和知识管理、实体安全和安保以及监督等。要实现这一目标，最有效的方式是建立有力的内部多利益攸关方治理机制，使所有相关部门参与其中。关于这种多利益攸关方和多层次治理机制，知识产权组织和国际民航组织提供了一些精心设计的范例。

116. **专门培训。**无论组织内由谁负责网络安全，无论网络安全职能集中在一个人或一个团队，还是分散在几项非全时资源中，重要的是，必须可以随时为承担安全相关职责的所有信通技术工作人员提供专门培训，以确保不断更新专门知识和技能。据报告，大多数组织已经为信通技术人员，譬如开发人员或系统管理员提供了这种培训，这种培训应得到进一步鼓励(图七)。在理想情况下，面向选定信通技术干事的优质网络安全培训方案和酌情开展的认证程序，应当成为这些信通技术干事所在部门工作计划的核心组成部分，并辅之以有保障的预算。如果不分配一些资源用于不断提高技能，信通技术人员就只能依靠自己或通过参与专业社区来维持专业知识水平。这种办法过于依赖个人的专业态度，不太可能持续。检查专员欣见一些组织表达了加强这一领域的意图，但注意到，即使在资源水平允许提供这种专门培训的情况下，大多数时候也是临时进行这种培训，而没有长期的培训目标或系统的办法。特别是在没有分配专门的人力资源能力以便以一致的方式管理网络安全的情况下，为被要求负责相关职能的工作人员提供适当的培训机会变得更加重要。

安全行动中心带来网络安全业务反应的一致性

117. **安全行动中心的主要职能。**安全行动中心是侧重于日常网络安全业务的组织单位。虽然各种形式的安全行动中心之间不可避免存在差异，但根据尽可能广泛的任务授权，安全行动中心负责通过预防、检测、分析和应对网络安全事件来监测实体的安全状况。网络安全专家经常说，安全行动中心由人员、技术和流程组成，是对来自各种实时来源的信息流进行收集、关联和分析的中心枢纽。由安全行动中心收集和处理的内部信息可能包括来自网络设备、服务器和托管应用程序、台式计算机和移动设备、实体安保系统和专用安全设备等来源的数据。安全行动中心还收集和处理来自外部信息源的威胁情报，通常查阅公开来源(包括公开的政府信息)和商业威胁情报，将这些情报与内部收集的数据相关联并进行分析，以寻找与新出现的威胁有关的迹象。鉴于安全行动中心的任务复杂并需要多种知识专长，设立和维护设备齐全并能够充分发挥作用的安全行动中心可能是复

杂而昂贵的任务。是否有必要设立这样一个中心，如果有必要，应在内部设立还是从外部提供商处采购，这是每个组织应根据其自身的需要所回答的问题。

118. **安全行动中心的内部、外包或混合解决方案：各组织的设置多种多样。**关于内部解决方案与外部解决方案的利弊，各参加组织的意见不一，检查专员在审查期间发现的安排和做法的多样性就证明了这一点。一些组织依靠虚拟或分布式安全行动中心，即中心的一些职能分散在非集中化的人员配置资源库中。一些实体已决定创建自己的内部中心，另一些实体则在使用商业提供商提供的外部中心，或者通过联合国国际电子计算中心的相关服务与其他实体共用一个中心，这些服务或单独使用，或与内部核心能力相结合。在某些情况下，使用这种混合解决方案的组织在不同的职能之间划分界限，与战略和监督有关的职能仍然由内部管理，而行动控制职能则移交给外部供应商，特别是在涉及全天候(“24/7”)监测能力的情况下。一些组织甚至不止使用一个安全行动中心，这使得这些组织能够将某些特别敏感的数据与委托外部机构管理的数据集分离开来。检查专员注意到，一些参加组织目前正在考虑将创建安全行动中心作为一种选择方案。

119. **安全行动中心安排所考虑的要素。**主张设立内部中心的理由包括，内部中心有能力更加迅速地对威胁和漏洞作出反应，并能够更好地控制终端设备，当然，内部中心的成本较高。据说对终端设备的更好控制是通过更直接地观察到终端设备及其状态而实现的，这样就有可能实时对终端的高风险态势进行补救。此外，内部中心被认为是集中网络安全职能的有效方式，而广泛的行业共识认为，集中网络安全职能有助于提高总体网络复原力。据报告，对联合国系统许多组织来说，管理内部安全行动中心的成本可能高到难以承受，而所获得的效益可能与这些组织的网络安全状况和相关的保护要求不相称。只有少数联合国实体承受得了维持成熟的网络安全方案所需的费用，因而仅依靠内部能力自主处理和应对威胁。此外，即使设法建立了适当的结构，可能也无法维持随时待命的常设网络安全专家队伍，这些专家须多才多能、训练有素，能够应对复杂的网络攻击，而网络攻击往往是偶然、不定期地发生，这意味着所需的知识专长会有一些变动。此外，一些组织认为，与其维持充分的内部能力来管理所有业务工作，不如利用外部专业提供商所提供的知识专长，这些提供商往往也有更多的资源投资于开发和研究，对于不断发展的网络安全领域，这些开发和研究被认为不可或缺。同时，有人指出，即使在实体选择外包的情况下，也需要具备充足的内部能力，实体内部要有一些核心网络安全职能的代表，这些代表掌握与内部工作流和流程有关的专业知识，也可以发挥与外部提供商有效对接的作用。在使用外部安全行动中心的情况下，供应商管理也成为关键的优先事项，必须确保进行彻底审核，合同中须有适当的法律保护条款，并避免供应商依赖或“锁定”。支持或反对外包安全行动中心的一些考虑因素可能还适用于涉及使用内部与外部能力管理网络安全的其他决定，方框 8 概述了这些考虑因素。

方框 8: 利用外部提供商提供安全行动中心和其他网络安全服务

优点：

- 确保可提供多样、最新和高度专业化的技能组合和工具
- 可能提高成本效率

- 有可能根据不断变化的威胁格局和波动的能力需求而扩大或缩小规模
- 被认为中立和公正

缺点：

- 面临供应商依赖(“锁定”)
- 对标准化服务和解决方案进行定制调整可能会遇到困难，导致次优和僵化的解决方案
- 更加依赖由管理人员直接控制的身份不明或未经审查的工作人员
- 敏感数据可能泄露给第三方
- 报告事件的透明度有限
- 费用

120. **安全行动中心可提高网络安全应对的一致性。**每个组织应根据成本效益分析，评估是否寻求创建安全行动中心，成本效益分析涉及的参数包括信通技术基础设施设置的复杂性，所管理的关键资产和流程的数量和类型，数据流的总量以及由此决定的威胁发生频率，这些可表明需要持续监测和保护的不同程度。检查专员希望强调，正式的安全行动中心不论规模和能力如何，其重要方面之一是使组织的日常监测和运作保持集中和一致。即使安全行动中心仅有非常小的团队，需要利用组织其他部门的信通技术人员或外部提供商，该中心仍然可以发挥关键的协调和同步作用，并提高组织的认识。**因此，检查专员建议行政首长在严格审查组织需求以及已经掌握的内部和外部能力的基础上，考虑创建安全行动中心或将现有能力精简为类似的机制这一选项，并确保能够充分证实决定赞成或反对设立安全行动中心的理由。**

K. 审视和报告全组织为提高网络复原力所作的努力

121. 本章详述的要素在多大程度上反映在组织的网络安全方法中，这直接影响有关组织识别、预防和检测网络威胁以及应对事件和从事件中恢复的态势和能力。考虑到现有的安排可能是由战略或业务选择驱动，也可能是由其他考虑因素决定，行政首长应启动一项全组织审查，以研究这些要素中的每一项在多大程度上纳入了相关组织的政策和做法。

122. 预计执行以下建议可提高联合国系统各组织在网络安全领域准备和应对措施的成效。

建议 1

联合国系统各组织的行政首长应当作为优先事项，至迟于 2022 年编写一份关于其组织网络安全框架的全面报告，并尽早提交给各自的立法和理事机构，报告中应涵盖本报告审视的有助于提高网络复原力的要素。

123. 应向立法和理事机构报告这种内部审查的结论，同时考虑到查明的强点和弱点，并提出进一步加强网络复原力的措施。检查专员认为，这可以使立法和理事机构更好地为就网络安全事项拟定明确的风险偏好陈述书提供高级别战略指导，并为实现预期的保护水平分配资源。如上所述，行政管理层应考虑定期向立法和理事机构报告网络安全事项。检查专员承认，这种报告中提供的信息某些部分可能具有敏感性，可能需要以适当的保密程度加以对待。**因此，建议行政管理层极尽谨慎地选择报告的方式和渠道，以便向各自的立法和理事机构提供充足的洞见，同时又不损害组织的防御。**

建议 2

联合国系统各组织的立法和理事机构应审议行政首长编写的关于有助于提高网络复原力的要素的报告，并在必要时对将在各自组织实施的进一步改进提供战略指导。

四. 从全系统角度审视网络安全

A. 网络安全——全系统优先事项？

124. **全系统网络安全合作——长期以来的优先事项。**多年来，会员国和联合国官员在尽可能高的级别将加强联合国系统的网络安全态势列为优先事项。例如，2008 年，大会鼓励秘书长作为首协会主席，促进联合国各组织之间在与信通技术、企业资源规划以及(尤其是)安全、灾后恢复和业务连续性有关的所有事项上深化协调与合作。[29] 2013 年，行政和预算问题咨询委员会在审查关于加强全秘书处信息和系统安全的建议执行进展情况报告时，鼓励秘书长继续推进全系统协作，并为进一步促进联合国系统各组织相互合作和共享信息安全解决方案寻求各种选项。[30] 更近一些，秘书长本人在 2019 年强调，必须加强联合国系统保护自己免受网络攻击的自身能力，这是首协会一级讨论的结论的组成部分。[31] 这方面的基本假设是，加强全系统层面的合作，包括采用联合办法和共同的业务解决方案，是提高整个系统保护水平的关键要素之一。

125. **采取联合战略办法的尝试。**如上所述，联合国系统各组织在网络环境中大都面临相同的挑战和威胁，这意味着有可能制定一种联合的应对办法。考虑到系统的安全至少部分取决于各个成员的安全状况，因为这些成员在不同层级相互联系，这样做也有充分的理由。在编写本审查报告期间，几个参加组织呼吁根据所有组织都须达到的一套最低标准，制定一项共同战略，由作为合作伙伴采取一致行动的各机构承担责任、执行和进行报告，这些合作伙伴受到在全系统达到一定成熟度水平这一共同目标的驱动。信息和通信技术网 2017 年的记录中提出了一项要求，即制定全系统网络安全战略，以便为在整个系统采取一致的网络安全做法建立基础。[32] 然而，这项倡议似乎没有实现，也没有以任何切实的方式推进。促进统一办法的其他尝试包括一项提案，即每年对各组织的网络安全措施进行调查，以制定内部成熟度基准，更好地评估系统的总体风险暴露。尽管进行了大量的准备工作，包括在 2018 年和 2019 年期间对约 20 个组织进行了两轮试点调查，但相关提案当时未能得到高级管理层的集体支持。反对这种标准制定工作的意见提出的主要论点是：一方面，组织设置和环境的多样性限制了集体评估的价值；另一方面，各实体没有为在组织之外分享内部网络安全评估做好充分准备，这一论点实际上是将网络安全风险作为甚至进行累积评估的障碍。在访谈中表达的意见表明，COVID-19 大流行可能改变了对网络安全的看法和心态，以前被认为雄心勃勃或不切实际的提案，今天或许更有可能引起兴趣和受到欢迎。事实上，在最近举行的机构间会议上，网络安全专家似乎又开始辩论是否有机会运用与首协会风险管理论坛最近采纳的模型类似的成熟度参考模型。

126. **确保最低限度防御水平的集体责任。**追求整个系统的全面统一，确实可能过于雄心勃勃，甚至不切实际，特别是考虑到对各组织成熟度的比较评估所得出的结论。正如智库 Gartner 所言，设法对各项机构网络安全安排和措施进行相互

[29] 大会第 63/262 号决议。

[30] A/68/7/Add.11, 第 6 段。

[31] CEB/2019/2, 第 39 段。

[32] CEB/2017/HLCM/ICT/9, 第 7-8 段。

比较，可能有助于就每个组织的相对成熟度作出表述，但无法就其中任何组织的绝对保护水平提供任何可靠的指示。[33] 然而，联合国系统各组织在声誉和业务方面具有交叉依赖关系，这使得各组织负有集体责任，须尽可能提高各个组织的标准，并相互帮助以达到标准。应当指出，最支持相关努力的正是那些拥有先进的网络安全框架和强大的内部或外部能力的组织。这个问题很微妙，但至关重要的是，联合国系统必须在参加组织各自的要求、各组织现有安排与全系统办法之间找到适当的平衡，全系统办法是要确定一项所有组织均须达到并有利于所有组织的最低标准。**检查专员认为，为联合国各组织，从而为整个系统确定基本保护水平和最低防御要求，仍然是值得继续追求的合理目标**。

127. **在业务方面创建共享能力的努力**。与预防、检测和应对网络威胁和攻击的全系统联合能力有关的问题，已在不同层级进行了多次辩论。大约 10 年前，信息和通信技术网发布了创建联合国计算机事件应对小组的路线图。[34] 这一倡议没有实现，因为当时无法就筹资模式达成一致。最近，信息安全特别利益小组重新开始评估创建联合国各实体共享安全行动中心的可行性，但该小组成员之间的讨论突显出仍然存在的一系列挑战(费用分摊，与各种原已存在的能力保持一致，就发生大规模攻击时支持措施的预期范围和优先等级达成一致等)。这些努力基于以下预期，即建立全系统事件应对能力将有可能实现大幅增效，同时也能提供更多的保护，特别是对无力维持备用能力以应对仍可能随时发生的攻击的组织而言。然而，这些尝试表明，有关目标虽然明确并得到了充分支持，但转化为实践的难度比预想的要大。经验表明，这些目标一旦达到一定的具体化程度，落实就变得困难起来。

128. **培训和提高认识领域能否作为全系统资源汇集的候选对象尚存争议**。一些提案似乎有望落实，但经过仔细审视后，却证明有一些争议，网络安全培训和提高认识领域就是其中一例。联检组最近的一份报告审查了与联合国系统学习方案有关的合作问题。[35] 其中一项审查结果是，不同的组织制定了类似的方案，工作明显存在重复。乍看上去，与网络安全有关的培训和提高认识资源似乎是全系统协作和资源汇集的自然选择。基于最终用户培训大都可以标准化的假设，并鉴于大部分相关学习材料不需要针对具体组织，因为各组织面临共同的威胁格局，在信息安全特别利益小组完成的第一批联合项目中，有一项涉及开发共同网络安全课程的核心组成部分，供成员调整和使用。这种课程开发办法似乎得到了一些组织的欢迎，这些组织选择采用联合国秘书处的在线信息安全意识培训模块，或者利用了联合国国际电子计算中心及其信息安全意识服务来定制和调整相关内容。然而，检查专员发现，各参加组织并没有对采取共同培训办法的好处形成强烈的共识。事实上，一些组织强烈反对标准化办法，特别提到与任务规定有关的具体情况或由通常漫长的集体开发进程所带来的制约，这种开发进程导致联合开发的内容很快过时，而且不容易被替换，同时还必须围绕“最小公分母”方式，如果没有进一步调整和扩展所需的大量后续投资，可能无法满足用户的期望和要求。鉴于这些考虑，一些组织开发了自己的培训模块，有时与外部提供者合作开

[33] Gartner, *The Urgency to Treat Cybersecurity as a Business Decision*, February 2020.

[34] CEB/2013/5, 第 38-39 段。

[35] JIU/REP/2020/2.

发，费用不菲。**检查专员仍然深信，联合国系统各组织将受益于某种统一的培训，即使对某些组织而言，这种培训可能需要加以调整。**

129. **优化网络安全资源。**受访的所有专家和管理人员一致认为，与私营部门实体相比，联合国各实体不论作为个体还是作为集体都是小行为体，在面对和应对有组织犯罪者实施的较复杂外部攻击或其他受到支持的攻击时，可用的资源充其量是有限的。与此同时，各参加组织为网络安全分配资源往往各自为政，并为追求自己的目的，有时是迫于应对某一特定事件的压力。联合国系统内有一种强烈的意识，即以联合方式处理网络安全问题能够提高效率。然而，关于在哪些领域汇集资源可能可行和有效，联检组各参加组织在答复中反馈不一。参加组织支持将一个领域作为潜在的费用节约的来源，即就外部服务提供者，尤其是商业和私营部门实体的参与进行更加密切的协调。许多组织确认使用了这类提供者，通常指定相同的公司提供相同或类似的服务，包括风险或漏洞评估、ISO 27001 审计或特定的软件解决方案，这意味着，每个组织要求这些公司遵照各自的内部筛选和供应商管理程序，同时还分别向这些公司付款。尽管存在一项有 20 个组织签署的相互承认协定，但只有少数组织表示受益于组织之间的谅解备忘录或类似安排，以利用彼此的采购程序或与网络安全保护和响应有关的服务合同。检查专员认识到，一些因素对这种联合举措的大规模实施构成限制，但要实现增效，这些举措仍然值得更多关注。检查专员通过访谈和问卷调查，查明了联合采购和广泛的协作采购所面临的一些挑战。联合国系统中不同的采购程序和规则形成了壁垒，限制了协作采购的应用。然而，一些障碍与规则和程序没有直接关系，而是与各组织的业务文化有关，这种文化可能不允许开放合作，而倾向于严格的组织控制。如联检组关于采购相关事项的报告[36] 所述，这方面的一些障碍包括高度集中采购与分散采购之间的业务理念差异，供资方式(譬如预付款)的差异，以及信通技术系统和应付款系统缺乏一致性。如果事实证明某些服务的联合采购不可行，参加组织至少应当竭尽全力，尽可能地协调工作。否则，不一致的采购做法可能促使商业提供商在整个系统内对同一服务收取不同的费用，从而造成一种竞争，这种竞争只对这些提供商有利，却会损害有关组织的财务利益。

130. **除协调举措和局部的业务解决方案以外，在全系统一级没有真正协同的努力。**网络安全在最高层级获得的重要地位和重大动力可以说为大力推动建立全系统能力创造了理想的条件。然而，尽管联合国系统内有一些重要的资源、机制和倡议，包括明显的政治意愿，但并没有明显的证据表明，在将这些鼓舞人心的言辞变为现实方面取得了进展。目前，没有一个实体正式负责推动与处理网络安全的统一办法有关的议程，也没有一个实体负责为联合国系统各组织制定和实施共同解决方案。目前，与网络安全有关的全系统努力在体制上集中于首协会下的机构间协调机制，在运作上得到联合国国际电子计算中心一定程度的支持，该中心是联合国系统几个组织某些共享服务的提供者。在本章中，检查专员审查各项体制和运作安排，包括这些安排之间似乎存在的某种程度的脱节，以及与网络安全事项有关的普遍的机构间动态(附件六)。检查专员还力求查明迄今为止取得的进展、目前的设置所固有的优势和局限性，以及有可能在哪些领域采取更有力的集体行动，以尽可能切实可行和合理地制订整个联合国系统的对策。

[36] 见 JIU/REP/2013/1.

B. 处理网络安全的机构间机制

131. **机构间机制长期关注网络安全。**自行政协调委员会的时代以来，网络安全一直以“信息(系统)安全”的表述出现在全系统层面的信息技术话语中。早在 1994 年，信息和通信技术网(自 2018 年起更名为数字和技术网)的前身成立的一个任务组就受托审查 1992 年发布的一套“联合国各组织信息系统安全准则”，[37] 这表明，甚至在更早的时候就对这一问题投入了相当大的关注和努力。应当指出，这些准则代表着全面、极其先进的努力，目的是在管理方面和业务方面摸清网络安全的不同层面并就此提供指导，该文件中使用的术语有些过时，但不应忽视的事实是，文件的内容和建议中有很大一部分即使在 30 年后的今天仍然具有重要性。

132. **持续关注协调一致的网络安全方法。**十年之后，协调应对网络威胁的设想仍然出现在正式记录中，2002 年，首协会的成员认识到：“尽管各组织的安全需要分为不同的类别(一些组织拥有极其机密和敏感的数据库)，但一些重要问题是所有组织共同面临的，必须紧急处理。”[38] 2010 年，“信息安全”一词似乎已被“网络安全”取代，当人们再次提出要确定网络安全的“全系统办法蓝图”，同时将网络威胁对“所有部门”的影响描述为“可能的网络海啸”时，[39] 网络安全获得了显著的势头。之后几年，管理问题高级别委员会也发表了类似的声明，称发现“在如何以最好的方式保护[联合国系统各组织]免受业务中断和安全威胁影响方面，有着相当大的共同点”，[40] 而信息和技术网指出，“加强各机构抵御网络威胁的能力必须仍然是优先事项”。[41]

133. **2013 年和 2014 年就网络安全和网络犯罪通过了具有里程碑意义的全系统文件。**2010 年，首协会委托管理问题高级别委员会和方案问题高级别委员会在国际电联和联合国毒品和犯罪问题办公室(毒品和犯罪问题办公室)的领导下联合处理这一问题，联合国贸易和发展会议(贸发会议)、开发署和教科文组织后来也参与了这项工作。这一贯穿各领域的举措最终促成关于网络安全和网络犯罪的联合国全系统框架于 2013 年被核可，[42] 以该框架为基础的关于网络安全和网络犯罪的联合国系统内部协调计划于 2014 年被核可。[43] 尽管这两份文件主要侧重于联合国工作的“外向”层面(即支持会员国就这一主题所作努力的方案活动)，但为确定联合国系统网络安全的“内向”层面提供了坚实的起点(方框 9)。然而，检查专员注意到，没有一个参加组织在审查报告编写期间提到有关框架或计划。虽然计划本身似乎并没有成为联合国系统持续使用的基准点，但检查专员确信，其中所载的核心原则和要素继续为活跃在该领域的相关机构间实体的工作计划提供信息。

[37] 信息系统协调咨询委员会，《联合国各组织信息系统安全准则》，纽约，1992 年。

[38] CEB/2002/HLCM/10, 第 8 段。

[39] CEB/2010/1, 第 53 段。

[40] CEB/2013/5, 第 36 段。

[41] CEB/2013/2, 第 58 段。

[42] 同上，第 85 段和附件三(关于网络安全和网络犯罪的联合国全系统框架)。

[43] 关于网络安全和网络犯罪的联合国系统内部协调计划，2014 年 11 月，内部文件。

方框 9: 关于网络安全和网络犯罪的全系统框架和内部协调计划

针对会员国对网络犯罪和网络安全的关切，首协会 2013 年第二届常会核可了关于网络安全和网络犯罪的联合国全系统框架，为联合国系统各组织之间的协调奠定了基础。

框架：

- 介绍关键概念的一些常见定义，并概述主题的范围
- 强调各有关实体相关任务之间的交叉
- 确立网络犯罪和网络安全方面方案制定和技术援助的基本原则
- 载有关于如何加强合作，向会员国交付相关技术援助的指南。

在该框架的基础上，2014 年制定了关于网络安全和网络犯罪的联合国系统内部协调计划，以指导联合国系统各组织在网络安全和网络犯罪领域的内部协调，重点围绕秘书长强调的有可能在整个联合国系统采取联合行动的五大事项。对于每个事项，该计划概述了一系列共同原则和行动要点，请各组织采纳。特别是，鼓励行政首长根据信息和通信技术网商定的培训大纲，为工作人员开发和启动借助于计算机的强制性网络安全培训课程，并创建一个跨组织的计算机事件应对小组。这些也是管理问题高级别委员会主席认为与该委员会工作具有关联性的行动要点(CEB/2014/5, 第 72 段)。

以下事项与本次审查的关联性特别大：

事项 1: 在各个机构和整个联合国系统确保有效的内部准备，以应对网络威胁，包括消除政策和资源方面的障碍，使各机构能够采取联合行动，通过将网络安全纳入风险评估和风险管理框架等办法，更好地共同保护联合国系统。

134. **信息安全特别利益小组作为主要的全系统网络安全专家论坛。**总体而言，审查发现，联合国系统处理网络安全问题的机构间机制早已建立，并且普遍在运作。信息安全特别利益小组成立于 2011 年，是联合国系统内促进机构间合作与协作，以优化成员组织内信息安全的主要机制，该小组向数字和技术网报告并接受其指示，在管理问题高级别委员会的总体指导下运作。根据该小组的职权范围，其成员被明确限定为首协会成员组织的首席信息安全干事或同等人员。如果成员组织没有这种职能，通常由一名信通技术干事代表各自的组织。信息安全特别利益小组的工作方法包括：举行年度专题讨论会，邀请外部发言者参加；在年度专题讨论会期间举行执行会议，进行正式决策；组织有时限的工作组，由牵头组织自愿推动审议所关心的议题。一些非首协会成员组织作为观察员参加信息安全特别利益小组的工作，但没有表决权，其中包括联合国国际电子计算中心。该小组由正式成员轮流担任主席，在编写本报告时，主席由联合国秘书处信息和通信技术厅担任。

135. **主要机构间部门作为交流论坛的效用得到确认。**信息安全特别利益小组是联合国网络安全从业人员定期聚集一堂，讨论整个系统的挑战、机遇和良好做法的官方论坛，已获得相当大的专业信誉。分析信息安全特别利益小组专题讨论会最新报告的内容证实，该小组内部就广泛的业务和战略问题进行了大量辩论并给

予高度关注，譬如云安全和云风险管理、数字身份管理、网络安全成熟度标准制定、信息安全意识培训，以及最近的共享安全行动中心和整合威胁情报服务的构想。事实上，约三分之二的参加组织在对联检组调查问卷的答复中表示，它们认为该小组有效促进了联合国各实体之间的合作与协调，并且重视该小组成员的实质性贡献以及与包括私营部门在内的外部专家交流的机会。主席为促进专业辩论和推进该小组的工作计划所作的努力受到许多成员的赞扬。与该小组的运作有关的一些较薄弱的方面已经得到处理，譬如信息安全特别利益小组专题讨论会举行的频率低，两届会议间隔期内互动有限，一些成员认为应当增加互动，以促进更持续和非正式的对话。针对这方面的明确需要，设立了一个专门的即时通信渠道，供信息安全特别利益小组成员之间直接进行非正式交流，以便在必要时迅速联络并分享信息。各首席信息安全干事对支持日常交流的努力给予好评，并确认在日常工作中积极使用了这些渠道。

136. **机构间机制在所有层级处理网络安全问题。**有证据表明，从信息安全特别利益小组本身到数字和技术网以及管理问题高级别委员会，各机制正在就网络安全进行积极辩论，并确认为网络安全至关重要。在数字和技术网层级(该网汇聚信通技术部门主管，接收信息安全特别利益小组的报告和建议，以核可和转交管理问题高级别委员会)，“信息安全和网络安全”被列入该网 2019 年修订版职权范围[44] 所载的 10 项目标。在实践中，数字和技术网可以说对信息安全特别利益小组的工作普遍持赞赏态度，因为数字和技术网仅在少数情况下偏离信息安全特别利益小组采取的立场，该小组的大部分建议都得到核可，有时在修改后核可。在管理问题高级别委员会层级(该委员会在制定 2013 年的框架和 2014 年的协调计划方面发挥了重要作用)，网络安全载入了该委员会各项战略计划，包括作为风险管理和复原力建设战略优先事项的一项要素，载入了最新的战略计划(2017-2020 年)。这项战略计划载有一项声明，指出管理问题高级别委员会将重新努力促进对网络威胁的监测和应对，包括在全系统一级执行减轻措施。[45] 然而，管理问题高级别委员会虽然在一般意义上清楚地认识到网络安全是令人关切的问题，但该委员会的记录表明其很少收到与网络安全有关的具体建议和事项。在这方面，检查专员注意到，在对联检组调查问卷的答复中，仅有三分之一的参加组织认为，信息安全特别利益小组为首协会机制上层的行动有效创造了动力。

137. **落实信息安全特别利益小组的建议和指导，要依靠该小组的成员。**在本次审查期间，检查专员发现，联合国系统在网络安全方面的机构间协调与合作尚未产生预期成果。虽然每年通过信息安全特别利益小组推进大量的概念性工作，网络安全问题也得到了高级管理层的关注，但在推进共享解决方案、共同或协同办法以及联合项目方面进展缓慢。就背景而言，值得回顾的是，2018 年修订的信息安全特别利益小组职权范围的最新版本[46] 反映了该小组对分享知识、经验和解决方案的承诺，特别是还包括执行联合项目。事实上，2018 年晚些时候，在信息和通信技术网过渡成为数字和技术网，并重新审视各个分组的任务规定之际，新更名的数字和通信网更进一步地作出决定：信息安全特别利益小组除促进信息安全领域的机构间协作和知识共享以外，还必须更加积极地设计和交付共享

[44] CEB/2019/HLCM/DTN/03/R1, 第 2 页。

[45] CEB/2016/HLCM/15, 第 13 页。

[46] CEB/2018/HLCM/ICT/3/Rev.1.

解决方案和创新。[47] 然而，数字和技术网虽然提出了让信息安全特别利益小组更多地参与系统解决方案实际开发的愿景，但却似乎没有在这方面相应地提供独立于该小组成员内部资源和个体参与水平的任何水平的业务能力。信息安全特别利益小组事实上缺乏有效的机制，无法促进落实和联合交付在机构间背景下制定的解决方案或达成的协议。检查专员注意到，关注自己的建议如何得到执行主要不是协调机构的责任，检查专员认为，整个系统缺乏经正式批准以接受首席信息安全干事集体指导并为共同利益服务的“业务部门”，这是阻碍在全系统网络安全办法方面取得进展的关键因素之一。本报告接下来的章节将更加详细地审视其他现有机制或机构能否合理地弥补执行中的差距。

138. **增强首席信息安全干事作为个体和群体的权能。**审查发现，信息安全特别利益小组成员的情况不尽相同，参与方式从工作层面到战略层面，不一而足，一些首席信息安全干事担任专业职类中的初级职等职位，另一些首席信息安全干事则担任中级至高级管理职务或领导整个部门。据信息安全特别利益小组成员称，该小组内部辩论的特点除了技术性强和讨论氛围坦率，成员的异质性据称对该小组内部的动态构成影响，并直接影响了该小组为联合国系统提供权威指导的能力。每个成员在各自组织的结构内被赋予的权能不同，在机构间实体代表组织作出承诺方面存在相关的限制，因此，无论是在有关组织内部，还是通过全系统协同行动集体发挥转型作用的机会有限。信息安全特别利益小组作为协调机构，在这方面面临与任何其他机构间机制相同的挑战，这些机制没有决策权，无法在系统一级直接强制性要求采取行动，这就是为什么期望在该论坛内实现落实是不现实的。同时，信息安全特别利益小组几乎无法影响其工作成果传达给每个组织高级管理层的方式。从数字和技术网的记录中可以明显看出对这些限制有充分的了解，这方面的证据是，数字和技术网呼吁自己的成员，即信通技术部门的主管增强首席信息安全干事的权能，尤其是通过授予他们更多的权力。[48] 还值得回顾的是，信息安全特别利益小组本身向数字和技术网报告，从而反映出在大多数组织中观察到的普遍的设置和相关的挑战，在这些组织中，首席信息安全干事向各自的信通技术部门主管报告。为抵消目前的设置产生的限制效应，**检查专员再次呼吁，在存在首席信息安全干事职能的组织，应扩大该职能的内部权能，包括扩大管理范围并使其尽可能独立于信通技术，在不存在首席信息安全干事职能的组织，应设立这一职能。**关于增强首席信息安全干事这一群体的权能，检查专员注意到，普遍没有兴趣让信息安全特别利益小组脱离数字和技术网并使该小组成为网络，从而提升该小组在机构间机制内的地位，使其能够直接向管理问题高级别委员会报告。一方面，反对这种转变的理由包括首协会机制内的网络、任务组和协调论坛广泛激增，这种状况本身被认为不太可能有助于推进网络安全问题或者有效确定该问题的优先等级。另一方面，普遍的看法似乎是，信息安全特别利益小组已经掌握充分和有力的渠道，可以通过数字和技术网以及管理问题高级别委员会，将网络安全考虑置于全系统战略讨论的优先位置。**检查专员重申，信息安全特别利益小组有效改善了联合国系统网络安全信息的共享，应当在不改变目前架构设置的情况下继续发挥作用。尽管如此，检查专员指出，需要设计一种机**

[47] CEB/2018/HLCM/ICTN/18, 第 6 页。

[48] 例如见 CEB/2017/HLCM/ICT/9, 第 8 页。

制，确保信息安全特别利益小组作为单独的实体，能够代表首协会和联合国系统提供战略指导。

C. 联合国国际电子计算中心作为网络安全服务的提供者

139. **重新审视联合国国际电子计算中心尚未发挥的潜力。**联检组 2019 年在关于云计算的报告中已经呼吁进一步审视各种条件，以更好地利用联合国国际电子计算中心及其为联合国系统提供的各种信通技术服务组合尚未发挥的潜力。联检组当时强调，进一步研究网络安全这种潜力的时机已经成熟。然而，考虑到联合国业务活动改革的更广泛视角，检查专员认为，有必要对联合国国际电子计算中心及其总体运作情况、业务模式、治理结构和任务进行单独、更具整体性的审查，这种审查甚至可以超越该中心作为信通技术服务提供者(客户目前包括但不限于联合国系统各组织)的既定作用的范围。联合国国际电子计算中心成立于 1971 年，在此之前，秘书长以相关机构间协调机制主席的身份，委托编写了一份详细的外部审计报告，该报告提交大会，任务是研究联合国、各专门机构和原子能机构的电子数据处理设施和需要。[49] 自 1971 年创立以来，该中心没有进行过这种审查，以追踪该中心的演变情况，并严格审视该中心应对联合国系统更多同时产生的需要的能力和内在潜力。**检查专员**注意到联检组曾呼吁查明这方面可能存在的障碍，并在不妨碍执行本报告所载正式建议的情况下，**设想今后可以对联合国国际电子计算中心进行全面分析，特别是寻求确定哪些结构、财务和行政方面的条件能够使该中心充分发挥潜力，成为整个联合国系统的战略伙伴和资源。**检查专员审查了联合国国际电子计算中心提供的网络安全服务，以及该中心的设置及其在这一特定领域自我定位的愿景。为本审查的目的，指导这一审查的问题之一是，该中心是否已经具备以及在多大程度上具备了成为联合国系统网络安全枢纽的条件。

任务和业务模式

140. **联合国国际电子计算中心的演变情况**(1971 年至 2021 年)。根据大会第 2741(XXV)号决议，依照联合国、开发署和卫生组织1971年缔结的协定备忘录，设立了联合国国际电子计算中心。该中心作为组织间设施，最初的创建目的，是向三个创始成员和其他用户提供“电子数据处理服务”，但其服务目录和客户群自 1970 年代以来发生了重大变化。联合国国际电子计算中心最为人知的是托管服务，以及为支持许多客户的企业资源管理系统提供共享信通技术基础设施，该中心的活动范围已经扩展到云计算、机器人流程自动化、区块链、软件开发、信通技术咨询和网络安全等多个领域。同样，该中心的客户群也大幅增长。该中心从一开始就被设想为将有更多客户加入的设施，到 2003 年，客户从最初的 3 个倍增至逾 25 个联合国系统组织，到 2021 年则增加到 70 个左右，其中包括联合国系统各实体和附属组织以及几个非附属政府间组织、国际非政府组织和国际金融机构。2003 年，该中心的基本文书得到修正，为该中心的运作提供了更广泛的法律基础和更详细的参与规则，增加了一份新制定的“任务”文件，以具体阐述并扩大了原始文件所载为数不多的基本规定。该文件由所有伙伴组织经由联合国国际电子计算中心管理委员会分别通过，规定了中心的治理结构、业务模式和

[49] A/8072.

参加的基本条件。如该文件所述，联合国国际电子计算中心的两项主要职能是提供信息技术服务，包括业务服务和培训，并努力确保服务范围满足伙伴组织的需要。

141. **联合国国际电子计算中心的任务和业务模式的基本原则。**联合国国际电子计算中心通过经更新的职权范围，加强了最初的成立宗旨(即作为面向联合国系统各组织的服务提供者)，并将该中心提供的服务与客户产生的具体需求密切联系起来。与此同时，重新拟订主要职能使该中心能够尽可能不受限制地在数据处理的局限范围之外寻求开展新的工作，从而除其它外，使该中心获得提供网络安全服务的自由，虽然其任务规定中并未明确提及网络安全服务。新文件中再次强调并进一步阐述的一项要素是共享基础设施和共享服务的概念，目的是为联合国国际电子计算中心的客户实现规模经济。这被称为联合国国际电子计算中心的共享服务模式，使该中心能够降低服务费用，降低幅度与订购相应服务的客户数量的增加成正比。而联合国国际电子计算中心创立 50 年以来保持不变的要素包括：(a) 采用成本回收模式，这种模式实际上要求所有产品由客户基于既定需要和集体批准预先供资，同时不产生任何盈余收入，也不为研究和开发活动提供任何预算余地；(b) 服务目录具有自愿性质，各组织可以选择缴费使用，也可以选择不使用，根据每项服务的具体情况逐一作出决定；(c) 依赖“东道组织”(世卫组织)，联合国国际电子计算中心在行政上和法律上仍然附属于世卫组织，依靠该组织提供的设施、行政能力和监管框架，以便能够签订合同、征聘、拨付资金和实际运作。

142. **复杂的治理结构反映由客户驱动的服务提供者角色。**该中心为确保服务组合与所服务的客户相关，通过联合国国际电子计算中心管理委员会，与各伙伴组织的代表密切合作建立了服务目录。管理委员会由 41 名成员组成，不代表该中心服务的全部客户，因为对伙伴组织和该中心服务的用户(统称为该中心的客户)进行了区分。[50] 只有伙伴组织是管理委员会成员，拥有表决权，对该中心受权开发哪些服务项目有发言权，而不是伙伴组织的客户(即单纯的“用户”)只能订购已经开发的现有服务。此外，在根据每项服务的具体情况逐项选择进入的模式下，并非所有管理委员会成员都是网络安全服务的客户，反之亦然(附件八)。这意味着一种理论上的风险，即妨碍开发或加强联合国系统部分组织但不是所有组织都有具体需要的服务。具体就网络安全服务而言，2020 年设立了一个非正式咨询小组，成员包括网络安全服务的前三大资助方(目前为开发署、难民署和粮农组织)，目的是密切关注所提供服务的质量和相关性，并查明更多采用共享解决方案的机会。该咨询小组与联合国国际电子计算中心网络安全服务科科长有直接的沟通渠道，不过，服务开发方面的最终决定权仍属于管理委员会。总体而言，审查发现联合国国际电子计算中心的治理架构复杂，反映了该中心当前业务模式的多层次性质。现有形式的这种架构能否纳入更加突出甚至是规定的作用，并为联合国系统适当发挥这种作用，而无须进行一些重大调整，这个问题不易回答。本章 D 节将进一步详细探讨这方面的一些挑战。

[50] 根据创始协定备忘录 2003 年的修正案，“伙伴组织”一语是指利用国际电子计算中心服务并已被管理委员会接受为伙伴组织的联合国系统任何组织，而“用户”一语是指各国政府、伙伴组织以外的政府间组织、经主任同意利用该中心服务的非政府组织和其他政府实体。

143. **联合国国际电子计算中心业务模式的利弊**。特定的服务一旦开发出来，订购该服务的所有客户都要支付使用费，使用费由管理委员会每年确定和审查，通常会下调，以反映规模经济，因为注册客户的增加降低了为所有客户提供相关服务的费用。在这方面，联合国国际电子计算中心自成立以来一直在严格的成本回收模式下运作，这种模式的优势是确保服务成本计算高度透明，促使该中心与客户不断协调，以及通过要求实际需求与据此开发和制作的服务尽可能保持一致，控制服务提供的范围。因此，商业和利润驱动的利益几乎可以排除在外，这是联合国国际电子计算中心与其他供应商的区别之一。同时，没有维持核心行政和管理职能的专门预算，[51] 这意味着这些费用必须计入所提供服务的收费。联合国国际电子计算中心的业务模式结合了成本回收和共享服务原则，事实证明，这对于实现该中心成为系统网络安全枢纽的愿景既是驱动力又是障碍。由此造成的情况是，联合国国际电子计算中心提供的服务依赖客户提供种子资金来支付开发新服务以满足需求所需的费用，而许多客户仅有能力购买在已订购用户数量足够多时才会开发的服务。这种情况有可能使财务实力较弱的机构系统性地处于不利地位，而这些机构的网络安全需求可能与有更多预算余地为特定服务预先提供资金的机构不同。

网络安全服务目录

144. **联合国国际电子计算中心在联合国网络安全格局中发挥关键作用**。在过去几年中，联合国国际电子计算中心已成为联合国系统网络安全方面的关键利益攸关方和资源。正如许多客户所证明的那样，该中心积累了相当多的网络安全知识专长和能力，并逐步扩大了服务提供范围，囊括网络安全领域的 13 项专业服务，通常使用“共同安全”这一品牌(图九和附件七)。这些服务涵盖网络安全治理层面和业务方面，联合国国际电子计算中心是以以下身份提供这些服务的：基础设施托管服务提供者，同时对托管数据、系统和应用的安全方面进行管理；专门的网络安全服务提供者；战略和管理问题顾问；或者事件的实际应对者，具体取决于所订购的服务类型。联合国国际电子计算中心提供的网络安全服务多种多样，反映出客户对网络安全服务的需求大幅增长。尽管网络安全相关产品仅占该中心服务目录的一小部分，仅占总供资额(截至 2021 年 1 月)的 6.1%，但该中心此类产品(现在和过去)的客户群包括 45 个组织，其中 21 个是首协会成员组织(共 31 个)，20 个是联检组参加组织(共 28 个)。尽管大约三分之一的组织没有被联合国国际电子计算中心的网络安全服务覆盖，特别是这其中还包括联合国秘书处，但如果不考虑该中心的作用和贡献，就很难设想今天联合国系统的网络安全状况。

[51] 联合国国际电子计算中心主任的 2016-2017 两年期报告和财务报表，2018 年 4 月发布，第 46 页。

图九

联合国国际电子计算中心网络安全服务概览(2021 年)

服务	联合检查组参加组织的数目(过去和现在的客户)
共同安全威胁情报	17
共同电子签名服务	14
事件应对	11
治理和首席信息安全干事支助服务	11
信息安全意识	10
漏洞管理	7
渗透测试	7
“网络钓鱼”模拟服务	6
共同安全行动服务	5
云安全评估	5
共同公钥基础设施	3
身份和访问管理	3
共同安全信息和事件管理	1

145. **共同安全威胁情报是联合国国际电子计算中心的旗舰网络安全服务。**在该中心提供的 13 项网络安全服务中，一些服务已经吸引了联合国系统内外的大量客户，而另一些服务尚未建立客户群。一项特别受欢迎的服务是该中心的共同安全威胁情报，有 17 个参加组织订购，这项服务可以被视为该中心的旗舰网络安全服务，证明了该中心的效用。共同安全威胁情报得到该中心绝大多数客户特别积极的评价，并满足了在系统层面阐述和一再重申的长期集体需要。该服务结合了威胁情报方面的各种内部和外部(包括商业和政府)来源，由联合国国际电子计算中心进行分析和筛选，以制作适合联合国环境和受众的易消化的信息包。在 2020 年 10 月举行的网络安全特别会议上，该中心的管理委员会批准了一项决议，请求所有伙伴组织和客户以可溯源或匿名的形式，与共同安全团队共享威胁情报和安全事件信息，以便进行分析并与更广泛的联合国系统共享。检查专员欢迎这项决定，但注意到，根据收到的资料，这项决定尚未得到全面执行。联检组所调查的大多数参加组织认为，这一领域适合在全系统一级进行更密切的合作，一些组织表示，除共享威胁情报，特别是漏洞指标以外，还可以就所采取的具体应对和恢复措施交流信息。然而，后一方面没有获得接受检查专员访谈的专家的一致支持，主要是由于保密性方面的关切。尽管如此，可以认为共同安全威胁情报是最有前途的网络安全服务，因为这项服务有可能顺理成章地获得全系统的全面订阅，并增强对系统的实际保护，这种保护甚至超过今天已经达到的水平。而联合国国际电子计算中心的整体网络安全服务组合可能就很难说具有同样的潜力。

146. **对联合国国际电子计算中心网络安全服务的评估褒贬不一。**尽管从结构方面说，联合国国际电子计算中心的客户可以密切控制向它们所提供的服务，但就服务满意度而言，参加组织的反馈相当不均衡，从“非常满意”到“非常不满意”。这可以归因于几项因素。一方面，20 个参加组织订购或者以往订购过该中心至少一项网络安全服务，这些组织所订购的服务数量和服务种类有一些差异，因此，各组织对服务满意度的评价也存在差异。相关组织网络安全框架成熟度的差异可能也影响到每个组织能够在多大程度上充分吸收和受益于所提供服务

的所有方面。另一方面，现在单独列出的一些服务过去捆绑在一起作为服务包提供，这本身招致一些批评，因为各实体必须订购服务包中并不需要的部分，才能利用需要或想要的部分。据报告，联合国国际电子计算中心于 2019 年停止了这种做法，现在允许客户充分灵活地选择最适合的服务水平和类型。此外，基本的满意度评级可能较笼统地说明客户与该中心的互动或服务体验的其他方面，使得这种评级不太可靠，不够细致，因而无法得出定论。鉴于这些限制，并鉴于检查专员的目的并不是要评估每项服务或联合国国际电子计算中心服务目录的整体效力，因此不可能辨别出对该中心持更加否定或肯定态度的组织在类型、规模或成熟度方面有哪些明显特征。总体而言，我们可以说，一些大大小小的组织高度赞赏该中心提供的网络安全服务，而同样数量的组织对该中心持严厉批评的立场。这种批评在某些情况下可能反映历史缺陷，而这些缺陷可能已被后来的发展所弥补，因此不应掩盖该中心作为网络安全服务提供者现在和将来所具有的潜力。然而，所表达的一些保留意见很可能切合现状，持续有效，甚至是针对反复出现的问题，因此应当得到非常认真的对待。无论如何，定期和细致的客户满意度评估可以提供宝贵的洞见，使该中心了解最好在哪些方面作出更大的努力，以回应客户的关切并及时吸引更多客户。此外，对作为网络安全服务提供者的联合国国际电子计算中心进行全面评估，可能有助于为该中心在网络安全领域的服务的总体质量和适用性提供更加客观的保证。

147. **认为利用联合国国际电子计算中心的服务所具有的优势。**客户所传达的利用联合国国际电子计算中心服务的理由包括：该中心熟谙联合国系统和联合国系统各组织的需要，因为该中心具有为它们开发定制服务的长期经验，受相同的行政规则和结构的约束，并与相关的机构间论坛接触。此外，该中心强调其具有几项比较优势，使之有别于商业服务提供商，这些优势包括：随着客户群的增长，服务费用逐步下降；不以利润为导向，因而关注将价格保持在可负担的水平，包括让寻找低成本选择的不太宽裕的组织负担得起；追求固有和共同的目标，即让联合国系统所有组织，包括作为联合国系统成员的该中心自身更加安全；有能力观察、适应并向客户直接学习，将取得的经验直接用于造福集体。联合国国际电子计算中心能够纵览整个系统及其所有组成部分，这也将该中心与往往只看到局部的商业提供者区别开来，从而确保该中心能够在任何特定客户的个体背景之外增加价值。检查专员认为，另一个令人信服的理由是，尽管存在现有的机构间机制，再加上中心的管理委员会这一基于代表制的治理层级，但没有一个实体的内在动机是追求联合国系统独特的集体利益，而不是追求实体成员的个体或者至多是团体(往往不可调和)利益。在这方面，联合国国际电子计算中心自视为中立、非政治性且无利害关系(由于采用成本回收模式)的全系统解决方案协调者，所考虑的是共同利益，而不是一些与极其稀缺的资源有关的考量，这些考量可能左右管理委员会成员，并使这些成员陷入潜在的利益冲突。

148. **认为把联合国国际电子计算中心作为网络安全提供者所具有的缺陷。**另一方面，一些组织对把联合国国际电子计算中心作为网络安全服务提供者作出了不那么赞许的评估，具体批评称，与商业提供商所能提供的服务相比，该中心的服务不那么物有所值。一些组织表示，它们的印象是，外部公司能够提供最先进的知识专长和工具，而联合国国际电子计算中心或任何一个组织即使在进行大量投资之后，所获得的能力也无法达到这种水平。客户中的其他声音反驳了这种印象，这些客户报告说，该中心近年来在知识专长和网络安全准备方面有了真正的

飞跃，这方面的证据是，该中心领导层在 ISO 认证和合规方面进行了大量投资，多样化地聘用专家，设立了一个不间断运作的共享安全行动中心，从而扩大了联合国国际电子计算中心的全天候监测能力，并加强了服务目录。然而，尽管作出了这些努力，但无法忽视的事实是，该中心仍然被认为在知识专长和物有所值方面持续存在差距，这种差距(可能确实)难以弥补。一些组织还指出，私营部门以更具竞争力的价格提供类似服务，一些答复者认为，尽管共享服务模式带来规模经济，但该中心对一些服务收费过高，而且收费方式不透明，使得这些服务对一些组织来说无法负担或不透明，对另一些组织来说性价比不高。事实上，联合国国际电子计算中心承认，与私营部门竞争超出其能力，甚至会在一些方面产生适得其反的效果。考虑到该中心的业务模式，如果有更多的客户加入，服务费用一般会降低，但费用恰恰在许多情况下是壁垒，从一开始就阻碍希望注册服务的组织加入。这一矛盾可以通过一些办法缓解，例如向适当的领域注入一些不太要求严格挂钩的资金，使该中心能够降低一些服务的费用，并有可能使费用低于私营部门提供商的收费，而不必试图完全取代这些服务。考虑到在私营部门增加价值更多、效率更高的领域与其竞争没有意义，行政首长应当探讨联合国国际电子计算中心能否成为商业提供商与联合国系统客户之间的接口，以降低合同费用，实现规模经济，最终提升议价能力。此外，联合国国际电子计算中心不妨结合上文所建议的对其网络安全服务的独立评估，对网络安全服务目录进行批判性的分析，以更好地辨别该中心可能具有比较优势的服务，并考虑在这些领域投入更多努力。最后，检查专员注意到，尽管联合国国际电子计算中心作为网络安全服务提供者，有时受到严厉的批评，但联合国系统利用了该中心提供的服务。

149. **在联合国国际电子计算中心现有任务范围内改进的机会。**虽然一些组织主张正式加强联合国国际电子计算中心作为联合国系统网络安全服务提供者的地位，但检查专员认为，很多改进可以在 2003 年修订的该中心的现有任务规定框架内实现，该框架已经为执行解决方案提供了坚实的基础，只要各利益攸关方多参与一点，这些解决方案就能发挥作用。即使由于相关的原因而有必要改变该中心的任务规定，这种改变也在该中心创始组织以及 2003 年签署该中心基本文书修正案的实体的集体权限之内，而不需要大会采取行动，直到将联合国国际电子计算中心作为实体，对其进行更加全面的分析，并分析该中心迄今取得的成就，以及有哪些可能导致该中心未发挥潜力的结构性原因可以通过大会采取行动来处理。检查专员认为，有一个关键方面需要从速或在不附加更多先决条件的情况下处理，即查明和处理现有结构和机制之间普遍存在的脱节以及现行供资模式中的一些制约，下文将对此加以详述。

D. 改善全系统战略方向与业务能力之间的联系

处理信息安全特别利益小组与联合国国际电子计算中心之间的体制脱节

150. **从形式上说，信息安全特别利益小组与联合国国际电子计算中心之间的关系有限。**鉴于参加信息安全特别利益小组这一机构间协调机制的组织与参加联合国国际电子计算中心管理委员会的组织之间有相当大的重叠(附件八)，人们会认为，信息安全特别利益小组是就可能适合联合国系统各组织的共享网络安全解决方案提供战略指导和指示的机构，而中心是联合国系统的业务执行机构。然而，这两个实体在形式上并没有联系，在实践中也不联合运作。在形式上，信息安全特别利益小组本身只发挥协调和信息共享作用，并没有受权以任何方式对联合国

国际电子计算中心发出指示，而联合国国际电子计算中心执行自己的管理委员会作出的决定，这些决定涉及为该中心的合作伙伴和客户(不包括联合国系统所有组织)开发的服务。在实践中，这两个机构之间的体制脱节或许不是决定性因素，但可能催生了一种动态，使联合国系统因错失更直接合作的机会而在增效方面付出高昂代价。

151. **实践中的互动不畅可归因于一系列因素。**事实上，联合国国际电子计算中心已获得信息安全特别利益小组的观察员地位，并参加该小组的讨论，但没有表决或提出辩论项目的权利。然而，该中心指出，它实际上被剥夺了在信息安全特别利益小组的论坛宣传服务目录或在该论坛要求就解决方案提供直接反馈的可能性。这一立场在一定程度上可以用联合国国际电子计算中心的性质解释，该中心是组织间设施，而不是依其地位可以获得首协会成员资格从而享有充分参与权的实体。还有人指出，有一种基本看法认为，联合国国际电子计算中心主要是联合国系统各组织的供应方，而不是合作伙伴，这进一步阻碍了该中心充分融入现有的机构间机制。考虑到该中心采用客户驱动型设置，并发挥为伙伴组织提供定制计算服务的作用，将该中心视为供应方的看法确有一定道理。与此同时，该中心公开地把自己描述为联合国实体和联合国系统的正式成员。事实上，该中心领导层一直明确表示，如果获得机会，愿意将联合国国际电子计算中心作为联合国系统的网络安全枢纽，而一些组织甚至认为，该中心应将网络安全作为核心业务。然而，联合国系统已获授权的机构间机制与作为网络安全服务的特权提供者，并有可能承担系统在这一领域业务部门角色的联合国国际电子计算中心之间的互动存在挑战，在这些挑战得到处理和解决之前，上述设想可能注定一直无法实现。

152. **事实上的平行结构。**不妨以联合国国际电子计算中心主办的共同安全会议为例，说明机构间机制与该中心之间的互动如何促进针对所查明的需要自发制定解决方案，但同时也在网络安全领域造成了重复。自 2019 年以来，该会议为中心的网络安全服务客户提供了就业务方面共同关心的事项交流信息，并就所提供的服务提供反馈的工具。该会议已成为网络安全工作日历上一项经常性和备受好评的活动，得到与会者的许多称赞，许多与会者是联合国系统组织，在信息安全特别利益小组内也有代表。就联合国国际电子计算中心的目标，即改善与联合国系统的伙伴关系以及服务提供的操作方面而言，共同安全会议可以说在某种意义上为该中心填补了空白，该中心寻求通过信息安全特别利益小组与各组织直接接触，但这种接触未能如其所希望的那样富有成效和具体。有人甚至可能说，该会议实际上已成为联合国系统很大一部分机构的主要论坛，这是信息安全特别利益小组这一现有协调机制无法开展更注重解决方案的辩论所导致的直接后果。这些积极、创新的动态的缺点是，共同安全会议可能将本来完全可以在信息安全特别利益小组内进行的一些讨论转移到了另一个论坛，而该论坛理论上主要向联合国国际电子计算中心的客户开放，而不是向整个系统开放。这两个结构实际上是平行的，而不是相互补充，它们服务于非常相似的目的，一个结构由首协会主持，另一个结构由联合国国际电子计算中心主持，两个结构的存在有可能造成进一步的脱节和竞争，导致无效、重复和重叠。这是对两者之间的互动管理不力所产生的有害副作用之一。

153. **需要进一步协同增效。**这两个实体在采取行动改善互动方式时，应参考这些意见。一方面，信息安全特别利益小组需要作为集体加紧努力，以更具战略性地履行任务，查明适合采取共同解决方案的领域，即使解决方案不是针对整个系

统，至少也要针对一批网络安全态势的改善将提升整个系统网络安全状况的组织。如果信息安全特别利益小组未能利用代表联合国系统拥有的权威声音做到这一点，联合国国际电子计算中心可能会被迫介入并占据这一空间，而这种介入和占据的方式仍然限于所服务的客户群。与此同时，如果该中心把握信息安全特别利益小组无意中造成真空所带来的机会，原则上是有利于联合国系统的，因为这具有创新潜力，但在进行时不应脱离负责全系统网络安全协调与合作的官方机构。两个实体都有责任积极设法改善两者之间的互动，无论是通过正式措施还是非正式措施。事实上，该中心一些订户较多的网络安全服务即使没有受到信息安全特别利益小组任何正式意义上的委托，也被认为受到在该小组进行的交流的启发，或者直接出自这种交流。特别是，如果联合国国际电子计算中心仍然致力于在成为联合国系统网络安全枢纽的道路上继续前进，而不仅仅是服务于自己的客户，就不能继续脱离代表这种枢纽所服务的各组织集体需要的专家群体。此外，信息安全特别利益小组作为集体，是促进在这方面开展更具建设性合作的关键要素之一。存在协同增效和增强互补性的潜力，但这一潜力迄今未得到充分发挥。

154. **参加组织重新考虑使用联合国国际电子计算中心的网络安全服务。**一些组织建议规定联合国系统各组织必须使用联合国国际电子计算中心的网络安全服务，通过这种方式处理这两个实体之间的普遍脱节。有组织认为，这种做法还可以加强该中心作为共享服务提供者的服务范围和影响，以加快潜在的增效和降低成本。这一愿景并非得到所有组织的认同，其实际效果可能适得其反。一方面，这将从外部对提供者和所提供的服务强加和施行人为的垄断，从而剥夺联合国系统各组织就最适合自身需要的服务提供作出评价和决定的能动性。另一方面，联合国国际电子计算中心内部有正常运作的治理机制，这些机制已经能够使该中心的行政管理层与客户就网络安全服务的构建进行正常交流。检查专员认为，干预这些机制既不谨慎，也没有必要。**不过，检查专员在 2019 年已经鼓励联合国系统各组织和联合国国际电子计算中心寻找更多的共同点，以更多的共享服务补充各组织的现有能力。**[52] 特别是，检查专员认为，或许有必要重新审视可能导致个别组织以往退订或不订购该中心网络安全服务的一些原因。这种审视必须非常细致，理想的情况是(重新)评估所提供的每项网络安全服务本身的价值。一些服务可能确实尚未达到成熟的程度，或者还无法充分响应各组织的需要，使系统所有成员决定订购这些服务。联合国国际电子计算中心应继续努力弥补这方面的任何差距。检查专员还承认每个组织的个体特征。最终应由各组织负责根据自己的具体需要作出相关决定，特别是考虑到，在内部创建或者通过与外部提供商的合同安排创建的信息系统、应用程序和其他技术安排具有多样性。

捐助方自愿捐款，以补充为联合国系统共同解决方案提供的资金

155. **自愿捐款作为直接支助的手段。**检查专员认为，现在应该考虑利用自愿捐款作为补充供资机制，以便为维护联合国系统的总体网络安全态势提供更直接的资源。提供指定用于全系统措施的自愿捐款，可以消除阻碍实施共享网络安全解决方案的一些绊脚石，因为各参加组织内部缺乏资源可能影响了这些组织为共同资金池捐款的意愿。使联合国系统有可能利用独立于成员各自预算的捐助方捐款来源，可以减轻一些压力，而造成这种压力的原因一方面是这些预算中的回旋余地非常有限，有太多的组织优先事项在争夺日益稀缺的资金，另一方面是联合国

[52] JIU/REP/2019/5.

国际电子计算中心的成本回收模式。就成本回收模式造成的压力而言，自愿捐款将使联合国国际电子计算中心能够为伙伴组织开发创新服务线，特别是那些依赖较不发达的内部能力或在创建一般网络安全安排方面资源较少的组织。这种办法与共享服务模式相结合，将通过保持较低的服务费，继续促进提高成本效益，并有可能吸引更多的客户，从而进一步扩大积极影响。募集和支出这种自愿捐款的机制最好置于作为整体的联合国系统的直接领导之下，例如作为首协会秘书处管理下的信托基金设立，受益于信息安全特别利益小组的实质性投入，还是最好置于实际上是联合国系统许多共享解决方案的既定提供者的联合国国际电子计算中心，这是检查专员与有关对话者协商考虑的问题之一。检查专员在研究了各种相关选择后确定，这种基金最好置于要求开发所需服务时的日常支出具有业务可见度的实体，也就是联合国国际电子计算中心。

156. **网络安全信托基金**。从原则上说，联合国国际电子计算中心的任务规定自 2003 年修正以来，纳入了使该中心能够募集自愿捐款的规定，最近已有通过这一渠道供资的具体项目的先例。这一机制迄今未得到充分使用，而战略性地利用该机制，从而积极主动地设计由联合国系统所有组织或几个组织共享的服务，有可能带来重大变革。更广泛地宣传这种可能性的存在，并完善使这种可能性变为现实的条件，将为希望直接捐款用于加强全系统网络安全的会员国提供机会，会员国可以根据适用于专用捐助的条款，捐款支持共享网络安全解决方案。这还将促进落实联检组 2019 年的建议，即建立一项供资机制，使联合国国际电子计算中心能够突破成本回收模式的制约，开展研究和开发活动，这可能进一步惠益于作为客户的联合国系统各组织。因此，检查专员建议，经过适当协商之后，联合国国际电子计算中心主任应当设立一个网络安全信托基金，专门用于设计和开发系统最需要的共享网络安全服务。为将这一机制与伙伴组织和客户向中心提供的其他资金来源进一步区分开来，谨慎的做法是设立一个专门的信托基金，并附加特殊条件，以确保该基金的治理不会重复现有的结构性偏向和潜在的利益冲突，也不会重复由中心管理委员会和相关的全系统机构间实体重叠但有区别的成员构成所导致的无益的动态。

157. **运作信托基金**。因此，这种供资机制的职权范围将是其成功的关键。在职权范围中，应澄清不同利益攸关方的作用和责任，应为哪些类型的服务提供资金，以透明的方式分配资金的程序，包括相关的报告规定。特别是，设立该基金应主要服务于为联合国系统各组织提供有形产出的目的。该基金可以主要用于资助研究与开发，以启动各组织明显有兴趣、但准备分担所需种子资金的初始用户数达不到足够数量的网络安全服务。同样，对于有明确需求，需要种子资金，或者需要降低成本以使更多组织早日加入的现有服务，该基金可用于扩大这些服务的范围或深度。虽然该信托基金总体上须遵照世卫组织的财务条例和细则(联合国国际电子计算中心在这些条例和细则下运作)，但有机会在该基金的治理中纳入与主管机构间实体进行协商的要素。这将有助于为整个系统，而不是仅为中心的客户制定共同解决方案，从而进一步提高现有资源的利用率。鉴于大会在为创立联合国国际电子计算中心提供基础方面发挥的作用，请大会注意关于设立网络安全信托基金的建议，并请会员国向该基金捐款。

158. 预计执行以下建议将加强联合国系统各组织之间的协调与合作。

建议 3

联合国国际电子计算中心主任应争取至迟于 2022 年底设立一个信托基金接受捐助方捐款，信托基金将补充该中心设计、开发和提供共享服务和解决方案的能力，以加强联合国系统各组织的网络安全态势。

建议 4

联合国大会至迟应在其第七十七届会议上注意到向联合国国际电子计算中心主任提出的关于设立共享网络安全解决方案信托基金的建议，并邀请希望加强联合国系统各组织网络安全态势的会员国向该信托基金捐款。

E. 使实体安保与网络安全更趋一致的机会

159. **联合国安全管理系统未涵盖网络安全。**大会根据其第 59/276 号决议设立了安全和安保部，该部承担一项全系统任务，即为联合国人员和资产的安全和安保制定政策和问责框架以及运作标准和程序。2004 年赋予安全和安保部的任务中没有明确提及网络安全，也没有提及保护数据和数字资产或更广泛的网络环境，[53] 这也许并不令人意外，因为网络安全领域的重大全系统进展出现在 2013 年和 2014 年。尽管安全和安保部表示，信息安全指南适用于全系统，但联合国安全管理系统及与之相关的政策文件尚未阐明实体安保与网络安全之间的交汇点，以确定联合国系统不同利益攸关方在这方面的责任。检查专员欣见在《联合国安全管理系统安保政策手册》中列入了名为“信息安全——敏感性、分类和处理”的预留标题，检查专员认为，这表明在一定程度上认识到网络安全考虑对实体安全和安保职能的相关性。然而，相关章节“尚待拟订”，安全和安保部对目前是否需要单立一章表达了保留意见。同时，如法律事务厅所证实，与既定的解释相反，即与相关公约和东道国协定中关于保护财产和资产的法律提法涵盖数字资产和通信相反，不能认为管辖联合国系统实体安全和安保职能的现有任务规定和相关政策框架涵盖网络安全。

160. **机构间安保管理网与信息安全特别利益小组。**机构间安保管理网的职权范围也没有具体提及网络安全，该网络为管理问题高级别委员会全面审查与联合国安全管理系统有关的政策和资源相关问题提供支持，并监测联合国系统所有行为体执行安全管理政策、做法和程序的情况。联检组进行的研究证实，机构间安保管理网仅在极少数情况下接触这一话题，主要是从利用信通技术加强总体实体安保流程的角度出发，譬如将信通技术用于身份和访问管理目的(例如探索将生物识别出入卡用于房舍和数字空间出入管理的备选方案)或者旅行安全许可的信通技术辅助认证程序。更近一些时候，信息安全特别利益小组关于在该小组与机构

[53] 安全和安保部表示，该部和联合国安全管理系统处理的安全风险具体类别为内乱、武装冲突、恐怖主义、犯罪和危害(非蓄意)。

间安保管理网之间“就共同关心的问题”建立协调机制的建议于 2019 年被数字和技术网采纳。[54] 然而，除特定的项目以外，检查专员无法找到表明上述意图已落实的证据。请有关机构间机制进一步探讨，可以哪些切实可行的方式创建更经常的联络渠道，以加强合作。在这方面，向检查专员提出的一项建议是，机构间安保管理网的主席和信息安全特别利益小组的主席互相参加对方实体的会议，可以促进交流经验教训。

161. **与国家主管部门就网络安全事件进行接触的蓝图。**在一个领域，为实体安全和安保所确立的程序可以为网络领域提供一些启发，这一领域即是就网络攻击与国家主管部门进行接触。检查专员在本审查报告第二章(第 35-37 段)中较详细地讨论了确定是否与国家主管部门联系的复杂内部程序，而没有讨论的问题是，一旦作出这种决定会发生什么，以及如何与各个政府对口单位进行联络。这一问题远非简单明了，因为在国家层面，最适当的对口单位既有可能是国家计算机应急响应(或准备)小组，或称计算机安全事件应对小组所隶属的负责部委(例如内政部、国防部、通信部或技术部，具体取决于各部的管辖权)，也有可能是存在于同一国家的平行能力，这些能力可能处于国家情报局之下，任务是实施可能具有政治层面的网络攻击。因此，在国家层面，未必存在正式接收联合国系统各组织有关报告的中央联络点，这可能使信息的适当传递变得复杂。为就管理与实体安保有关的危机提供指导，《联合国安全管理系统安保政策手册》规定，指定官员“应请东道国政府指定联络点，这些联络点有权在危机影响联合国在该国的工作时调动和协调支助”。[55] 可以探讨类似的办法，作为处理网络事件的蓝图，同时承认，指定官员将受益于其组织网络安全职能就这些事项提供的专家咨询意见。

162. **系统内缺乏传递、接收和传送与网络相关信息的机制。**同样，应当制定从政府接收与网络相关信息的内部安排，但检查专员在审查过程中无法清楚地看出这些安排。一些对话者暗示，各政府对口单位抱有一些困惑，不清楚当在国家一级发现的网络攻击显示与联合国系统一个或多个组织有关联时，应与哪个组织联系，也不清楚应使用何种联络渠道。据称，这种情报通常可以获得并可随时共享，但没有任何机制负责将情报可靠地传递和传送给联合国系统内预定的接收者，特别是因为，外部实体不清楚这些情报可能涉及联合国系统的哪些成员。据称，这反过来又导致以往错失保护和捍卫组织资产免遭入侵的机会，因为无法确保这种网络情报的接受者具备可据以采取行动的必要知识专长。因此，既定的外交联络渠道被认为不够有效，导致各个组织和整个联合国系统未能在网络安全方面获益。

163. **采取统一办法的可取性和适当性。**上文第 35 至第 37 段解释了一些因素导致联合国系统各组织目前在与国家主管部门合作方面的做法不一致。问题在于，这方面的不一致是否会造成更多挑战，包括在管理东道国关系方面的潜在声誉风险，特别是在以下情况下：总部设在同一国家或者在同一国家驻留的几个联合国组织，就网络安全事项与相同的主管部门接触(或不接触)，却在合作事项上采取不同办法。**检查专员请管理问题高级别委员会集体思考对这种合作采取统一办法**

[54] CEB/2019/HLCM/DTN/02 和 CEB/2019/HLCM/DTN/07, 第 4-5 页。

[55] 《联合国安全管理系统安保政策手册》，D 节—在安保问题上与东道国的关系，第 14(d)段，“危机管理”。

的可取性和适当性，并在这方面制定相应的指南。信息安全特别利益小组、机构间安保管理网和法律顾问网完全有能力将各自的知识专长用于联合审查这一事项，并探讨安全方面的潜在增益、相关挑战，特别是通过指定组织联络点，包括在系统一级指定联络点，来传递、接收和传送网络威胁和风险信息的可行性。检查专员考虑到联合国国际电子计算中心参加了机构间安保管理网，并注意到该中心已表示，如果被正式赋予相关角色，它愿意代表联合国系统各组织，在整合与网络安全事件有关的信息和向国家主管部门通报信息方面发挥作用。虽然报告和与国家主管部门合作是每个组织自己职权范围内的事项，但联合国国际电子计算中心能够获得信息，使其据以辨别针对不同组织的攻击之间的联系和潜在的相互依存关系，而这些组织大概无一能够自行整合信息，这一事实是增强该中心在报告和合作事项中潜在作用的理由，应当加以探讨。因此，有关机构间机制在考虑这方面可能的统一办法时，还应邀请相关的利益攸关方，包括联合国国际电子计算中心，并研究这些利益攸关方的潜在贡献，特别是在联合国国际电子计算中心代表联合国系统收集、关联和分析网络入侵的法证证据的能力方面。

164. **使实体安保与网络安全更趋一致。**更广泛地说，并鉴于数字和技术网的前身于 1992 年制定的信息系统安全准则[56] 已经触及信息系统安全与实体安保之间的联系，而且这一问题在 2013 年和 2014 年各相关机构的讨论中再次出现，[57] 检查专员认为，现在应该重新努力，以使实体安保职能和网络安全职能更趋一致，确保提供尽可能高的保护，防止复杂的威胁。安全和安保部作为整个系统的中央主管部门和标准制定实体，可在承认现有交汇点方面发挥关键作用，并可成为促使组织文化发生重大转变的关键推动者。事实上，在联合国系统内，对实体安保的威胁已经得到极其严肃的对待，没有人质疑立即和有效地应对实体威胁的必要性。检查专员发现，在为各组织应对网络威胁的办法赋予同样的紧迫感方面，整体思路出现了一种谨慎的演进，但还需要有更多演进，以期将安全和安保部已经广泛采用的基于风险的方法和以问责为中心的结构化应对办法，从单纯的实体领域扩大到网络领域。这并不意味着应修订已经赋予安全和安保部的全系统任务，以纳入网络安全。检查专员承认，应对网络威胁行为体构成的新挑战，需要安全和安保部目前所不具备的资源和专门知识，如果不进行重大调整，就不可能移交这方面的任何一部分责任。在这一方向采取的任何行动都需要进行结构改革，包括大会采取行动，以及与联合国安全管理系统各利益攸关方进行广泛的内部协商和协调，包括就本报告其他部分(第 68 段)所述的与所需行政和财务资源以及需要提高安保人员技能相关的方面进行协商和协调。审查表明，围绕这一问题的全系统辩论目前还没有形成定论，以系统内可用的知识专长，尤其是机构间安保管理网和信息安全特别利益小组一级的知识专长为基础，重新努力并进行更仔细的审查，将会使这种辩论受益。因此，检查专员建议秘书长探索进一步利用联合国系统实体安保与网络安全趋同的机会，并研究可能的利用方式的益处和局限。向大会提交的与这一事项有关的报告，应当尽可能地参考负责处理网络安全问题的相关机构间协调机制与机构间安保管理网之间将进行的协商的结果，并酌情参考联合国国际电子计算中心的投入。

[56] 《联合国各组织信息系统安全准则》。

[57] CEB/2013/5, 第 40 段；机构间安保管理网第十九届会议(2013 年，无文号文件)和机构间安保管理网第二十届会议(2014 年，无文号文件)。

165. 预计执行以下建议将提高联合国系统应对网络安全威胁的成效。

建议 5

秘书长至迟应向联合国大会第七十八届会议提交一份报告，探索更多利用实体安保与网络安全之间趋同趋势的机会，以便确保以更具整体性的方法保护联合国人员和资产，并说明相应加强现有结构的必要措施，同时特别注意安全和安保部在这方面的潜在作用。

附件一

与网络安全和网络犯罪有关的政府间工作流

引言和用语

国际社会在若干政府间场合就网络安全相关问题进行了辩论。

一方面，大会的不同委员会以及向大会报告或以其他方式与大会相关联的机构审查了这一主题。一个工作流侧重于网络犯罪(1990 年代初被称为涉及计算机的犯罪)，另一个工作流侧重于从国际安全角度看信息和电信(包括信通技术安全及相关主题)。

另一方面，一些参加组织(例如国际电联、裁军事务厅、毒品和犯罪问题办公室、知识产权组织、开发署、贸发会议和原子能机构)的任务规定包括了网络安全的各个方面，这些方面受制于这些组织所支持的政府间进程。

尽管“网络犯罪”和“网络安全”这两个术语是从不同角度处理同一问题，但这两个术语不能互换。可以说，网络犯罪侧重于网络攻击的实施以及攻击者参与(借助网络或依靠网络的)非法活动所须承担的刑事责任。而网络安全涉及防御这类攻击，关注重点是攻击目标和防御，而不是犯罪者。

本附件概述联合国系统各组织层面不同的政府间工作流，工作流的起源和当前的工作，以及工作流之间的关系(如果有)。

工作流一：网络犯罪

自 1990 年代以来，网络犯罪被提上全球议事日程。表明国际社会认识到需要专门关注方案工作的网络层面，并需要投资于民族国家抵御网络攻击的能力(由联合国系统相关组织提供技术援助支持)的第一份书面记录可以追溯到 1990 年，最初是在打击跨境犯罪的背景下产生的。具体而言，大会第 45/121 号决议核可了第八届联合国预防犯罪和罪犯待遇大会的建议，特别是关于涉及计算机的犯罪的决议，其中呼吁各国加大努力，以更有效地打击涉及计算机的违法行为。大会第三委员会(社会、人道主义和文化委员会)在“打击为犯罪目的使用信息和通信技术行为”[1] 的标题下继续就这一主题开展工作，而预防犯罪和刑事司法委员会(经济及社会理事会的一个职司委员会)在“网络犯罪”的标题下开展相关工作。相关工作得到毒品和犯罪问题办公室的实务和行政支持。

为制定一项关于网络犯罪的国际公约而正在开展的工作。自 2010 年以来，一个不限成员名额政府间专家小组(被称为“网络犯罪问题政府间专家小组”)一直在努力编撰一项“对网络犯罪问题的全面研究报告”，该小组是在预防犯罪和刑事司法委员会的主持下，为开展上述研究而召集的。[2] 由此产生的成果加速涌现，并成熟为一项单独的努力，旨在就网络犯罪起草一项具有法律约束力的文书。该

[1] 大会第 73/187、第 74/247 和第 75/539 号决议，以及第 55/63 和第 56/121 号等较早的决议。

[2] 大会第 65/230 号决议。

文书的起草和谈判进程由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(被称为“特设委员会”)进行监督，该委员会由大会于 2019 年设立，并于 2020 年启动工作。[3] 这一进程的最终成果将主要针对作为所产生的公约缔约国的民族国家。该文书提供的法律框架主要用于规范在国家一级的罪犯(网络罪犯)个人待遇，因此对联合国系统各组织处理网络安全的办法没有什么直接影响。因此，本次审查对相关努力的关注有限。

工作流二：从国际安全角度看信息和电信

在另一个政府间工作流中，从 1998 年起，“考虑信息安全领域的现存威胁和潜在威胁”开始出现在大会各项决议中，这些决议在新引入、之后又一再提出的题为“从国际安全角度看信息和电信领域的发展”的议程项目之下。[4] 在大会第一委员会(裁军和国际安全委员会)下运作的两个政府间机构已着手处理这一主题，这两个机构是：(a) 政府专家组，由秘书长提名的专家组成，成员名额有限制，专家以个人身份任职，[5] 自 2004 年设立第一个专家组以来，目前已经设立了第六个此类专家组；[6] (b) 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(向联合国所有会员国开放，2018 年设立)。[7] 这两个小组的主要目标是“考虑信息安全领域的现存威胁和潜在威胁及为对付这些威胁可能采取的合作措施”，[8] 和“进一步制定[决议中所列]国家负责任行为的规则、规范和原则及其实施方式”。[9] 不限成员名额工作组和第六个政府专家组分别于 2021 年 3 月和 5 月完成了工作并通过了共识报告。[10] 最近新设立的 2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组预计将审议上一个工作组(涵盖期间为 2019-2020 年)的工作，并于 2021 年召开首次会议。[11] 这些机构的工作得到联合国裁军事务厅在实务和行政方面的支持。

联合国系统各组织在网络安全方面的任务

联合国系统几个组织的实务和技术合作任务涉及网络安全的各个方面。一个例子是国际电联，除其他外，国际电联主办信息社会世界峰会年度论坛，该论坛是推动信通技术促进发展问题的主要工具；国际电联也是信息社会世界峰会行动方针 C5“建立使用信通技术的信心和安全”的唯一协调方。承担这一角色的国际电联与主要利益攸关方合作，除其他外，帮助各国采取国家网络安全战略，建立国家事件应对能力，部署国际安全标准，保护儿童免受网上威胁和建设能力。在大会第二委员会(经济和金融委员会)拟定的题为“创建全球网络安全文化”的各项

[3] 大会第 74/247 号决议。

[4] 见大会第 53/70 号决议及其后续决议，最新的一项是第 75/240 号决议。

[5] 见大会第 58/32 号决议。

[6] 见大会第 73/226 号决议。

[7] 见大会第 73/27 号决议。

[8] 见大会第 58/32 号决议，第 4 段。

[9] 见大会第 73/27 号决议。

[10] 见 A/75/816。

[11] 见大会第 75/240 号决议。

大会决议中，[12] 提到了在信息社会世界峰会开展的一些工作。任务规定中包含网络安全部分的其他组织包括毒品和犯罪问题办公室、知识产权组织、开发署、贸发会议、裁军事务厅和原子能机构，许多其他组织也在不同程度上承担网络安全方面的任务。

在首协会框架下汇编了联合国系统各组织在网络安全和网络犯罪方面的任务和主要活动简编，目的是概述这些组织多年来在各自的任务和侧重点范围内，如何以各种方式参与提供技术援助和支助，以促进在该领域制定政策。然而，该简编仍然是一份内部文件，事实证明，这项任务过于艰巨，无法确定和更新。该简编提供了大量证据，证明了联合国系统各组织就这一主题开展的方案工作具有多样性和分散性。在这方面，方案问题高级别委员会一再指出，联合国系统必须采取协调一致的办法，同时铭记每个组织各自的任务具有互补性和一定程度的重叠。[13]

[12] 见大会第 57/239 号和第 64/211 号决议。

[13] 例如见 CEB/2010/HLCP-XX/CRP.7，第 3 段；CEB/2010/6，第 38-43 段；CEB/2011/HLCP-XXII/CRP.6；和 CEB/2014/6，第 42-49 段。

附件二

基于风险的网络安全方法的一些要素

除将网络安全正式纳入组织的机构风险登记册或风险矩阵之外，检查专员还希望着重指出基于风险的网络安全方法的三个方面，这些方面可能加速实现相关效益：(a) 具有针对性、系统性和适应性的风险评估方法；(b) 高级别战略风险偏好和风险承受能力陈述书；(c) 网络安全专家有适当的机会为风险管理过程提供专门知识；(d) 采用渗透测试作为风险管理工具。

- **有针对性的风险评估**。网络安全风险评估必须进行调整，以适合组织运作的环境，适当考虑一些标准，譬如组织的任务规定、财务和人员能力、业务模式、持有或拥有的信息类型，并考虑组织的特殊性，特别是网络安全事件会如何影响授权任务的执行，包括在分散的环境或不同的外地工作地点。一些参加组织参照行业标准来支持其风险评估进程，这可以被视为一种良好做法，前提是所参照的标准本身是根据在多大程度上适合所涉组织的情况而选择的(第 59-64 段)。除对风险评估进行调整以外，还应强调周期性方面，这不仅有助于采取系统方法，而且能够确保框架的适应性，最好能够对可能与定期审查周期不一致的不断变化的威胁格局作出临机反应。

- **风险偏好和风险承受能力陈述书**。更具战略性的网络安全风险管理办法的一个关键组成部分是阐明风险偏好和风险承受能力，最好是在立法机构和理事机构以及有关组织行政管理层的参与下进行(第 53-54 段)。最有意义的风险偏好和风险承受能力陈述书建立在对网络安全风险进行全面和定期评估的基础上，这种评估涵盖所有类别的网络安全威胁，不仅限于对手造成的威胁，也不仅限于组织外部的威胁(第 25-29 段)，并且既从信通技术部门收集有关机构信息系统状况和已知漏洞的信息，又本着全组织办法从业务单位收集信息。如以一套精心选择和设计的有意义的网络安全指标为依据，确定适当的风险偏好变得至关重要。这是针对具体组织的进程，将推动进一步的管理决定，譬如创建内部(而不是外包)机构网络安全能力；为该进程划拨资源；将文书和政策指导纳入监管框架；投资和在升级时作出事件应对决策。在知识产权组织和原子能机构这种管理特别敏感信息的组织，默认情况下的风险偏好可能很低。以往遭受过重大网络安全事件，可能也会使组织的风险偏好降低，但有可能导致对网络防御的过度投资，进而可能产生虚假的安全感。

- **网络安全专业人员参与风险管理流程**。为网络安全专业人员提供充分的机会，以便为机构风险管理流程提供信息，这似乎是理所当然的，但在许多组织远未成为现实。相关投入的形式和周期性不是决定性的，但网络安全专业人员以可靠(不受阻碍和非临时性)的方式接触组织内部风险管理的驱动力至关重要，应当以系统的方式确立，确保在组织风险管理框架的设计、实施和监测阶段反映出关键的网络安全考虑。在一些有首席信息安全干事职位的组织中，首席信息安全干事参

加机构风险管理委员会，或者被任命为委员会正式成员。就这一安排收到的反馈是积极的，将该安排作为各组织的做法可能具有价值。

- **渗透测试作为风险管理工具。**渗透测试(通常简称为“pen”测试)是经授权模拟针对组织的网络、系统和人力资源的实际攻击，同时使用攻击者通常运用的工具和手法，以期查明组织保护措施的漏洞，评估现有减轻风险措施的有效性，以及测试应对和恢复程序。渗透测试主要由外部承包商进行，所依据的规则旨在进行有针对性和有效的评估，同时尽量减小对组织资产和流程造成严重损害的可能性。一些参加组织利用了这一工具，在一些情况下，是在一段时间内聘用不同的承包商(例如交替聘用)，这些承包商最好具有多样的特质，任务是攻击相关组织(“红队”)和测试防御准备情况(“蓝队”)。有一个组织采用了将外部承包商(模拟攻击)与该组织安全行动中心成员(防御攻击)联合起来的办法，使各队之间能够就结果和可能的减轻行动进行实时沟通(“紫队”)。无论是使用一个还是多个承包商，渗透测试都是一项要求很高的活动，需要进行扎实的准备，并仔细选择值得信赖的专家评估员(充当攻击者)，因为即使是允许临时访问敏感系统和信息也存在真实的风险。然而，渗透测试是复杂、有效的风险管理工具，可用于支持业务连续性规划；渗透测试也是可靠的方法，可以从各种角度迅速了解组织的网络安全态势，突出组织总体防御中的漏洞或隔离区域内的特定漏洞(取决于测试的设定范围)。

附件三

联合检查组参加组织提到的关于网络安全的主要行业标准

ISO 27001(国际标准化组织，2005 年)[1]

ISO 27001 主要用于审计和合规目的，主要侧重于在网络安全防御的技术领域应当达到的标准，并提供相关指导。该标准遵循一套总体控制规范，包括 14 个控制域，旨在将网络安全纳入组织的业务目标和风险管理实践。主要控制域涵盖信息安全政策、资产管理、访问控制、操作和通信安全、事件管理和合规。该框架由于其特点，似乎最适合用于审查和审计资源充足的大型组织的网络安全措施。

美国国家标准和技术研究所的框架，1901 年[2]

美国国家标准和技术研究所通过确定组织的目标和优先事项，并通过举办适当的行动，为了解网络安全风险提供灵活和具有适应性的指导。这项最后更新于 2015 年的框架除了包括内部指南以外，还参照了其他标准、指南和做法，譬如互联网安全中心控制措施、国际标准化组织国际标准、信息和相关技术控制目标等。国家标准和技术研究所的行动计划确定了五项核心职能(识别、保护、检测、应对和恢复)，并将信息和决策流归入组织内的不同层级。由于该标准采用高度整体性的方法，似乎特别适合于界定组织的网络安全战略和政策。

信息和相关技术控制目标(信息系统审计与监督协会，1996 年)[3]

信息和相关技术控制目标是一个信息技术治理和管理框架，以最佳做法为基础，帮助各组织实现在合规和风险管理领域的目标，并使这些组织的信息技术战略与组织目标保持一致。该框架的办法遵循能力水平概念，强调使服务适合组织的需要。根据这一国际标准，信息安全方面被归为风险管理以及业务服务连续性和可用性的组成部分。除内部材料外，信息和相关技术控制目标还参照了其他标准和指南，包括美国国家标准和技术研究所的框架、ISO 27001 和互联网安全中心控制。信息和相关技术控制目标中包含的最为相关的协调目标包括信息技术风险管理、信息安全、合规性以及业务服务连续性和可用性。就网络安全指导而言，该标准似乎特别适合已经将信息和相关技术控制目标用于信通技术治理和管理框架的组织。此外，这项标准可以通过与其参照的其他标准(互联网安全中心控制、美国国家标准和技术研究所的框架和 ISO 27001)相结合来扩展。

信息技术基础设施库(大不列颠及北爱尔兰联合王国中央计算机和电信局，1980 年代)[4]

信息技术基础设施库是一套信通技术服务管理准则，包括一系列出版物，就信通技术服务交付以及各组织所需的必要程序和资源提供相关指导。该标准由联合王

[1] 可查阅 www.iso.org/home.html.

[2] 可查阅 www.nist.gov.

[3] 可查阅 www.isaca.org/credentialing/cobit/cobit-foundation.

[4] 可查阅 www.axelos.com/best-practice-solutions/itil.

国中央计算机和电信局于 1980 年代制定，由一套五卷本出版物组成，每卷涵盖信通技术服务管理周期的不同阶段。主要事项包括服务价值界定、业务发展、服务资产、市场分析和服务提供者类型。从 2005 年起，信息技术基础设施库最佳做法促进了 ISO 20000 标准的制定并与该标准保持一致。

互联网安全中心控制，2008 年[5]

该标准也被称为关键网络安全控制，提供了一套基于行业最佳做法的建议。虽然互联网安全中心控制主要以技术为导向，但也包括一些从更广泛的组织层面处理网络安全的控制，譬如提高认识培训和事件应对。该框架中的实施组似乎相当切实可行也非常有用，侧重于根据组织的规模、能力、技能、可利用的资源和数据敏感性实施行动。主要控制包括清单和资产、漏洞管理、安全配置、电子邮件和网络浏览器保护、数据恢复和保护、事件应对和渗透测试。事实证明，在已纳入网络安全层面风险框架的中小型组织，特别适合采用这种办法来实施网络安全防御战略。

[5] 可查阅 www.cisecurity.org/controls/.

附件四

联合国系统各组织的网络安全监管框架

(a) 网络安全监管框架的层次

战略层面	通常为单个文件，包含高层以充满抱负的措辞发表的陈述	确定组织愿景、目标和重大原则；概述基本的治理以及组织作用和责任；还有可能将网络安全作为业务决策加以阐述，包括陈述组织的风险承受能力或风险偏好	适用于组织的实体一级，主要由高级管理层负责执行
政策层面	一系列相互独立的文件，包含规范性、可据以采取行动的措辞，通常作为正式的行政通知发布	阐明支撑信息安全管理系统的组织原则，同时制定具有约束力的内部条例和细则，其中载有宗旨声明和按主题组织的相关行动(例如信息分类、风险管理、业务连续性和灾后恢复、信通技术数据和资产可接受的使用方式)，并指定具体的作用和责任	适用于所有工作人员，并包含在不遵守的情况下受到纪律处罚的可能性
程序层面	一系列准则或标准作业程序，通过描述旨在建立系统性做法的过程支持更高级别的政策	就应采取的具体步骤或应避免的行为提供详细指导(遵守密码使用惯例，运行定期防病毒扫描和软件更新，在使用作为赠品获得的 U 盘之前先进行扫描等)	可以适用于所有人员或者针对具体职位(例如信通技术人员、档案和记录管理人员以及采购专业干事)
技术层面	一系列技术规程，目的是确保正确和统一的执行	概述细致、分步骤的指导，需要具备与主题事项有关的丰富的专门技能才能应用和执行。相关主题除其它外，可能包括数据库配置、网络安全和云安全	主要针对技术专家

资料来源：联检组编写。

(b) 参加组织的信息和通信技术战略以及专门的网络安全政策文件

参加组织	将网络安全作为组成部分的信息和通信技术机构战略	专门的网络安全政策文件
联合国秘书处	有，《联合国的信息和通信技术》(A/69/517)和大会第 69/262 号决议	有，《联合国秘书处信息安全政策指令(2013 年)》
艾滋病署	无，《信通技术战略(2017-2020 年)》不包括网络安全	无，艾滋病署正在制定一项全球网络安全计划，其中也将包括网络安全政策
贸发会议	遵循联合国秘书处信息和通信技术战略	有，遵循联合国秘书处网络安全战略
开发署	有，《信息技术战略(2020-2023 年)》	有，《信息安全政策(2016 年)》
环境署	遵循联合国秘书处信息和通信技术战略	有，遵循联合国秘书处网络安全战略
人口基金	有，《信息和通信技术战略(2018-2021 年)》	有，《信息和通信技术安全政策》
人居署	遵循联合国秘书处信息和通信技术战略	有，遵循联合国秘书处网络安全战略
难民署	有，《信息技术战略(2020-2022 年)》(正在审查最后草案)	正在制订。
儿基会	有，《信息和通信技术战略》	有，《儿基会信息安全战略计划(2018-2022 年)》
毒品和犯罪问题办公室/维也纳办事处	遵循联合国秘书处信息和通信技术战略	有，遵循联合国秘书处网络安全战略
项目署	信通技术五年战略(正在制订)	有，《信息安全》
近东救济工程处	有，《信息管理部战略(2019-2020 年)》	有单独的信息安全政策(有待最终批准)
妇女署	有，《信息和通信技术战略(2018-2021 年)》	有，《信息安全政策》
粮食署	有，《机构信息技术战略(2016-2020 年)》	有，《机构信息和通信技术安全政策(2015 年)》
粮农组织	有，《信息和通信技术数字战略(2017 年)》	有，《信息安全政策》
原子能机构	有，《业务技术战略规划(2015-2020 年)》	有，《信息安全标准》
国际民航组织	有，《信息和通信技术数字战略(2017 年)》(正在审查)	有，《信息安全政策(2007 年，第二次修订版)》
劳工组织	有，《信息技术战略(2018-2021 年)》	有，《电子信息安全，政策声明(2010 年)》
海事组织	有，《信息和通信技术战略计划(2019-2023 年)》	有，《信息安全风险管理(2015 年)》
国际电联	无，国际电联采用更具整体性的方法，引入了组织复原力管理系统，包括进行详细的业务影响分析来摸清战略风险，制订业务影响战略，以及危机管理、业务连续性和信通技术灾后恢复	无
教科文组织	有，《知识管理和信息和通信技术战略(2018-2021 年)》	有，已纳入企业风险管理框架和《行政手册》(《信息和信息技术安全政策》)

参加组织	将网络安全作为组成部分的信息和通信技术机构战略	专门的网络安全政策文件
工发组织	机构信息和通信技术战略(2019-2021 年)	无
世旅组织	无，信息和通信技术战略不包括网络安全	无，正在制订。
万国邮联	无，万国邮联信通技术战略将于 2021 年 12 月颁布	无
世卫组织	有，《信息管理和技术战略(2019 年)》	有，《网络安全战略》
知识产权组织	有，《信息和通信技术战略》(正在制订新战略)	有，《信息安全政策和标准以及下一代信息安全战略(2021-2024 年)》
世界气象组织	有，《信息和通信技术战略(2020-2023 年)》	无

附件五

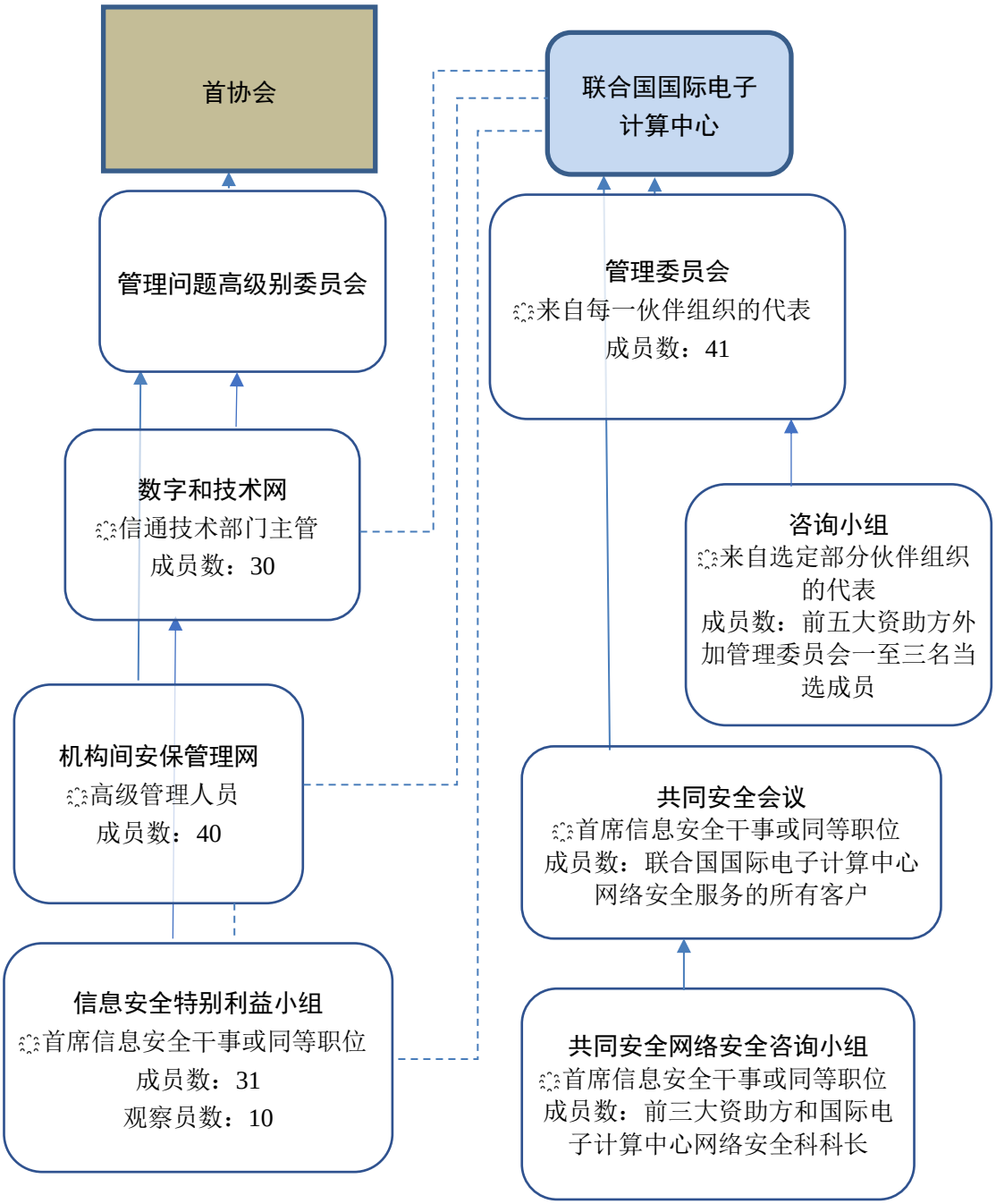
联合检查组参加组织截至 2021 年 1 月的网络安全安排和统属关系

参加组织	网络安全事项由专用或专门的内部能力管理	网络安全由(处于其他信通技术职能中的)组织信通技术部门涵盖	使用了联合国国际电子计算中心提供的“首席信息安全干事即服务”或安全治理服务	向信通技术主管(或同等人员)报告
联合国秘书处	√		X	√
艾滋病署		√	X	√
贸发会议		√	√(当前客户)	√
开发署	√		X	√
环境署		√	X	√
人口基金	√ (首席信息安全干事待招聘)	√ (至招聘完成为止)	√(当前客户)	√
难民署	√		X	√
儿基会	√		√(当前客户)	√
毒品和犯罪问题办公室/维也纳办事处		√	X	√
项目署	√		X	首席信息安全干事向首席财务干事和行政主任报告
近东救济工程处	√		X	√
妇女署		√	√(以往客户)	√
粮食署	√		√(以往客户)	√
粮农组织	√		√(当前客户)	√
原子能机构	√		X	√
国际民航组织	√		√(以往客户)	首席信息安全干事直接向行政主管报告
劳工组织	√		X	√
海事组织		√	X	√
国际电联	√		X	√
教科文组织	√		√(当前客户)	√
工发组织		√	X	√
世旅组织		√	X	√

参加组织	网络安全事项由专用或专门的内部能力管理	网络安全由(处于其他信通技术职能中的)组织信通技术部门涵盖	使用了联合国国际电子计算中心提供的“首席信息安全干事即服务”或安全治理服务	向信通技术主管(或同等人员)报告
万国邮联		√	X	√
世卫组织	√		√(以往客户)	√
知识产权组织	√		X	安全和信息保障司司长承担首席安保干事角色，同时负责实体安保和信息安全，向行政、财务和管理部门助理总干事报告
气象组织		√	√(当前客户)	√

附件六

网络安全方面的机构间体制和运作安排



资料来源：联检组编写。

附件七

联合检查组参加组织截至 2021 年 1 月订购的联合国国际电子计算中心网络安全服务概览

网络安全服务	简介	目前正在订购的联合检查组参加组织数目	以往订购过或完成过项目的联合检查组参加组织数目
共同安全威胁情报	持续和及时地从机构成员、商业安全公司、服务提供者、联邦、州和地方政府机构、执法机构及其他可靠来源收集信息，使订购服务的实体能够共享任何相关和可据以采取行动的实体安保和网络安全信息以及任何事件信息。	17	
共同电子签名服务	提供支持数字签名的能力。	14	
信息安全意识	提供战略咨询服务，以帮助组织建立最先进、有效的信息安全意识战略；业界领先的基于云的学习实验室；传播支持，包括讯息、简报、海报等交付成果；以及门户支持。	7	3
漏洞管理	将流程和技术结合起来，提供对漏洞和配置缺陷的持续识别和补救。除其他外，手段包括主机和应用程序漏洞扫描、安全配置检查和互联网足迹监测。	6	1
治理和首席信息安全干事支助服务	信息安全管理系统服务，目标是保护组织资产，减轻声誉受到负面影响、丢失相关信息和遭受恶意行为的风险，并减轻对知识产权、敏感数据和声誉构成的风险。	6	5
“网络钓鱼”模拟服务	测试各组织信息安全意识方案的有效性。工具包括设计和执行“网络钓鱼”模拟活动和后续报告。	6	
共同安全行动中心服务	提供监测、分析和应对网络安全事件的专门知识，使订购服务的实体能够结合使用技术流程和解决方案，及时应对安全事件。	4	1
事件应对	提供基于行业标准的事件处理程序，用于分析与事件相关的数据，并实时确定对任何组织安全事件的适当应对措施。	4	7
云安全评估	针对多个云解决方案的评估、迁移、实施和完全托管的运营支持以及成本管理。	4	1
渗透测试	能够识别信息安全控制中的弱点，并确定对手能够在多大程度上渗透被测试的网络或系统。	3	4

网络安全服务	简介	目前正在订购的联合检查组参加组织数目	以往订购过或完成过项目的联合检查组参加组织数目
共同公钥基础设施	提供和管理公钥和私钥加密以及数字签名，从而为电子交易和数据传输创造安全的环境。	3	
身份和访问管理	收集、分析和提供关于身份和访问管理应用程序的信息。	2	1
共同安全信息和事件管理	提供对应用程序和网络硬件生成的安全警报的实时分析。	1	

资料来源：联合国国际电子计算中心服务目录(2021 年 7 月)和各参加组织对联检组调查问卷的答复。

附件八

截至 2021 年 1 月，各参加组织在网络安全领域活跃实体中的成员资格

参加组织	数字和技术网 (第三十三届会议，2019 年)	信息安全特别利益小组 (第八次专题讨论会，2019 年)	联合国国际电子计算中心管理委员会 (2020 年)	联合国国际电子计算中心的网络安全服务客户 (过去和当前)
联合国秘书处	√	√	√	X
艾滋病署	√	X	√	X
贸发会议	√	X	√	√
开发署	√	√	√	√
环境署	√	X	√	X
人口基金	√	√	√	√
人居署	√	X	X[1]	X
难民署	√	√	√	√
儿基会	√	√	√	√
毒品和犯罪问题办公室/维也纳办事处	X	X	X[2]	√
项目署	√	X	√	√
近东救济工程处	√	X	√	√
妇女署	√	√	√	√
粮食署	√	√	√	√
粮农组织	√	X	√	√
原子能机构	√	√	√	√
国际民航组织	√	X	√	√
劳工组织	√	√	√	√
海事组织	√	X	√	√
国际电联	√	√	√	√
教科文组织	√	X	√	√
工发组织	√	√	√	√
世旅组织	X	√	X	√

[1] 联合国国际电子计算中心通报说，联合国秘书处代表人居署参加了管理委员会。

[2] 联合国国际电子计算中心通报说，联合国秘书处代表毒品和犯罪问题办公室/联合国维也纳办事处参加了管理委员会。

参加组织	数字和技术网 (第三十三届会议，2019 年)	信息安全特别利益小组 (第八次专题讨论会，2019 年)	联合国国际电子计算中心管理委员会 (2020 年)	联合国国际电子计算中心的网络安全服务客户 (过去和当前)
万国邮联	X	√	√	X
世卫组织	X	√	√	√
知识产权组织	√	√	√	√
气象组织	√	√	√	√

附件九

网络安全相关术语词汇表

“僵尸放牧”，僵尸网络	僵尸网络是大量遭到入侵的计算机，这些计算机被用来产生和发送垃圾邮件或病毒，或者以拒绝服务攻击方式向网络发送大量讯息，使网络不堪重负。 资料来源：ESCAL Institute of Advanced Technologies，安全术语词汇表 www.sans.org/security-resources/glossary-of-terms/
泄漏	有意或无意地泄露信息，从而对信息的保密性、完整性或可用性产生不利影响。 资料来源：加拿大网络安全中心 https://cyber.gc.ca/en/glossary
分布式拒绝服务攻击	利用多个遭到入侵的系统攻击单个目标的攻击方式。大量讯息涌入目标系统，迫使目标系统关闭，并拒绝向合法用户提供服务。 资料来源：加拿大网络安全中心 https://cyber.gc.ca/en/glossary
加密	一种数学函数，通过使信息仅能被拥有解密密钥者读取来保护信息。 资料来源：国家网络安全中心(英国) www.ncsc.gov.uk/information/ncsc-glossary
终端设备	在分布式网络中充当用户终端的任何网络连接设备，譬如台式计算机、笔记本电脑、智能手机、平板电脑、打印机或其他专用硬件，如零售点终端机或零售亭。 资料来源：Barracuda Networks Inc.，词汇表 www.barracuda.com/glossary/endpoint-device
防火墙	置于两个网络之间的安全屏障，用于控制两个网络之间可能通过的流量的数量和种类。防火墙可以保护本地系统资源不被外部访问。 资料来源：加拿大网络安全中心 https://cyber.gc.ca/en/glossary
物联网	由日常联网设备组成的网络，这些设备能够相互连接和交换信息。 资料来源：加拿大网络安全中心 https://cyber.gc.ca/en/glossary
恶意软件	设计在未经所有者同意的情况下渗透或破坏计算机系统的软件。恶意软件的常见形式包括计算机病毒、蠕虫、特洛伊木马、间谍软件和广告软件。 资料来源：加拿大网络安全中心 https://cyber.gc.ca/en/glossary
“网络钓鱼”	第三方试图通过模仿或欺骗通常众所周知的特定品牌，从个人、团体或组织获取保密信息，通常是为了经济利益。“钓鱼者”试图诱使用户泄露个人资料，譬如信用卡号、网上银行证书和其他敏感信息，随后可能利用这些信息实施欺诈行为。 资料来源：加拿大网络安全中心 https://cyber.gc.ca/en/glossary

勒索软件	一种恶意软件，用户除非支付一定金额的赎金，否则无法访问系统或数据。 资料来源：加拿大网络安全中心 https://cyber.gc.ca/en/glossary
影子 IT	部门或个人在组织内的信息技术或安全团队不知情的情况下使用硬件或软件。 资料来源：思科 www.cisco.com/c/en/us/products/security/what-is-shadow-it.html
社会工程	操纵他人执行特定行动或者泄露对攻击者有用的信息。 资料来源：国家网络安全中心(英国) www.ncsc.gov.uk/information/ncsc-glossary
“鱼叉式网络钓鱼”	使用欺骗性的电子邮件，以说服组织内部的人员透露用户名或密码。与涉及群发邮件的“网络钓鱼”不同，“鱼叉式网络钓鱼”规模小，针对性强。 资料来源：加拿大网络安全中心 https://cyber.gc.ca/en/glossary
电邮地址欺骗	伪造传输的发送地址，以非法进入安全系统。 资料来源：国家安全系统委员会(美国) https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf
虚拟专用网络	一种专用通信网络，通常在一家公司内部或由几家不同的公司或组织使用，以在更广域的网络上传递信息。虚拟专用网络通信通常被加密或编码，以使流量不受来自承载虚拟专用网络的公共网络上其他用户的影响。 资料来源：加拿大网络安全中心 https://cyber.gc.ca/en/glossary
漏洞	信息系统或其环境的设计或执行中出现的缺陷或弱点，可被利用来对组织的资产或运作造成不利影响。 资料来源：加拿大网络安全中心 https://cyber.gc.ca/en/glossary

附件十

参加组织须就联合检查组建议采取的行动一览表

			联合国及联合国各基金和方案																	专门机构和原子能机构											
		预期影响	电算中心	联合国	艾滋病署	贸发会议	国际贸易中心	开发署	环境署	人口基金	人居署	难民署	儿基会	毒品和犯罪问题办公室	项目署	近东救济工程处	妇女署	粮食署	粮农组织	原子能机构	国际民航组织	劳工组织	海事组织	国际电联	教科文组织	工发组织	世旅组织	万国邮联	世卫组织	知识产权组织	气象组织
报告	供采取行动		☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
	供参考		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	建议 1	**f**		**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**
	建议 2	**f**		**L**	**L**			**L**	**L**	**L**			**L**		**L**		**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**
	建议 3	**c**	**E**																												
	建议 4	**c**		**L**																											
	建议 5	**f**		**E**																											

图例：

L: 供立法机构作决定的建议

E: 供行政首长采取行动的建议

☐ **：** 不需要该组织采取行动的建议

预期影响： **a:** 加强透明度和问责；**b:** 传播良好/最佳做法；**c:** 加强协调与合作；**d:** 增强连贯性和一致性；**e:** 加强控制和合规；**f:** 提高效力；**g:** 节省大量资金；**h:** 提高效率；**i:** 其他。