ITU-D 网络安全项目

全球网络安全指数 - GCIv5

修订和最终问卷

目录

全球网络安全指数 GCIv5 -
变更日志和定义

修订后的 GCIv5 问卷，包括前几版全球网络安全指数的相应措施、关键术语的定义以及指标/框架的理由

图例

代码- [版本号] – 相应版本号中问题/部分的代码

理由- [版本号] – 针对相应版本中的问题给出的任何逻辑或背景理由

全球网络安全指数指标（按支柱划分）

法律措施

理由-GCIv5：立法是一项关键措施，可为实体提供统一的框架，使其符合共同的监管基础，无论是在禁止特定犯罪行为或最低监管要求方面。法律框架概述了各利益攸关方的角色、职责和责任。网络安全法可以定义为有五个基本问题："1) 我们要保护什么？2) 我们在哪里保护谁？3) 我们如何确保安全？4) 我们什么时候保护？5) 我们为什么要确保安全？"[1]数据安全是网络安全的重要组成部分，但不是唯一的组成部分，因为网络安全包括"存储数据的系统和传输数据的网络"。[2]

法律措施还允许一个国家制定基本的违规应对机制：通过调查和起诉犯罪以及对违规或违法行为实施制裁。法律保护一般安全，保障公民的权利免受他人滥用，并确保防止滥用最新技术。立法框架设定了全面的最低行为标准，适用于所有人，并且可以在此基础上建立进一步的网络安全能力。最终，目标是使各国能够制定适当的立法，以便在全球范围内统一做法，并为可互操作的措施提供环境，促进国际打击网络犯罪。

可以根据处理网络安全和网络犯罪的法律机构和框架的存在和数量来衡量法律环境。该子组由以下绩效指标组成：

1 网络犯罪法

代码-GCIv5：Legal1

理由-GCIv5：网络犯罪法规定未经授权（无权）访问、干扰、拦截计算机、系统和数据。这些法律可以采取实体法和/或程序法、公法和/或私法、普通法、判例法、成文法、行政法或其他适用的法律形式。

1.1 关于未经授权的在线行为的法律

代码-GCIv5：Legal1.1

理由-GCIv5：各种在线行为会对在线活动的安全性和信心产生负面影响。其中一些行为已在国际协议中有所提及，例如 2011 年欧洲理事会网络犯罪公约（"布达佩斯公约"）。有关此类行为的现行立法可以为执法提供明确的指导方针，提供司法明确性，并对受这些行为影响的人提供补偿。

1.1.1 贵国是否有针对非法访问设备、计算机系统和数据的现行立法？

代码-GCIv5：Legal1.1.1

理由-GCIv5：各种在线行为会对在线活动的安全性和信心产生负面影响。解决此类行为的一种方法是通过立法。这个问题的目的是衡量一个国家在 GCI 问卷调查时是否有有效的具体立法来解决非法访问设备、计算机系统和数据的问题，这反过来又会导致对隐私、财产或个人尊严的损害，以及其他伤害或损害。已计划、已起草和目前尚未生效的立法在此不予考虑。

1.1.2 贵国是否有针对非法干扰（通过数据输入、更改和/或删除）设备、数据和计算机系统的立法？

代码-GCIv5：Legal1.1.2

---

[1] https://heinonline.org/HOL/P?h=hein.journals/ilr103&i=1022

[2] https://heinonline.org/HOL/P?h=hein.journals/ilr103&i=1022

理由-GCIv5：各种在线行为会对在线活动的安全性和信心产生负面影响。解决此类行为的一种方法是通过立法。这个问题的目的是衡量一个国家在 GCI 问卷调查时是否有有效的具体立法来解决对设备、数据和计算机系统的非法干扰（通过数据输入、更改和/或删除）。已计划、已起草和目前尚未生效的立法在此不予考虑。

1.1.3 贵国是否有针对非法拦截设备、数据和计算机系统的立法？

代码-GCIv5：Legal1.1.3

理由-GCIv5：各种在线行为会对在线活动的安全性和信心产生负面影响。解决此类行为的一种方法是通过立法。这个问题的目的是衡量一个国家在 GCI 问卷调查时是否有针对非法拦截设备、数据和计算机系统的具体立法。已计划、已起草和目前尚未生效的立法在此不予考虑。

1.1.4 贵国是否有针对在线身份的实体法？

代码-GCIv5：Legal1.1.4

理由-GCIv5：越来越多的在线活动需要人们能够以可靠和值得信赖的方式在线识别自己。法律，无论是针对在线活动、其他身份相关法律的一部分还是其他，都有助于为在线身份使用、管理和行为提供法律依据。

1.2 贵国是否有与计算机相关伪造有关的现行立法？（盗版/侵犯版权）？

代码-GCIv5：Legal1.2

理由-GCIv5：信任是数字生态系统的基础。与计算机相关的伪造侵蚀了这种信任。与计算机相关的伪造包括“未经授权故意输入、更改、删除或限制计算机数据，从而导致不真实的数据，意图使之看起来像是合法的，或者可用于合法目的，而不管此数据是否直接可读和可理解”[3]。“例如，如果犯罪者修改了来自金融机构的真实电子邮件并将修改后的版本发送给多个收件人（也称为“网络钓鱼”），就会出现这种情况。一些国家的做法是要求原始计算机数据与旨在创建具有约束力的法律义务的文档相关。其他则只要求犯罪者打算将由此产生的修改版本视为法律义务或对其采取行动。”[4]

1.3 网络安全法

代码-GCIv5：Legal1.3

理由-GCIv5：鉴于在线活动中反社会行为的抑制活动，使用户和社区感到不安全，以下衡量了对某些行为的监管。对这些行为的监管通常必须仔细平衡人权和《联合国人权公约》等采用的其他价值观。请注意，法律不需要明确提及它们适用于在线数字/环境，但在该国内部，司法机构认可它们适用于数字/在线环境。

1.3.1 贵国是否有适用于种族主义和仇外在线材料的现行立法？

代码-GCIv5：Legal1.3.1

理由-GCIv5：种族主义和仇外心理的在线材料对在线社区产生重大负面影响，包括减少多样性、煽动分歧，并可能对个人造成伤害。针对种族主义和仇外心理的现行立法应该明确，便于个人理解和遵守。接受技术中立的立法；如果存在相关的法律声明、法庭之友、判例法、过去的起诉或其他适当材料证明适用于在线情况，则该立法无需具体说明它适用于在线种族主义和仇外材料。

1.3.2 贵国是否有适用于有损个人尊严/诚信的在线骚扰和虐待的现行立法？

代码-GCIv5：Legal1.3.2

---

[3] https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/computer-related-offences.html

[4] http://www.unodc.org/documents/organized-crime/cybercrime/cybercrime_questionnaires/Member_State_questionnaire.xls

理由-GCIv5：有损个人尊严/诚信的骚扰和虐待会对人们产生重大的负面影响，尤其是当它发生在网上时。现行立法为执法部门提供指导，指导执法部门如何处理案件，并为受影响的人提供补偿机会，最终促进在线信任和安全。接受技术中立的立法；如果存在相关的法律声明、法庭之友、判例法、过去的起诉或其他适当的材料证明适用于在线情况，则该立法无需具体说明它适用于在线骚扰和虐待或仇外材料。

2 网络安全法规

代码-GCIv5：Legal2

基本原理-GCIv2：网络安全法规规定了针对数据保护、入侵通知、网络安全认证/标准化要求、网络安全措施的实施、网络安全审计要求、隐私保护、儿童上网保护（COP）、数字签名和电子交易、以及互联网供应商的义务的规则。法规通常是法律的实施框架，规定了法律应如何执行。各国可以通过明确、一致、适用和最新的法规来改进其对网络安全的承诺。

2.1 贵国是否有与个人数据保护相关的法规？

代码-GCIv5：Legal2.1

理由-GCIv5：个人数据监管加强数据管理，明确数据持有者的责任和个人权利。它可以规定数据持有者对他们如何使用个人数据负责，并确保组织不会滥用收集的数据。

2.2 贵国是否有与隐私保护相关的法规？

代码-GCIv5：Legal2.2

理由-GCIv5：隐私保护法规确保个人数据受到保护，组织在如何使用数据方面是透明的，并且个人有权访问和更正其个人数据。法规可以禁止组织在未经个人同意的情况下出售或共享个人数据。隐私保护可以确保个人可以对其个人数据进行控制。滥用个人数据可能助长网络犯罪和削弱对数字技术的信任。

2.3 贵国是否有适用于私营部门参与方的与通报数据泄露/事件相关的法规？

代码-GCIv5：Legal2.3

基本原理-GCIv5：数据泄露会通过财务和身份盗窃、负面声誉影响以及对数据持有者的惩罚性后果对个人、企业和政府产生负面影响。有效的监管可以包括数据泄露通知，要求参与方及时向个人、企业和政府通报数据泄露。这将允许个人、企业和政府采取措施保护自己免受数据泄露可能造成的伤害。数据泄露通知法规可以鼓励数据管理方面的优秀做法，要求及时通知，并为受影响的人提供追索权。

2.4 贵国是否有适用于国家政府机构、部门或其承包商的与网络安全审计要求相关的法规？

代码-GCIv5：Legal2.4

理由-GCIv5：有关网络安全审计要求的法规可以通过鼓励机构、部门和承包商寻找和修复其系统中的漏洞来促进发现网络安全风险并推动更好的网络安全实践。此外，法规可以鼓励机构、部门和承包商遵循网络安全的最佳做法并遵循国际标准。

2.5 贵国是否有适用于国家公共部门参与方的与网络安全标准相关的法规？

代码-GCIv5：Legal2.5

理由-GCIv5：公共部门参与方通常是网络攻击的目标。因此，重要的是这些参与方拥有强大的网络安全保护措施，以便他们能够保护自己和公民。制定适用于国家公共部门参与方的与网络安全标准相关的法规有助于确保这些参与方更好地免受网络攻击，并确保他们在网络安全方面遵循最佳做法。

标准包括但不限于以下各项：云安全知识（云安全联盟）、CISSP、SSCP、CSSLP CBK、网络安全取证分析师（ISC²）、GIAC、GIAC GSSP（SANS）、CISM、CISA、CRISC（ISACA）、CompTIA、C|CISO、CEH、ECSA、CHFI（EC 理事会）、OSSTMM（ISECOM）、PCIP/CCISP（关键基础设施研究所）、Q/ISP、软件安全工程师证书（安全大学）、CPP、PSP、PCI（ASIS）、LPQ、LPC（丢失防护研究所）、CFE（欺诈审查师认证协会）、CERT 认证计算机安全事件处理程序（SEI）、CITRMS（消费者金融教育研究所）、CSFA（网络安全研究所）、CIPP（IAPP）、ABCP、CBCP、MBCP（DRI）、BCCP、BCCS、BCCE、DRCS、DRCE（BCM）、CIA、CCSA（内部审计研究所）、（专业风险管理师国际协会）、PMP（项目管理研究所）、那些与 ISO 27001 信息安全管理系统标准要求、ISO 28000 供应链管理安全、ISA 62443 工业自动化和控制系统安全等相关的标准。

2.6 贵国是否有针对在政府服务和应用程序（e-govt）中使用数字签名和电子交易的法规？

***代码-GCIv5*：** Legal2.6

***基本原理-GCIv5*：** 政府越来越多地在其服务和应用程序中使用数字签名和电子交易。这种向电子系统的转变有很多好处，包括提高效率和安全性。但是，如果没有适当的法规，这些系统可能无法有效或安全地使用。

监管有助于确保公民可以相信他们的数据是安全的，并且政府系统高效可靠。

2.7 贵国是否有与未经请求的通信（也称为垃圾邮件）相关的法规？

***代码-GCIv5*：** Legal2.7

***理由-GCIv5*：** 通过规范未经请求的通信，各国可以为所有人创造更安全、更愉快的在线体验。这些法规有助于保护公民免受垃圾邮件的负面影响，并防止垃圾邮件发送者利用他人。

2.8 贵国是否有与识别和保护国家关键基础设施相关的法规？

***代码-GCIv5*：** Legal2.8

***理由-GCIv5*：** 通过确定和保护国家关键基础设施，一个国家可以管控网络相关风险。保护关键国家基础设施的法规有助于一个国家规划如何应对重大灾难或侵略，确保其能够快速有效地应对重大灾难或袭击。一个国家还需要制定从重大灾难或袭击中恢复的计划。

2.9 贵国是否有与保护上网儿童相关的法规？

***代码-GCIv5*：** Legal2.9

***理由-GCIv5*：** 通过相关法规解决保护上网儿童问题，相关机构和参与方能够采取行动并实施具体要求和规则，以应对和打击针对儿童和青少年的在线/网络犯罪。从行业运营商到执法部门和民间团体利益攸关方，这些规则必须由社会各部门和各阶层的广泛利益攸关方实施，这些利益攸关方应共同采取行动，支持为儿童和青少年营建安全可靠的数字环境。

技术措施

理由-GCIv5：技术是抵御网络威胁和恶意在线代理的第一道防线。如果没有足够的技术措施和能力来检测和应对网络攻击，各国及其各自的实体仍然容易受到网络威胁的影响。ICT 的出现和成功只有在信任和安全的环境中才能真正发展。因此，各国需要能够制定战略，为软件应用程序和系统建立公认的最低安全标准和认证方案。在开展这些工作的同时，还需要建立一个专注于在国家层面处理网络事件的国家实体，至少要有一个负责的政府机构，以及一个相应的国家监测、告警和事件响应框架。

技术措施可以根据一个国家是否认可或创建了处理网络安全问题的技术机构和框架以及其数量来衡量。该子组由以下绩效指标组成：

1 国家CERT/CIRT/CSIRT或SOC

代码-GCIv5： Tech1

理由-GCIv5： 国家层面的有效机制和体制结构对于发现、预防、响应和减轻网络威胁和事件是必要的。计算机事件响应小组（CIRT）、计算机安全事件响应小组（CSIRTS）、计算机应急响应小组（CERT）和安全运营中心（SOC）[5]负责保护、发现和响应网络安全事件，并且可以提高国家管控网络安全事件的能力。CIRT 或 SOC 可用于建立支持国家实施国家网络安全战略的知识库，以及保护关键信息基础设施的方法；支持培育国家网络安全文化和生态系统，以及相关的提高认识举措；支持开发相关的国家网络安全平台，例如电子政务服务、国家身份和访问管理框架；并进一步使该国能够发展和增强其事件响应和协调能力。

1.1 贵国是否拥有全面运作的国家/政府CIRT/CSIRT/CERT或SOC？

代码-GCIv5： Tech1.1

理由-GCIv5： 计算机事件响应小组（CIRT）、计算机安全事件响应小组（CSIRTS）、计算机应急响应小组（CERT）和安全运营中心（SOC）负责保护、发现和响应网络安全事件。具备如下条件的 CIRT/CSIRT/CERT 和 SOC 视为可全面运作：

- 定义明确且经过批准的组织结构
- 配备训练有素的有资质人员
- 建有安全设施（实施适当措施以保护设施免受物理和环境威胁）
- 为其运作制定和实施了详细的流程和程序
- 采用和实施了运作所需的技术
- 实施了与主要利益攸关方和合作伙伴互动的流程
- 有效和高效地向其负责区域提供服务。

实施 CIRT 的初始过程可能涉及评估（衡量建立 CIRT 的准备情况，以及相关利益攸关方参与所需的准备工作）、设计（为 CIRT 准备详细设计文件）和建立过程（实施基础设施、与利益攸关方、服务区域建立关系、建立授权流程、服务、启动运作以及申请国际协会会员资格）。

1.2 国家CIRT/CSIRT/CERT或SOC活动

代码-GCIv5： Tech1.2

理由-GCIv5： 一个国家的计算机事件响应小组（CIRT）、计算机安全事件响应小组（CSIRTS）、计算机应急响应小组（CERT）和安全运营中心（SOC）负责保护、发现和响应网络安全事件。它是网络安全事件报告的中心点。它还提供信息和技术援助，帮助相关组织预防、减轻和应对

[5] https://ieeexplore.ieee.org/document/9296846

网络事件。此外，国家 CIRT 或 SOC 对网络安全问题进行研究，并制定应对网络事件的最佳做法和导则。

1.2.1 贵国/政府CIRT/CSIRT/CERT或SOC是否开展和实施网络安全宣传活动？

代码-GCIv5： Tech1.2.1

理由-GCIv5： 国家 CIRT 或 SOC 可以在开展网络安全宣传活动中发挥重要作用；作为中央协调机构，他们可能会越来越多地了解当前和新出现的网络威胁、网络安全挑战、漏洞、对网络安全主要发展趋势的见解、网络安全的技术发展以及发现和应对网络威胁的最佳做法。为加强网络安全文化建设并促进有关网络安全措施、优秀做法和行为的知识，CIRT/CSIRT/CERT 或 SOC 应根据收集到的有关不断变化的威胁的信息，设计、执行和/或协调针对不同利益攸关方量身定制的网络安全宣传举措和活动，这些举措和活动是基于所收集的、关于不断变化的威胁状况、网络安全主要发展趋势和最佳做法的信息。

1.2.2 贵国/政府CIRT/CSIRT/CERT或SOC是否定期进行网络安全演习（CyberDrill）？

代码-GCIv5： Tech1.2.2

理由-GCIv5： 网络安全演习是有计划的活动，组织在此期间模拟网络中断以开发或测试相关能力，例如预防、发现、缓解、响应网络中断或从网络中断恢复。与相关利益攸关方定期举行的网络安全演习是增强网络安全准备和恢复能力的积极措施。CIRT/CSIRT/CERT 或 SOC 应定期制定和开展网络事件/危机管理演习，包括全国任何相关的公共或私营实体，以测试其事件响应能力。

1.2.3 贵国/政府CIRT/CSIRT/CERT或SOC是否提供公开的网络安全咨询？

代码-GCIv5： Tech1.2.3

理由-GCIv5： 公开可用的网络安全咨询确保各机构和部门了解潜在的网络安全威胁并采取预防措施。此外，咨询可有助于促进对网络安全威胁做出协调一致的响应。

1.3 国家/政府CIRT/CSIRT/CERT或SOC是否隶属于FIRST和/或在TF-CSIRT的列出名单中？

代码-GCIv5： Tech1.3

理由-GCIv5： 隶属于 FIRST 的国家 CIRT 或 SOC 受益于 CIRT 的全球网络、培训和资源、由 FIRST 员工提供的专业知识以及合作和分享最佳做法的机会。满足 FIRST 的资格标准需要各国的积极承诺。此问题将考虑是否在 TF-CSIRT 列出名单上的现状。

1.4 上述国家/政府CIRT/CSIRT/CERT或SOC是否隶属于区域性CIRT（例如APCERT、PACSON、AFRICA CERT、ENSIA、OIC、OAS）？

代码-GCIv5： Tech1.4

理由-GCIv5： 与区域性 CIRT 的从属关系包括与任何其他地区 CIRT 小组的任何正式或定期关系。加入地区 CIRT 或 CERT 有很多益处，包括知识和经验交流。区域性 CIRT 和 CERT 通常能够分享与国家情况相关的相关知识和经验。

2 行业CERT/CIRT/CSIRT或SOC

代码-GCIv5： Tech2

理由-GCIv5： 行业 CERT/CIRT/CSIRT 或 SOC 为在特定行业工作的成员提供服务，例如金融行业、学术界、能源、卫生、电信、公用事业、关键基础设施等。行业 CIRT 或 SOC 通过量身定制的专业威胁情报和服务为其成员提供服务。各国可能与其他国家设有联合的行业 CIRT 或 SOC，因为行业 CIRT 或 SOC 服务于多个国家特定行业的服务区域。就本指标而言，不接受军用 CIRT。

2.1 贵国是否设有行业性CIRT/CSIRT/CERT或SOC？

代码-GCIv5： Tech2.1

理由-GCIv5：行业 CERT/CIRT/CSIRT 或 SOC 为在特定行业工作的成员提供服务，例如金融行业、学术界、能源、卫生、电信、公用事业、关键基础设施等。行业 CIRT 或 SOC 通过量身定制的专业威胁情报和服务为其成员提供服务。各国可能与其他国家设有联合的行业 CIRT 或 SOC，因为行业 CIRT 服务于多个国家特定行业的服务区域。就本指标而言，不接受军用 CIRT。具备如下条件的行业 CIRT/CSIRT/CERT 和 SOC 视为可全面运作：

- 定义明确且经过批准的组织结构
- 配备训练有素的有资质人员
- 建有安全设施（实施适当措施以保护设施免受物理和环境威胁）
- 为其运作制定和实施了详细的流程和程序
- 采用和实施了运作所需的技术
- 实施了与主要利益攸关方和合作伙伴互动的流程
- 有效和高效地向其负责区域提供服务。

部分实施的行业 CIRT 可能涉及评估（衡量建立行业 CIRT 的准备情况，以及相关利益攸关方参与所需的准备工作）、设计（为 CIRT 准备详细设计文件）和建立过程（实施基础设施、与利益攸关方、服务区域建立关系、建立授权流程、服务、启动运作以及申请国际协会会员资格）。

2.2 行业CIRT/CSIRT/CERT或SOC活动

代码-GCIv5：Tech2.2

理由-GCIv5：一个行业计算机事件响应小组（CIRT）或行业计算机安全事件响应小组（CSIRTS）、行业计算机应急响应小组（CERT）或行业安全运营中心（SOC）负责保护、发现和响应网络安全事件。

行业 CIRT 或 SOC 是行业内网络安全事件报告的中心点。它还提供信息和技术援助，以帮助行业内的组织预防、减轻和应对网络事件。此外，行业 CIRT 或 SOC 对网络安全问题进行研究，并制定应对网络事件的最佳做法和指南。

2.2.1 行业CIRT、CSIRT或CERT或SOC是否为该行业开展和实施网络安全宣传活动？

代码-GCIv5：Tech2.2.1

理由-GCIv5：行业 CIRT 或 SOC 可以在针对特定行业开展网络安全意识宣传活动中发挥重要作用。作为该行业的中央协调机构，他们深入了解与其利益攸关方相关的网络安全趋势。基于特定行业和一般威胁情报，行业 CIRT 可以帮助开展和实施针对各个行业相关利益攸关方群体的宣传活动，以改进网络安全行为。

2.2.2 行业CIRT、CSIRT或CERT或SOC是否定期参加国家网络安全演习（CyberDrill）？

代码-GCIv5：Tech2.2.2

理由-GCIv5：网络安全演习是有计划的活动，组织在此期间模拟网络中断以开发或测试相关能力，例如预防、发现、缓解、响应网络中断或从网络中断恢复。行业 CIRT 参与国家网络安全演习是提高整体网络安全能力的一项积极措施。

2.2.3 行业CIRT、CSIRT或CERT或SOC是否在其服务区域内共享行业相关事件？

代码-GCIv5：Tech2.2.3

理由-GCIv5：共享行业相关威胁情报可以使行业利益攸关方更加了解相关威胁和漏洞，并提高事件响应时间和有效性。此外，这有助于对政府、私营部门和公众的网络安全事件做出更协调的响应。

3 实施网络安全标准的国家框架

代码-GCIv5：Tech3

理由 GCIv5：实施网络安全标准的国家框架包括政府批准（或认可）的框架（或多个框架），用于通过国际公认的网络安全标准对专业人员进行认证和认可。这些认证、认可和标准包括但不限于以下内容：云安全知识（云安全联盟）、CISSP、SSCP、CSSLP CBK、网络安全取证分析师（ISC²）、GIAC、GIAC GSSP（SANS）、CISM、CISA、CRISC（ISACA）、CompTIA、C|CISO、CEH、ECSA、CHFI（EC 理事会）、OSSTMM（ISECOM）、PCIP/CCISP （关键基础设施研究所）、Q/ISP、软件安全工程师证书（安全大学）、CPP、PSP、PCI（ASIS）、LPQ、LPC（丢失防护研究所）、CFE（欺诈审查师认证协会）、CERT 认证计算机安全事件处理程序（SEI）、CITRMS（消费者金融教育研究所）、CSFA（网络安全研究所）、CIPP（IAPP）、ABCP、CBCP、MBCP（DRI）、BCCP、BCCS、BCCE、DRCS、DRCE（BCM）、CIA、CCSA（内部审计研究所）、（专业风险管理师国际协会）、PMP（项目管理研究所）、那些与 ISO 27001 信息安全管理系统标准要求、ISO 28000 供应链管理安全、ISA 62443 工业自动化和控制系统安全等相关的标准。

3.1 贵国政府是否有实施/采用国家或国际公认的网络安全标准框架？

代码-GCIv5：Tech3.1

理由-GCIv5：实施网络安全标准的国家框架包括政府批准（或认可）的框架（或多个框架），用于实施/采用国家或国际公认的网络安全标准。框架可以为标准的实施/采用定义计划或路线图，利益攸关方将参与其中，流程将用于未来的更新，其他方法则指导实施。
标准包括但不限于以下内容：云安全知识（云安全联盟）、CISSP、SSCP、CSSLP CBK、网络安全取证分析师（ISC²）、GIAC、GIAC GSSP（SANS）、CISM、CISA、CRISC（ISACA）、CompTIA、C|CISO、CEH、ECSA、CHFI（EC 理事会）、OSSTMM（ISECOM）、PCIP/CCISP（关键基础设施研究所）、Q/ISP、软件安全工程师证书（安全大学）、CPP、PSP、PCI（ASIS）、LPQ、LPC（丢失防护研究所）、CFE（欺诈审查师认证协会）、CERT 认证计算机安全事件处理程序（SEI）、CITRMS（消费者金融教育研究所）、CSFA（网络安全研究所）、CIPP（IAPP）、ABCP、CBCP、MBCP（DRI）、BCCP、BCCS、BCCE、DRCS、DRCE（BCM）、CIA、CCSA（内部审计研究所）、（专业风险管理师国际协会）、PMP（项目管理研究所）、那些与 ISO 27001 信息安全管理系统标准要求、ISO 28000 供应链管理安全、ISA 62443 工业自动化和控制系统安全等相关的标准。

3.2 实施/采用国家或国际公认的网络安全标准的框架是否涉及关键基础设施？

代码-GCIv5：Tech3.2

理由-GCIv5：将关键基础设施作为实施/采用国家或国际公认的网络安全标准的任何框架的一部分，对于增强关键基础设施的保护和恢复能力并帮助他们减少漏洞和有效管理网络安全风险至关重要。

组织措施

理由-GCIv5：组织措施对于国家网络安全态势的恰当实施是必要的。政府需要制定战略目标，并在实施、交付和衡量方面制定全面计划。需要建立并启用治理结构，将网络安全态势付诸实施，监测实施情况并评估结果。如果没有明确界定的伙伴组织网络，不同部门和行业开展的跨行业、民间团体和学术界的共同努力就会变得各自为政、互不关联，从而阻碍在网络安全能力发展方面实现国家协调统一的努力。

组织结构可以根据在国家层面组织网络安全发展的机构和战略的存在和数量予以衡量。建立有效的组织结构对于促进网络安全发展、打击网络犯罪和发挥跟踪、预警和事件响应的作用以确保新举措和现有举措之间的机构内、跨部门和跨境协调是必要的。该分组由以下绩效指标组成：

1 国家网络安全战略

代码-GCIv5：Org1

理由-GCIv5：国家网络安全战略为资源分配提供了框架[6]，以确定国家网络安全目标，并为实施这些目标确定资源的优先级，旨在提高一个国家的安全性和复原力[7]。它还使得政府能够在国家层面上与所有相关利益攸关方合作。此外，国家网络安全战略可能有助于促进创新，保护隐私和公民自由。国家网络安全战略应明确确定国家网络安全目标，并确定实施这些目标的治理结构[8]。

1.1 贵国是否制定了国家网络安全战略（NCS）或政策，是独立的还是其他文件的一部分？

代码-GCIv5：Org1.1

理由-GCIv5：毫无疑问，网络安全对所有国家来说都是一个至关重要的问题。国家网络安全战略为分配资源以保护国家关键基础设施提供了框架。它还使得政府能够与私营部门合作，识别和缓解网络威胁。此外，国家网络安全战略有助于促进创新，保护隐私和公民自由。

1.2 国家网络安全战略优先领域

代码-GCIv5：Org1.2

理由-GCIv5：一项具备优先领域的国家战略有助于协调应对网络风险。由于每个国家都面临不同的网络安全挑战，关注网络安全的具体领域有助于各国确定资源的优先级，协调应对网络威胁。大多数制定国家网络安全战略的指南可能侧重于不同的优先领域，如“制定国家网络安全战略”[9]。对于某些战略而言，优先领域也可以指“重点领域”[10]。问题 1.2.1 至 1.2.4 包括可在一个国家的国家网络安全战略中考虑的优先领域。然而，各国可能有其他优先领域。

1.2.1 贵国的国家网络安全战略是否涉及国家关键基础设施的保护？

代码-GCIv5：Org1.2.1

理由-GCIv5：国家关键基础设施包括从电网和供水系统到交通网络和金融机构的一切。如果其中任何一项崩溃，一个国家就会陷入混乱。这就是为什么国家网络安全战略应该包含一项计划，以确保关键基础设施得到良好的保护，因为它们对维护公共秩序和安全不可或缺，对一个国家的经济非常重要，对国家安全至关重要。

---

[6] https://cybersecurity.att.com/blogs/security-essentials/cybersecurity-strategy-explained
[7] https://www.enisa.europa.eu/topics/national-cyber-security-strategies
[8] https://ncsguide.org/the-guide/
[9] http://download.microsoft.com/download/B/F/0/BF05DA49-7127-4C05-BFE8-0063DAB88F72/Developing_a_National_Strategy_for_Cybersecurity.pdf
[10] https://ncsguide.org/the-guide/

1.2.2 贵国的国家网络安全战略是否纳入了生命周期管理原则，并定期进行监测、评估和更新？

代码-GCIv5： Org1.2.3

理由-GCIv5： 一个国家的国家网络安全战略（NCS）应包含生命周期管理原则[11]，并定期进行监测、评估和更新，以确保战略保持有效性和相关性。这有助于确保识别和处理与某一特定战略相关的风险，并按需调整战略以反映环境的变化。生命周期管理方法还有助于确保所有利益攸关方参与战略的制定和实施，并且各方均清楚地了解自身的角色和责任。这有助于确保战略得到有效实施，而且各方都朝着同一个目标努力。最后，通过使用生命周期管理原则，可以监测战略的实施情况并评估其结果。这有助于在必要时及时调整方向，并有助于确保战略始终具有相关性和有效性。

1.2.3 贵国的国家网络安全战略是否有确保与网络安全专家和利益攸关方进行定期磋商的机制？

代码-GCIv5： Org1.2.4

理由-GCIv5： 网络安全格局不断变化，有必要建立机制，确保定期对国家网络安全战略予以更新。网络安全专家可以就最新的威胁以及如何最好地应对这些威胁提供宝贵的输入意见。在国家网络安全战略的过程中，还需要征求企业和公民等利益攸关方的输入意见，以确保更有效的政策结果。他们可以提供关于战略实施情况的反馈，并提出改进建议。通过征求专家和利益攸关方的意见，国家网络安全战略可以根据国家的需要实现量身定制。

1.2.4 贵国是否制定了实施网络安全战略的明确行动计划/路线图？

代码-GCIv5： Org1.2.5

理由-GCIv5： 实施网络安全战略的明确行动计划/路线图是保护一个国家的数字基础设施和公民的关键部分。没有计划，就很难分配资源和衡量进展，这可能导致缺乏有效性和覆盖面方面的差距。一份明确的行动计划/路线图可以帮助确保所有利益攸关方都了解他们在实施战略中的角色和责任，而且计划应该是可实现且现实的。它还有助于跟踪和评估战略的长期影响，以便做出任何必要的调整。

2 负责机构

代码-GCIv5： Org2

理由-GCIv5： 负责机构是负责管理网络安全的主管部门。这一主管部门应该是一个领导者（无论是个人还是实体），将之提升到政府的最高层并牢牢地固定在那里，以提供指导、协调行动并监测网络安全活动和计划的实施。这样一个国家主管部门还应作为管理实体，界定和澄清角色、责任、过程、决策权以及确保有效网络安全态势所需的各项任务。

2.1 贵国在国家层面是否有机构或部委负责网络安全问题？

代码-GCIv5： Org2.1

理由-GCIv5： 在国家层面负责网络安全的国家机构或部委可以支持一致的网络安全威胁管理和积极主动的网络安全行动。该机构或部委应与其他政府部门、私营部门、民间团体和其他相关参与方合作，制定和实施国家网络安全战略。

2.2 贵国是否有机构或部委负责与国家关键基础设施保护有关的网络安全问题？

代码-GCIv5： Org2.2

---

[11] https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide

理由-GCIv5：在国家层面负责关键基础设施的机构或部委支持业务的复原力和连续性。关键基础设施可包括水、电和电信等基本服务，这些服务对社会运转至关重要。负责关键基础设施的国家机构或部委可以通过与相关利益攸关方合作，帮助防止或减轻这些设施中断的影响。

2.3 贵国是否有负责监督国家网络安全能力发展的机构、部委、任务组或其他机构？

代码-GCIv5：Org2.3

理由-GCIv5：以协调和全面的方式发展必要的网络安全技能和能力，可以减少发生网络安全事件的可能性并提高复原力。网络安全是一个多层面的问题，需要多个政府机构和私营部门实体的协调与合作。

2.4 在贵国，保护上网儿童举措和活动的协调是否属于任何机构、部委、任务组或其他机构的责任范围？

代码-GCIv5：Org2.5

理由-GCIv5：利益攸关方和目标群体之间的协调以及确保对活动进行监督，对于确保保护上网儿童（COP）干预措施的相互补充非常重要。在国家层面协调保护上网儿童举措和活动的责任，可以是一个独立机构、部委、任务组或其他机构的职责，也可以是任何此类机构更大责任范围的一部分。

3 网络安全衡量指标

代码-GCIv5：Org3

理由-GCIv5：网络安全衡量指标包括官方认可的国家或具体到行业的基准对照或参考，用于衡量网络安全发展、风险评估战略、网络安全审计以及其他用于评级或评估最终表现便于未来改进的工具和活动。例如，ISO/IEC27004[12]涉及信息安全管理方面的相关衡量。

3.1 在国家层面是否进行网络安全审计？

代码-GCIv5：Org3.1

理由-GCIv5：基于安全考虑、法规或其他指导性文件，可在国家层面进行网络安全审计。即使有网络安全审计法规，国家层面的有效网络安全审计是必要的。这些审计的输出结果可以是审计报告、演示文稿、备忘录或其他类似材料。

网络安全审计旨在识别潜在漏洞。一旦确定了这些潜在漏洞，就可以对它们进行评估并确定优先级，从而确定它们对组织构成的风险程度。有各种各样的工具可以用来评估这些漏洞，包括漏洞扫描器、渗透测试器和红队演习。每种工具都有各自的优缺点，选择合适的工具来完成工作非常重要。一旦确定了漏洞，重要的是确定它们对组织构成的风险水平。

3.2 是否有用于评估国家层面网络安全风险的衡量指标/工具？

代码-GCIv5：Org3.2

理由-GCIv5：评估国家层面的网络安全风险的衡量指标因国家而异，应该反映一个国家的具体威胁、能力和挑战。可以使用各种衡量指标来完成这项工作，包括影响因素、概率因素和资产价值。通过使用这些衡量指标，可以确定每个漏洞所带来的风险水平和严重程度，并采取适当的纠正措施[13]。ISO/IEC 27004[14]提供了可用于监测、衡量、分析和评估网络安全相关风险的安全技术。

---

[12] https://www.iso.org/standard/64120.html

[13] https://www.oas.org/es/sms/cicte/ENGcyberrisk.pdf

[14] https://www.iso.org/standard/64120.html

3.3 是否采取措施利用网络安全能力成熟度模型、网络就绪指数或任何其他相关评估工具来评估国家层面的网络安全发展水平？

代码-GCIv5： Org3.3

理由-GCIv5： 评估网络安全发展水平可以使各国了解其网络安全基础设施的成熟度和可靠性，具体评估措施可能因国家而异。一些评估国家层面网络安全发展水平的常用工具包括网络安全成熟度模型[15]、网络就绪指数[16]或一个国家采取的任何其他措施。本问题中的评估工具不包括国家参与国际电联全球网络安全指数。

4 保护上网儿童战略和举措

代码-GCIv5： Org4

理由-GCIv5： 保护上网儿童（COP）是各项旨在保护儿童在使用互联网时免受伤害或剥削的战略和举措的总称。这可以包括确保儿童使用适龄的软件和过滤工具，教育父母和儿童保持上网安全。有各种不同的 COP 战略和举措，通常是为满足目标国家儿童的具体需求而量身定制的。

4.1 贵国是否有与当前保护上网儿童举措相关的针对保护上网儿童的国家战略？

代码-GCIv5： Org4.1

理由-GCIv5： 《保护上网儿童指南》建议制定一项专门的、单独的全面 COP 战略，因为该战略应涵盖与儿童有关的领域，如健康、幸福和技能发展。如果 COP 战略被纳入其他文件时，它往往不够全面，而且往往只侧重于防止性虐待或儿童色情。

4.2 贵国是否在国家层面部署了政府报告机制和能力来帮助保护上网儿童？

代码-GCIv5： Org4.2

理由-GCIv5： 向公众提供报告机制，以识别、跟踪和跟进与上网儿童有关的问题，使个人能够识别和报告影响上网儿童的问题。这些机制也可以包括技术能力，如内容警告。CIRT 和执法机构可以提供报告机制。理想情况下，应提供各种制度，如国家帮助热线或带有转介和支持系统的在线门户网站。

---

[15] https://gcscc.ox.ac.uk/cmm-2021-edition

[16] https://www.potomacinstitute.org/images/CRIndex2.0.pdf

能力建设措施

GCIv5-说明：能力建设是《全球网络安全指数》中法律、技术和组织措施的内在要求，也是推动数字化发展的力量。能力建设项目旨在培养本地技能、知识和信心，从而缩小技能差距并建立更具包容性的技术生态系统。此外，提供包容性数字服务的能力越来越依赖于熟练的劳动力。提高网络安全的能力建设框架可包括提高认识，并可根据研发项目、教育和培训项目以及经认证的专业人员和公共部门机构的存在性和数量来衡量。

1 公众网络安全宣传活动

GCIv5-代码： CapDev1

GCIv5-说明： 公众网络安全宣传活动的主要目的是影响网上安全行为的采用。为了实现有意义的行为改变，公众宣传活动需要让人们相信这些信息是有意义的，帮助他们了解如何做出反应，并说服他们愿意根据其他优先事项做出反应。[17]宣传活动面临着许多挑战，尤其是因为它们需要大量的努力和技能，而且“恐惧诱导很少会引起行为变化”。[18]有针对性的宣传活动可以调整干预措施，以便更好地解决这些问题。

1.1 贵国政府是否开展了专门针对中小微企业的公众宣传活动？

***GCIv5*-代码：** CapDev1.1

***GCIv5*-说明：** 微型、小型和中型企业（SME）是一个国家经济的重要组成部分，需要了解可能影响其业务的网络安全威胁。它们在提高网络安全方面面临具体挑战，如缺乏资源和技术专长。有针对性的干预措施可以应对这些具体挑战，并侧重于最大限度地扩大对中小微企业的影响。网络安全宣传活动，特别是针对中小企业的活动，可以向中小微企业提供如何保护自己免受网络攻击的信息，以及在受到攻击时如何应对的信息。

1.2 贵国政府是否开展了专门针对一般私营部门的公众宣传活动？

GCIv5-代码： CapDev1.2

GCIv5-说明： 任何私营部门参与者都面临网络安全挑战。除了中小微企业的具体需求之外，关于私营部门面临的网络安全风险的公众宣传活动也有助于改善行为。

1.3 贵国政府是否开展了专门针对地方、市级和国家级公共部门机构和公共部门工作人员的公众宣传活动？

GCIv5-代码： CapDev1.3

GCIv5-说明： 公共部门机构可以从网络安全宣传活动中受益。网络安全宣传活动是专门为公共部门工作人员设计的，它们提供了关于如何保护敏感数据和关键基础设施的重要信息。

1.4 贵国政府是否开展了专门针对民间团体的公众宣传活动？

GCIv5-代码： CapDev1.4

GCIv5-说明： 民间团体组织可能成为网络攻击的目标。这些攻击可能包括在线骚扰、数据窃取或财务信息窃取。民间团体组织需要了解风险并保护自己。这包括培训他们的员工，使用安全的密码，并拥有最新的杀毒软件。各国可以通过提高认识来帮助保护这些重要组织免受伤害，从而帮助它们安全地保护它们的组织、网络和公民数据。

---

[17] Rogers, R.W. Attitude change and information integration in fear appeals. Psychological Reports, 56, (1985) 183–188
Witte, K. Message and conceptual confounds in fear appeals: The role of threat, fear and efficacy. The Southern Communication Journal, 58(2), (1993) 147-155.
https://ora.ox.ac.uk/objects/uuid:cfed4907-d32a-4450-b075-ad37477b10d8

[18] https://ora.ox.ac.uk/objects/uuid:cfed4907-d32a-4450-b075-ad37477b10d8

1.5 贵国政府是否开展了针对普通民众的公众宣传活动？

GCIv5-代码： CapDev1.5

GCIv5-说明： 网络安全不仅仅是企业和政府的事。公民最容易受到网络犯罪的侵害，但他们往往缺乏保护自己的知识和工具。网络罪犯不断寻找窃取数据、金钱或身份的新方法。他们可以通过侵入计算机系统、窃取密码或创建虚假网站来做到这一点。在国家一级，政府可以提高公民的认识来保护他们。教育公民使用强密码、打开电子邮件时要小心，以及永远不要在网上泄露个人信息等来保护自己。他们还应该了解诈骗或网络钓鱼攻击的警告标志。各国政府应致力于提高全体公民的网络安全意识，并敦促每个人采取必要措施在网上保护自己。

1.6 贵国政府是否开展了专门针对老年人（年长者）的公众宣传活动？

GCIv5-代码： CapDev1.6

GCIv5-说明： 随着我们的人口继续老龄化，越来越多的老年人将使用互联网和电子设备。不幸的是，这使他们成为网络罪犯的主要目标。由于以下几个原因，老年人更容易受到网络威胁：他们可能没有意识到使用互联网带来的危险，缺乏保护自己的技术技能，可能更容易上当受骗，不太可能报告网络犯罪。为此，各国政府正在提高老年人的网络安全认识，以确保上网安全并保护他们的个人信息。

1.7 贵国政府是否开展了专门针对有具体需求人士（包括残疾人士在内）的公众宣传活动？

GCIv5-代码： CapDev1.7

GCIv5-说明： 随着残疾模式日益从医学转向人权，解决有具体需求的人士面临的社会障碍，例如“建筑和交流障碍、社会态度和结构”[19]，可以提高残疾人的能力和安全。还更加需要专门针对残疾人的网络安全认识和培训。残疾人更容易受到网络攻击，原因有很多，包括他们不熟悉技术，依赖他人帮助，以及不愿意寻求帮助。因此，教育和提高认识至关重要，政府需要确保所有社区成员都参与到我们的网络安全工作中。通过公众宣传活动满足这一群体的需求，对于实现包容性和有效的网络安全能力建设非常重要。

1.8 贵国政府是否开展了专门针对父母、教育工作者和儿童的公众宣传活动，作为保护上网儿童（COP）工作的一部分？

GCIv5-代码： CapDev1.8

GCIv5-说明： 政府应推动开展专门针对父母和教育工作者的公众宣传活动，使他们能够获得更多关于儿童和青少年面临的风险和危害的知识，并提高处理 COP 相关问题的能力。

1.9 贵国政府是否开展了专门针对儿童的公众宣传活动，作为保护上网儿童（COP）工作的一部分？

GCIv5-代码： CapDev1.9

GCIv5-说明： 随着上网时间的增加，儿童变得易受伤害。儿童特别容易受到网络威胁，因为他们可能没有意识到危险，也可能不具备与成人同等水平的网络安全知识和经验。各国政府应推动开展针对儿童的公众宣传活动，帮助他们获得关于他们可能在网上遇到的各种风险的知识，提高他们识别和减轻这些风险的能力，并推动采用负责任的上网行为。

2 培训网络安全专业人员

GCIv5-代码： CapDev2

GCIv5-说明： 技能发展可以支持打造一支有能力的新式网络安全队伍。网络安全工作人员的培训需要不断努力应对这一领域的变化和发展。

---

[19] https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e777?rskey=sn89T4&result=201&prd=MPIL#

2.1 贵国政府是否开发了或支持开发针对网络安全专业人员的网络安全培训课程？

GCIv5-代码： CapDev2.1

GCIv5-说明： 随着越来越多的企业将运营转移到网上，对网络安全专业人员的需求空前增加。但通常情况下，这些专业人员缺乏必要的培训来保护他们的雇主免受网络攻击。网络安全培训之所以重要，有几个原因，包括帮助网络安全专业人员建立强大的网络安全基础、掌握实际应用知识的能力、了解最新的网络安全趋势和发展，以及帮助他们发展必要的技能来保护其组织的网络和数据。

2.2 贵国是否有国内或国际上获得认可的网络安全专业人员认证项目？

GCIv5-代码： CapDev2.2

GCIv5-说明： 网络安全认证项目有助于确保在这一领域工作的专业人员保持高标准。这有助于提高网络安全专业人员的整体素质，有助于保护个人和组织免受潜在伤害。此外，各国可以在网络安全专业人员及其客户之间建立信任。拥有一个获得普遍认可的认证项目有助于确保所有相关方能够信任与他们合作的专业人员的资质。

2.3 针对国家特定部门专业人员的网络安全教育项目/培训

GCIv5-代码： CapDev2.3

GCIv5-说明： 在一个国家内部，在不同部门工作的专业人员可以从解决他们面临的具体问题和情况的网络安全项目/培训中受益，并努力使他们具备所需的适当技能。

2.3.1 贵国政府是否开发了或支持针对国家级执法部门的网络安全教育项目或培训？

GCIv5-代码： CapDev2.3.1

GCIv5-说明： 警察、执法人员等执法部门在助力保护我们的国家免受网络攻击方面发挥着至关重要的作用。他们可以帮助发现和调查网络犯罪，并与企业和其他组织合作来改善其网络安全态势。执法部门需要配备必要的知识和工具来应对这些日益增长的威胁。网络安全培训可以帮助他们更好地了解最新的威胁，发现恶意活动，并保护他们的网络。

2.3.2 贵国政府是否开发了或支持针对国家级国家司法人员的网络安全教育项目或培训？

GCIv5-代码： CapDev2.3.2

GCIv5-说明： 国家司法人员在确保国家安全和保障方面发挥着至关重要的作用，他们需要具备应对网络安全威胁的知识和工具。在规划国家网络安全培训时，需要考虑对司法和其他法律行业人员的网络安全培训，对法官、初级律师、出庭律师、代理人、律师、律师助理和其他法律和执法专业人员的专业和技术培训。

2.3.3 贵国政府是否开发了或支持针对中小微企业的网络安全教育项目或培训？[未评分]

GCIv5-代码： CapDev2.3.3

GCIv5-说明： 中小微企业需要网络安全培训，因为它们持有大量敏感数据，在发生网络攻击时，这些数据可能被窃取或损害。此外，中小微企业往往不知道与使用技术相关的风险，并且可能没有必要的工具或资源来保护其数据。网络安全培训可以帮助中小微企业了解与使用技术相关的风险以及如何保护其数据。此外，培训可以帮助中小微企业识别可疑活动和应对网络攻击。通过向中小微企业提供保护其数据所需的工具和知识，各国反过来可以帮助保护其经济发展。

2.3.4 贵国政府是否开发了或支持针对一般私营部门的网络安全教育项目或培训？

GCIv5-代码： CapDev2.3.4

GCIv5-说明： 私营部门日益面临范围、规模和复杂性不断扩大的网络风险，这些风险影响着企业的财务、声誉和财产。由于技术只是网络安全的一个组成部分，实施政策和项目来改变私营部门人们的行为可以增强韧性并降低网络风险。

2.3.5 贵国政府是否开发了或支持针对一般公共部门/政府官员的网络安全教育项目或培训？

GCIv5-代码： CapDev2.3.5

GCIv5-说明： 公共部门为公民和企业提供基本服务。为了安全地提供服务，公共部门参与者需要深入了解网络安全以及如何保护自己及其选民免受数字威胁。司法和执法部门以外的公共部门/政府官员可以从网络安全教育项目和培训中受益。

2.3.6 贵国政府是否开发了或支持针对金融、卫生、电信、交通和/或能源部门参与者的网络安全教育项目或培训？

GCIv5-代码： CapDev2.3.6

GCIv5-说明： 网络安全问题通常因部门而异。鉴于金融、卫生、电信、交通和能源部门的关键作用，对这些参与者进行有针对性的培训可以支持一个国家的整体网络安全态势。

2.3.7 贵国政府是否开发了或支持针对青年人的网络安全教育项目或培训？

GCIv5-代码： CapDev2.3.8

GCIv5-说明： 传统上，政府会介入来纠正负面的市场外部性，并支持以其他方式得不到充分服务的群体。在政府开发和支持网络安全教育项目和培训这个领域，私营部门可能因缺乏有力回报而无法被激励参与。政府可以通过财政拨款、学习支持、学徒支持等方式提供支持。考虑从事网络安全职业的青年人可能更需要这种支持，因为他们缺乏自己投资教育的财务资本。

2.3.8 贵国政府是否开发了或支持针对教育工作者的网络安全教育项目或培训，如保护上网儿童教育项目？

GCIv5-代码： CapDev2.3.9

GCIv5-说明： 由于教育工作者在儿童和青少年教育中的作用，他们有能力向儿童和青少年传授积极的网络安全行为。为教育工作者提供网络安全相关问题的培训，如保护上网儿童，表明各国正在努力采取长期的网络安全措施，支持教育工作者在下一代互联网用户上网时开展工作。

3 作为国家学术课程的网络安全教育项目

GCIv5-代码： CapDev3

GCIv5-说明： 为了培养更具网络安全能力的人口，将网络安全的基本原则纳入国家学术课程可以使各年龄段的学生更好地应对网络安全风险。

3.1 贵国政府是否开发了或支持任何被纳入初等教育学术课程的网络安全教育项目？

GCIv5-代码： CapDev3.1

GCIv5-说明： 小学生，或那些处于 ISCED（国际教育标准分类）1 级的学生，刚开始他们的学校教育，通常学习阅读、写作和数学的基本技能。[20]在这一阶段整合活动以建立网络安全行为的基础，有助于提高终身的网络意识和安全。然而，这一阶段的儿童可能还不具备独立评估网络安全风险的批判性思维技能和服务机构，因此具有特定的风险。[21]这一阶段的活动可以包括保护上网儿童活动。

3.2 贵国政府是否开发了或支持任何被纳入中等教育学术课程的网络安全教育项目？

GCIv5-代码： CapDev3.2

GCIv5-说明： 在 ISCED 2 级和 3 级学校教育方案中，中学生经常参与旨在“为终身学习和人类发展奠定基础，且教育系统可在此基础上进一步扩大教育机会”的教育活动，然后“旨在完成

---

[20] http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf

[21] https://www.weforum.org/agenda/2020/03/we-need-to-start-teaching-young-children-about-cybersecurity/

中等教育，为高等教育做准备，或提供与就业相关的技能，或两者兼而有之”。[22]在这一阶段引入网络安全不仅可以帮助学生掌握更加安全的上网技能，还可以促进他们对技术和网络安全的兴趣，从而为他们的职业生涯打下基础。

3.3 贵国政府是否开发了或支持任何被纳入高等教育学术课程的网络安全教育项目？

GCIv5-代码： CapDev3.3

GCIv5-说明： 高等教育阶段（也被称为 ICSED 5-8 级）的学生通常已经完成了义务教育课程。高等教育项目可包括以下课程：向参与者提供专业知识、技能和能力（ICSED 5）；向参与者提供中级学术和/或专业知识、技能和能力，最终获得第一级学位或同等资格（ICSED 6）；向参与者提供高级的学术和/或专业知识、技能和能力，最终获得第二级学位或同等资格，如硕士学位或同等水平（ICSED 7）；或者，获得高级研究资格，如博士级资格（ICSED 8）。[23]在这些教育阶段解决网络安全问题可以支持具有网络意识和能力的劳动力，并促进以研发为目的的能力建设。

4 网络安全研究和发展（R&D）项目

GCIv5-代码： CapDev4

GCIv5-说明： 公共、私营和学术部门的研发工作可以通过发展人的能力、开发新技术和新产品以及更好地了解风险和缓解措施来支持网络安全工作。研发工作可以包括技术和非技术性解决方案。

4.1 贵国的私营部门参与者是否开展网络安全相关的研发活动？

GCIv5-代码： CapDev4.1

GCIv5-说明： 私营部门主导的研发表明，私营部门愿意投资于网络安全领域的进一步发展和创新，并改善市场上现有的网络安全解决方案。

4.2 贵国的国家公共部门参与者是否开展网络安全相关的研发活动？

GCIv5-代码： CapDev5.2

GCIv5-说明： 公共部门参与者积极参与网络安全相关的研发活动有助于更好地发现和补救一个国家网络安全基础设施中的漏洞。它还可以推动制定用于保护一国关键基础设施的网络安全解决方案。公共部门开展的与网络安全有关的研发活动也可以为网络攻击做准备。就这个问题而言，公共部门参与者应属于国家政府，而不是州或地方政府。

4.3 贵国的学术机构是否开展网络安全相关的研发活动？

GCIv5-代码： CapDev5.3

GCIv5-说明： 学术界在网络安全相关的研发工作中发挥着至关重要的作用。学术界贡献前沿研究和新思维，培养下一代专业人员，并充当私营部门和公共部门之间的桥梁。

4.4 贵国是否有为评估ICT产品的网络安全性而开展的项目/举措，如标示或认证计划？

GCIv5-代码： CapDev4.2

GCIv5-说明： 据以评估 ICT 产品网络安全性的认证和标示计划有助于推动制造商提高网络安全标准，提供可核查性，并便利消费者选择产品。各国可根据国情和需求实施不同类型的计划。

5 国家网络安全产业

GCIv5-代码： CapDev5

---

[22] http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf

[23] http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf

GCIv5-说明：发展和支持国家网络安全产业既能支持国内应对和改善网络安全挑战的能力，又能带来积极主动的网络安全管理。

5.1 贵国国内是否有网络安全产业？

GCIv5-代码：CapDev5.1

GCIv5-说明：支持网络安全发展的有利的经济、政治和社会环境将激励网络安全私营部门的发展。公众宣传活动、人力资源开发、能力建设和政府激励措施将推动网络安全产品和服务市场的发展。本国网络安全产业是这种有利环境的试金石，将推动网络安全创业公司和相关网络保险市场的发展。

5.2 贵国是否有任何推动贵国网络安全产业发展的组织或协会？

GCIv5-代码：CapDev5.4

GCIv5-说明：各组织和协会可以通过促进知识交流、人才培养、获得投资和资金等途径，加强积极参与的网络安全产业。这些组织和协会可以得到产业的支持，也可以得到国家政府或其他机构的支持。

6 政府激励机制

GCIv5-代码：CapDev6

GCIv5-说明：安全性投资可以产生积极的外部效应，而这些外部效应并没有被投资者或努力者所获得。为了解决潜在的网络安全投资不足或努力不足的问题，政府可以介入，提供提高网络安全性的激励措施，如资金、监管或其他机制。这可以提高一国的网络安全水平，使其超过在没有支持的情况下可能发展起来的水平。

6.1 政府在网络安全领域是否存在鼓励能力建设的激励机制？

GCIv5-代码：CapDev6.1

GCIv5-说明：政府激励机制可以激励网络安全能力建设，如开展研究、参与继续教育或制定新的能力建设项目，激励机制如补助金、奖学金、费用支持、贷款或就业机会。

6.2 政府是否制定了任何推动网络安全产业发展或进一步发展的激励机制？

GCIv5-代码：CapDev6.2

GCIv5-说明：鉴于网络安全等信息产品的性质，可能会发生垄断。[24]为了推动新组织和现有组织出现新的想法和做法，并鼓励各种参与者和利益攸关方参与网络安全工作，政府可以以货币补助、减免税费、名誉利益、有利的合同条款等形式提供激励措施，或鼓励公司、组织和个人参与网络安全生态系统建设。

6.3 贵国政府是否有鼓励网络安全相关研发活动的激励机制？

GCIv5-代码：CapDev6.3

GCIv5-说明：当现有的市场力量没有产生预期的结果时，政府激励机制是有用的。由于网络安全相关的研发活动带来的好处可以对整个社会产生积极的外部效应，政府可以通过各种方式鼓励网络安全相关的研发活动，如通过补助、贷款机制、有利的贸易和商业环境、合同、支持大学活动等。

---

[24] https://www.econstor.eu/bitstream/10419/199018/1/CESifo-Forum-2018-4-p23-28.pdf

合作措施

理由-GCIv5：网络安全要求所有部门和领域的投入，需要从利益攸关多方的角度加以解决。合作加强了对话和协调，从而创造了更加全面的网络安全应用领域。鉴于网络安全跨越了部门、地理和资源层面，需要在私人、公共、区域和国际层面进行合作。扩大合作举措可以促使开发更强大的网络安全能力，帮助阻止重复和持续的在线威胁，实现更好地调查、拘捕和起诉恶意代理。

国家和国际合作可以根据伙伴关系、合作框架和信息共享网络的存在情况和数量加以衡量。

1 网络安全双边协议

代码-GCIv5：Coop1

理由-GCIv5：双边协议（一对一协议）指任何官方认可的、一国政府与他国政府或区域性政府间组织跨境共享网络安全资产（即交流信息、专业知识、政策、技术和其它资源）以应对跨境网络冲突风险的国家伙伴关系。该指标亦衡量协议是否具有法律约束力或有待批准。资产可以指共享专业人员（借调、配置或其他暂时性人员调动）、设施、设备和其它工具及服务。

1.1 与其它国家的网络安全双边协议

代码-GCIv5：Coop1.1

理由-GCIv5：双边协议（一对一协议）指任何官方认可的、一国政府与他国政府跨境共享网络安全资产（即交流信息、专业知识、政策、技术和其它资源）的国家伙伴关系。国与国之间分享知识和专长有助于建立强大的事件响应能力，并制定应对网络安全风险的积极措施。

1.1.1 贵国是否将共享网络安全信息作为与其它国家双边协议的一部分内容？

代码-GCIv5：Coop1.1.1

理由-GCIv5：涉及信息共享的网络安全协议表明各国加强了网络安全承诺，因为它们有助解决潜在风险、开展威胁评估，并就网络安全相关行动进行合作。

1.1.2 贵国是否将网络安全能力开发作为与其它国家双边协议的一部分内容？

代码-GCIv5：Coop1.1.2

理由-GCIv5：促进双边网络安全能力开发的协议通过分享最佳做法、提高人员技能、加强协作、提高认识以及制定和实施与网络安全相关的操作程序，增强了各国主动应对网络风险的能力。

1.2 与国际和区域组织的网络安全双边协议

代码-GCIv5：Coop1.2

理由-GCIv5：鉴于区域政府间组织的重要性，各国越来越多地以单个国家的身份或作为其区域政府间组织成员身份的一部分，与欧洲联盟、东盟（ASEAN）、西非国家经济共同体（ECOWAS）、美洲国家组织（OAS）、非盟（AU）等其它区域政府间组织就网络安全签订合作协议，以跨境共享网络安全资产，例如，交流信息、专业知识、技术和其它资源。

1.2.1 贵国或贵国作为成员加入的区域政府间组织是否将网络安全信息共享作为与其它区域和国际组织双边协议的一部分内容？

代码-GCIv5：Coop1.2.1

理由-GCIv5：涉及信息共享的网络安全协议表明各国加强了网络安全承诺，因为它们有助解决潜在风险、共享威胁评估数据，并就网络安全相关行动进行合作。

1.2.2 贵国或贵国作为成员加入的区域政府间组织是否将网络安全能力开发作为与其它区域和国际组织双边协议的一部分内容？

代码-GCIv5：Coop1.2.2

理由-GCIv5：各国与区域政府间组织关于网络安全能力开发的网络安全双边协议可以通过分享最佳做法、提高人员技能、加强协作、提高认识以及制定和实施与网络安全相关的操作程序来增强网络安全能力。

2 与其它国家的网络安全多边协议

代码-GCIv5：Coop2

理由-GCIv5：加入书面多边协议需要就与网络安全相关的关键定义和参数达成一致，并为推进网络安全制定共同议程。它们还可以进一步推动树立信心的措施，作为创建积极反馈机制以建立和平关系的一部分。

2.1 贵国是否为包括网络安全信息共享在内的网络安全多边协议的一部分？

代码-GCIv5：Coop2.1.1

理由-GCIv5：涉及信息共享的网络安全协议表明各国加强了网络安全承诺，因为它们有助解决潜在风险、共享开展威胁评估的数据，并就网络安全相关行动进行合作。

2.2 贵国是否为包括能力开发共享在内的网络安全多边协议的一部分？

代码-GCIv5：Coop2.1.2

理由-GCIv5：加入包括能力开发在内的书面多边协议可以支持网络安全态势较弱的国家的能力开发工作，并支持树立信心的措施。

3 与网络安全相关的司法互助条约（MLAT）[25]

代码-GCIv5：Coop3

理由–GCIv5：鉴于网络安全的跨国性质，就影响另一国主权的威胁采取行动需要明确的合作机制，在司法事务方面尤其如此。司法互助（例如以司法互助条约（MLAT）的形式）的形式各不相同，包括文件的送达、证据的传递、调查协助等。[26]

3.1 贵国是否通过与其它国家或区域或政府间组织的双边或多边协议加入有关网络安全的司法互助条约（MLAT）？

代码-GCIv5：Coop3.1

理由-GCIv5：鉴于网络安全的跨国性质，就影响另一国主权的威胁采取行动需要明确的合作机制，在司法事务方面尤其如此。司法互助（例如以司法互助条约（MLAT）的形式）的形式各不相同，包括文件的送达、证据的传递、调查协助等司法互助（例如以司法互助条约（MLAT）的形式）的形式各不相同，包括文件的送达、证据的传递、调查协助等。[27]

4 公私伙伴关系（PPP）

代码-GCIv5：Coop4

理由-GCIv5：公私伙伴关系一直是由意识形态原因和追求物有所值所驱动的趋势的一部分。[28] 特别是在网络安全领域，新的创新往往来自于私营部门，参与 PPP 可以帮助政府更快地从这些新的创新中受益，并可能改善网络安全。然而，PPP 也带来了许多挑战，例如委托代理问题、外部性管理、合同谈判的复杂性、合同灵活性和有效评估。[29]

---

[25] https://www.unodc.org/e4j/en/organized-crime/module-11/key-issues/mutual-legal-assistance.html

[26] https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e966?rskey=XSl5yx&result=1&prd=MPIL

[27] https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e966?rskey=XSl5yx&result=1&prd=MPIL

[28] https://read.oecd-ilibrary.org/governance/public-private-partnerships_9789264046733-en#page5

[29] https://read.oecd-ilibrary.org/governance/public-private-partnerships_9789264046733-en#page66

4.1 贵国政府是否就网络安全与国内企业结成PPP关系？

代码-GCIv5：Coop4.1

理由-GCIv5：由于固有的网络效应，与国内企业结成 PPP 关系可以促进国内网络安全生态系统，使国内私营部门参与者能够发展和扩展其技能、系统和服务。

4.2 贵国政府是否就网络安全与驻贵国的外国企业结成PPP关系？

代码-GCIv5：Coop4.2

理由-GCIv5：网络安全作为一种信息商品，受制于网络效应和从规模中获得的专业知识。[30]从各种国情或背景中获得网络安全专业知识的国际参与者可以为寻求加强国家网络安全的政府提供额外的裨益。与外国参与者结成 PPP 关系的政府可以利用这些专业知识来实现自身的增长和安全。

5 机构间伙伴关系

代码-GCIv5：Coop5

理由-GCIv5：一个国家内不同政府机构间的任何国内官方伙伴关系均可以促进政府对网络安全风险的响应。伙伴关系可包括各部委、部门、项目和其它公共部门机构之间的信息或资产共享伙伴关系。就本节而言，不考虑不同国家的机构间或政府间组织之间的机构间伙伴关系。

5.1 在贵国，不同国家政府机构之间是否存在关于网络安全的专门的机构间协调流程？

代码-GCIv5：Coop5.1

理由-GCIv5：一个国家内不同政府机构间的任何国内官方伙伴关系均可以促进政府对网络安全风险的响应。伙伴关系可包括各部委、部门、项目和其它公共部门机构之间的信息或资产共享伙伴关系。就本节而言，不考虑不同国家的机构间或政府间组织之间的机构间伙伴关系。

[30] https://www.econstor.eu/bitstream/10419/199018/1/CESifo-Forum-2018-4-p23-28.pdf

定义

术语	缩写	定义	来源	示例	提及的问题（GCIv4）
学术界		大学学术界	牛津英语词典		Tech2；CapDev4.1.3；CapDev6.2
学术机构		作为大学学术界组成部分的机构	牛津英语词典		CapDev4.1.3
协议		国家或其他参与方之间以书面形式达成的、受国际法制约的对等承诺，不论是否包含在一份或两份或多份相关文书中	改编自《维也纳条约法公约》		
双边协议		由相关决策机构签署的两方（包括国家、区域性机构或组织）之间的书面协议	GCIv2		Coop1；Coop1.1；Coop1.1.1；Coop1.1.2；Coop1.1.3
能力开发		能力开发是一个变化的过程。它通常等同于增加职员数量，额外提供培训和讲习班。虽然单独的培训和讲习班可能是综合能力开发规划的一部分，但光靠其本身是不够的。例如，对个人的培训并不能确保这种培训随后在工作场所加以实施。能力开发必须更加广泛，以解决改善卫生系统的问题，从而提高绩效并确保可持续性。它应评估系统目前的运行情况，以及哪些领域需要支持；例如：开发和实施卫生信息系统、培训分析数据的职员、制定强有力的财务管理政策和流程、或改善关键卫生产品的供应和分配	UNDP https://www.undp-capacitydevelopment-health.org/en/capacities/		Org2.3；CapDev1；CapDev6.1；Coop1.1.2
儿童上网保护	COP	儿童上网保护旨在保护儿童和青少年免受可能在网上遇到的威胁和风险。儿童上网保护的概念包括采取全面的做法，为儿童和青少年创建安全、适龄、包容和参与性的数字化空间，其特点为：•面对威胁时的应对、支持和自助；•防范危害；•确保保护儿童和为在儿童成长为数字化公民的过程中，在实现保护和提供机遇之间实现动态平衡；•维护儿童和社会的权利和责任。	https://www.itu-cop-guidelines.com/		Legal1.3.3；Tech1.2.4 Tech4；Org1.3；Org2.4；CapDev1.6
关键基础设施（亦参见：国家关键基础设施）		受到中断或破坏时，会削弱公共卫生与安全、商业和国家安全或这些事项的多个组合的关键系统、业务和功能。	https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf	这些系统包括但不限于：国防系统、银行和金融、电信、交通、卫生、能源等。	Tech1.2
关键信息基础设施	CII	若受到中断或毁坏，将对公民的健康、安全或经济福祉以及一国政府的有效运作产生严重影响的材料和数字资产、网络、服务和设施	国际关键信息基础设施保护（CIIP）手册 2008/2009 年	这些系统包括但不限于：电话交换机、互联网交换机、无线网络、卫星等	
网络犯罪法		网络犯罪法为互联网、计算机和相关数字技术的使用以及公众、政府和私营组织的行动提供了行为准则和行为标准；证据规则和刑事诉讼程序，以及网络空间的其它刑事司法事宜；以及规定...	https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html		Legal1
网络安全审计要求		安全审计是对信息系统安全进行定期的系统化评估。典型的审计可包括评估系统的物理配置和环境、软件、信息处理程序和用户行为的安全性	GCIv4		Legal2.3n

术语	缩写	定义	来源	示例	提及的问题（GCIv4）
网络安全生态系统		围绕网络安全和网络安全中的参与者社区，具有共同演化的角色和责任	改编自 James Moore《竞争的衰亡》（*The Death of Competition*）。1996	例如，法律、技术、商业和政策专业人士就网络安全相关问题共同努力	CapDev5.1、CapDev6.2
网络安全的弹性		从安全入侵或攻击中恢复的能力。国家网络安全弹性计划确保国家能及时有效地对抗、承受、应对任何（自然的或人为的）灾害的影响并从灾害中恢复，包括通过依赖外部服务保护和恢复其重要的服务和功能。	https://www.itu.int/en/ITU-T/focusgroups/ssc/Documents/website/web-fg-ssc-0090-r7-technical_report_on_ICT_infrastructure_for_resilience_security.doc		Tech1.3
网络安全条约和协议		两个国家、组织或其它团体之间与网络安全有关的专门条约或协议	https://guides.ll.georgetown.edu/c.php?g=363530&p=4821478		
数据泄露通知		泄露通知的法律或规定要求被入侵的实体向管理部门、客户或其他方通知入侵情况，采取措施补救因入侵造成的损害。这些法律的制定是为了应对不断增加的对包含个人身份信息的消费者数据库的入侵行为。	GCIv2		Legal2.2
非法访问		当针对整个计算机系统或其任何部分的访问属于未经授权的故意访问，任一方可以认定，通过侵害安全措施，或侵害连接到另一计算机系统的计算机系统，并带有获得计算机数据的意图或其它不诚实意图的行为是犯罪行为。	GCIv2		Legal1.1.1
非法监听		未经授权，从计算机系统或在计算机系统内，通过技术手段，对非公开传输的计算机数据（包括来自携带此类计算机数据的计算机系统中的电磁辐射）的故意监听。	GCIv2		Legal1.1.3
非法干扰		“未经授权而故意对计算机数据进行毁坏、删除、破坏、更改或限制”以及“未经授权，通过输入、传输、破坏、删除、恶化、更改或限制计算机数据，故意严重阻碍计算机系统的运行”	GCIv2,		Legal1.1.2
事件通知		CIRT 或其它机构向相关利益攸关方通知网络安全事件。			Legal2.2
机构间伙伴关系/协议		一个国家内不同政府机构之间的任何国内官方伙伴关系均可以促进政府对网络安全风险的响应。伙伴关系可包括各部委、部门、项目和其它公共部门机构之间的信息或资产共享伙伴关系。就本节而言，不考虑不同国家的机构间或政府间组织之间的机构间伙伴关系。	GCIv2		Coop5
机构间协调流程		两个或多个政府机构之间就各种问题进行协调，以便努力实现共同的目标和活动			Coop5.1
中小微企业	MSMEs	中小微企业的定义可能因国家而异。在可能的情况下，应使用中小企业金融论坛跟踪的定义		https://www.smefinanceforum.org/data-sites/msme-country-indicators	CapDev1.1；CapDev2.3.3
多边协议		多边协议（一对多协议）指官方认可的国家的或具体部门的任何合作项目，由政府与多个外国政府或国际组织进行的跨境网络安全信息或资产的共享（例如合作或交流信息、专业知	GCIV2		Coop3；Coop3.1.1；Coop3.1.2

术语	缩写	定义	来源	示例	提及的问题（GCIv4）
		识、技术和其它资源）。还可包括批准与网络安全相关的国际协议，如《非洲联盟网络安全和个人数据保护公约》、《布达佩斯网络犯罪公约》等			
国家关键基础设施（亦参见：关键基础设施）		受到中断或破坏时，会削弱公共卫生与安全、商业和国家安全或这些事项的多个组合的关键系统、业务和功能。	https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf		Legal2.7；Org1.1.1
国家 CIRT		CIRT（计算机事件响应组）、CERT（计算机应急响应组）或 CSIRT（计算机安全事件响应组）是负责协调和支持国家层面的计算机安全事件或事故响应的具体的组织实体。它们在各国负责提供识别、防御、响应和管理网络威胁的能力，并加强该国网络空间的安全。这种能力需要与收集自身情报相结合，而非依赖于对安全事件的二次报告（无论是来自 CIRT 所在地区还是来自其它来源的事件）。可以为军用，也可为民用	来自 GCI2。		
网上虐待					Legal1.3.2
网上骚扰		通过电子邮件、直接信息或不良网站发送的消息，目的在于通过个性化的攻击对个人或一群人进行欺凌或骚扰。	GCIv4		Legal1.3.2
上网安全		指与私人以及个人或产权有关的信息的各种安全风险相关的互联网安全实现最大化，以及增强用户的自我保护，以免受网络犯罪的侵害。	GCIv4		Legal1.3
有具体需求人士		因身体残疾、学习或行为困难等引起的特殊要求（特别是在教育环境中的要求）	牛津英语词典	“具体需求，名词及形容词”。牛津英语词典（OED）网络版。2021 年 6 月。牛津大学出版社。https://www.oed.com/view/Entry/253889?redirectedFrom=special+needs（于 2021 年 8 月 30 日访问）。	
个人数据保护		个人数据是与已识别或可识别的自然人有关的任何信息。个人数据保护是维护个人数据的过程。	https://gdpr-info.eu/issues/personal-data/ 定义来自《通用数据保护条例》（GDPR）	自愿性标准 ITU-T X.1058|ISO/IEC 29151 为政府和行业提供了一个有价值的参考点，因为它们加大了对个人数据保护的力度。X.1058 确立了数据保护控制的目标，规定了所需的控制措施并为其实施提供了导则。它显示了这些控制措施的安排如何满足组织的风险和影响评估所确定与个人数据保护相关的要求。	Legal2.1a

术语	缩写	定义	来源	示例	提及的问题（GCIv4）
政策		政策是一个组织或一个国家为实现长期目标而采用或设计的规则、原则、指南或结构，通常以易于访问的书面格式定义。制定政策是为了推动和影响组织内部所做的各项重大决策，并将所有活动保持在既定的边界范围内。	新定义		Org1.1
中学后非高等教育（ISCED 4 级）	ISCED 4 级	中学后非高等教育提供以中等教育为基础的学习经历，为进入劳动力市场和高等教育做准备。它旨在让个人获得低于高等教育复杂程度的知识、技能和能力。ISCED 4 级或中学后非高等教育的课程通常旨在为完成 ISCED 3 级课程的个人提供升入高等教育或就业所需的非高等教育资质，这是他们的 ISCED 3 级资质无法授予其获得的内容...	http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf	http://uis.unesco.org/en/isced-mappings	CapDev3.4n
初等教育（ISCED 1）		ISCED 1 级或初等教育的课程通常旨在为学生提供阅读、写作和数学（即识字和算术）的基本技能，并为学习和理解知识、个人和社会发展的核心内容奠定坚实基础，为中等教育做好准备。它的重点在于在基本的复杂水平上进行学习，几乎没有任何专业化内容... 年龄往往是该级别唯一的入学要求。惯常或法定入学年龄通常不低于 5 岁且不高于 7 岁。	http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf	http://uis.unesco.org/en/isced-mappings	CapDev3.1
隐私保护		互联网隐私是通过互联网发布的个人数据的隐私和安全级别。该术语含义宽泛，包括用于保护敏感和私人数据、通信和偏好内容的各种因素、技巧和技术。此类立法可见《数据保护法》。	GCIv2		Legal2.1b
公私伙伴关系	PPP	私营方与政府实体之间为提供公共资产或服务而达成的长期合同，其中私营方承担重大风险和管理责任，报酬与绩效挂钩。 注：由于缺乏正式的法律定义，PPP 通常以功能为特征。联合国秘书长提议了两种类型。第一种类型确定了五大主要职能：a）政策对话，例如信息和通信技术任务组、世界水坝委员会、全球疫苗免疫联盟（GAVI）；b）宣传，例如联合国艾滋病规划署（UNAIDS）与媒体伙伴关系，以提高对艾滋病的认识；c）调动私人资金，例如联合国基金会和国际伙伴关系基金、联合国贸易和发展会议-国际商会外国投资项目；d）信息和学习，例如联合研究和培训项目；e）业务交付，例如联合国-LM 爱立信实地首发举措、联合国-微软难民登记项目（联合国导则 18-32）。第二种类型确定了四大职能：a）宣传，例如全球改善营养联盟、全球肥皂洗手 PPP 关系；b）制定规范和标准，例如全球报告举措、关于金融行业企业责任的“谁在乎谁成为赢家”项目；c）共享资源和专业知识，例如世界粮食计划署-TNT“移动世界”物流项目；以及 d）利用市场促进发展，例如联合国妇女发展基金（UNIFEM）-欧舒丹乳木果油生产举措、工发组织（UNIDO）-菲亚特印度汽车零部件项目（联大《秘书长关于加强联合国与所有相关伙伴，特别是私营部门的合作的报告》[2005 年 8 月 10 日]。《联合国导则》界定了几种合作模式和各模式使用的标准法律安排，或简单地定义为：公共和私营部门之间的合作项目。该绩	https://ppp.worldbank.org/public-private-partnership/overview/what-are-public-private-partnerships https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1084?rskey=CTIBOr&result=1&prd=MPIL		

术语	缩写	定义	来源	示例	提及的问题（GCIv4）
		效指标可以通过官方认可的国家或特定部门的 PPP 关系的数量加以衡量，这些 PPP 关系用于在公共和私营部门之间共享网络安全信息（威胁情报）和资产（人员、流程、工具）（即用于信息、专业知识、技术和/或资源合作或交流的官方合作伙伴关系），在国内和国际层面皆如此。			
法规		管理行为或实践的规则或原则；特别是由有关部门建立和维护的此类指令。	牛津英语词典	“规定，名词及形容词”。OED 网络版。2021 年 6 月。牛津大学出版社。https://www.oed.com/view/Entry/161427?redirectedFrom=regulation（于 2021 年 8 月 30 日访问）。	Legal2、Legal2.1、Legal2.2
研究和开发	R&D	研究和实验开发（R&D）包括创造性、系统性的工作，以增加知识储备 – 包括人类、文化和社会的相关知识 – 并设计可用知识的新应用。“R&D”一词涵盖三类活动：基础研究、应用研究和实验开发。一项活动要成为 R&D 活动，必须满足五大核心标准。此活动必须具有：•新颖性（旨在获得新发现）•创造性（基于原创的而非显而易见的概念和假设）•不确定性（不确定最终结果）•系统性（有待规划和预算）•可转让和/或可重复性（形成的结果可复制）。	经济合作发展组织（OECD）（2015 年），《弗拉斯卡蒂手册（2015）：研究与实验开发数据采集和汇报导则》（Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development） http://uis.unesco.org/en/glossary-term/research-and-experimentaldevelopment-rd		CapDev4.1；CapDev4.1.1；CapDev4.1.2；CapDev4.1.3
中等教育（ISCED 2 级和 3 级）	ISCED 2 级和 3 级	ISCED 2 级或初中教育的课程往往建立在 ISCED 1 级的学习成果之上。其目的通常是为终身学习和人类发展奠定基础，教育系统可在此基础上扩大进一步教育的机会。一些教育系统可能已提供 ISCED 2 级的职业教育课程，为个人提供与就业相关的技能 ISCED 3 级或高中教育的课程往往旨在完成中等教育，为高等教育做好准备，或提供与就业相关的技能，或两者兼而有之。 自 ISCED 1 级起，完成 8 至 11 年的教育后，开始进入 ISCED 3 级。	http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf	http://uis.unesco.org/en/isced-mappings	CapDev3.2
高等教育（ISCED 5-8 级）	ISCED 5-8 级	ISCED 5 级或短期高等教育的课程往往旨在为参与者提供专业知识、技能和能力。通常以实践为基础，具有职业特定性，为学生进入劳动力市场做好准备。但是，这些课程也可能提供通往其它高等教育项目的途径.....	http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-	http://uis.unesco.org/en/isced-mappings	CapDev3.3

术语	缩写	定义	来源	示例	提及的问题（GCIv4）
		ISCED 6 级或学士学位或同等水平的课程往往旨在为参与者提供中级学术和/或专业知识、技能和能力，最终获得第一级学位或同等资格。 ISCED 7 级或硕士学位或同等水平的课程往往旨在为参与者提供高级学术和/或专业知识、技能和能力，最终获得第二级学位或同等资格…… ISCED 8 级或博士学位或同等水平的课程主要旨在获得高级研究资格。ISCED 该级别的课程致力于高等学习和原创研究，往往仅由大学等以研究为导向的高等教育机构提供。在学术和专业领域均存在博士课程……	education-isced-2011-en.pdf		
排外主义		不喜欢外来的或被视为外来的人士、文化和习俗，或对此抱有偏见。	牛津英语词典	“排外主义，名词”。OED 网络版。2021 年 6 月。牛津大学出版社。https://www.oed.com/view/Entry/230996?redirectedFrom=xenophobia（于 2021 年 8 月 30 日访问）。	Legal1.3.1
国家举措		为系统地解决具体问题而在国家层面开展的活动	GCIv2	国家举措通常旨在解决组织的具体关切领域。示例包括人权、教育或环境。它们可以是各项目标，也可以是通过“创建项目”界面指定给一个或多个成员的具体目标。	
计算机伪造		与计算机相关的伪造涉及出于欺诈目的在网上冒充合法的个人、当局、机构和其它实体	https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/computer-related-offences.html#:~:text=Computer%2Drelated%20forgery%20involves%20impersonation,entities%20online%20for%20fraudulent%20purposes		Legal1.2
未经请求的通信或垃圾信息		未经过接收方请求的电子化通信，例如电子邮件、短信、社交媒体或电话。垃圾信息是指批量发送的此类未经请求的通信	GCIv2		Legal2.7
数字签名		数字签名是用于验证信息、软件或数字文件真实性和完整性的数学技术。	GCIv2		Legal2.6
电子交易		电子交易指企业、家庭、个人、政府和其它公共或私营组织之间以计算机网络为媒介，销售或购买商品或服务；此类立法文件示例包括《电子商务法》、《电子签名法》、《电子交	GCIv2		

术语	缩写	定义	来源	示例	提及的问题（GCIv4）
		易法》等，其中也可包括建立认证机构管理机构的法规。			
网络安全标准		存在经政府批准（或支持）的一个框架（或多个框架），用以实施国际公认的公共部门（政府机构）及关键基础设施（即使是由私营部门运营的基础设施）的网络安全标准。这些标准包括但不限于由以下机构制定的标准：ISO、国际电联、互联网工程任务组（IETF）、电子和电气工程师学会（IEEE）、电信行业解决方案联盟（ATIS）、结构化信息标准促进组织（OASIS）、3GPP、3GPP2、互联网架构委员会（IAB）、互联网协会（ISOC）、行业规范组（ISG）、ISI、欧洲电信标准研究所（ETSI）、区域间标准化论坛（ISF）、RFC、ISA、国际电工技术委员会（IEC）、北美电力可靠性委员会（NERC）、美国国家标准与技术研究院（NIST）、美国联邦信息处理标准（FIPS）、支付卡行业数据安全标准（PCI DSS）等； 或 认证/标准化方面的网络安全法规要求在一国领土内运营的实体满足特定、最低限度的认证/标准化要求。根据所在经济领域，此类要求可能存在变化。这些标准包括但不限于以下机构指定的标准：ISO、国际电联、IETF、IEEE、ATIS、OASIS、3GPP、3GPP2、IAB、ISOC、ISG、ISI、ETSI、ISF、RFC、ISA、IEC、NERC、NIST、FIPS、PCI DSS 等		GCIv4 定义和 GCIv2	Legal2.5
网络安全演习（例如网络演练）		有计划地开展活动，在活动中某个组织会模拟网络中断，以此发展或测试针对网络中断的防护、检测、缓解、响应或恢复等能力。	GCIv4		Tech1.2.2
网络演练		网络演习是一年一度的活动，在此期间模拟网络攻击、信息安全事件或其他类型的中断，以测试组织的网络能力，从能够检测安全事件到能够做出适当响应并最大限度地减少任何相关影响。通过网络演习，参与者能够验证策略、计划、程序、流程和能力，以实现准备、预防、响应、恢复和操作的连续性。	国际电联定义	https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybedrills-2020.aspx	Tech1.2.2
网络安全咨询		CIRT 咨询：向公众分享有关新兴网络威胁的信息以及建议采取的行动。	GCIv4		Tech1.2.3
FIRST 成员		事件响应与安全组论坛的正式成员或联络成员。论坛网址：www.first.org	GCIv4		Tech1.3
区域性 CIRT/CERT/CSIRT 成员		与国外的其它任何 CERT 的正式或非正式关系，作为任何一个区域性 CERT 的成员。区域性 CERT 的示例包括亚太 CERT（APCERT）、非洲 CERT（AFRICACERT）、出口组证书（EGC）、伊斯兰合作组织（OIC）和 OAS。	GCIv4		Tech1.4
行业 CERT/CIRT/CSIRT		行业 CIRT/CSIRT/CERT 是指对影响具体行业的计算机安全或网络安全事件做出响应的实体。医疗、公共设施、应急服务和金融行业等重要行业一般都会成立行业 CERT。与政府 CERT 不同，行业 CERT 仅向某一行业的机构提供服务。	GCIv2		Tech2.1

术语	缩写	定义	来源	示例	提及的问题（GCIv4）
国际网络安全合作		两个或多个政府、国家机构、国家监管机构、国家 CIRT、民间社会组织或学术界之间的协作			Org1.8
报告机制和能力		如全国求助热线，以及与国际求助热线系统相连的热线。这些需要与转诊和支持系统加以连接			Org4.3
提高公众网络安全认识的活动		提高公众认识包括向尽可能多的公民开展宣传活动，以及通过非政府组织（NGO）、机构、组织、ISP、图书馆、本地工会、社区中心、社区大学和成人教育项目、学校和家长—教师组织普及安全的在线网络行为。包括建设提高公众认识的门户和网站、传播配套材料，以及其它有关活动。	GCIv4		CapDev1
安全运行中心	SOC	“SOC 是在所有安全操作的核心运行的组织单位。它通常不被视为单个实体或系统，而是作为管理和加强组织整体安全态势的复杂结构。其职能是通过人员、流程和技术来检测、分析和响应网络安全威胁和事件。这些活动可以形式化为 SOC 的七个维度或职能领域。虽然人们广泛接受 SOC 对公司安全至关重要，但 SOC 仍被认作被动的响应型防御机制” “计算机安全事件响应组：此术语常可与 SOC 互换使用，尽管它主要关注攻击发生后的响应部分。CSIRT 是负责协调和支持计算机安全事件响应的组织单位。CSIRT 可归类为独立的团队，也可归类为 SOC 的一部分” “网络运行中心：网络运营中心（NOC）负责监督问题的识别、调查、优先级排序、升级和解决。但在 NOC 中解决的问题是不同的，因为 NOC 关注影响组织网络性能和可用性的事件。由于事件可能发生在所有系统上而非仅发生在网络中，因此 NOC 与 SOC 团队合作对组织是有益的。” “安全情报中心：‘安全情报中心（SIC）’这一术语于 2017 年首次用于描述 SOC 的继任机构。它旨在提供比 SOC 更全面、更一体化的视图，并且可以在同一处对安全情报进行完全可视化和管理。因此，可将若干技术（例如信息安全（IS）知识管理、大数据处理）结合在一起。” “安全信息和事件管理：SIEM 是许多 SOC 不可或缺的组成部分，涵盖了大部分技术要求。它负责以集中的方式收集与安全相关的数据。因此，它通过关联日志事件来提供安全分析功能。其它功能支持使用上下文数据进行丰富、规范异构数据、报告和告警。为实现威胁信息的交换，SIEM 提供了与网络威胁情报交换平台的连接，并通过提供可视化的安全分析能力，让人工安全分析师加以参与。它包括通过长时间存储事件数据实现的日志管理功能。”	https://ieeexplore.ieee.org/document/9296846		