全球网络安全指数（GCI）2015/16 年问卷调查指南

本文件仅供参考。全球网络安全指数（GCI）旨在衡量各国在全球网络安全议程五大支柱中践行网路安全承诺的情况，包括：法律措施、技术措施、组织措施、能力建设和合作。

本问卷调查将为确定全球网络安全指数（GCI）2015/16 得分而提出的问题与 ITU-D 第 2 研究组问题 3 所要求的问题结合起来。问卷分相互独立的三节，前两节问题的答案为是或否，最后一节列出了开放式问题。问卷调查需在线填写，每个答卷人均将得到一个唯一的 url（来自国际电联的官方邮件），以妥善保存。答卷人填写答复时可上传相关文件（和 url），作为补充信息。

答卷人在问卷调查中提供的信息应不具有保密性质。

第 1 节

1. 是否存在相关网络立法？

1.1. 是否存在相关网络立法？

Exp: 网络犯罪立法指针对未授权访问、数据和系统干扰或拦截、滥用计算机系统的法律。此类法律条款包括程序法、现有关于快速保护存储电脑数据、创建工单、实时收集电脑数据、引渡、互助、保密和使用限制的条文；以及关于网络犯罪或计算机滥用的案例法，还包括内容相关犯罪的法律条文。条款可为国家刑法、数据保护法、信息自由法、版权/知识产权法的一部分。

1.1.1. 是否存在实质性网络犯罪法律？

Exp: 实质性法律指所有类别的公法和私法，包括关于合同、不动产、侵权、遗嘱的法律，以及实质上确立、定义和管理权利的刑法。

1.1.1.1. 是否存在与未经授权访问电脑、系统和数据相关的条款？

Exp: 未经授权的访问指使用他人账户或通过猜测/破解密码和窃取身份等不正当手段，访问电脑、系统和数据。

1.1.1.2. 是否存在与未经授权干扰、篡改电脑、系统和数据相关的条款？

Exp: 未经授权的干扰/篡改行为指通过改变系统、电脑或数据的初始状态，扰乱该系统、电脑或数据的行为，包括输入、破坏、删除或常见的改变电脑数据的行为。

1.1.1.3. 是否存在与未经授权拦截电脑、系统和数据相关的条款？

Exp: 未经授权的拦截行为指非法获取非公开传输的电脑数据。

1.1.2. 是否存在程序性网络犯罪法律？

Exp: 指法院听取、决定民事法律诉讼、刑事或行政程序中具体事宜时依据的规则。规则在制定时旨在确保法院在审理案件时以公正、一贯的方式应用正当程序或基本公正原则。

1.1.2.1. 是否存在与快速保护存储电脑数据相关的条款？

Exp: **数据保护是国家主管部门要求个人或组织履行的义务，即在具体时间段内妥善保管某一具体类型的数据，防止丢失或篡改。**

1.1.2.2. 是否存在与创建工单相关的条款？

Exp: 创建工单是国家主管部门要求个人或组织履行的义务，即在具体时间段内向执法官员发送可用的、具体类型的电脑数据。

1.1.2.3. 是否存在与搜索、获取存储的电脑数据相关的条款？

Exp: 搜索、获取电脑数据指通过措施授权主管部门搜索、访问本国境内的电脑系统和存储的电脑数据的措施，包括立法措施。

1.1.2.4. 是否存在与实时收集电脑数据相关的条款？

Exp: 实时收集数据指通过措施授权主管部门实时收集或记录本国境内以计算机系统传输的数据，包括立法措施。

1.1.2.5. 是否存在与引渡网络罪犯相关的条款？

Exp: 引渡指一国在收到另一国正式请求后，将在请求国司法管辖区内受网络犯罪指控或判刑的个人移交至该国司法管辖区的程序。

1.1.2.6. 是否存在与互助相关的条款？

Exp: 指两国或多国通过签署协议收集、交换信息，以落实公共法或刑法。

1.1.2.7. 是否存在与保密和使用限制相关的条款？

Exp: **一方在遵守特定保密条款的条件下可使用向其提供的数据，或只能将数据用于具体商定的用途。**

1.1.3. 是否存在与网络犯罪或计算机滥用相关的案例法？

Exp: 计算机滥用方面的违法行为可包括黑客入侵、未经授权访问计算机系统及蓄意传播恶意和破坏性软件（恶意软件）。未经授权访问并篡改电脑的行为可包括改变软件和数据、改变密码和设置阻止他人访问系统，以及干扰系统正常操作，对系统造成损害。

1.2. 是否存在网络安全立法或规定？

Exp: 规定指基于并旨在实施具体立法的规则。规定通常由履行某项立法宗旨或条款的监管机构执行。因此，网络安全规定将指定各利益相关方遵循的原则。规定源自相关法律，并成为其一部分，主要针对数据保护、入侵通知、网络安全认证/标准化要求、网络安全实施、网络安全审计要求、隐私保护、儿童在线保护、数字签名和电子交易、以及互联网提供商义务。

1.2.1. 是否存在数据保护立法或规定？

Exp: 与个人、商业和政府数据保护，防范未授权访问、篡改、破坏或使用相关的规定。

1.2.2. 是否存在系统和网络保护立法或规定？

Exp: 旨在保护系统和网络免受有害干扰的法律措施。

1.2.3. 是否存在入侵通知立法或规定？

Exp: 入侵通知法律或规定要求被入侵实体向管理部门、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。为应对不断增加的入侵包含个人数据的消费者数据库行为，制定了这些法律。

1.2.3.1. 对于数据？

Exp: 入侵通知法律涉及数据外泄。

1.2.3.2. 对于系统和网络？

Exp: 入侵通知法律涉及系统和网络入侵。包括网络安全维护标准，或保护加密的消费者数据的其它基本要求。

1.2.4. 是否存在网络安全认证/标准化立法或规定？

Exp: 认证/标准化方面的网络安全规定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、ITU、IETF、IEEE、ATIS、OASIS、 3GPP、3GPP2、 IAB、 ISOC、 ISG、 ISI、 ETSI、 ISF、 RFC、 ISA、 IEC、 NERC、 NIST、 FIPS、PCI DSS 等。

1.2.4.1. 对于公共领域？

Exp: 规定指某公共领域内必要的网络安全认证/标准化。

1.2.4.2. 对于私营领域？

Exp: 规定指某私营领域内必要的网络安全认证/标准化。

1.2.5. 立法或规定是否实施网络安全措施？

Exp: 网络安全措施包括但不限于技术和组织性措施，如：防火墙、访问控制列表、完全规则和责任、网络犯罪保险（自付）。

1.2.5.1. **对公共领域？**

1.2.5.2. 对于关键基础设施运营商？

Exp: 关键基础设施是一国安全、安防、经济安全和公共安全的关键系统，包括但不限于国防系统、银行和金融、电信、交通、健康、能源等。

1.2.5.3. 对私营领域？

1.2.6. 立法或规定是否实施网络安全审计？

Exp: 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物理配置和环境、软件、信息处理程序和用户行为的安全性。

1.2.6.1. 对公共领域?

1.2.6.2. 对关键基础设施？

1.2.6.3. 对私营领域？

1.2.7. 是否存在具体说明隐私保护的立法或规定？

Exp: 互联网隐私指通过互联网发布的个人数据隐私和安全水平。本条含义宽泛，指保护敏感和私人数据、通信和偏好数据的多种因素、技巧和技术。此类立法示例见《数据保护法》。

1.2.8. 是否存在与数字签名和电子交易相关的立法和规定？

Exp: 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。电子交易指企业、家庭、个人、政府和其他公私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》、《电子交易法》等，其中可包括建立认证机构管理单位的规定。

1.2.9. 是否存在与互联网服务提供商责任和义务相关的立法或规定？

Exp:互联网服务提供商负责因其用户行为引起的盗版侵权。提供商有责任向警方、CERT 或其它负责机构/国家部门通报源自其基础设施的违法网络操作，此为主动网络监督的要求。

1.2.10 是否存在与遏制或抑制垃圾邮件相关的立法或规定？

1.3. 是否存在针对执法官员、司法人员和其他法律人员的网络安全培训？

Exp: 法律人员电脑安全培训的正式程序。

1.3.1.对执法人员（警官和执法机构）？

1.3.2.对司法和其他法律人员（法官、法务官、法庭律师、辩护律师、律师、律师助理等）？

1.3.3.是否存在经常性培训？

Exp: 定期或重复组织的培训。

2. 是否出台了技术措施？

2.1. 是否存在具有国家责任的 CIRT、CSIRT 或 CERT？

Exp: CIRT 指计算机事件响应小组，CSIRT 指计算机安全事件响应团队，CERT 指计算机应急响应小组。这些小组均可指定接收安全漏洞报告、分析报告并回复发送方的实体。国家 CSIRT/CIRT/CERT 指赋予国家责任的实体，通过当地团体监督、管理及处理网络安全事件，包括学术界、执法部门、公民社会、私营部门（经济集团或重要团体、关键信息基础设施（能源、健康、交通、金融等））和政府部门。在出现攻击时，还与其它国家 CIRT，以及地区和国际机构进行有效协调。

2.1.1. 是否具有政府授权？

Exp: 由政府决定支持或是政府组织的一部分。

2.1.2. CIRT、CSIRT 或 CERT 是否进行经常性的网络安全演练？

Exp: 根据计划，该组织会模拟网络中断，开发或测试防护、探测、消减、响应或恢复等能力。这种演练是否定期或重复举行？

2.1.3. CIRT、CSIRT 或 CERT 是否隶属于 FIRST?

Exp: 事件响应和安全小组论坛的正式成员或联络成员。

2.1.4. CIRT、CSIRT 或 CERT 是否隶属于其它 CERT 机构（区域 CERT）?

Exp: 与国内或国外其它 CERT 存在正式或非正式关系，区域 CERT 的成员。

2.2. 是否存在政府 **CERT?**

Exp: 政府 CERT/CIRT/CSIRT 指应对仅影响政府机构的电脑安全或网络安全事件的实体。除反应式服务外，政府 CERT 也可参与漏洞分析和安全审计等主动服务。与服务公私领域的国家 CERT 不同，政府 CERT 仅向公共领域的机构提供服务。

2.3. 是否存在部门 **CERT?**

Exp: 部门 CERT/CIRT/CSIRT 指应对影响具体部门的电脑安全或网络安全事件的实体。医疗、公共设施、应急服务和金融行业等重要部门一般会设立部门 CERT。与服务公共领域的政府 CERT 不同，部门 CERT 仅向某一部门的机构提供服务。

2.4. 是否存在实施网络安全标准的框架？

Exp: 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（即使是私营部门运营的）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、ITU、IETF、IEEE、ATIS、OASIS、3GPP、3GPP2、IAB、ISOC、ISG、ISI、ETSI、ISF、RFC、ISA、IEC、NERC、NIST、FIPS、PCI DSS 等。

2.4.1. 在公共领域？

2.4.2. 在私营领域？

2.5. 是否存在网络安全专业人员认证及鉴定框架？

Exp: 存在经政府批准（或支持）的一个框架（或多个框架），用于根据国际公认的安全标准来开展专业人员的认证和鉴定工作。这些认证、鉴定和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)、(无建议)认证、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-计算机安全时间处理机构认证 (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)等。

2.5.1. 在公共领域？

2.5.2. 在私营领域？

2.6. 是否实施了应对垃圾邮件的技术机制和能力？

2.7. 是否存在残障人士能够获取的与网络安全相关的特定工具和技术措施，如反病毒或反垃圾邮件软件？

3. 是否存在组织性措施？

3.1. 是否存在网络安全国家战略？

Exp: 国家网络安全战略或信息基础设施保护国家规划方面的政策指国家正式确定和支持的政策，可包括以下责任：为政府（地方、区域和联邦或国家）各个层面规定明确的职责，其中要清晰定义作用和责任；鼓励私营部门参与政府牵头的举措，并建立合作关系来推动网络安全；政府确定关键利益相关方的路线图。

3.1.1. 国家战略是单独存在的吗？

Exp: 国家网络安全战略可包含在国家信息、技术或安全战略外的文件中。

3.1.1.1. 是否针对私营部门？

Exp: 战略为私营部门的各方定义了网络安全的角色和责任。

3.1.1.2. 是否针对公共部门？

Exp: 战略为公共部门的各方定义了网络安全的角色和责任。

3.1.1.3. 是否存在与关键信息基础设施保护相关的章节？

Exp: 战略包括关键信息基础设施保护规划。

3.1.1.4. 是否存在治理蓝图？

Exp: **战略中包括的蓝图为战略的成果、完成情况设定了里程碑。**

3.1.1.5. 是否对战略做经常性修订？

Exp: 根据可能产生影响的国家、技术、社会、经济和政治发展情况对战略进行更新。

3.1.1.6. 战略是否开放公共讨论？

Exp: 战略向所有利益相关方开放讨论，包括基础设施运营商，ISP，学术界等。

3.1.1.7. 战略是否包括国家灾备计划？

Exp: 国家灾备计划确保国家以及时有效的方式从灾难（自然或人为）影响中恢复，包括保护及恢复必要的基础结构和功能。

3.1.2. 国家网络安全战略是否作为一部分包含在更广泛的国家战略中？

3.1.2.1. 是否存在与关键信息基础设施保护相关的章节？

Exp: 关键基础设施是一国安全、安防、经济安全和公共安全的关键系统，包括但不限于国防系统、银行和金融、电信、交通、健康、能源等。

3.1.2.2. 网络安全部分是否存在治理蓝图？

3.1.3.是否定义了公共部门的重点？

3.1.4.若尚未实施网络安全战略，是否在制定中？

3.1.5.现有或正在制定的战略是否包含与残障人士相关的行动？

3.2. 是否存在负责网络安全的国家实体/机构？

Exp: 负责机构指实施国家网络安全战略/政策的机构，可包括常设委员会、官方工作组、咨询理事会或跨部门中心。此类机构也可直接负责国家CIRT。负责机构可存在于政府内，也可有权要求其他机构和国家实体实施政策和标准。

3.2.1. 是否存在负责关键信息基础设施保护的机构？

3.2.2. 是否存在作为垃圾邮件相关问题联络处的国家机构？

3.3. 在国家层面是否存在衡量网络安全发展的指标？

Exp: 存在官方认可的国家或具体到行业部门的标杆或参考，用于衡量网络安全发展、风险评估战略、网络安全审计和其它工具和活动，通过评级或评估结果提升未来的性能。例如，基于与信息安全管理相关的度量 ISO/IEC 27004。

3.3.1. 是否定期进行网络安全风险评估？

Exp: 包括风险识别、风险分析和风险评估的系统程序。

3.3.1.1. 是否存在用于评估风险的网络安全标杆？

3.3.1.2. 评级或评估结果是否能提升未来的表现？

3.3.2.是否进行经常性网络安全审计？

Exp: 安全审计是信息系统安全的系统化评估，用于衡量系统遵循既定标准的情况。全面的审计通常评估系统物理配置和环境、软件、信息处理程序和用户行为的安全性。

3.3.2.1. 网络安全审计是否是强制性的？

Exp:通过内部或部门规定或遵循认证标准 ISO270001 实施。

4. 是否存在能力建设活动？

4.1. 本国是否存在标准化机构？

Exp: 标准化是技术成熟水平的良好指标，关键领域新出现的标准也突出了标准的重要意义。虽然网络安全一直属于国家安全问题，不同国家处理的方式也不尽相同，但普遍认可的标准支持常见的方式。这些标准包括但不限于以下机构指定的标准：ISO、ITU、IETF、IEEE、ATIS、OASIS、3GPP、3GPP2、IAB、ISOC、ISG、ISI、ETSI、ISF、RFC、ISA、IEC、NERC、NIST、FIPS、PCI DSS 等。

4.1.1. 是否制定了自己的网路安全标准？

Exp: 网络安全标准是常见于公开出版资料中的技术，旨在保护用户或组织的网络环境。网络环境包括用户自身、网络、设备、所有软件、程序、存储或传输的信息、应用、服务和与系统直接或间接连接的系统。主要目标是降低风险，包括防止或消除网络安全攻击；一些国家采用国际标准，根据本国环境进行改编使其成为国家标准。其它国家（具有高级研发能力）根据采用情况制定标准，获得国际认可，为新国际标准做出贡献。

4.1.2. 是否采用现有国际网络安全标准？

Exp: 网络安全标准是常见于公开出版资料中的技术，旨在保护用户或组织的网络环境。网络环境包括用户自身、网络、设备、所有软件、程序、存储或传输的信息、应用、服务和与系统直接或间接连接的系统。主要目标是降低风险，包括防止或消除网络安全攻击；一些国家采用国际标准，根据本国环境进行改编使其成为国家标准。其它国家（具有高级研发能力）根据采用情况制定标准，获得国际认可，为新国际标准做出贡献。

4.2. 是否收集国家或部门网络安全最佳实践或指定指南？

Exp: 最佳实践是指拥有实证成功记录的方法或程序。采用最佳实践不仅可以降低失败的可能性，还能提升效率。

4.3. 是否存在网络安全研发项目方面的投资？

Exp: 网络安全研究项目包括但不限于恶意软件分析、密码学研究，以及系统漏洞和安全模型和概念研究。网络安全开发项目指硬件或软件解决方案的开发，包括但不限于防火墙、入侵防护系统、诱捕系统和硬件安全模块。设立统筹的国家机构将提高不同机构之间的协调和资源共享。

4.3.1. 在公共部门？

4.3.2. 在高等教育机构？

4.3.3. 是否存在国家认可的监督网络安全研发活动的机构？

4.4. 是否制定和实施了提高公众对网络安全认识的活动？

Exp: 提高公众认识的活动包括促进公共传播活动的努力，以及通过 NGO、机构、组织、ISP、图书馆、本地工会、社区中心、电脑商店、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。此类活动包括开放提高公众认识的门户和网站，传播支持材料，采用网络安全措施。

4.4.1. 对于组织？

Exp: 针对各组织的提高公众认识的活动。

4.4.2. 对于公民社会？

Exp: 提高广大民众认识的活动。

4.4.2.1. 对于成年人(>18 岁)？

4.4.2.2. 对于年轻人(12-17 岁)？

4.4.2.3. 对于儿童(<12 岁)？

4.4.3. 作为提高公众认识活动的一部分，是否向公众告知使用网络安全软件、硬件或基于服务的解决方案的益处？

4.4.4. 公众是否能够获取此类网络安全软件、硬件或基于服务的解决方案？

Exp: 例如，作为提高公众认识活动的一部分，免费或以优惠价格向公众提供。

4.5. 本国组织/政府是否开发或支持开发网络安全领域的专业培训课程？

Exp: 存在国家或具体部门的教育和专业培训项目，促进针对劳动力（技术、社会科学等）的网络安全课程，以及促进公共或私营部门的专业人才认证。

4.5.1. 对于组织？

4.5.2. 对于公共部门？

4.5.3. 对于公民社会？

4.6. 本国组织/政府是否开发或支持开发网络安全教育项目或学术课程？

Exp: 在学校、大专、大学或其它教学机构存在、促进国家教育课程和项目，对年青一代进行网络安全相关技能和职业的培训。网络安全相关技能包括但不限于设置高强度的密码，不在网络上透露个人信息。网络安全相关职业包括但不限于密码专家、数字取证专家、事件响应员、安全架构师和渗透测试员。

4.6.1. 在小学？

4.6.2. 在初中学？

4.6.3. 在高等教育中？

4.7. 政府在网络安全领域是否存在鼓励能力建设的激励机制？

Exp: 政府通过税费减免、拨款、资助、贷款、提供设施和其它经济和金融激励方式在网络安全领域鼓励能力建设的激励措施，包括成立本国认可的专属机构，监督网络安全能力建设活动。激励措施增加了网络安全相关服务和产品的需求，提高了网络威胁的防范能力。

4.7.1. 是否存在本国认可的专属机构，监督网络安全能力建设活动？

4.8. 是否存在本国的网络安全产业？

Exp: 支持网络安全发展的有利经济、政治和社会环境将激励网络安全私营领域的增长。提升公众意识的活动，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

4.8.1. 是否存在网络保险市场？

Exp: 作为保险产品，网络保险旨在保护企业和个人用户免于基于互联网的风险，以及与信息技术基础设施和活动相关的普遍风险。

4.8.1.1 对于在开放市场中没有能力获取网络风险保险的企业和其它实体，是否提供补贴？

4.8.2. 是否存在发展网络安全产业的激励措施？

Exp: 指标考察在网络安全领域鼓励，政府通过税费减免、拨款、资助、贷款、提供设施和其它经济和金融激励方式鼓励能力建设的措施，包括成立本国认可的专属机构，监督网络安全能力建设活动。激励措施增加了网络安全相关服务和产品的需求，提高了网络威胁的防范能力。

4.8.2.1. 是否向网络安全创业公司提供支持？

Exp: **具有支持网络安全创业公司和中小企业（SME）的机制（税费激励、技术园区、自贸区等）。**

5. 是否存在合作措施？

5.1. 是否存在网络安全合作双边协议？

Exp: 双边协议（一对一协议）指任何官方认可的国家或具体部门的合作机制，由政府与他国政府、地区实体或国际组织跨境共享网路安全信息或资产。

5.1.1.与主权国家？

5.1.1.1. 协议是否具有法律约束力？

Exp: 共同法律用语说明双方有意达成协议，部分行为已是法律要求或禁止的行为。

5.1.1.1.1. 对于信息共享？

Exp: 信息共享指共享威胁情报。

5.1.1.1.2. 对于资产共享？

Exp: 资产共享指共享专业人员（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。

5.1.1.2. 协议是否不具有法律约束力、非正式或等待批准？

5.1.1.2.1. 对于信息共享？

5.1.1.2.2. 对于资产共享？

Exp: 资产可包括人力资源、设施、设备等。

5.1.2.与国际组织？

5.1.2.1. 协议是否具有法律约束力？

5.1.2.1.1. 对于信息共享？

5.1.2.1.2. 对于资产共享？

Exp: 资产可包括人力资源、设施、设备等。

5.1.2.2. 协议是否不具有法律约束力、非正式或等待批准？

5.1.2.2.1. 对于信息共享？

5.1.2.2.2. 对于资产共享？

Exp: 资产可包括人力资源、设施、设备等。

5.2. 是否存在网络安全合作的多边或国际协议？

Exp: 多边协议（一对多协议）指任何官方认可的国家或具体部门的项目，由政府与多个外国政府或国际组织（即信息、专长、技术和其他资源上的合作或交流）跨界共享网络安全信息或资产。可包括批准与网络安全相关的国际协议，如《网络安全和个人数据保护非洲联盟公约》、《网络犯罪布达佩斯公约》等。

5.2.1. 协议是否具有法律约束力？

5.2.1.1. 对于信息共享？

5.2.1.2. 对于资产共享？

Exp: 资产可包括人力资源、设施、设备等。

5.2.2. 协议是否不具有法律约束力、非正式或等待批准？

5.2.2.1. 对于信息共享？

5.2.2.2. 对于资产共享？

Exp: 资产可包括人力资源、设施、设备等。

5.3. 本国组织/政府是否参加应对网络安全的论坛/协会？

5.4. 是否存在公私伙伴关系？

Exp: 公私伙伴关系（PPP）指的是在公共和私营部门之间开展的项目。该绩效指标可以通过官方认可的在公共部门和私营部门（即信息、专长、技术和/或资源交换或合作的官方伙伴关系）之间分享网络安全信息（威胁情报）和资产（人员、程序、工具）的国家或具体部门的 PPP 数量衡量，包括国际和国内 PPP。

5.4.1. 与本地企业？

5.4.1.1. 对于信息共享？

5.4.1.2. 对于资产共享？

5.4.2.与外国企业？

5.4.2.1. 对于信息共享？

5.4.2.2. 对于资产共享？

Exp: 资产可包括人力资源、设施、设备等。

5.5. 是否存在机构之间的合作关系？

Exp: 绩效指标指一国内（不包括国际伙伴关系）不同政府机构之间的官方伙伴关系，包括部委、部门、项目和其他公共机构之间的信息或资产共享伙伴关系。

5.5.1. 对于信息共享？

5.5.2. 对于资产共享？

Exp: 资产可包括人力资源、设施、设备等。

第 2 节

1. 是否存在儿童在线保护措施？

1.1. 是否存在与儿童在线保护相关的立法？

Exp: 通常有必要存在一个实体法律机构，明确规定在真实世界中任何针对儿童的犯罪行为在互联网或其他任何电子网络上也属违法，原则上适用。也有必要制定新的法律或改编现有法律规定某些只可能发生在互联网

上的行为不合法，例如在线引诱儿童进行或观看色情表演，或“鼓动”儿童在现实世界举行以性为目的的集会（《国际电联儿童在线保护决策者指南》）。

1.2. 是否存在负责儿童在线保护的机构/实体？

Exp: 存在致力于儿童在线保护的国家机构。

1.2.1. 是否存在报告与儿童在线保护相关问题的公共机制？

Exp: 有意者可通过电话、电子邮件、网页等形式报告与儿童在线保护相关的事件或担忧。

1.2.2. 是否存在儿童在线保护的技术机制和能力？

1.2.3. 政府或非政府机构是否组织过任何活动，为利益相关方提供儿童在线保护的知识和支持？

1.2.4.是否存在儿童在线保护教育项目？

1.2.4.1. 对于教育者？

1.2.4.2. 对于家长？

1.2.4.3. 对于儿童？

1.3. 是否存在儿童在线保护国家战略？

1.4. 是否组织了提高儿童在线保护意识的活动？

1.4.1.1. 对成年人(>18 岁)？

1.4.1.2. 对青少年(12-17 岁)？

1.4.1.3. 对儿童(<12 岁)？

第 3 节

附录：基于调查的观点

1. 在您看来，将提高网络安全认识作为实现网安全的基本措施的重要意义如何？
   a. 不重要
   b. 比较重要
   c. 重要
   d. 非常重要
2. 在贵国，提高网络安全认识的活动针对哪类人群？
   a. 儿童
   b. 青少年
   c. 学生
   d. 老年人
   e. 残障人士
   f. 私营机构
   g. 政府机构
   h. 其他
3. 下列哪个群体更具有针对性？请按针对性高低从 1 至 6 进行排列。
   a. 儿童
   b. 青少年
   c. 学生
   d. 老年人
   e. 残障人士
   f. 私营机构
   g. 政府机构
   h. 其他
4. 当前提高网络安全认识的活动针对那些问题？（多选）
   a. 互联网安全
   b. 隐私
   c. 欺诈
   d. 网络钓鱼
   e. 恶意软件
   f. 儿童在线保护
   g. 其他
5. 每个问题的重要程度如何？请按重要性从高到低排列并说明每项的原因？
   a. 互联网安全
   b. 隐私
   c. 欺诈
   d. 网络钓鱼
   e. 恶意软件
   f. 儿童在线保护
   g. 其他
6. 在网络安全方面，您是否获得过国际电联的协助或与国际电联合作？
   a. 如果是，请具体说明，并谈谈您对电联的协助/合作效率的看法，告诉我们在哪些网络安全领域需要电联。
   b. 如果否，请说明原因并告诉我们如何能提供协助？