国际电联电信发展部门（ITU-D）
网络安全项目

全球网络安全指数 – GCIv5

参考模型（方法）

International Telecommunication Union • Place des Nations • CH-1211 Geneva 20 • Switzerland
Tel : +41 22 730 5111 • Fax: +41 22 730 5545/730 5484 • E-mail: bdtmail@itu.int • www.itu.int/itu-d

目录

国际电联电信发展部门（ITU-D）网络安全项目 1
历史和背景 3
范围 3
概念框架 4
计算方法 4
附件 A 支柱和指标定义 6
法律措施 6
1.1. 网络犯罪法 6
1.2. 网络安全条例 6
技术措施 6
1.1. 国家/政府计算机事件响应团队 6
1.2. 行业 CERT/CIRT/CSRIT 6
1.3. 国家网络安全标准实施框架 6
组织措施 7
1.1. 国家网络安全战略/政策 7
1.2. 负责机构 7
1.3. 网络安全衡量指标 7
1.4. 保护上网儿童（COP）战略和举措 7
能力发展措施 7
1.1. 公众网络安全认识的宣传 7
1.2. 培训网络安全专业人员 7
1.3. 网络安全教育项目作为国家学术课程的一部分 7
1.4. 网络安全研发（R&D）项目 8
1.5. 国家网络安全产业 8
1.6. 政府激励机制 8
合作措施 8
1.1. 网络安全双边协议 8
1.2. 网络安全多边协议 8
1.3. 网络安全法律互助协议 8
1.4. 公私合作伙伴关系 8
1.5. 跨机构合作伙伴关系 8

历史和背景

全球网络安全指数（GCI）于 2015 年首次发布，通过确定网络安全的优势和增长领域以及突出良好做法，帮助各国加强对网络安全的承诺。通过收集的数据，GCI 强调成员国实施适合本国环境的网络安全承诺，推广良好做法，并树立全球网络安全文化。

国际电联全权代表大会第 130 号决议（2018 年，迪拜，修订版）规定了 GCI 的范围和框架，涉及加强国际电联在树立使用信息通信技术的信心和提高安全性方面的作用。具体而言，请成员国“支持包括全球网络安全指数（GCI）在内的国际电联网络安全举措，以促进制定政府战略，分享跨行业跨部门信息”。最终目标是树立全球网络安全文化并将网络安全纳入信息通信技术的核心。

全球网络安全指数之前的版本遵循国际电联电信发展部门（ITU-D）第 45 号决议（2022 年，基加利，修订版）的建议，该决议明确定义了通过全球网络安全指数（GCI）所做的工作，并建议电信发展局（BDT）“考虑 GCI 的结果，以指导其网络安全相关举措，特别是考虑到通过 GCI 流程确定的差距”。

之前的版本包括：

版本名称	GCIv1	GCIv2	GCIv3	2020 年 GCI（GCIv4）
版本号	1	2	3	4
参与国家	105 个国家	136 个国家	155 个国家	169 个国家
收集的数据年份	2013-14 年	2016 年	2017-2018 年	2020 年
发布年份	2015 年	2017 年	2019 年	2021 年
说明	与 ABI Research 合作			

在版本之间，含各指标、子指标和微指标的 GCI 调查问卷在与 ITU-D 研究组课题“保障信息和通信网络的安全：国际电联成员国培育网络安全文化的最佳做法”磋商后进行更新。

由于成员国对 GCI 的持续关注，国际电联正在根据第 45 号决议（2022 年，基加利，修订版）的建议与 GCI 专家组磋商，编撰第五版（GCIv5）。

范围

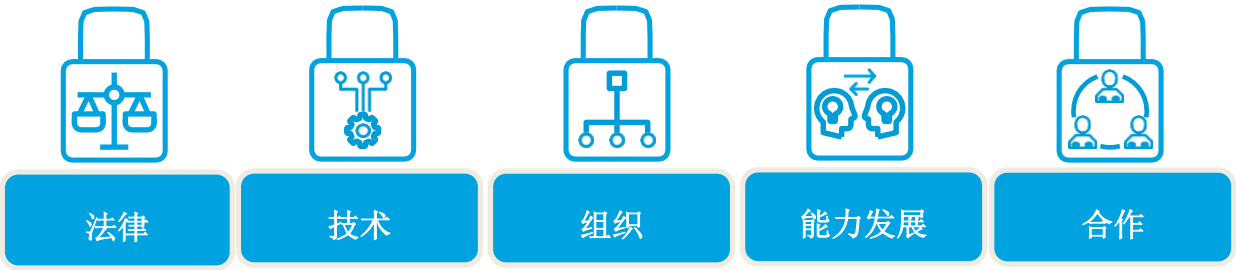
全球网络安全指数（GCI）是基于《全球网络安全议程》（GCA）的五个支柱，将各种网络安全指标整合为措施的综合指数。这些支柱构成了 GCI 的五个支柱。GCI 的主要目标是衡量：

- 各国网络安全承诺的类型、水平和随时间变化的发展情况；
- 全球视角下的网络安全承诺进展；
- 区域性视角下的网络安全承诺进展；
- 网络安全承诺鸿沟：各国在参与网络安全举措程度上的差异。

全球网络安全指数旨在帮助各国确定网络安全领域中需改进的方面，从而帮助提高世界各地网络安全的整体水平。GCI 还收集良好做法，各国可以借鉴，以改进各自的网络安全做法并采用更统一的方式。

概念框架

全球网络安全指数重点围绕以下五个支柱，作为各国网络安全承诺的优先重点领域：



法律措施： 法律、规定和政策等立法工具定义了网络安全相关关键问题（如禁止特定犯罪行为或最低监管要求）的权利、责任和保护。

技术措施： 如果没有足够的技术措施和能力用来发现和应对事件，成员国及其各自的实体仍然易受网络风险，可能削弱数字技术的益处。因此，成员国需要能够制定战略，为软件应用和系统建立可接受的最低安全标准和认证方案。可以根据成员国认可或创建的处理网络安全的技术机构和框架衡量技术措施。

组织措施： 组织措施对于适当执行国家举措很有必要。成员国需要制定广泛的战略目标，附实施、交付和衡量的全面计划。需要建立国家机构等结构，以便将网络安全战略付诸实施，并评估计划的成败。组织结构可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。

能力发展措施： 能力发展贯穿法律、技术和组织措施。了解网络安全技术、风险和影响有助于制定更好的立法、更好的政策、更好的战略以及更好地组织角色和责任。能力发展包括发展基本人口、工作涉及网络安全的专业人员和该领域专家的知识以及技能。

合作措施： 网络安全工作建立在所有受影响的部门和学科之上时会更加成功，并且需要采用统筹兼顾的利益攸关多方方式处理。合作加强对话和协调，帮助创造更加全面的网络安全应用领域。合作可包括联合举措、信息共享、培训和其他活动等，将专业人员、官员和其他寻求改善网络安全的主体联系起来。

计算方法

第五版 GCI 问卷调查分为五个支柱：法律、技术、组织、能力发展和合作措施，共包括 20 项指标，64 个子指标和 28 个微指标，以 83 个问题为基础。这些问题旨在平衡网络安全承诺中有意义的细化，同时保持高层视角。指标可参见 GCI 问卷调查（附件 A）。

指标的选择根据：

- 与《全球网络安全议程》支柱的相关性；
- 与全球网络安全指数范围和概念框架的相关性；
- 成员国准确回答问题的能力；
- 通过二级数据交叉验证的可能性。

这一版本使用三元（是、部分、否）答案来消除基于意见的评价和对特定答复类型的任何可能偏差。此外，简单的三元概念可实现更快、更复杂的评估，因为不要求冗长的答案，这会加快并简化提供答案和进一步评估。答卷人应仅确认是否存在预先确定的特定网络安全解决方案。

为确保准确性，将要求各国通过上传支持文件和 URL 的功能支持各自的回答。将为每个支柱增加评论部分，使各国能够提供良好做法，讲述具有影响力的网络安全演进故事。

对于第五版和所有未来版本，GCI 将根据 2022 年 6 月在卢旺达基加利召开的 WTDC（世界电信发展大会）第 45 号决议，以承诺级别重新调整结构，其中成员国建议 GCI 采用基于层级的国家分组方法而非排名，以便对各国优势和改进领域提供更有意义的评估。因此，方法专家组会议将负责确定合适的层级框架。

GCI总体流程

1 根据成员国和GCI专家组的反馈，修订GCI问卷调查。问卷调查提交至第2研究组会议供进一步讨论。

2 根据ITU-D第45号决议（2022年，基加利，修订版），“GCI专家组”将继续就方法、结构、问题和权重的相关事项向全球网络安全指数提供建议。

3 组建信函通信组作为GCI专家组的工作组，由专家和有意愿的成员国代表组成，提供对问卷调查的建议和反馈。

4 在BDT管理层批准问卷调查或将其部分或全部提交供信函通信组进一步反馈之前，BDT秘书处根据与信函通信组的磋商情况做出适当修订。

5 发出获得批准的调查问卷，翻译为联合国所有六（6）种正式语文。

6 召开另外两场GCI专家组工作组会议，就层级和权重分配进行磋商。

7 BDT主任通过信函邀请国际电联所有成员国和巴勒斯坦国参与GCI调查。这些信函旨在通报GCI，并请他们指定联系人，负责收集所有相关的国家数据并完成GCI问卷调查。

8 正式请指定联系人通过在线门户答复问卷调查。

9 BDT秘书处对答复问卷调查的国家开展二级数据收集，其中包括：

- 识别任何缺失的答复、支持文件、链接等。
- 联系人在必要时提高答复的准确性。
- 更正后的问卷调查草案发送给每位联系人最终批准。
- 经过确认的问卷调查用于分析、评分和排名。

10 BDT秘书处对未答复问卷调查的国家开展初级数据收集，其中包括：

- 国际电联使用可公开获取的数据和在线研究起草对问卷调查的初步答复。
- 调查问卷草案发送给联系人审查。
- 联系人提高准确性并返回问卷调查草案。
- 更正后的问卷调查草案发送给每位联系人最终批准。
- 经过确认的问卷调查用于分析、评分和排名。

11 在考虑GCI专家组提出的关于层级和权重的建议情况下，编写一份含主要趋势和最佳做法总结的报告。

注：如果某一国家未提供 GCI 问卷调查联系人，国际电联将与《国际电联全球通信录》中的机构联系人建立联系。

附件 A
支柱和指标定义

法律措施

立法是为各实体提供统一框架的关键措施，使其符合共同的法律法和监管基础，无论是禁止特定犯罪行为还是最低监管要求。

法律环境可以根据处理网络安全和网络犯罪的法律机构和有效框架的存在予以衡量。它由以下绩效指标组成：

1.1. 网络犯罪法

实体法是指所有类型的公法和私法，包括所有实质上创造、定义和规范权利的合同法、不动产法、侵权法、遗嘱法和刑法。

1.2. 网络安全条例

条例是管理行为或做法的规则或原则；尤其是此类指令由权力机构[1]确立和维护。条例以规则为基础，旨在执行特定的立法。网络安全条例指针对数据保护、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、保护儿童上网、数字签名和电子交易、以及互联网服务提供商义务的法律。

技术措施

如果没有足够的技术措施和能力用来发现和应对事件，成员国及其各自的实体仍然容易受到网络风险的影响。这种风险可能会损害采用数字技术带来的好处。因此，成员国需要有能力制定战略，为软件应用和系统建立公认的最低安全标准和认证方案。可以根据成员国认可或创建的处理网络安全的技术机构和框架衡量技术措施。该分组由以下绩效指标组成：

1.1. 国家/政府计算机事件响应团队

CIRT（计算机事件响应团队）、CERT（计算机应急响应团队）或CSIRT（计算机安全事件响应团队）是具体的组织实体，负责协调和支持对国家层面计算机安全事件或事故的响应。它们肩负国家责任，提供识别、防御、响应和管理网络威胁的能力，并加强国家的网络空间安全。这种能力需要与收集情报相结合，而非依靠来自 CIRT 或其他来源的安全事件二级报告。

1.2. 行业 CERT/CIRT/CSRIT

行业 CIRT/CSIRT/CERT 是指对影响具体行业的电脑安全或网络安全的事件做出响应的实体。医疗、公用事业、应急服务、能源、学术界和金融行业等重要行业一般都会成立行业 CERT。

1.3. 国家网络安全标准实施框架

通过一个（或多个）国家级的框架，用于实施国际公认的针对公共部门（政府机构）和关键基础设施（包括私营部门运营的）的网络安全标准至关重要。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。

---

[1] https://www.oed.com/view/Entry/161427?redirectedFrom=regulation

组织措施

组织和程序措施对于适当执行任何类型的国家举措都是必要的。成员国需要制定一个广泛的战略目标，并在实施、交付和衡量方面制定一个全面的计划。需要建立国家机构等结构，以便将战略付诸实施，并评估计划的成败。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。该分组由以下绩效指标组成：

1.1. 国家网络安全战略/政策

制定政策以促进网络安全是国家的首要任务之一。国家网络安全战略应定义维护国家关键信息基础设施的弹性和可靠性，包括公民的安全和保障；保护公民、组织和成员国的物质和知识资产；对网络攻击做出反应，防止对关键基础设施的网络攻击；尽量减少网络攻击造成的破坏和恢复时间。

1.2. 负责机构

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。此类机构也可只负责国家 CIRT。

1.3. 网络安全衡量指标

有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、网络安全审计和其他工具和活动，通过评级或评估结果提升未来的性能。例如，基于 ISO/IEC27004 的指标用于衡量信息安全管理。

1.4. 保护上网儿童（COP）战略和举措

国家保护上网儿童战略应制定行动计划，促进全球儿童的安全在线环境。有必要出台制定规则和目标的一套政策，明确在现实世界中任何针对儿童的犯罪行为原则上也可在互联网或其他任何电子网络上实施。

能力发展措施

能力发展是前三项措施（法律、技术和组织）的内在要求。了解技术、风险和影响有助于制定更好的法律、更好的政策和战略，以及更好地组织各种角色和责任。这一领域的研究通常是从技术角度进行的；然而，许多社会经济和政治影响适用于这一领域。

促进网络安全的能力发展框架应包括提高认识活动和资源提供。该分组由以下绩效指标组成：

1.1. 公众网络安全认识的宣传

提高公众认识的活动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。

1.2. 培训网络安全专业人员

有针对特定行业的专业培训计划，以提高公众的认识（即网络安全的国家宣传日、周或月），促进针对不同职业（技术、社会科学等）劳动力的网络安全教育，以及推动公共或私营部门的专业人士获得证书。

该指标还包括是否有政府批准（或认可）的使用国际公认的网络安全标准对专业人员进行认证和考核的框架（或多个框架）。这些认证、考核和标准包括但不限于以下举例：云安全知识（云安全联盟）、CISSP、SSCP、CSSLP CBK、网络安全取证分析师（ISC²）等等。

1.3. 网络安全教育项目作为国家学术课程的一部分

在学校、大专、大学或其他教学机构建立国家教育课程和项目并进行推广，对年轻一代进行网络安全相关的技能和职业培训。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。

1.4. 网络安全研发（R&D）项目

该指标衡量的是私有、公共、学术、非政府或国际机构是否有对国家网络安全研发计划的投资。它还衡量了是否有经国家认可的监督该计划的制度化的机构。

1.5. 国家网络安全产业

支持网络安全开发的有利经济、政治和社会环境会激励网络安全相关私营企业的增长。提升公众意识的活动、人力资源开发、能力发展和政府激励措施将推动网络安全产品和服务市场的发展。本土成长的网络安全产业是这种有利环境的证明，将推动网络安全创业公司和相关网络保险市场的发展。

1.6. 政府激励机制

该指标考察政府是否有任何激励措施，用于鼓励网络安全领域的能力发展，无论是通过税费减免、拨款、资助、贷款、提供设施，还是通过其他的经济或财务激励方式，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。

合作措施

网络安全需要所有部门和领域的投入，因此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，从而创造了一个更加全面的网络安全应用领域。不同领域之间以及私营部门运营商内部的信息共享最困难。国际层面的情况更加如此。该分组由以下绩效指标组成：

1.1. 网络安全双边协议

双边协议（一对一协议）指官方认可的国家的或具体部门的所有合作机制，由政府与他国政府或区域实体进行的跨境网络安全信息或资产的分享（例如合作或交换信息、专长、技术以及其他资源）。

1.2. 网络安全多边协议

多边协议（一对多协议）指官方认可的国家的或具体部门的所有合作项目，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分享（例如合作或交换信息、专长、技术以及其他资源）。

1.3. 网络安全法律互助协议

其中也可包括批准载有法律互助和网络安全相关条款的国际协议。

1.4. 公私合作伙伴关系

公私合作伙伴关系（PPP）指在公共和私营部门之间开展的合作项目。可采用私营主体与政府实体之间提供公共资产或服务的长期合同形式，其中私人一方承担重大风险和管理责任，薪酬与绩效挂钩[2]。这项绩效指标衡量的是官方正式认可的国家的或具体部门的 PPP 项目的数量，无论国内还是国际公共部门与私营部门之间分享网络安全信息和资产（人员、程序、工具）（即通过正式的伙伴关系进行合作或交换信息、专长、技术和/或资源）。

1.5. 跨机构合作伙伴关系

这项绩效指标指本成员国内不同政府机构之间的所有正式合作伙伴关系（不包括国际伙伴关系），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合作伙伴关系。

---

[2] https://ppp.worldbank.org/public-private-partnership/overview/what-are-public-private-partnerships