附件 1

职责范围

国际电联/电信发展局网络安全项目

全球网络安全指数（GCI）权重专家组

职责范围

2020 年 8 月

全球网络安全指数（GCI）

全球网络安全指数(GCI)于 2015 年首次发布，帮助各国确定网络安全领域需要改进的领域，并激励它们采取行动提高排名，从而提高全球网络安全的整体水平。通过收集的数据，GCI 强调成员国可以实施适合本国环境的做法，推广良好实践，并培育全球网络安全文化。

国际电联全权代表第 130 号决议（2018 年，迪拜，修订版）规定了 GCI 的范围和框架。该决议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。产生指标、子指标和微指标的 GCI 调查问卷是第 2 研究组第 3 号课题（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）经磋商后制定和批准的。

GCI 权重专家组

专家组的目标是确定 GCI 指标、子指标和微指标的权重，并为未来版本提出对 GCI 问卷的修改建议。

GCI 专家组成员的任命旨在为在 GCI 模式内为点数分配提供全面和公正的建议。专家组关于指标和子指标权重的建议应反映特定指标对成员国总体网络安全承诺的重要性。专家组的具体活动包括：

- 如本文件附件 B 所示，为主要指数和子指数的计算提供输入；
- 为 GCI 未来可能的版本提供输入。

在特殊情况下，经大多数人同意，专家组可以为下一版 GCI 推荐审议问题。

国际电联将担任专家组的秘书处。除了参加 GCI 会议前几轮工作的专家之外，专家组对国际电联成员国和部门成员开放。

专家组的组成应反映区域多样性、性别多样性、专业技能多样性以及包括政府、私营部门和学术界在内的不同利益攸关方之间的平衡。

加权程序

总体评估流程遵循以下步骤：

1) 国际电联将向每个专家组成员提供所有相关材料，特别是：
   a) 包含 GCI 问题的加权电子表格、
   b) 职责范围，包括操作指南和指标说明（本文件）；
2) **2020 年 10 月 15 日**将举行一次 GCI 专家组会议，讨论该程序，并回答问题。
3) 首次会议后，专家组成员将独立填写权重电子表格，并在 **2020 年 10 月 31 日**前向 gci@itu.int 提交他们对每个指标、子指标和微指标的权重建议。
4) 一旦专家组成员单独提交了所有建议，加权建议将被平均并汇编成一个单一的加权电子表格。
5) 平均权重建议将与专家组成员分享。

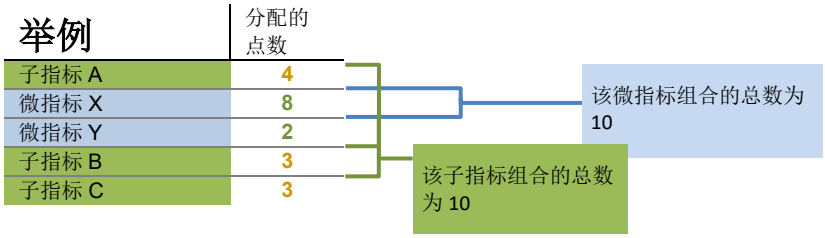
附件 A

如何分配权重

您应只审议您所述专长的支柱的权重。分配给您并未表明专长的支柱的权重将不予考虑。

GCI 建立在嵌套的分层模型上。该模型的每个“分支”在这里将被称为一个组合，例如一个指标组合、一个子指标组合和一个微指标组合。

在每个组合中，您可以分配 10 个点。您应基于自己的专长，给更重要的指标/子指标/微指标分配更多的分数。



如何使用权重电子表格

这些说明针对电子表格 *GCI-Questionnaire-weightage-calculation.xlsx*。

该文件设计用于微软电子表格。某些功能可能在其他程序中不起作用。

开始

1) 输入您的姓名。
2) 在您评估权重的支柱上划勾。这些支柱应与您所示专长领域相符。
3) 为寻找您提供输入的支柱，可点击每个支柱的名称或图标。

输入权重

4) 通过在单元格中键入数字或使用滚动按钮增加或减少数字更改指标、子指标或微指标的权重。

   a) 您在一个组合有 10 个点数。如果您分配过多或过少，组合的所有单元格都会变成红色，如下所示：

   b) 上下滚动箭头将改变整数的数量。

   c) 若要输入分数，请以=开头。例如，= 1/3 用于输入⅓。

   d) 如果您不想分配所有的 10 分，或者想超额分配，请在评论中注明。当对专家的回复进行算术平均时，您的权重将在 10 中得到重新平衡。

5) 您可以在“备注”栏中留下您对指标、子指标或微指标权重的任何意见。

6) 您可以点击 GCIv4 定义链接，以更好地理解任何指标的含义。

7) “GCI 总权重”部分根据您的给分显示该指标在最终 GCI 中的权重。您不能编辑或更改这些单元格。

收尾

1) 完成后，点击“另存为”（有关如何执行此操作的信息，请参考微软支持说明），在末尾添加您的姓名。

示例：*GCI-Questionnaire-weightage-calculations-**NAME**.xlsx*

2) 将您的电子表格附在电子邮件中，并在指定日期前通过电子邮件发送给 gci@itu.int。

附件 B

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：

- **网络犯罪实体法**

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。

- **网络安全法规**

监管基于规则，旨在执行一条具体的法律。

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：

- **国家/政府事件响应小组**

计算机事件响应团队，即 CIRT/CSIRT/CERT，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。

- **行业 CIRT/CSIRT/CERT**

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、公共设施、科研界、应急服务和金融行业等重要行业一般都会成立行业 CERT。

- **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。

- **保护上网儿童**

这一指标衡量是否存在一个专门负责保护上网儿童的国家机构，是否有一条报告有关上网儿童问题的热线，以及是否有任何帮助保护上网儿童的其他技术机制和能力。

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：

- **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。

- **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。此类机构也可直接负责国家的 CIRT。

- **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。

能力建设措施

能力建设是前三项措施(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建设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：

- **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。

- **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。

- **国家教育项目或学术课程**

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。

- **网络安全研发项目**

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。

- **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与网络安全有关的私营部门的增长。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。

- **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建设，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：

- **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）。

- **参与国际机制（论坛）**

这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》和其他。

- **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）。

- **公私合作伙伴关系**

公私合作伙伴关系（PPP）指的是在公共和私营部门之间开展的合作项目。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）。

- **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。