|  |  |
| --- | --- |
| **理事会2021年会议 2021年6月8-18日，理事磋商会虚拟会议** |  |
|  |  |
|  |  |
| **议项：PL 1.4** | **文件 C21/71-C** |
| **2021年4月22日** |
| **原文：英文** |

|  |
| --- |
| 秘书长的报告 |
| 《全球网络安全议程》使用指南 |

|  |
| --- |
| 概要  理事会2019年会议责成秘书长向下届理事会会议同时提交：(1) 一份说明国际电联目前如何利用[《全球网络安全议程》](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx)（GCA）框架的报告以及(2) 在成员国的参与下，为国际电联使用GCA制定相应的导则，供理事会审议和批准（[C19/117](https://www.itu.int/md/S19-CL-C-0117/)、[C19/58](https://www.itu.int/md/S19-CL-C-0058/)）。  按照这些指示，已在首席法官（已退休）Stein Schjolberg先生（高级专家组（HLEG）前主席）、Solange Ghernaouti教授和Noboru Nakatani先生的支持、成员国的参与下，制定了导则草案，供理事会审议和批准。必须注意的是，这项工作并非意在、也不解决与修订GCA相关的事项。  根据通函（[CL-20/55](https://www.itu.int/md/S20-SG-CIR-0055/en)）中规定的导则草案制定流程，2020年4月23日和2021年3月1日与信息社会世界峰会（WSIS）所有利益攸关方举行了公开磋商，以便其就导则草案提供意见。该文件的前一版本最初是为提交理事会2020年会议拟定的[C20/65](https://www.itu.int/md/S20-CL-C-0065/en)号文件，但该文件未得到审议。  需采取的行动  本文件将提交理事会，供其酌情**审议**和**批准**。  \_\_\_\_\_\_\_\_\_\_\_\_\_\_  参考文件  [全权代表大会第130号决议（2018年，迪拜，修订版）](https://www.itu.int/en/council/Documents/basic-texts/RES-130-E.pdf)  [全球网络安全议程（GCA）](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx)[、理事会C21/36](https://www.itu.int/md/S21-CL-C-0036/en)号文件 |

**目录**

**页码**

[**第1节 引言 4**](#_Toc70947916)

[背景情况 4](#_Toc70947917)

[环境 5](#_Toc70947918)

[GCA作为全球行动框架的持续相关性和适用性 8](#_Toc70947919)

[**第2节 支柱1：法律措施 8**](#_Toc70947920)

[引言 8](#_Toc70947921)

[2008年以来法律格局的演变 8](#_Toc70947922)

[利用支柱1 – 法律措施的导则 10](#_Toc70947923)

[**第3节 支柱2：技术和程序措施 11**](#_Toc70947924)

[引言 11](#_Toc70947925)

[自2008年以来技术和程序措施领域的演变 12](#_Toc70947926)

[利用支柱2 – 技术和程序措施的导则 13](#_Toc70947927)

[**第4节 支柱3：组织结构 14**](#_Toc70947928)

[引言 14](#_Toc70947929)

[2008年以来组织结构格局的演变 14](#_Toc70947930)

[利用支柱3 – 组织结构的导则 15](#_Toc70947931)

[**第5节 支柱4：能力建设 16**](#_Toc70947932)

[引言 16](#_Toc70947933)

[2008年以来能力建设格局的演变 16](#_Toc70947934)

[利用支柱4 – 能力建设的导则 17](#_Toc70947935)

[**第6节 支柱5：国际合作 18**](#_Toc70947936)

[引言 18](#_Toc70947937)

[2008年以来国际合作格局的演变 18](#_Toc70947938)

[利用支柱5 – 国际合作的导则 20](#_Toc70947939)

[**第7节 GCA框架的一般性导则 21**](#_Toc70947940)

第1节 引言

**1.1** 在迪拜举行的国际电联2018年全权代表大会通过了[第130号决议](https://www.itu.int/en/action/cybersecurity/PublishingImages/Lists/resolutions/AllItems/Res%20130.pdf) – 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。其中该决议做出决议，利用国际电联《全球网络安全议程》（GCA）框架，进一步指导国际电联在树立使用信息通信技术（ICT）的信心并提高安全性方面的工作。

**1.2** 在通过第130号决议之前举行的全体会议讨论中，国际电联秘书长满意地指出，在讨论决议草案的过程中，GCA的价值得到了广泛认可。他呼吁全体会议接受保留“做出决议”第12.1段，这将方便国际电联利用GCA引导其开展的有关树立使用ICT的信心并提高安全性的工作。在此方面，他将寻求理事会以及负责处理GCA工作的高级别专家组前主席Stein Schjolberg大法官的建议和意见。[[1]](#footnote-1)

**1.3** [GCA](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx)高级别专家组前主席向国际电联理事会2019年会议提交了一份报告，建议为更好地利用《全球网络安全议程》详细制定适当的导则。[[2]](#footnote-2)理事会责成秘书长向下届理事会会议同时提交：(1) 一份说明国际电联目前如何利用GCA框架的报告以及(2) 在成员国的参与下，为国际电联使用GCA制定适当的导则，供理事会审议和批准。[[3]](#footnote-3)

**1.4** 按照这些指示，在首席法官（已退休）Stein Schjolberg先生（HLEG前主席）的支持、成员国的参与下，已制定国际电联使用GCA的导则草案，供理事会审议和批准[[4]](#footnote-4)。秘书长还感谢Solange Ghernaouti教授（洛桑大学瑞士网络安全顾问和研究组）对GCA支柱2和支柱4相关章节的指导和贡献，并感谢Noboru Nakatani先生（国际刑警组织全球创新中心前执行主任）对GCA支柱3相关章节的指导和贡献。必须注意的是，这项工作并非意在、也不解决与修订GCA相关的事项。

**1.5** 根据第[CL-20/55](https://www.itu.int/md/S20-SG-CIR-0055/en)号通函规定的导则草案制定流程，2020年4月23日和2021年3月1日与WSIS所有利益攸关方举行了两次公开磋商，以便其就导则草案提供意见（公开磋商）。160多名参与者出席了会议，并就导则草案逐节提供了反馈。公开磋商前后收到的所有书面意见均已公布在GCA[网站](https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx)上。

背景情况

**1.6** 根据信息社会世界高峰会议（WSIS）和国际电联全权代表会议的指导，国际电联的一个根本作用是树立使用信息通信技术（ICT）的信心并提高其安全性。

**1.7** 在WSIS会议上（2005年），各国元首和世界领导人委托国际电联担任C5行动方面--树立使用信息通信技术（ICT）的信心并提高安全性[[5]](#footnote-5) — 的推进方。针对这一任务，国际电联于2007年出台了GCA，作为该领域国际合作的框架。

**1.8** GCA由五个支柱或工作领域组成：法律措施；技术和程序措施；组织结构；能力建设和国际合作。该议程旨在开展合作和提高效率，鼓励所有相关伙伴之间开展合作，并以现有举措为基础，避免工作重叠。

**1.9** 由此，GCA高级专家组（HLEG）于2007年10月成立，目的是协助国际电联秘书长为成员国制定促进网络安全的战略建议。首席法官Stein Schjolberg法官（已退休）担任该专家组主席。

**1.10** HLEG由独立的利益攸关多方全球专家组组成，其近百名专家成员来自世界各地。在2008年8月的主席报告（HLEG 2008年报告）中，专家组向国际电联秘书长提出了涉及所有战略支柱的意见和建议。[[6]](#footnote-6) HLEG主席在报告中强调：

网络攻击在收入损失、敏感数据丢失、设备损坏、拒绝服务攻击和网络中断等方面产生的关联成本很高。日益增长的网络威胁危及网络信息社会的未来发展和潜能。此外，网络空间无国界：网络攻击可以在几分钟内对不同国家造成不可估量的损害。网络威胁是一个全球性问题，需要拿出一个利益攸关各方参与的全球性解决方案。

**1.11** 2008年，围绕GCA五大支柱开展的工作是全球网络安全问题处理方式的一项重大创新。自2008年GCA报告提交以来，十多年已经过去。总体而言，全世界对信息通信技术是实现联合国可持续发展目标（SDG）的至关重要手段这一点已有共识，且人们认识到，要实现这一点，就必须人人和处处树立对使用信息通信技术的信任和信心。因此，树立使用信息通信技术（ICT）的信心并提高安全性的目标比以往任何时候都更是实现可持续发展目标的一项不可或缺的目标。

环境

**1.12** GCA五大支柱所提供的框架得到了国际电联成员的广泛赞赏，总体上经受住了时间的考验，并继续在WSIS成果文件的框架内，特别是在C5行动方面概述的原则框架内，为网络安全方面的国际合作提供着广泛的框架。2008年HLEG主席报告中的相关建议现今仍有现实意义[[7]](#footnote-7)，同时也应认识到报告中有几个具体方面可视为已经过时或被其他事件取代。

**1.13** 毫无疑问，自2008年以来，ICT的面貌已发生翻天覆地的变化，现今ICT支撑着社会的各个部门，以及大部分关键性基础设施。[[8]](#footnote-8)世界正在目睹新技术的迅速出现和采用，其示例包括：

• 随着物联网的广泛普及，成百上千亿个联网新设备也催生了大量新的潜在薄弱环节；

• 人工智能作为一种数据（尤其是大数据）利用工具不断发展，有助于人类能够做出更明智的决策，同时也有助于机器在没有人类干预的情况下自主做出所谓的智能决策，但这也带来了安全和信任以及捍卫人权方面的挑战；

• 5G等通信新技术和新标准允许以比现行可用速率高出几个数量级的速率进行通信；

• 量子计算提供的计算速度远远超出了当前的能力，从而带来了巨大的机遇，但也尤其使现有的密码算法面临着风险；

• 新的安全技术，如分布式账本技术（区块链即为其主流实施之一），为保护系统和相关数据提供了更好的手段。世界上越来越多的国家也正在更多地采用数字身份系统。

**1.14** 此外，自2008年以来，随着社交网络在全球范围内的广泛采用，全球ICT生态系统的发展方向受到显著影响。一些社交网络的用户数量超过了许多国家的人口总和—例如，截至2020年，脸书（Facebook）的每月活跃用户数量接近28亿[[9]](#footnote-9)。在连通世界各地的人们、模糊地理界限以及以前所未有的规模和速度提供便捷的信息和机会方面，社交媒体发挥了关键作用。它也带来了严重的信任问题—关于用户及其所生成数据的隐私和安全、社交网络上可用信息是否真实和可信、传播仇恨内容等。[[10]](#footnote-10)

**1.15** 此外，其他因素，如暗网的出现，继续引起全世界对网络空间犯罪活动的日益关注，特别是在获取恶意工具、服务和内容等方面。

**1.16** 鉴于这些发展，包括政府在内的所有利益攸关方越来越认识到需要采取从保护关键性基础设施到保护用户隐私的多种紧急行动来促进网络安全。作为可能对所有国家构成国家安全威胁的问题，网络安全已成为政府最高政治级别的议程，他们越来越多地投资于治理和行政措施，以推动采取政府总动员（whole-of-government）的应对措施，从而加强国家的网络复原力。

**1.17** 新冠肺炎病毒（COVID-19）大流行病进一步凸显了ICT对卫生和安全以及保持我们的经济和社会向前发展的重要性。从远程工作和电子商务再到远程医疗和远程学习，ICT服务和基础设施不断满足着人们的关键需求。COVID-19危机还凸显了应对社会高度依赖ICT所带来的快速演进和严峻的网络安全挑战的必要性。

**1.18** 在GCA的框架内，五大支柱中的每一支柱都在过去十年中以其特有的方式发生了演变。

**1.19** 截至2020年，超过125个国家签署和/或批准了不同的网络安全和网络犯罪公约、宣言、导则或协议，如[2001年《欧洲委员会网络犯罪公约》](http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185)（《布达佩斯公约》）、[《上海合作组织成员国政府关于确保国际信息安全领域合作的协议》](http://eng.sectsco.org/documents/)（2009年）和[《非洲联盟网络安全和个人数据保护公约》](https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection)（2014年）。

**1.20** 根据联合国大会（UNGA）决议，政府专家组（GGE）[[11]](#footnote-11)和不限成员名额工作组（OEWG）[[12]](#footnote-12)研究了与在国际安全背景下使用信息通信技术（ICT）有关的若干问题，除其他外，包括在网络空间促进负责任的国家行为、国际法对网络空间的适用性、能力建设以及在网络空间实施和进一步发展建立信任措施的必要性。

**1.21** 创新型ICT，如云计算、软件定义网络（SDN）、网络功能虚拟化（NFV）、5G、大数据、人工智能等，模糊了市场和地理界限，使得网络安全生态系统日益充满活力和复杂性。新技术和新的商业参与者可能导致人们面临新的脆弱性和威胁，特别是因为在设计阶段，私营部门对性能、市场份额和成本的关注往往高于对安全的投资。在处理此类技术时，有许多问题构成了重大挑战，如通过设计确保安全性（因为产品从设计阶段开始就一直是脆弱的），通过认证方案、协议和标准在产品和服务的整个寿命周期中增强对产品和服务的信心，合法使用用户生成的数据，同时保护用户隐私，从而找到减少和控制漏洞数量的方法。标准化和定期认证/认可程序有助于通过设计培育安全文化，进而建立对这些技术的信任和信心，从而有助于减少脆弱性的数量和影响。然而，安全标准化，即制定安全的技术和程序措施，仍然是一项不断变化的具体目标，因为这酌情需要技术先进的行业、精通技术的监管机构和有能力的执法机构协同工作。

**1.22** 一些国家、区域和国际组织已经成立，以解决网络安全问题。国家和区域层面举措的一些示例包括AFRIPOL、AMERIPOL、GCCPOL、大洋洲网络安全中心（OCSC）、澳大利亚网络安全中心（ACSC）、欧洲网络犯罪中心（EC3）、俄罗斯国家计算机事件协调中心和印度网络犯罪协调中心（I4C）。国际实体方面，最近的努力包括全球网络安全能力中心（GCSCC）、全球网络专业知识论坛）GFCE）、国际刑警组织全球创新中心（IGCI）、世界经济论坛（WEF）全球网络安全中心、美洲国家组织美洲反恐怖主义委员会（CICTE）、西非国家经济共同体（ECOWAS）、南部非洲发展共同体（SADC）等。

**1.23** 此外，缺乏网络安全的技术、法律、组织和人员层面的技能和专门知识也可对重要的国家基础设施产生不利影响。许多ICT最终用户目前可能不完全了解网络安全问题，或不具备必要的技能或工具来最好地保护其数据、隐私和资产，包括妇女和儿童在内的更脆弱的用户尤其面临风险。建立有助于实现有效的网络安全文化的技能、能力和措施仍然是一项至关重要的挑战。

GCA作为全球行动框架的持续相关性和适用性

**1.24** 考虑到不断变化的ICT环境，包括国际电联在其职责范围内和作为WSIS C5行动方面的推进方所开展的活动，利用GCA开展的活动也一直在演变。

**1.25** GCA与国际电联为树立使用ICT的信心并提高安全性而开展的工作相得益彰。作为框架，该议程适用于全球、区域和国家各个层面，议程应继续如此实施。国际电联在其职责范围内，在GCA框架的的指引下，一直努力汇聚不同的利益攸关方，就一些举措开展合作，包括协助成员国制定其国家网络安全战略，通过制定和执行国际安全标准加强其基础设施，建立其计算机事件响应小组，部署保护上网儿童的举措以及建设必要的人员能力和技能。在GCA的框架内，已启动了保护上网儿童等各种利益攸关多方举措。[[13]](#footnote-13)

**1.26** 为了加强利用GCA的努力，在随后的章节中提供进一步的指导。在制定这一指南时，考虑了HLEG 2008年报告中的建议、此后国际电联的活动、2008年以来该领域的发展情况以及[从成员国和其他利益攸关方收到的输入意见](https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx)（根据第[CL-20/18](https://www.itu.int/md/S20-SG-CIR-0018/en)和[CL-20/55](https://www.itu.int/md/S20-SG-CIR-0055/en)号通函）。

**1.27** 在承认五大支柱相互依存的同时，每一节讨论一个具体的GCA支柱，并提出具体的使用导则。第2节着重于法律措施。第3节涵盖技术和程序措施。第4节涉及能力建设。第5节阐述组织结构，第6节涉及国际合作。第7节提出一些关于使用GCA框架的一般性跨领域导则。

第2节 支柱1：法律措施

引言

**2.1** 网络安全的法律层面是促进ICT使用信任的关键因素之一。

**2.2** HLEG 2008年报告指出，GCA的支柱1旨在寻求促进合作，并就立法应对措施向国际电联秘书长提供战略性意见和建议，以解决网络安全方面不断变化的法律问题，其中包括如何通过立法以国际兼容方式处理通过ICT实施的犯罪活动。讨论指出，国际电联可详细制定作为导则的、各国制定网络犯罪示范立法的战略。该报告还建议参考相关的区域性举措。

2008年以来法律格局的演变

**2.3** 2008年后，区域组织已制定诸多关于网络安全的公约、宣言、协议和导则。如上所述，许多国家签署和/或批准了不同的网络安全和网络犯罪公约、宣言、导则或协议，这导致了国际层面的各自为政和花样翻新。**2.4** 如上文第1节所述，在联合国系统内，联合国大会还建立了两个进程以讨论ICT使用的安全问题 – 政府专家组（GGE）和不限成员名额工作组（OEWG）。自2004年以来，联合国大会设立了六个政府专家组，研究在国际安全背景下使用ICT构成的威胁以及如何应对这些威胁，最近的一个专家组是2019/2021年[在国际安全背景下促进网络空间负责任的国家行为政府专家组](https://www.un.org/disarmament/group-of-governmental-experts/)（[第73/266号决议](https://dig.watch/instruments/resolution-ares73266-advancing-responsible-state-behaviour-cyberspace-context-international)）。在其调查结果中，2014/2015年政府专家组一致认为，国际法规定的现有义务适用于国家使用ICT，各国必须履行其尊重和保护人权和基本自由的义务。2018年，成立了[从国际安全角度看信息和电信领域发展OEWG](https://www.un.org/disarmament/open-ended-working-group/)（第73/27号决议），由“所有感兴趣的国家”参与，讨论信息安全领域的现有和潜在威胁以及应对这些威胁的可能合作措施；进一步发展国家负责任行为的规则、规范和原则；国际法如何适用于各国对ICT的使用；建立信任措施；能力建设；以及在联合国主持下建立广泛参与的定期机构对话的可能性。2019-2021年OEWG会议于2021年3月以协商一致方式通过了其[《最后实质性报告》](https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf)，其中重申国际法，特别是《联合国宪章》适用于网络空间，并进一步建议各国支持国际法、国家立法和政策领域的能力建设工作，因为这将使所有国家能够促进就国际法如何适用于各国使用ICT达成共识。随着第75/240号决议设立了2021-2025年信息通信技术安全和使用问题不限成员名额工作组，预计OEWG将继续开展工作。

**2.5** 联合国系统内也启动了若干举措和进程，以帮助确定和应对全球网络安全带来的法律挑战。例如，在这方面通过了一些联合国大会决议，如[联合国大会2019年12月27日关于打击为犯罪目的使用信息通信技术的决议（第74/247号决议）](https://undocs.org/pdf?symbol=en/A/RES/74/247)，该决议决定设立一个代表所有区域的不限成员名额的特设政府间专家委员会，以拟订一项关于打击为犯罪目的使用信息通信技术的全面国际公约。

2.6鉴于上述情况，各国在这些不同论坛上不断讨论它们之间以及与其他利益攸关方之间需要的进一步合作，以寻求在网络空间背景下理解、解释和维护国际法的全球共同点，特别是通过促进信息和最佳做法的更多交流。

法律措施与新技术

**2.7** 一些专家建议，网络空间中有犯罪意图的新技术和新行为方式应被纳入刑法。[[14]](#footnote-14) 许多国家已经通过或正在准备制定涵盖其中一些行为的新法律。重要的是，在这方面制定的任何适当的法律措施都要符合其人权义务。可能影响法律措施的近期和新兴技术及趋势的一些示例如下：

**a) 全球网络攻击**

针对重要通信和信息基础设施的全球网络攻击已成为国际和国家安全威胁。政府、国际组织和私人机构都是此类全球网络攻击的目标。因此，有必要制定强大的国家法律框架以应对这一挑战。

**b) 社交网络中的犯罪行为**

相关方面呼吁采取措施打击社交网络中的非法行为，如仇恨言论。解决这些问题的新举措已经出现 – 比如联合国与科技公司脸书、微软、推特和YouTube之间的[打击恐怖主义全球互联网论坛伙伴关系](https://www.gifct.org/about/)。

**c)** **物联网（IoT）**

智能技术正在改变全球人口的生活、互动和工作方式。[[15]](#footnote-15) 最近，世界各地发生了多起网络基础设施遭到被黑客入侵的连接设备僵尸网络攻击的事件，范围从网络摄像头到路由器。随着5G等新技术的出现，无处不在的互联设备已经成为现实，风险可能会增加。

**d)** **人工智能（AI）**

算法透明度，包括所采取行动的可追溯性，是为部分或全部自动化系统做出的决定建立问责制和责任的一个非常重要的因素，从而确保对ICT应用和服务的信任。专家指出，对于几种类型的人工智能技术，如深度学习，很难澄清如何达到结果。随着自动化决策过程在消费者和业务应用程序和服务中变得越来越普遍，对这些过程所提供的分析和决策的责任和义务的法律方面的要求将变得更加明确。[[16]](#footnote-16)

**e) 对上网儿童的性虐待和剥削**

[《联合国儿童权利公约》（CRC）](https://www.ohchr.org/en/professionalinterest/pages/crc.aspx)于1989年通过。《公约》第34条要求缔约国采取适当措施，保护儿童免遭一切形式的性剥削和虐待**。**2002年，[《儿童权利公约关于买卖儿童、儿童卖淫和儿童色情制品问题的任择议定书》](https://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx)生效。随着互联网和社交媒体的发展，网上儿童性虐待已经蔓延。专家们呼吁采取综合办法防止这种虐待。[[17]](#footnote-17) 这些措施包括防止开发和访问包含儿童性虐待相关内容的网站，包括拦截、过滤或其他类似技术。2021年3月，儿童权利委员会通过了[关于数字环境下儿童权利的第25号一般性意见（2021年）](https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en)，解释了缔约国应如何在数字环境下执行《儿童权利公约》，并就相关立法、政策和其他措施提供了指导。

2.8 程序法--一般原则

通过必要的程序法来确立起诉网络空间犯罪行为的权力和程序，被认为是全球预防、调查和起诉网络犯罪并确保网络安全的一项重要法律措施。然而，一些专家指出，这种权力和程序对于起诉通过计算机系统实施的其他刑事犯罪也可能是必要的，相关法规可适用于收集所有刑事犯罪的电子形式的证据。[[18]](#footnote-18) 所有程序法都应符合国际人权法规定的义务和标准。在这方面，注意到国家主权原则适用于网络空间，也有人要求和讨论探索可能有助于合法获取已实施端到端加密的通信内容的机制，同时确保公民的基本权利和安全得到保护。[[19]](#footnote-19)一些利益攸关方警告说，任何此类机制都将削弱互联网的安全，并将全球经济、许多人依赖的关键服务以及公民的生命置于更大的伤害风险之中。

**2.9** 鉴于上述各节，显然，各国应继续采取适当的法律措施，保护对维护重要的社会功能（如人民的健康、安全、安保、经济或社会福祉）至关重要的重要通信和信息基础设施（以及任何相关资产、系统或其一部分），并防止可能对这些重要基础设施造成重大影响或使其无法运行的任何中断或破坏。

利用支柱1 – 法律措施的导则

**2.10** 如前所述，GCA的五大支柱都是相互依存的，其中关于法律措施的支柱贯穿于各项支柱。

**2.11** 自GCA问世以来，国际电联的工作集中于那些符合其核心职责范围与专业特长的网络安全领域，主要是技术和发展领域，不包括那些与成员国在国防、国家安全、内容和网络犯罪方面采取法律或政策原则有关的领域，这类领域属于成员国的主权范畴。因此，关于支柱1下的活动，国际电联主要侧重于利用谅解备忘录（MOU）等机制，促进与其他相关国际组织和利益攸关方（如国际刑警组织和联合国毒品和犯罪问题办公室（UNODC））的合作行动，这些组织和利益攸关方可能在这一领域负有向各国提供援助的主要责任。这包括通过[国际电联网络犯罪立法资源和UNODC网络犯罪知识库](http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html)等资源，帮助成员国了解网络安全的法律方面问题。还开展工作，协助加勒比、撒哈拉以南非洲和太平洋岛屿的成员国统一ICT法规和立法，包括网络犯罪法律框架。

|  |
| --- |
| **2.12** 鉴于技术的迅速进步，各组织和国家采取的措施需要不断发展，以跟上变化的步伐。这给网络安全挑战带来了新的复杂性，因此需要从各种不同的角度进行仔细审查。在这方面，支柱1的拟议使用导则如下：  **a)** 国际电联应继续努力促进利益攸关多方就解决网络安全问题的相关挑战进行讨论和合作，特别是加强与合作伙伴和其他利益攸关方的关系，以便在这方面向成员国提供援助。  **b)** 国际电联应继续在其职责范围内与合作伙伴合作开发和维护网络犯罪立法资源等资源，以帮助成员国了解网络安全的法律方面问题，同时支持成员国之间交流经验和知识，以支持它们努力制定包括立法在内的这方面的框架。  **c)** 国际电联应与适当的伙伴协作，促进更好地理解新兴技术对现有法律措施构成的网络安全相关挑战和风险，并促进国家、区域和国际层面的案例研究和良好做法交流。  **d)** 所有利益攸关方还需要采取适当的法律措施实施有效方案，防止或禁止传播与儿童性虐待和剥削有关的网上材料，包括采取预防行动，侦查、瓦解和摧毁用于制作和/或传播与儿童性虐待和虐待有关的网上材料的网络、组织或结构，并建立机制，在查明和保护受害者的同时，侦查和起诉罪犯。在这方面，国际电联应继续加强保护上网儿童计划，将其作为一个与合作伙伴和利益攸关方合作的平台，促进交流各方面的知识、信息、活动和成果，包括能够促进和支持各国在这一关键问题上采取行动的法律措施。 |

第3节 支柱2：技术和程序措施

引言

**3.1** GCA在各种相关举措的制定和实施过程中起到了指导作用，帮助促进国际、区域和国家层面有关网络安全的讨论不断成熟。无论是在战略还是在行动层面，有必要通过连贯一致的方式满足对有效和高效的网络安全措施的需求，但这仍然是一项重大挑战。

**3.2** 现今，在网络外交和国际对话领域，GCA的支柱1、3、4和5所确定的层面似乎变得越来越重要，并常常超越支柱2。然而，技术问题往往是所有其他支柱的根源。通过技术和程序（如行政，运行和管理）措施管理网络风险仍然至关重要，尤其是在关键性基础设施方面。鉴于国际电联作为联合国专门机构和全球标准制定组织（SDO）所发挥的长期作用，因此完全有能力推进安全相关标准和技术措施领域的工作。

自2008年以来技术和程序措施领域的演变

**3.3** 技术（当前的和新兴技术）以及由此产生的数字做法在不断发展演变。这一充满活力的技术层面在某种程度上独立于GCA的其他支柱，并且在很大程度上是独立发展演进的，对其他四项支柱的需求和主题影响的考虑有限。

**3.4** 为了使所有基础设施、应用和服务正常运行，制定和实施标准是根本。此外，重要的是，在制定标准时，还必须考虑到相关的人权义务。

**3.5** 国际电联拥有多个利益攸关方成员，为制定国际电联成员国自愿采用的全球ICT标准提供了一个独特的全球平台。在国际电联内部，ITU-T 第17研究组是安全标准工作的牵头研究组，已发布了200多项侧重于安全的标准。该研究组目前正在多个新兴技术领域开展工作，包括金融技术安全、物联网安全（包括工业互联网安全）、智能交通系统安全、分布式账本技术、量子密钥分发、反垃圾邮件机器学习、5G安全、边缘计算、个人身份信息保护、多方计算以及网络防御中心的创建、运行和自动化导则等。在实施HLEG 2008年报告中关于“协作”的建议（例如，2.1、2.6、2.7、2.10、2.12、2.16）过程中，第17研究组收集并充实完善用于公众访问的ICT安全标准数据库[[20]](#footnote-20)，其中包括来自13个主要SDO的2600项现有和正在进行的ICT安全标准，包括3GPP、ATIS、ETSI、电气和电子工程师学会、IETF、国际标准化组织/国际电工委员会JTC 1、国际电联、OASIS、OneM2M等。

**3.6** 尽管ITU-T第17研究组仍是安全标准的主要研究组，但大多数（如果不是全部的话）其他研究组也在其各自的研究领域内处理与安全方面相关的问题，如物联网及其应用（包括智慧城市和社区）方面的第20研究组、下一代网络方面的第13研究组或多媒体编码、系统和应用等方面的第16研究组。关于新兴技术的各焦点组，如人工智能与卫生、机器学习和5G、数字分类账技术、网络量子信息技术等，也处理与安全相关的挑战。重要的是，各研究组之间需密切合作—第17研究组发挥协调/牵头作用--以便在ICT产品/服务开发周期的整个标准化过程中保持尽可能高的端到端安全性。

标准化倡议的激增和加强合作的必要性

**3.7** 国际网络安全标准化具有挑战性，因为技术范围广，不同部门出现了不同的参与者，对于可能缺乏实际网络安全能力和技术技能的发展中国家来说尤其困难。

**3.8** 在此方面，HLEG 2008年报告建议2.1现在比以往任何时候都更加正确：“关于加强与国际电联以外的现有网络安全工作合作的机会，国际电联应与现有的外部专业知识中心合作，以确定、促进和推动采用得到强化的安全程序和技术措施s”[[21]](#footnote-21)。

**3.9** 此外，如HLEG 2008年报告建议2.2所述，国际电联被确定为处理与技术和程序措施有关的国际标准化进程和标准的“全球高级培训中心”[[22]](#footnote-22)。为实现这一点，应该鼓励技术更先进的国家及其私营部门参与国际电联的活动，并协作制定技术和程序标准，包括与安全有关的标准。

**3.10** 在互惠的基础上，继续加强与其他SDO的协调与协作非常重要，这样才能确保端到端安全性、设计安全性、风险评估以及产品整个寿命周期的互操作性。

**3.11** HLEG 2008年报告强调了“解决软件产品中薄弱环节的主要措施，包括身份认证方案、协议和标准”的重要性[[23]](#footnote-23)。在这方面，国际电联应考虑到新技术和要求，继续调整其工作。对于这其中的每项技术/领域，都应该考虑以下要求：

• 在设计阶段，异构ICT生态系统中的每个元素和接口都需具有设计安全性/默认安全性；

• 需要适当衡量指标来确定实施阶段的安全水平；

• 需要定期评估和认证流程，以便在部署后的整个寿命周期中认证数据集/产品/系统/服务的安全水平。

利用支柱2 – 技术和程序措施的导则

|  |
| --- |
| **3.12** HLEG 2008年报告中与支柱2有关的建议仍然有效。鉴于上述情况，特为支柱2提出以下导则：  **a)** 国际电联研究组应侧重于新兴技术，以便研究和制定相关技术的使用安全导则，并为成员国及时自愿应用这些导则，以应对不断变化和升级的网络威胁提出建议。  **b)** ITU-T各研究组应就安全相关问题的研究建立密切合作机制--由第17研究组发挥协调/牵头作用--以便在ICT产品所有成分和接口的整个标准化过程中保持尽可能高的端到端安全性。  **c)** 应鼓励在国际电联与其他SDO互惠的基础上进行密切协调和协作，以确保在整个产品周期内保持不同应用和服务的端到端产品安全性。  **d)** 国际电联应继续分发全球ICT安全标准。鼓励其他标准化组织和行业团体向ITU-T提交其技术和程序措施标准，以作为ITU-T建议书通过。  **e)** 国际电联应继续努力成为“全球高级培训中心”，在其职责范围内就网络安全的技术和程序措施提出建议（如《2008年HLEG报告》所述），特别是通过激励其成员更多地参与国际电联的相关标准化活动和通过战略伙伴关系予以实现。  **f)** 国际电联应继续鼓励其成员启动/参与基于统一标准的、旨在实现国际网络安全认证方案的相互认证安排。 |

第4节 支柱3：组织结构

引言

**4.1** 国家、区域和国际协调层面的组织结构可以根据合作的目的是战略性的还是操作性的来分析。在战略结构中，组织更强调建立协作关系，而非在网络事件中开展联合行动。另一方面，在操作性结构中，组织形成紧密的信息共享系统来快速交流信息，对网络事件做出快速反应。当比较世界各地不同的组织结构时，这种区别会很有帮助。

**4.2** 在国家层面，需要有效的机制和组织结构对网络威胁和事件可靠地做好准备和应对。这种机构的缺乏和国家能力的缺乏为充分和有效应对网络攻击带来了挑战。国家“计算机事件响应团队”（CIRT）在完善国家层面的就绪水平和复原力方面发挥着举足轻重的作用。

2008年以来组织结构格局的演变

**4.3** 过去十年在支柱3方面取得了重大进展。已经成立了许多国家、区域和国际组织来解决网络安全问题。

**4.4** 国家和区域举措的示例包括：非洲警察组织（AFRIPOL）、美洲警察组织（AMERIPOL）、海湾国家警察组织（GCCPOL）、大洋洲网络安全中心（OCSC）、澳大利亚网络安全中心（ACSC）、欧洲网络犯罪中心（EC3）、印度网络犯罪协调中心（I4C）和网络犯罪报告门户、日本国家事件就绪和网络安全战略中心和网络犯罪控制中心（JC3）、马来西亚国家网络安全管理局（NACSA）、法国国家网络安全管理局（ANSSI）、立陶宛国家网络安全中心（NCSC）、瑞士国家网络安全中心， 英国国家网络安全中心（NCSC）、美国国际网络犯罪协调小组（IC4）、俄罗斯计算机事件国家协调中心、集体安全条约组织计算机事件响应咨询协调中心（CCC CSTO）、美洲国家组织美洲反恐怖主义委员会（CICTE）和网络安全计划、沙特阿拉伯国家网络安全管理局（NCA）以及卢旺达国家网络安全管理局。

**4.5** 尽管成员国对CIRT的投资不断增加，而且国家CIRT独立开展区域和国际外联活动，但仍有85个国家未成立国家CIRT – 鉴于网络威胁的全球性质，这种情况令人严重关切。[[24]](#footnote-24)

**4.6** 国际电联通过其发展局，正在与成员国、合作伙伴和区域/国际组织合作，建设国家和区域层面的能力，部署能力，并协助建立和加强CIRT。迄今为止，国际电联已进行了80多次CIRT就绪情况评估，以帮助各国评估其国家网络安全准备和事件应对能力。[[25]](#footnote-25)国际电联为成员国建立/加强22个CIRT项目提供了支持。[[26]](#footnote-26) 为对各国进行评估，国际电联与事件响应与安全团队论坛（FIRST）、全球网络安全能力中心等伙伴协作工作。

**4.7** 在国际组织方面已存在几项倡议，在此列举其中一些示例：

• [全球网络安全能力中心](https://www.oxfordmartin.ox.ac.uk/cyber-security/)（GCSCC）是研究高效和有效网络安全能力建设的国际中心，并与国际电联协作制定了[国家网络安全战略制定指南（NCS](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx)），该指南目前正用于提供关于国家网络安全战略（NCS）的动手练习，并为各国制定有效的国家网络安全战略框架的良好做法提供培训。

• [全球网络专业技能论坛](https://www.thegfce.com/)（GFCE）成立于2015年，旨在交流良好做法，并为各国、国际组织和私营部门提供网络能力建设方面的专业知识。GFCE和国际电联是[计算机安全应急响应小组（CSIRT）成熟举措](https://cybilportal.org/projects/csirt-maturity-initiative-3/)的共同发起方，并在[打击网络犯罪工具包](https://www.itu.int/en/ITU-D/Cybersecurity/Documents/worldbank-combating-cybercrime-toolkit.pdf)等网络安全活动方面开展了合作。

• [国际刑警组织全球创新中心](https://www.interpol.int/en/News-and-Events/News/2014/INTERPOL-Global-Complex-for-Innovation-opens-its-doors)（IGCI）于2015年在新加坡成立，为国家执法部门提供专门的业务支持和培训，以应对不断变化的犯罪情况。2018年，国际电联和国际刑警组织签署了一项合作协议，为国际刑警组织和国际电联建立一个正式框架，以便在各自职责和资源范围内互利合作，在使用ICT方面建立信任并加强安全性。

• 世界经济论坛（WEF）在2018年启动了新的[全球网络安全中心](https://www.weforum.org/centre-for-cybersecurity/)，旨在为政府、企业、专家和执法机构建立一个全球平台，就网络安全挑战开展协作。同年，国际电联和WEF同意合作促进旨在减轻网络威胁的网络安全项目和举措，并探讨进一步合作、以促进网络安全的机会。

利用支柱3 – 组织结构的导则

|  |
| --- |
| **4.8** 虽然认识到HLEG2008年报告中的建议很好地指导了国际电联在支柱3下的努力，并继续具有相关性，但以下拟议导则--特别是与国际电联电信发展局（BDT）的工作相关--可能有助于加强这方面的努力：  **a)** 国际电联应继续协助发展中国家建立CIRT和其他相关技术单位/组织。  **b)** 国际电联应优先考虑尚未建立适当网络安全组织结构的国家。  **c)** 国际电联应促进参与努力建立可持续国家组织结构的各种国家、区域或国际组织之间更加开放和包容的协作和协调，以确保有效提供支持和避免重复工作。  d**)** 国际电联应加大努力，衡量成员国的机构承诺，利用全球网络安全指数等工具，促进网络安全，将其作为数字化转型工作贯穿各领域的促进因素。  **e)** 尤其是对国家机构而言，国际电联应协助成员国制定战略，建立政府总动员协调框架，以改善国家网络安全工作的协调一致和跨领域实施。  **f)** 国际电联应继续通过网络演练等活动，促进区域和全球网络安全组织结构之间的更大协作。 |

第5节 支柱4：能力建设

引言

**5.1** 在所有利益攸关方之间发展和部署适当的技能、网络安全文化和良好做法是一个至关重要的问题。

**5.2** 所有国家和所有组织都需要有足够和必要的人力资源和技能来：

• 实施战略和操作性网络安全措施；

• 进行国家网络安全风险评估；

• 管理与网络安全事件发生相关的危机；

• 加强数字基础设施和服务的强健性和复原力；

• 确立一致的流程、技能和做法。

**5.3** 还必须指出，鉴于ICT的迅速发展以及接入和连接方面已经存在的问题，最终用户 – 特别是妇女、儿童、老年人、残疾人和有具体需求的人群 – 往往更容易受到网络安全威胁和事件的影响。因此，除了提高对与弱势最终用户相关的网络安全威胁的认识之外，与网络安全相关的教育计划，可能是降低整个社会网络安全风险的关键。

2008年以来能力建设格局的演变

**5.4** 由于网络安全具有全球性，并涉及一系列广泛的问题，如ICT的使用或滥用、技术措施、经济、法律和政治问题，因此发展全球网络安全文化以提高网络安全链中每个参与者的理解水平非常重要。在发展网络安全文化时，主要挑战之一是正确确定什么是全球和国际问题，什么是当地的具体需求，因为文化主要依赖于当地和当时的因素。国际技术标准可有助于确定与网络安全文化技术和程序层面相关的关键性全球和一般性问题。

**5.5** 保护数字基础设施的集体对策非常重要。随着技术变革通过ICT走向更大和永久的互连，这一点越来越紧迫。[[27]](#footnote-27) 所有可以连接的东西都可能受到破坏。此外，纳米技术带来的组件小型化，包括各种智能和自主芯片，导致这些芯片被集成到涉及我们所有活动的技术中。

**5.6** GCA已成为能力建设工作的一个创新和有效的跨学科框架，相关参与方可在此基础上继续出台全球性的、可调度的和具体的解决方案，以便进行有效协作。GCA框架已设立，以便为应对建设包容性和安全的信息社会的挑战提供支持。

**5.7** HLEG 2008年报告在这方面提出的建议今天仍然适用。考虑到国际电联所做的工作，特别是自2006年第一次发布[发展中国家网络安全指南](https://www.itu.int/pub/D-STR-SECU-2006)以来，并根据GCA框架和HLEG 2008年报告，成员国在能力建设方面开展了广泛的工作，包括国家、区域和国际层面的培训、提高认识和教育活动。

**5.8** 国际电联利用GCA框架，继续协助各国特别建设必要的人力和技能，确定国家网络安全战略，帮助发展管理计算机事件响应团队的（CIRT）技能并开发保护上网儿童的资源。

**5.9** 例如，在提高认识方面，必须承认[全球网络安全指数（GCI](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx)）的贡献。衡量成员国对网络安全的承诺的GCI自2015年首次推出以来，由于成员国、私营部门、学术界和其他方面的需求强烈，因此已成功发布三次。通过致力于提高认识，GCI继续通过分享有效实施网络安全的良好做法，支持成员国改善其在网络安全方面的水平。事实证明，GCI是提高认识和能力建设的宝贵手段，应继续得到利用和加强。

利用支柱4 – 能力建设的导则

**5.10** 应在国家层面采取具体行动，建设或提高各利益攸关方的网络安全能力，以便能够解决国家和国际网络安全问题。由于能力建设活动主要在国家层面开展，因此应向国家参与方分配适当的资源。[[28]](#footnote-28)

**5.11** 此外，从全球角度来看，增强人力资源能力需要一个一般性的、模块化的和灵活的网络安全教育框架，以应对提高公众认识的需求，并为特定专业人员提供量身定制的教育课程。应特别关注这一领域的性别差距。有许多未开发的人力资本可以为网络安全领域做出贡献，包括仍然只占网络安全劳动力20%的女性。[[29]](#footnote-29)

**5.12** 学校或大学正规教育的质量和公众意识的提高在一定程度上取决于研究的质量、成熟度和相关性。

**5.13** 此外，重要的是要重视微型、小型和中型企业（MSME）的能力建设，这些企业通过获得确定和管理网络风险以及以安全和可持续的方式利用ICT资产 （包括宽带和互联网）的能力，现已成为日益壮大的数字化经济的关键力量之一。

|  |
| --- |
| **5.14** 鉴于上述情况，GCA和HLEG 2008年报告在这一支柱下所含的建议继续提供一个强有力的框架，可以加强和促进能力建设的跨学科方式。考虑到这一点，特建议国际电联通过其电信发展局（BDT）：  **a)** 继续促进参与网络安全能力建设的各国家、区域或国际组织之间更加开放和包容的协作和协调，以确保影响力并避免重复工作。  **b)** 在国家和国际网络安全能力建设团体的支持下，继续支持发展中国家的网络安全能力建设努力。  **c)** 继续与感兴趣的伙伴和其他能力开发团体合作，协助发展中国家制定国家网络安全战略、计划、政策和事件响应能力。  **d)** 继续努力加强缩小标准化差距的能力，包括应要求向各国提供技术援助。  **e)** 加强宣传并促进成员国交流良好做法，以帮助网络安全专业知识落后的国家改善其网络安全状况，并缩小能力差距。  **f)** 继续发展其能力建设活动，同时考虑到对新技能的需求，以适应新兴技术的安全需求。在这方面，应加强与学术界、私营部门和成员国的合作。  **g)** 在能力建设工作中，继续特别关注妇女、儿童、残疾人和有具体需求人群以及老年人等更弱势群体的需求。  **h)** 继续发展和加强作为能力建设和增强认识手段的GCI。  **i)** 制定“网络安全教育计划发展和实施指南”，旨在支持成员国为小学、中学、大学和成人专业教育系统的青年开发/采用网络安全课程，以促进在全球培训更多的网络安全专业人员并提高各行各业和所有未来专业人员的网络安全意识。  **j)** 利用国际电联的学术和私营部门成员（已进行），通过国际电联的年度人工智能惠及人类全球峰会，继续促进不同利益攸关方之间确定与网络安全相关的研究活动或对话，特别是在新兴技术领域。  **k)** 向成员国、行业和其他利益攸关方传播工具、资源和良好做法，以支持他们努力建设MSME应对安全挑战的能力，并建立对使用ICT的信任感和信心。  **l)** 继续促进培育网络安全文化。 |

第6节 支柱5：国际合作

引言

**6.1** 从过去十年来看，显然没有任何一家实体或组织能够单独应对当前和新出现的一系列网络安全挑战。这些挑战可以通过所有利益攸关方之间密切协作和协调的伙伴关系来解决，以帮助建立一个普遍可用、开放、安全和可信赖的ICT生态系统。

**6.2** 因此，关于国际合作的支柱5是GCA的跨领域支柱 – 构成在使用ICT方面建立信任、信心和安全的各个方面的基础。在HLEG 2008年报告中，这一支柱旨在制定应对网络威胁的国际合作、对话和协调战略。

2008年以来国际合作格局的演变

全球高级别对话

**6.3** 关于网络安全各个方面的讨论 – 包括技术方面、网络犯罪、隐私、数据保护等 – 普遍反映在许多论坛和进程中。其中一些由包括国际电联或其他国际组织在内的联合国不同机构主办，另一些由其他利益攸关方发起以及各种其他国际和区域论坛。

**6.4** 虽然所有论坛和进程在提高认识和增进理解方面都做得很好，但重要的是要确定这些不同努力之间的协同作用，以便国际社会能够走到一起，找到解决方案。

**6.5** 联合国平台具有强大的召集能力，完全有能力在国层面促进所有国家的利益攸关方在应对网络空间相关挑战方面的合作、对话和协调。正如HLEG 2008年报告所强调的，考虑到国际电联作为ICT专门机构在联合国系统中的地位，国际电联可以在其职责范围内继续在发展领域中发挥重要作用。

**6.6** 虽然HLEG 2008年报告[[30]](#footnote-30)建议1.15提议召开一次“全球会议”，但也可以更好地利用WSIS进程产生并随后得到加强的现有大会、论坛和进程 – 有关发展事务的[WSIS论坛](https://www.itu.int/net4/wsis/forum/2020/)和有关治理事务的[IGF](https://www.intgovforum.org/multilingual/)。WSIS论坛是利用ICT促发展（ICT4D）团体最大的年度聚会，提供若干机制，将全球社会汇聚一起，讨论和确定在树立使用ICT的信心并加强安全性（C5行动方面）的、有关发展挑战的具体解决方案，其中包括行动方面推进方会议、高级别对话和有针对性的利益攸关方会议。

**6.7** 过去十年的一个重要进展是，各国政府最高层认识到网络安全的关键重要性。这反映在许多国家通过政府总动员方式采用的数字化转型战略、建立跨部门中央协调机制、通常直接向国家元首或政府首脑报告等方面。

**6.8** 另一个相关的发展是在技术先进的国家和地区之间进行了大量的双边讨论。

国际利益攸关多方伙伴关系

**6.9** 国际电联作为WSIS C5行动方面的唯一推进方，在促进国际合作方面取得了各种成功。

**6.10** 国际电联已建立一系列利益攸关多方伙伴关系，手段包括：

• 正式机制，如谅解备忘录（MoU）或类似安排（如与FIRST、国际刑警组织、UNODC、WEF和其他方面的安排）；

• 与来自所有利益相关方团体的80多个实体合作开展的保护上网儿童等举措[[31]](#footnote-31)；或

• 诸如焦点组的机制，例如数字账本技术、量子技术、人工智能与卫生等的焦点组，这些为所有利益攸关方讨论新兴技术中的信任和信心问题提供了一个平台。

### 6.11 在过去十年中，国际电联的利益攸关多方成员显著增加，特别是私营部门公司和学术机构的范围，使本组织受益于193个成员国和近900个私营部门公司、大学以及国际和区域组织的广泛成员，从而反映了当今数字社会迅速变化的性质。

联合国系统内更好的协调

**6.12** 如本文件第2.4和2.5段所述，联合国大会建立了一些联合国进程，以帮助应对确保国际网络空间安全的挑战。这些包括GGE和的工作。除其他外，2019-2021年[《OWEG最后实质性报告》](https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf)得出结论认为，未来的定期机构对话不应重复联合国现有的侧重于其他问题的数字层面的任务、努力和活动，联合国主持下的任何未来定期机构对话机制都应是一个以行动为导向的进程，有具体目标，建立在以往成果的基础上，并具有包容性、透明性、共识驱动性和成果基础。考虑到这一点，重要的是国际电联的工作应对联合国系统目前在这方面正在进行的工作，特别是上述联合国大会进程，起到相辅相成的作用。

**6.13** 联合国系统任务的复杂表述有时会妨碍务实和有效的协调方式，因此，联合国大家庭必须继续努力协调其努力，包括精简网络安全方面的方案和活动，以便更加有效。

**6.14** 因此，重要的是，要努力在联合国内部就正确制定方案和倡议的需要和要求达成共识，这些方案和倡议将有效支持政府、行业和所有其他相关利益攸关方所做的努力。

**6.15** 2010年迈出了重要的第一步，加强了联合国各机构在网络安全方面向成员国提供援助的内部协调。国际电联和联合国毒品和犯罪问题办公室（UNODC）与33个联合国机构协作，牵头开展了为期两年的、旨在制定联合国全系统“网络安全和网络犯罪框架”的工作，于2013年11月得到联合国系统行政首长协调会（CEB）的首肯。

**6.16** 虽然这是关键性一步，但还需要进一步的系统性变革，以确保有效的协调。联合国秘书长将数字合作列为优先事项[[32]](#footnote-32)，这提供了这样一个机会，即通过利用包括CEB在内的各种机构间机制，满足整个联合国大家庭继续改善内部协调与合作的需要。

利用支柱5 – 国际合作的导则

|  |
| --- |
| **6.17** 鉴于这一支柱的跨领域性质，并考虑到国际电联广泛的与不同行业的协作和伙伴关系，因此国际电联所有部门都必须密切合作，利用有效的部门间协调机制和指定联系人，在内部和外部协调努力。HLEG 2008年报告在这方面的建议仍然具有现实意义，且根据上一节提供的信息，特为利用支柱5进一步提出了以下导则：  **a)** 在全球网络安全问题上，联合国在促进所有国家之间以及与私营部门和其他利益攸关方的合作、对话和协调方面发挥着独特的作用。考虑到国际电联在联合国系统中作为ICT专门机构和C5行动方面（树立使用ICT的信心并提高安全性）唯一推进方的地位，国际电联应在其职责范围内各领域继续在相关发展中发挥主导作用。  **b)** 基于WSIS进程，并考虑到联合国秘书长的数字合作高级别小组的努力 – 特别是建议4（全球信任与安全承诺），国际电联应将不同参与方聚集一起从而帮助加强推进工作。可通过WSIS论坛利用C5行动方面相关进程提供的机制以及IGF等提供的机制实现这一目标。  **c)** 鉴于网络威胁的全球性质，应继续鼓励主要参与方之间的双边和多边讨论，同时还应促进包括私营部门和其他利益攸关方在内的更广泛群体之间的更广泛讨论。国际电联可在其职责范围内各领域的此方面发挥促进作用–与合作伙伴合作，帮助所有利益攸关方在联合国这一更广泛的全球环境内内汇聚在一起。  **d)** 国际电联应继续探索建立伙伴关系的创新、灵活和敏捷机制，同时考虑到快速发展的技术行业和正在出现的一系列新实体 – 特别是初创企业和MSME。  **e)** 国际电联应继续与联合国系统内的其他主要机构接触，协调联合国秘书处内部的努力，并简化其有关网络安全的方案和活动，以便更有效地为全球社会服务。 |

第7节 GCA框架的一般性导则

|  |
| --- |
| **7.1** 制定GCA使用导则的过程产生了一些广泛的跨领域导则，这些导则适用于国际电联和GCA五大支柱的工作并与之相关。由于认识到各支柱之间紧密联系，且国际电联及其成员需努力就网络安全行动达成整体和全面性愿景，因此下文提出这些一般性导则：  **a)** 鉴于致力于网络安全并推动不同方面进展的利益攸关方、组织、伙伴关系和场所激增，所以国际电联应继续加强和扩大其协作和参与，以造福所有此类利益攸关方，从而加强知识共享以及信息和专业知识的交流，同时避免重复工作。  **b)** 国际电联应成为活跃在该领域的其他利益攸关方和组织就网络安全的不同方面开展的各种全球活动、倡议和项目的信息库--这些利益攸关方和组织可能在相关具体方面负有主要任务、作用和/或责任 – 以便使国际社会能够方便地获取所有这些资源。  **c)** 国际电联根据GCA开展的所有工作都应利用GCI等工具，遵循对其成员的需求和目标的明确评估以及满足这些需求和目标所需的交付成果，并符合专门为此设计的适当衡量标准。  **d)** 国际电联应继续在其职责范围领域内跟踪新兴ICT的发展和使用情况，以指导成员国和利益攸关方了解这些技术的安全方面问题，并酌情了解其在应对网络威胁方面的潜在应用。  **e)** 鉴于网络安全固有的跨国和跨行业影响，国际电联应促进有助于成员国以政府总动员方式解决这一问题的活动、倡议和项目。 |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. 2018年11月15日（星期四）在迪拜举行的全权代表大会第十七次全体会议的会议记录，以下网站提供：<https://www.itu.int/md/S18-PP-C-0174/> [↑](#footnote-ref-1)
2. 转呈GCA高级专家组前主席的报告（C19/58），国际电联，2019年5月8日，以下网站提供：<https://www.itu.int/md/S19-CL-C-0058/en> [↑](#footnote-ref-2)
3. 第六次全体会议摘要记录（C19/117），国际电联，2019年6月20日，以下网站提供：<https://www.itu.int/md/S19-CL-C-0117/> [↑](#footnote-ref-3)
4. 如欲了解更多关于流程的信息以及从成员国收到的输入意见，请访问：<https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx> [↑](#footnote-ref-4)
5. WSIS成果文件，2005年，以下网站提供：[https://www.itu.int/net/wsis/outcome/booklet.pdf](https://www.itu.int/net/wsis/outcome/booklet.pdf" \o "https://www.itu.int/net/wsis/outcome/booklet.pdf) [↑](#footnote-ref-5)
6. Schjolberg法官：HLEG主席报告，2008年，以下网站提供：<https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx> [↑](#footnote-ref-6)
7. HLEG2008年报告中的建议附有会议期间与每项建议相关的意见和讨论的附加说明摘要。虽然HLEG成员未就每一项建议达成充分的共识，但大多数HLEG专家在许多建议上都达成了广泛的一致意见。 [↑](#footnote-ref-7)
8. [欧洲议会和欧洲联盟理事会2013年8月12日关于攻击信息系统的指令取代了理事会框架决定（2005）](https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040)，其对关键性基础设施的定义如下：位于成员国的资产、系统或其一部分，对于维护重要的社会功能、人民的医疗卫生、安全、安保、经济或社会福祉至关重要，并且由于未能维护这些功能而造成的中断或破坏将对成员国产生重大影响。 [↑](#footnote-ref-8)
9. 截至2019年第４季度，全球每月活跃的脸书用户数量，可访问：<https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/> [↑](#footnote-ref-9)
10. 马克·扎克伯格：互联网需要新的规则，让我们从这四个领域开始。华盛顿邮报，2019年3月30日，网址：<https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html> [↑](#footnote-ref-10)
11. 政府专家组见：<https://www.un.org/disarmament/group-of-governmental-experts/> [↑](#footnote-ref-11)
12. 不限成员名额工作组见：<https://www.un.org/disarmament/open-ended-working-group/> [↑](#footnote-ref-12)
13. 有关更多信息，请参考以下内容：

    - 国际电联向国际电联理事会提交的关于树立使用ICT的信心并提高和安全性的年度活动报告，可查阅： <https://www.itu.int/en/council/2021/Pages/default.aspx>

    - 向理事会2020年会议提交的关于国际电联利用GCA的报告，可查阅：<https://www.itu.int/md/S21-CL-C-0036/en>。 [↑](#footnote-ref-13)
14. Stein Schjolberg,，《网络犯罪史》（第3版，2020年2月） [↑](#footnote-ref-14)
15. 欧洲联盟委员会启动了名为[Horizon 2020](https://ec.europa.eu/programmes/horizon2020/en)的开发物联网潜力的方案，以及支持实验和创新的2016-2017年工作方案。邀请各方针对多个主题提出建议，还包括：物联网安全和隐私。高度分布式、异构和动态物联网环境中端到端安全的高级概念。方法必须是全面的，包括识别和认证、数据保护以及在设备和系统级别防范网络攻击。这些应解决相关的安全和隐私要素，如保密性、用户数据意识和控制、完整性、复原力和授权（见2015年10月13日欧盟委员会第C (2015) 6776号决定。） [↑](#footnote-ref-15)
16. T.Ballell，《人工智能的法律挑战：新兴技术的破坏性特征及评估其可能法律影响的建模》，《统一法评论》，第24卷，第2期，2019年6月，第302-314页，可访问：<https://doi.org/10.1093/ulr/unz018> [↑](#footnote-ref-16)
17. 示范法律框架可以是[欧洲议会和理事会2011年12月13日](https://ec.europa.eu/anti-trafficking/legislation-and-case-law-eu-legislation-criminal-law/directive-201192eu_en)关于打击对儿童的性虐待和性剥削以及儿童色情制品的[第2011/92/EU号指令](https://ec.europa.eu/anti-trafficking/legislation-and-case-law-eu-legislation-criminal-law/directive-201192eu_en) [↑](#footnote-ref-17)
18. Judge Stein Schjolberg（2018年）和Judge Stein Schjolberg（2019年），见： <https://www.cybercrimelaw.net/Cybercrimelaw.html> [↑](#footnote-ref-18)
19. 例如：https://www.justice.gov/olp/lawful-access [↑](#footnote-ref-19)
20. 国际电联标准概况，以下网站提供：  
    <https://www.itu.int/net4/ITU-T/landscape#?topic=0.1&workgroup=1.3935&searchValue=&page=1&sort=Revelance> [↑](#footnote-ref-20)
21. HLEG 2008年报告，第9页第2.1段，同6 [↑](#footnote-ref-21)
22. HLEG 2008年报告，第9页第2.2段，同6 [↑](#footnote-ref-22)
23. HLEG 2008年报告，第9页第2段，同6 [↑](#footnote-ref-23)
24. 国家CIRT，国际电联，以下网站提供：<https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx> [↑](#footnote-ref-24)
25. 同上 [↑](#footnote-ref-25)
26. 同上 [↑](#footnote-ref-26)
27. Tim Berners-Lee，30年过去了，网络的下一步是什么？（30 years on, what’s next #ForTheWeb？），2019年3月12日，（可在 <https://webfoundation.org/2019/03/web-birthday-30/>查阅）-- 在网络30周年纪念日上他在一封公开信中指出，虽然网络创造了机会，让边缘化的群体发出了自己的声音，让我们的日常生活变得更容易，但同时也为骗子创造了机会，让那些散播仇恨的人发出了声音，让各种犯罪变得更容易。 [↑](#footnote-ref-27)
28. S. Ghernaouti，网络空间的犯罪、冲突与安全，洛桑高工（EPFL）出版社，2013年 [↑](#footnote-ref-28)
29. Laurence Bradford, “网络安全需要女性: 原因如下”，2018年10月18日，请访问：  
    <https://www.forbes.com/sites/laurencebradford/2018/10/18/cybersecurity-needs-women-heres-why/#5a7a3cc447e8> [↑](#footnote-ref-29)
30. HLEG 2008年报告，第9页第1.15段，同6 [↑](#footnote-ref-30)
31. 更多信息，见：<https://www.itu.int/en/cop/Pages/partners.aspx> [↑](#footnote-ref-31)
32. 更多信息请访问：<https://www.un.org/en/digital-cooperation-panel/> [↑](#footnote-ref-32)