

全球网络安全指数

2020



全球网络安全指数2020

衡量对网络安全所做的承诺



致谢

全球网络安全指数（GCI）是联合国信息通信技术（ICT）专门机构国际电信联盟（ITU）提出的一项倡议，通过各国和其他国际组织内众多专家和贡献者的工作来塑造和改进。国际电联感谢所有合作伙伴和贡献者在为GCI提供支持方面所做的辛勤工作和承诺，更重要的是，他们帮助推动了我们对网络安全承诺的共同理解。

国际电联想特别强调指出的是通过ITU-D第2研究组和电信发展局（BDT）管理咨询组收到的各文稿，以及他们在修改GCI问卷调查表方面所做的工作。BDT网络安全小组感谢国际电联成员提名专家在权重处理过程中提出建议。有关权重处理和专家参与的更多信息，请参见有关方法论的章节。来自国际电联成员的以下专家输入意见为指配和确定权重提供了宝贵支持：

Abdelaziz Alzarooni先生（电信和数字政府监管局（TDRA），阿拉伯联合酋长国）、Marco Gercke博士/教授（德国网络犯罪研究所）、Melissa Hathaway女士（美国波托马克政策研究所）、Vanessa Copetti Cravo（巴西国家电信管理局（ANATEL））、Scott James Shackelford先生（印第安纳大学，网络安全和互联网治理计划，美利坚合众国）、Gueric Goncalves先生（ANNSI，贝宁）、Eng Emmanuel Thekiso教授（BOCRA，博茨瓦纳）、Dlamini先生（信息通信技术部，斯威士兰）、Fillemon Johannes先生（信息通信技术部，纳米比亚）、Palakiyem ASSIH先生（非洲网络防御S.A.S.，多哥）、Nawa J. Samatebele先生（赞比亚信息通信技术管理局，赞比亚）、Gonzalo Díaz de Valdés Olavarrieta先生（智利）、Jessica Machado Álvarez女士（古巴主管部门，古巴）、Eng. Raquel Piña（委内瑞拉）、Mtro. Jacobo Bello Joya（安全和公民保护秘书处国民警卫队，墨西哥）、Renzo Zegarra先生（交通和通信部，墨西哥）、Junior McIntyre先生（加勒比电信联盟（CTU），特立尼达和多巴哥）、Fernando Hernandez先生（乌拉圭通信监管机构，乌拉圭）、Anne-Rachel Inné女士（美国互联网号码注册机构（ARIN），美利坚合众国）、Mohammad Odeh Alsalamín先生（约旦）、Nada Khater女士（数字经济和创业部，约旦）、Yusuf Ahmed Buhijji先生（交通和通信部，巴林王国）、Aziza Al Rashdi女士（交通、通信和信息部，阿曼）、Abdulrahman AlHassan先生（国家网络安全局（NCA），沙特阿拉伯）、Eng. Mohammad Alawi（电信和信息部，巴勒斯坦国）、Khalili Urahman Kabirzoy先生（阿富汗根认证机构（ARCA），阿富汗）、Nasratullah Ghafoory先生（阿富汗根认证机构（ARCA），阿富汗）、Xu Ming女士（工业和信息化部，国家计算机网络应急响应小组，中国）、Wan Xinxin女士（工业和信息化部，国家计算机网络应急响应小组，中国）、Catherine M. Subhyadas女士（通信部，斐济）、Puan Lyana Shohaimay（通信和多媒体部，马来西亚）、Puan Nurul Adiah Hani Husin（通信和多媒体部，马来西亚）、Yan Naung Soe先生（国家网络安全中心，信息技术和网络安全部，缅甸）、Jakkrapong Chavong先生（数字经济与社会部，泰国）、Alan Olegovich Khubaev先生（信息安全部，俄罗斯）、Andrey Sergeevich Zhivov先生（国际合作部，俄罗斯）、Ilgыз Turganbaev先生（吉尔吉斯共和国信息技术和通信国家委员会，吉尔吉斯共和国）、Muhamedjan Alymkulov先生（吉尔吉斯共和国信息技术和通信国家委员会，吉尔吉斯共和国）、Vladimir Yuryevich Shurin先生（白俄罗斯共和国统一企业安全服务信息安全部，白俄罗斯）、Nestoras Chouliaras先生（电信和邮政总秘书处，数字治理部，希腊）、Egl Vasiliauskaitė女士（立陶宛共和国国防部，立陶宛）、Tadas Šakūnas先生（立陶宛共和国国防部，立陶宛）、Radoja女士（塞尔维亚）、Matej Šalmík先生（国家网络安全中心SK-CERT，斯洛伐克）、Rastislav Janota先生（国家网络安全中心SK-CERT，斯洛伐克）、Aidan Murchland先生（英国）、Miguel Pinto先生（BitSight，美利坚合众国）、Nunil Pantjawati女士（印度尼西亚）、Intan Rahayu女士（印度尼西亚）、Makaireh JONGA先生（冈比亚计算机安全与事件响应小组（gmCSIRT），冈比亚）、Banchale Gufu女士（肯尼亚）、Sonam

Choki女士（信息技术和电信部，不丹）、Aqeel Taha Saadoon（信息通信技术秘书处，伊拉克）和Thar Kadhim Ali（CERTIraq，伊拉克）。

国际电联网络安全小组感谢GCI联系人，他们从各自国家收集了有关网络安全承诺的数据。如果没有GCI国家联系人，这份报告是不可能完成的。

小组感谢为本报告提供支持的众多国际电联同事和实习生。

小组向不经意间在清单中遗漏的任何个人或组织表示道歉，并向所有为 GCI 做出贡献的人表示感谢。

如对本出版物有任何意见或疑问，请通过gci@itu.int联系国际电联网络安全小组。

© ITU 2021保留所有权利。未经国际电联事先书面许可，不得以任何方式部分或全部复制本出版物的任何部分。

免责声明

本出版物中使用的名称和材料的表述并不意味着国际电联对任何国家、领土、城市或地区或其当局的法律地位，或者对其边界或界线的划定表达任何意见。提及特定公司或某些制造商的产品并不意味着国际电联认可或推荐这些公司或产品优先于未提及的其他类似性质的公司或产品。除了错误和遗漏之外，专有产品的名称用首字母大写来区分。

国际电联已采取所有合理的预防措施来核实本出版物中包含的信息。然而，资料的发行没有任何明确或隐含的担保。资料的解释和使用责任由读者自负。本出版物中表达的意见、调查结果和结论不一定反映国际电联或其成员的观点。

ISBN:

978-92-61-33925-8（电子版）

978-92-61-33935-7（EPUB版）

978-92-61-33945-6（Mobi版）

前言



对安全可靠的网络空间的需求变得比以往任何时候都重要，尤其是在我们越来越依赖“数字生命线”的情况下。尽管存在不确定性、焦虑和变化，但COVID-19大流行的最大挑战之一是找到有效的相互联系的方法。甚至在大流行之前，网络安全对确保我们安全上网而言也是至关重要的，网络安全确保我们能够执行关键的日常功能。

我深受人们适应这种不确定环境之能力及使用技术来寻找创造性解决方案的鼓舞。许多组织，包括国际电信联盟，都在努力应对远程工作带来的新挑战。网络安全从根本上与远程工作交织在一起，从管理视频通话参与者到确保安全地共享文档。因此，国际电联继续与各国开展合作，以提高效率和更加积极主动，并在最需要我们的领域产生影响。

全球网络安全指数于2015年首次推出时，很少有人能想象我们目前所处的境地。通过衡量各国做出的网络安全承诺的类型及其普遍性，全球网络安全指数的本最新迭代版本将有助于促进采取进一步行动，以实现复苏和增长所需的安全数字生态系统。

本次迭代表明，尽管机会主义行为者利用了我们信息的渴望、我们对大流行的恐惧、转向在家工作和远程学习、对医疗保健系统的依赖等，仍有许多国家在应对网络安全挑战的承诺方面取得了诸多进展。

全球网络安全指数报告显示，许多国家颁布了新的网络安全法律和法规，以解决隐私、未经授权的访问和上网安全等领域面临的问题。它还强调，需要建立战略和机制来建设能力并帮助政府和企业更好地准备和缓解日益增长的网络风险。世界上半以上的国家现拥有计算机事件响应小组（CIRT），近三分之二的国家拥有某种形式的国家网络安全战略以指导其总的网络安全态势。

全球网络安全指数表明，网络安全确实是一个发展问题，迫切需要通过培育知识、提升技能和建设能力来解决发达国家与发展中国家之间日益扩大的网络能力差距。我们需要通过在发展中世界数字基础设施、数字技能和资源等方面的深入研究和建设能力来弥合这一差距。

我希望全球网络安全指数将继续成为政府、政策制定者、网络安全专家和学术界一个有用的能力发展工具，以确定需要改进的领域并强调指出增强国家网络安全所需的最佳做法。

我对各国积极并富有成效地参与本项工作和做出贡献表示感谢，特别要感谢参与了本次指数迭代的开发、数据收集和验证。我还要感谢所有参与工作组工作进程的人员，感谢他们的支持和指导。我诚邀国际电联所有成员国继续向我们通报其在网络安全相关承诺方面的最新进展，以便我们能够有效地分享经验、研究和解决方案，为所有人创建一个值得信赖的网络空间。



多琳•伯格丹-马丁女士

国际电联电信发展局（BDT）主任

内容提要

全球网络安全指数（GCI）于2015年由国际电信联盟（ITU）首次推出，旨在衡量193个国际电联成员国和巴勒斯坦国¹对网络安全的承诺，通过提高对全球网络安全状况的认识，帮助他们确定需要改进的领域并鼓励各国采取行动。随着网络安全风险、优先事项和资源的演进，GCI也进行了调整，以更准确地反映各国采取的网络安全措施。

本报告旨在更好地了解各国对网络安全的承诺、找出差距、鼓励采用良好做法，并为各国改善其网络安全态势提供有用的见解。

各国已报告使用GCI来促进：

- 通过正式建立的论坛进行讨论，以实现自我评估和更好的协调；
- 收集有关用于在国家层面管理网络安全的总体国家举措和资源的见解；
- 以良好做法、合作伙伴和区域邻国为基准；
- 提高各利益攸关方对国家层面协调需求的认识。

GCI结果表明，网络安全议程的所有五个支柱都得到了整体改进和加强，但网络能力方面的区域差距仍然存在。报告突出阐述了各国用作例证的做法。

衡量的国家	收集年份	来自各国的联系人	提交的问卷调查表	自2018年以来中位数总分增长率
194	2020	169	150	9.5%



该指数涵盖了跨越五个支柱的、关于成员国网络安全承诺的82个问题：

- 法律措施；
- 技术措施；
- 组织措施；
- 能力发展措施；
- 合作措施。

¹ 巴勒斯坦国根据全权代表大会第99号决议（迪拜，2018年，修订版）参与国际电联的工作。

下表显示了每个支柱的具体指标的全球承诺。

	法律措施		
	衡量关于网络犯罪和网络安全法律法规	167	有某种形式的网络安全立法的国家 数据保护法规
	衡量通过国家和部门特定机构实施技术能力的情况	133	关键基础设施法规
		97	
	技术措施		
	衡量通过国家和部门特定机构实施技术能力的情况	131	积极主动的CIRT
	衡量通过国家和部门特定机构实施技术能力的情况	104	参与区域CIRT
		101	儿童上网保护报告机制
	组织措施		
	衡量实施网络安全的国家战略和组织	127	国家网络安全战略
	衡量实施网络安全的国家战略和组织	136	网络安全机构
		86	报告的儿童上网保护战略和举措
	能力发展措施		
	衡量有关网络安全能力发展的提高认识活动、培训、教育和激励措施	142	各国开展提高网络安全认识的举措
	衡量有关网络安全能力发展的提高认识活动、培训、教育和激励措施	94	有网络安全研发计划的国家
		98	报告称有国家网络安全产业的国家
	合作措施		
	衡量机构、公司和国家之间的合作伙伴关系	166	参与网络安全公私合作伙伴关系的国家 有网络安全双边协议的国家
	衡量机构、公司和国家之间的合作伙伴关系	90	有网络安全多边协议的国家
		112	

影响得分的全球网络安全指数的变化

- 本版全球网络安全指数基于创纪录的成员参与所报告的数据，从2013-2014年迭代中的105份回复，到2020年返回150份问卷调查表。
- 对GCI问卷调查表做了更新。对有关五个支柱（法律措施、技术措施、组织措施、能力发展措施和合作措施）中每个支柱的问题都重新做了定义、添加或删除，以反映网络安全安全问题和工作的变化。问卷调查表的变化会影响结果，这些变化是影响国家得分和排名的一个因素。
- 权重与之前的迭代不同，部分反映了问题结构的变化以及问题的添加和删除。
- 指标权重基于专家建议。国际电联成员提名的专家在权重过程中提出建议，根据相对网络安全的重要性来为指标分配权重。权重分配的变化会影响国家得分和排名。
- 准备了一个章节来提供有关GCI问卷调查表之结构、组成和最近变化的更多信息（附件A）。
- 许多国家、尤其是表现最好的国家，在得分方面越来越接近，这就是为什么应对单个排名做出仔细解释的原因。
- 一些国家拒绝验证所收集的数据或者参与本版全球网络安全指数。有关这些国家（标有*）的数据不应被视为得到了代表该国之任何代表的正式认可。由于这些数据是通过在线研究收集的，因此需要将缺失的元素解释为未找到而不是不存在。

此外，在某些情况下，国家参与可能对得分产生积极影响，因为一个国家对问卷调查表的贡献越多，就越有可能找到肯定的答复。

各国擅长的领域很多，还有可以进一步加强共工作的领域，不应鼓励各国过于关注排名。

对于未提交问卷调查表答复的国家，案头研究是通过官网和其他资源上的公开信息进行的。对于开展了案头研究的国家，收集的数据可能无法准确反映该国的网络安全态势。GCI不包含估算的数据。

目录

致谢	ii
前言	iv
内容提要	vi
表和图目录	x
1 全球网络安全指数：背景与状况	1
2 关键主题	2
2.1 法律措施：规划未来的干预措施	2
2.2 技术措施：增加部署 CIRT/CERT	5
2.3 组织措施：调整战略	7
2.4 能力发展措施：发展网络安全能力	12
2.5 合作措施：解决集体网络安全行动	18
2.6 儿童上网保护	21
2.7 结论	22
3 GCI结果：得分和排名	24
3.1 全球得分和国家排名	24
3.2 区域得分和国家排名	27
4 2020年全球网络安全指数：国家概况	30
非洲	30
美洲区域	52
阿拉伯国家区域	69
亚太区域	80
独联体区域	99
欧洲	104
词汇表	127
附件A：方法论	128
附件B：全球网络安全指数问卷调查表（第4版）	134

表和图目录

表目录

表1: 有NCS和CIRT的国家数量	10
表2: 参与国际和/或国内PPP的国家数量	21
表3: GCI结果: 全球得分和排名	24
表4: GCI结果: 非洲区域	27
表5: GCI结果: 美洲区域	27
表6: GCI结果: 阿拉伯国家区域	28
表7: GCI结果: 亚太区域	28
表8: GCI结果: 独联体区域	29
表9: GCI结果: 欧洲区域	29
表A1: 全球网络安全指数参与情况和数据收集年份	128
表A2: GCI 2020支柱描述	129
表B1: GCI问卷调查表: 法律措施	134
表B2: GCI问卷调查表: 技术措施	137
表B3: GCI问卷调查表: 组织措施	140
表B4: GCI问卷调查表: 能力发展建设	143
表B5: GCI问卷调查表: 合作措施	147

图目录

图1: 有数据保护法律的国家数量	2
图2: 采取违规通知措施的国家数量	3
图3: 对窃取个人信息有立法的国家数量	3
图4: 关于身份盗窃以及数据与隐私保护的立法, 绘制在互联网接入上 (人口百分比)	4
图5: 关于非法访问的立法	4
图6: 对网络骚扰有立法的国家	5
图7: 有国家CIRT的国家数量	6
图8: 部门CIRT的数量	7
图9: 着手解决关键基础设施和弹性问题的国家数量	9
图10: 互联网用户 (按CIRT和国家网络安全战略覆盖范围分列)	9
图11: 未连接人口的规模 (按CIRT和国家网络安全战略覆盖范围分列)	10
图12: 作为NCS一部分的生命周期评估	11
图13: 在国家层面执行的国家网络安全审计	11
图14: 在国家层面用于评估网络空间相关风险的指标	12
图15: 全球网络安全指数和未连接人口	13
图16: 可持续发展目标 (8、9、10)	13
图17: (与互联网普及率相比, 每个国家的) 提高公共网络安全认识活动得分	14

图18: 针对中小企业、私营部门和政府机构开展提高网络安全认识活动的国家数量	15
图19: 为专业人士提供特定网络安全教育计划/培训的国家数量	16
图20: 将网络安全课程纳入国家学术课程的国家数量 (按教育阶段分列)	17
图21: 有网络安全能力发展激励机制的国家数量	18
图22: 参与双边网络安全协议的国家数量	19
图23: 有双边网络安全协议的国家数量 (按涵盖的主题分列)	19
图24: 参与多边网络安全协议 (已签署和已批准) 的国家数量	20
图25: 国际活动参与情况	20
图26: 国际电联儿童上网保护系列报告	21
图27: 有儿童上网保护战略的国家	22

1 全球网络安全指数：背景与状况

全球网络安全指数（GCI）的第四次迭代与其之前版本发生在非常不同的时间。当全球网络安全议程于2007年首次启动时，第一部iPhone手机距离发布还有一个月的时间，而Facebook对美国大学以外的用户才开放一年的时间。有10亿人上网，有人担心所创建的数据量（255EB）会超出可用的存储量¹。如今，智能手机重塑了日常生活，社交媒体已融入更大的社会领域。目前，有35亿人上网，数字世界估计达到了44ZB，由于云计算，没有了存储不可用的风险²。此外，ICT的扩散影响了更广泛的生态系统，为新的组织（例如，电子政务服务）以及新的经济和生产范式（例如，工业4.0和更广泛的数字经济）带来了可能。

所有国家都在一定程度上受到数字鸿沟的影响，作为依赖数字系统的经济、社会和政府的关键推动者，对网络安全应赋予高度优先级。

COVID-19大流行极大地影响了社会的运作方式。随着大流行于2020年4月开始蔓延，Akamai指出互联网流量增加了30%³。从远程办公到远程学习，技术在保持人们连通方面发挥了关键作用。为了让数字时代发挥其潜力，一个值得信赖且安全的网络空间至关重要。在世界卫生组织宣布COVID-19为大流行病以及新管理系统和疫苗接种一年后，我们对数字技术的依赖继续增长。随着世界连通更多的未连接的人，必须确保一个安全可靠的网络空间。

人们越来越认识到网络安全风险⁴。持续的大流行造成了不信任，尤其是在网络上。GCI中收集的数据是关于网络安全问题更广泛对话的开始，围绕该对话的当地背景和观察对塑造前进的道路而言至关重要。

为了帮助在大流行后创建一个值得信赖和安全的网络空间，GCI可以作为了解大流行如何影响网络安全工作以及各国如何着手解决网络安全和信任问题的一个跳板。例如，一些国家报告在法律的批准和生效、CIRT的实施或改进、国家网络安全战略的制定或修订以及能力建设工作的交付方面出现了延误。甚至合作协议也不再受益于面对面的互动和协作。

随着世界的不断变化，政府评估网络安全方面的政策和做法非常重要。随着网络安全的演进和调整，其衡量方式也在不断变化。GCI更新了有关CIRT的作用、合作协议、组织框架和提高公众认识的问题。虽然随着时间的推移，这些变化使得GCI的可比性降低，但本次迭代更准确地反映了各国当前的承诺。

¹ http://core.xsomo.com/jm/images/web/File/white%20papaers/Expanding_Digital_Universe_IDC_WhitePaper_022507.pdf

² <https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/>

³ <https://blogs.akamai.com/2020/04/can-the-internet-keep-up-with-the-surge-in-demand.html>

⁴ <http://reports.weforum.org/global-risks-report-2020/executive-summary/>

2 关键主题

2.1 法律措施：规划未来的干预措施

今天的许多挑战削弱了网络信任，并阻止了数字社会充分发挥其全部潜力。例如，因全球网络犯罪而造成的损失估计从2020年的低至1万亿美元⁵，发展到了2021年的高达6万亿美元⁶。制定法律和监管框架以保护社会并促进安全可靠的数字环境至关重要，并且应该是任何国家网络安全工作的开始。

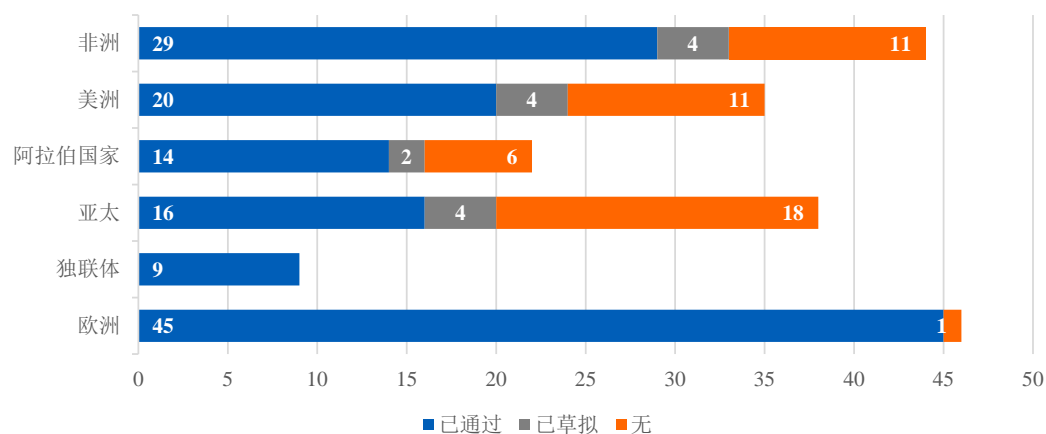
法律和监管框架包括制定法律、确定网络空间非法活动的构成，以及调查、起诉和执行此类法律所需程序工具的定义；为一组国家利益攸关方建立网络安全基线和合规机制；以及确保与国际义务相一致的程序。

第四版全球网络安全指数通过衡量是否存在以下内容来评估一个国家法律框架内的网络安全干预措施：

- 公共和私人利益攸关方必须遵守的基本要求；
- 禁止有害行为的法律文书。

数据保护

图1：有数据保护法律的国家数量



来源：国际电联

数据保护立法可采取监管的形式，例如，可以强制组织披露网络安全漏洞或提出年度审计要求。

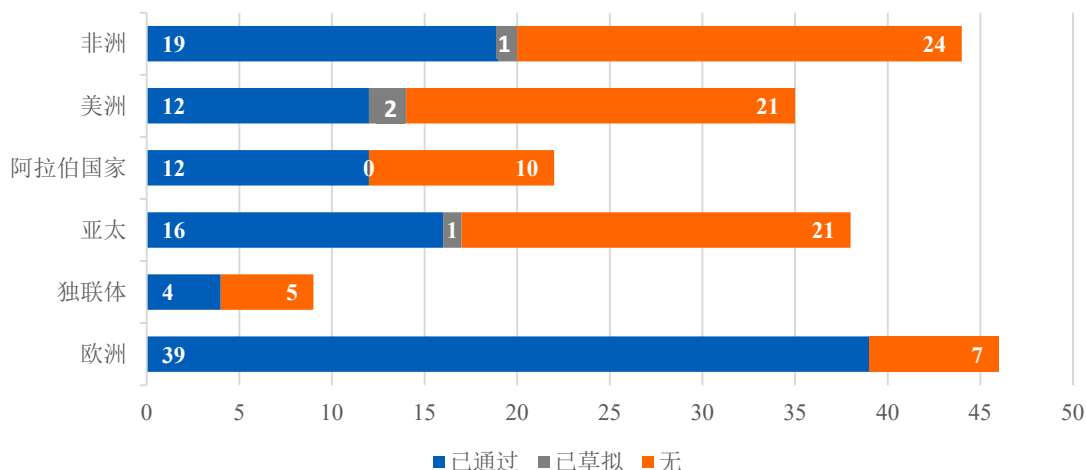
⁵ <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf>

⁶ <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>

从表面上看，隐私倡导者可能会注意到，许多已制定了数据保护和隐私法规的国家已经努力在更新它们。此外，133个国家已将保护和隐私法规签署成为法律，15个国家正在起草过程中，46个国家尚未制定相关法规。许多国家对现有的法规进行了更新，以反映新的协议和规范。

自上次迭代以来，更多国家实施了要求通报违规的措施。在本版本中，102个国家在立法和政策中引入了数据泄露和事件通报要求。

图2：采取违规通知措施的国家数量



来源：国际电联

网络身份和数据盗窃

虽然各国已对非法访问采取行动，但网络身份和数据盗窃立法仍缺乏关注，网络身份保护非常重要，尤其是在当前向数字环境转变的情况下。世界人口已经通过社交媒体和工作实践转移到网上，这需要相当大的安全性，因为被盗的身份可在个人上和职业上对日常生活带来危害。

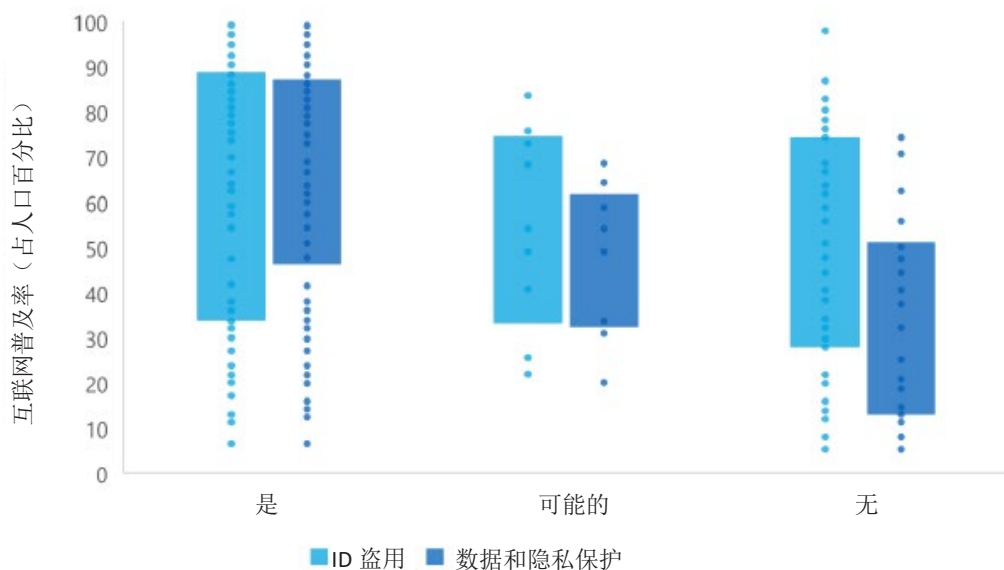
图3：对窃取个人信息有立法的国家数量



来源：国际电联

如图4所示，在查看互联网普及率中位数和平均数时，互联网普及率高的国家比互联网普及率低的国家更有可能制定网络数据保护法律或法规。相比之下，数据和隐私保护法规更可能出现在互联网普及率高的国家。这些趋势部分地反映了经济状况、整体发展和政府数字化战略。值得注意的是，一些国家通过积极制定与身份盗窃以及数据和隐私保护相关的法律，为更大的互联网渗透做好了准备。

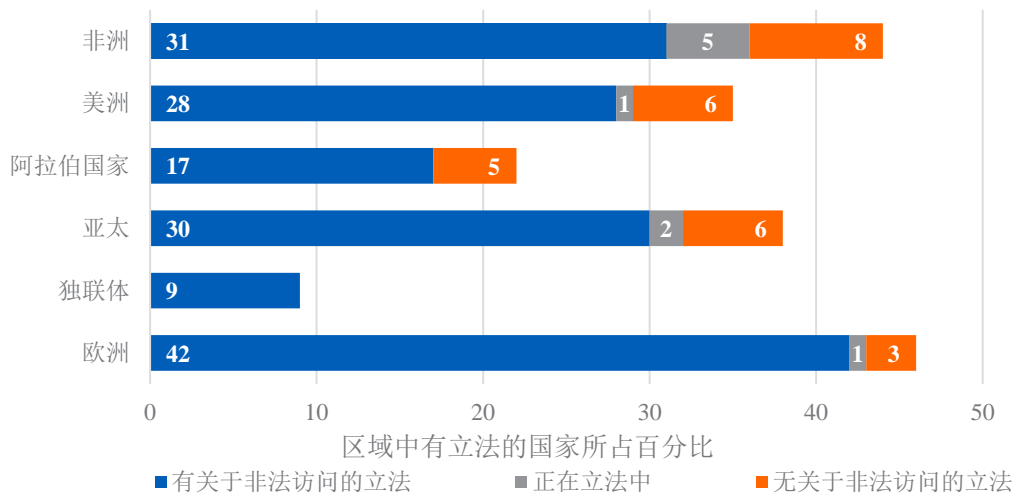
图4：关于身份盗窃以及数据与隐私保护的立法，绘制在互联网接入上（人口百分比）



来源：国际电联世界电信/ICT指标

如图5所示，大多数国家都有关于非法访问的立法，各区域之间几乎没有显著差异。

图5：关于非法访问的立法



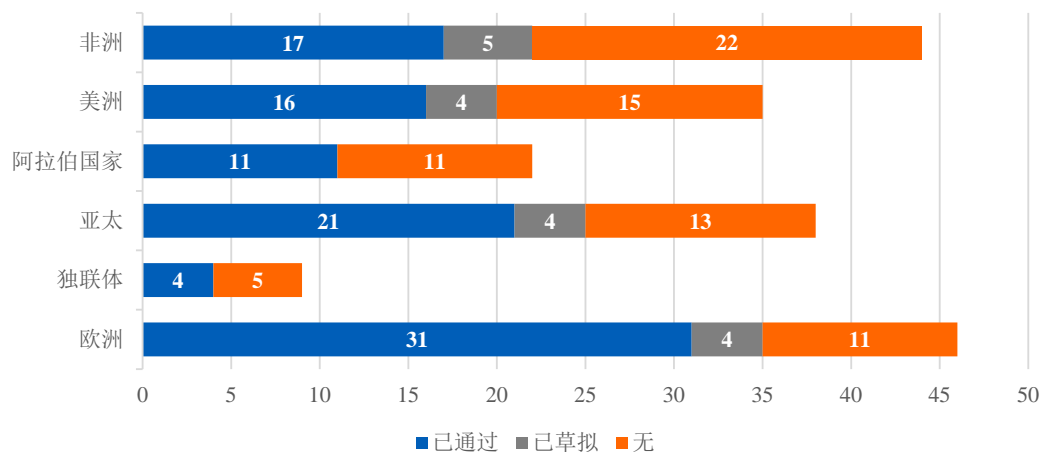
来源：国际电联世界电信/ICT指标

网络反社会行为

网络反社会行为是一项持续的挑战，各国正在增加立法支持。GCI衡量两个方面的问题：网络骚扰，以及网络种族主义和仇外心理。

网络骚扰仍然是一个长期存在的问题：2020年，在美国，“41%的美国人亲身经历过某种形式的网络骚扰”⁷，欧盟至少有十分之一的女性经历过网络骚扰⁸。在对32个国家的成年人进行的一项调查中，五分之一的成年人报告说经历过网络仇恨言论⁹。

图6：对网络骚扰有立法的国家



来源：国际电联世界电信/ICT指标

在全球范围内，有100个国家通过了将网络骚扰和滥用行为定为刑事犯罪的立法，17个国家正在起草和实施这些措施，77个国家没有关于该主题的立法。然而，什么是滥用通常是不明确的。

解决网络种族主义和仇外心理的工作有待进一步明确，但相当多的国家正在朝着这个方向起草某种形式的法律。一些国家正在将有关种族主义和仇外心理的线下法律扩展或调整到网络情形中。构成犯罪的门槛差别很大，因为在一个国家可能合法的行为在另一个国家可能构成应受惩罚的犯罪。然而，一些国家已决定制定专门针对网络种族主义行为的条款。

2.2 技术措施：增加部署 CIRT/CERT

在国家层面，需要有效的机制和制度结构来可靠地应对网络威胁和事件。计算机事件响应小组（CIRT）或计算机应急响应小组（CERT）使各国能够使用集中联系人在国家层面对事件做出响应，并促进快速和系统的行动，使各国能够从经验中学习并建立网络安全弹性。

⁷ <https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/>

⁸ https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/factsheet_lets_put_an_end_to_violence_against_women_en.pdf

⁹ https://blogs.microsoft.com/on-the-issues/2020/11/13/microsoft-study-online-risks-world-kindness-day/#_edn1

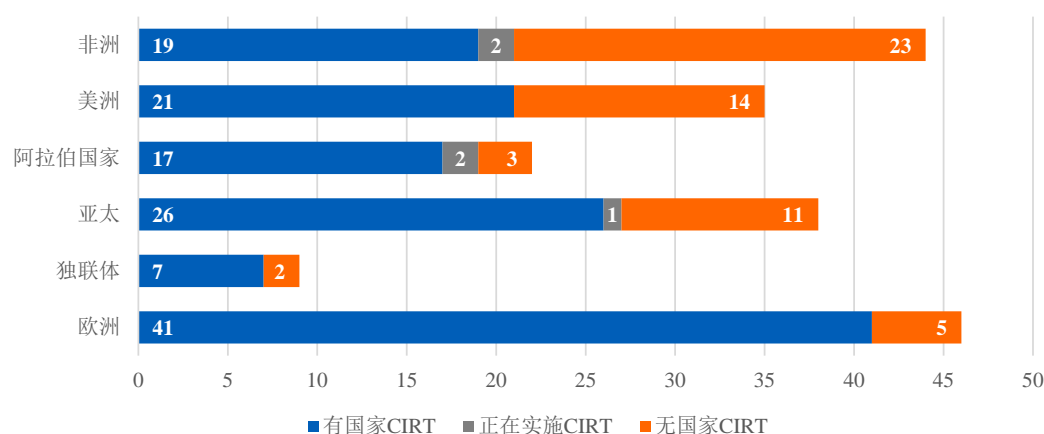
国家CIRT通常根据立法或国家政策来制定和实施。CIRT可以是政府机构的一部分，也可以隶属于特定部委或其他实体。在国家缺乏时间、知识或资源来建立国家CIRT的情况下，一些国家会将CIRT职责外包给第三方。

正在建立新的CIRT

截至2020年底，已有131个国家建立了国家CIRT，包括自2018年全球网络安全指数以来新建立的10个国家。目前有另外4个国家CIRT正在开发中。

虽然许多国家在实施CIRT方面取得了进展，但许多国家、尤其是最不发达国家（LDC）在建立CIRT方面面临重大障碍。缺乏资源、技术知识、网络安全生态系统、研究和开发、优先排序以及政治意愿都可能阻碍旨在应对网络安全挑战的技术措施方面的努力。

图7：有国家CIRT的国家数量



来源：国际电联

尽管非洲区域在技术领域并不领先，但自2018年全球网络安全指数以来又开发了六个CIRT，该区域已从13个国家有国家CIRT增加到了19个国家。美洲区域有21个CIRT，阿拉伯国家区域有17个国家有国家CIRT。然而，在独联体区域，只有2个国家没有国家CIRT，在欧洲区域，只有6个国家没有国家CIRT。

GCI还跟踪CIRT活动。在131个已实施的CIRT中，有11个参与了以下所有活动：

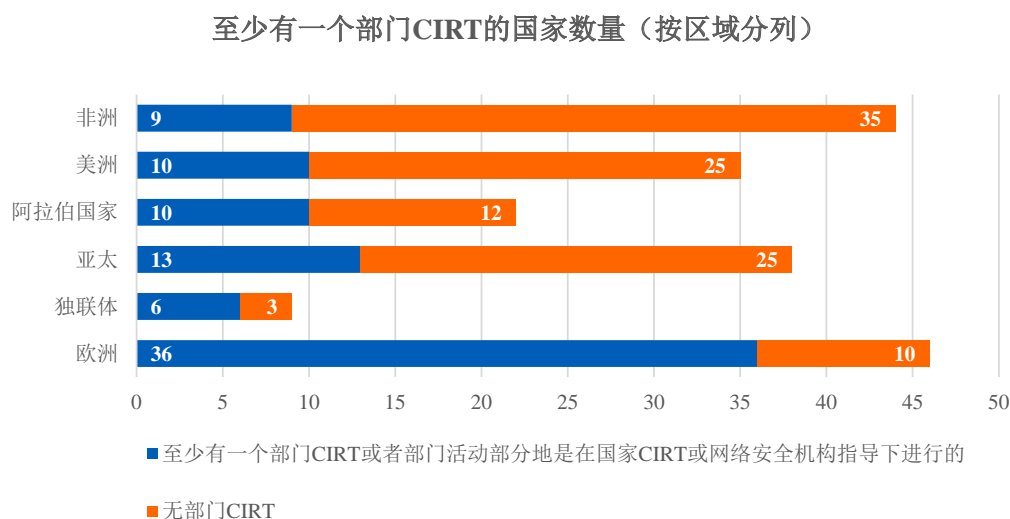
- 通过提供技巧、指南、手册、培训和视频来提高网络安全意识和儿童上网保护；
- 向IT专家提供网络安全建议；
- 在过去两年间开展了网络演习；
- 参与区域CIRT和FIRST¹⁰；

¹⁰ www.first.org

- 由可信的介绍人进行认证¹¹或进行其他公认认证。

国家CIRT解决国家层面的问题，而特定部门的CIRT则解决特定部门的网络安全需求，例如，卫生、交通、电信、公用事业。其他类型的CIRT服务于跨国公司或大型公司、私立大学等，在本GCI报告中未跟踪研究这些其他类型的CIRT。

图8：部门CIRT的数量



来源：国际电联

如图8所示，三分之二的国家没有特定部门的CIRT。在有特定部门CIRT的76个国家中，有37个国家开展了宣传活动、网络演习，并与其社区公开地或保密地分享了与事件和威胁有关的信息。

2.3 组织措施：调整战略

组织措施检查各国家内应对网络安全问题的治理和协调机制。组织措施包括确保维持最高行政层面的网络安全，将相关的角色和职责分配给各种各样的国家实体，并使之对国家网络安全态势负责。

在拥有强大电信基础设施的国家中，并不总是存在组织措施。将可持续发展电信基础设施指数十年行动中关于数字政府的2020年联合国电子政务调查数据、部分电子政务就绪指数¹²与组织措施中的总分进行比较表明，虽然存在疲软趋势，但仍有许多国家目前在电信基础设施措施方面做得比较好，但没有组织措施来解决网络安全问题。

缺乏足够的组织措施可导致国家网络安全治理缺乏明确的责任和问责制，并可阻碍有效的政府内和部门间协调。

¹¹ www.trusted-introducer.org/

¹² <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020>

最新国家网络安全战略的重要性

国家网络安全战略（NCS）通常是国家网络安全层面组织措施的关键基石。根据国际电联有关制定国家网络安全战略的指南，NCS是一个综合框架或战略，必须以多利益攸关方的方式来制定、实施和执行，以处置政府当局、私营部门和民间社会各方有关预防、准备、响应和事件恢复的协调行动¹³。

越来越多的国家正在制定国家网络安全战略（NCS），以更加结构化的方式来管理网络安全。一个NCS可带来多种好处，包括国家召集相关利益攸关方、明确国家优先事项以及规划网络安全能力发展。

随着全球网络安全指数的成熟，人们越来越关注定期更新其NCS的国家，以确保它们适应不断变化的现实。事实上，有NCS是各国积极显示关注网络安全问题姿态的第一步，但需要根据网络安全威胁和优先事项的变化定期进行修订。各国在更新NCS时通常采用一个4-5年的时间框架。一些国家选择了更长的时间框架，跨越十年或更长的时间。

有127个国家制定了国家网络安全战略，无论是当前的、五年以上的还是正在起草中的，其中60个国家通过修订和制定新的网络安全战略或更新其行动计划，在制定更明确的目标方面取得了进展。

保护关键基础设施/国家弹性

国家网络安全战略发展过程中的一个重要方面是制定一套明确的、有关保护关键基础设施的目标。确保国家层面的业务连续性是各国面临的一项持续挑战。电网、净水厂和交通系统等关键基础设施继续面临网络安全风险。影响关键基础设施的事件的潜在后果很严重，该战略应引起对旨在降低严重后果事件之可能性和升级的风险管理工作的更多关注。

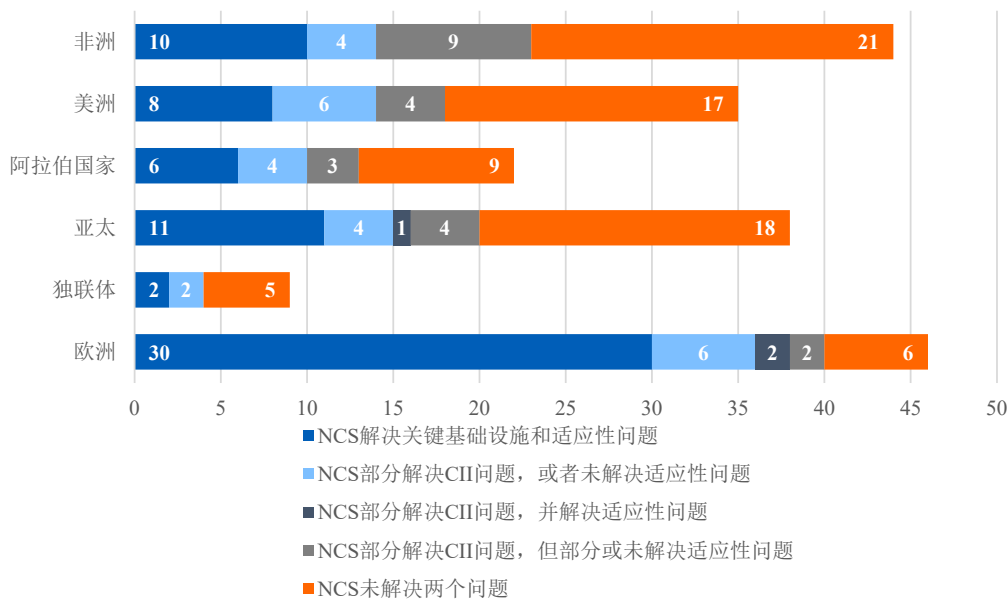
明年，有关关键基础设施的网络安全支出预计将增加到90亿美元，到2021年将达到1059.9亿美元¹⁴。随着关键基础设施与其他劳动力一样转向与社会保持一定距离的工作条件，它们需要平衡增加的攻击面。ABI Research指出，网络安全投资因区域、行业和连通性而异，其中国防、金融服务和ICT方面的支出最高，但工业领域的支出落后¹⁵。

¹³ <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx>

¹⁴ <https://www.abiresearch.com/press/cybersecurity-spending-critical-infrastructure-surpass-us105-billion-2021/>

¹⁵ <https://www.abiresearch.com/press/cybersecurity-spending-critical-infrastructure-surpass-us105-billion-2021/>

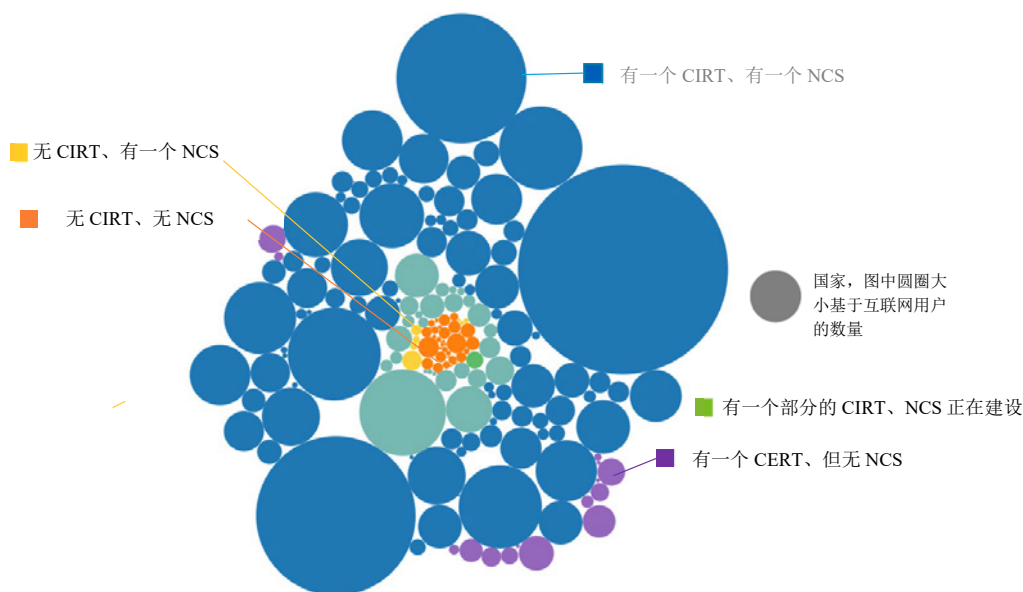
图9：着手解决关键基础设施和弹性问题的国家数量



来源：国际电联

作为关键基础设施和弹性的一部分优先考虑网络安全问题不仅体现在预算承诺中，还体现在国家网络安全战略中。国家网络安全战略更多地涉及关键基础设施和/或网络安全弹性。然而，许多国家尚未做到这两点。

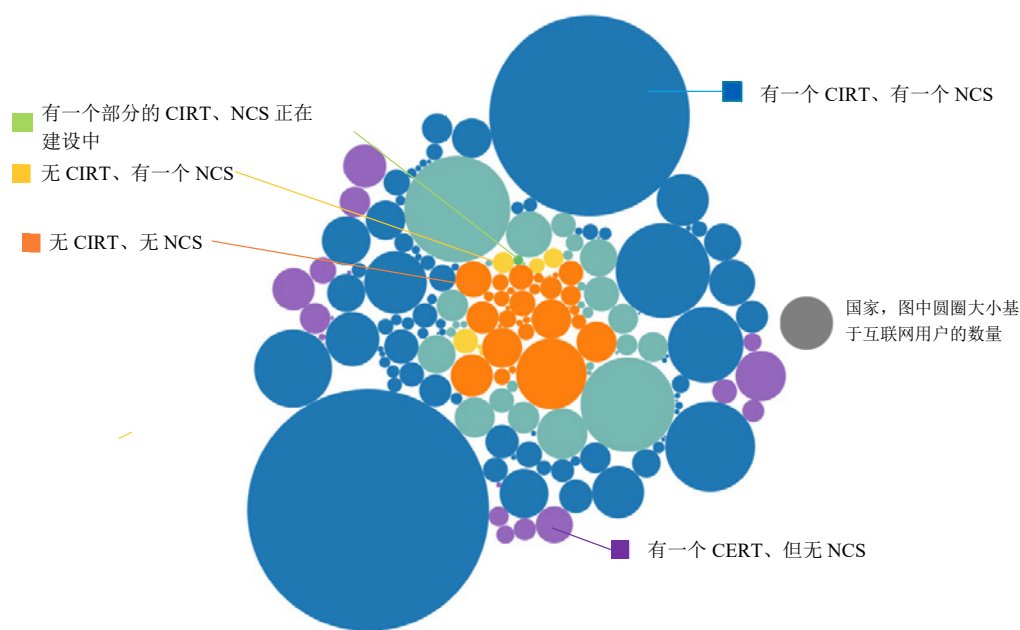
图10：互联网用户（按CIRT和国家网络安全战略覆盖范围分列）



来源：全球网络安全指数、国际电联世界电信/ICT指标

从互联网用户数量来看世界各国时，超过95%的互联网用户位于既拥有国家网络安全战略又拥有国家CIRT的国家中。

图11: 未连接人口的规模 (按CIRT和国家网络安全战略覆盖范围分列)



来源: 全球网络安全指数、国际电联世界电信/ICT指标

然而，连接较少的国家通常缺乏NCS和/或国家CIRT。9%的未连接人口生活在没有国家CIRT或国家网络安全战略的国家中，另外15%生活在没有战略但有国家CIRT的国家中。超过一半的最不发达国家没有CIRT，60%缺乏或尚未开启制定国家网络安全战略的进程。

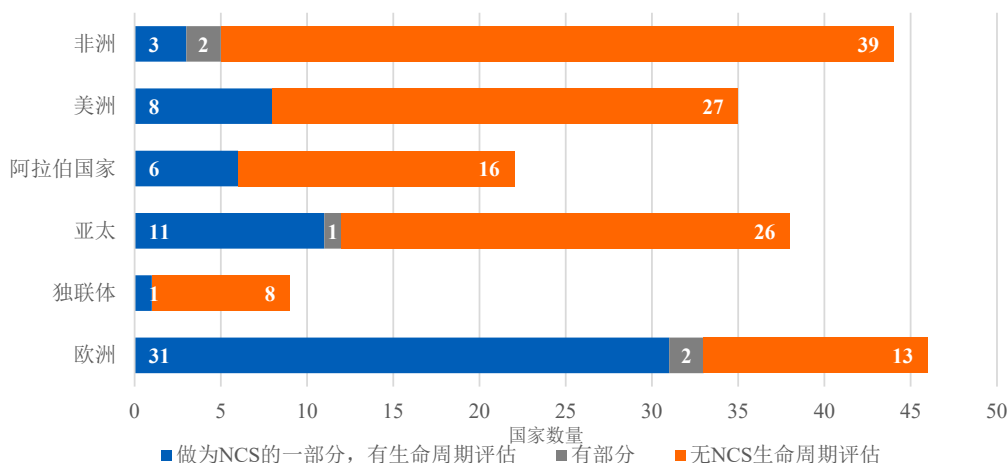
表1: 有NCS和CIRT的国家数量

	有NCS	NCS正在建设中或者>5年	无NCS
有国家CIRT	90个国家	29	18
无国家CIRT	7	1	49

来源: 国际电联

没有国家战略的国家不太可能拥有CIRT。毫不奇怪，在没有CIRT的63个国家与没有NCS的67个国家当中，有49个国家既没有CIRT也没有NCS。

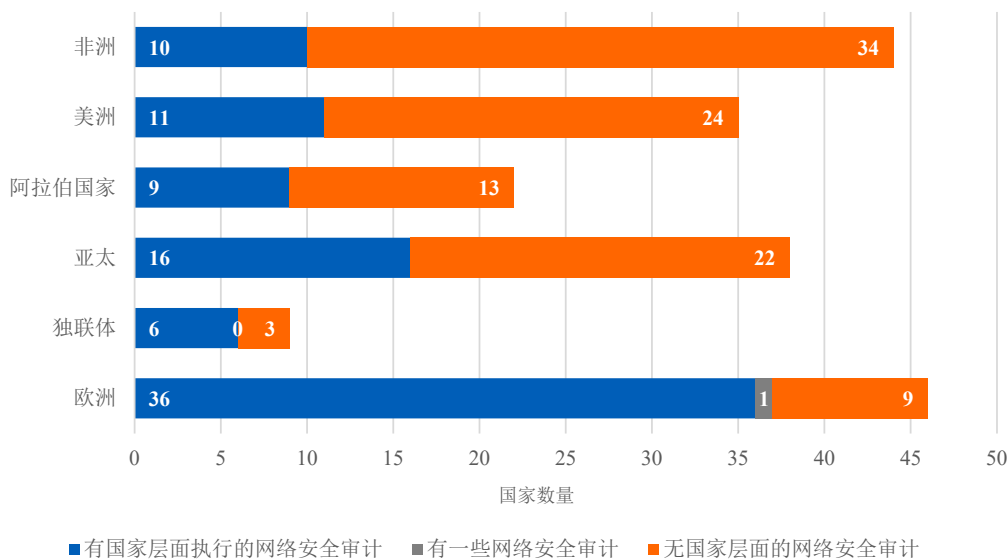
图12: 作为NCS一部分的生命周期评估



来源: 国际电联

制定国家网络安全战略是有关网络安全态势的积极的第一步, 但需要定期更新和修订。许多有NCS的国家并没有根据网络安全威胁和优先事项的变化定期进行修订和调整。在有最新NCS的98个国家中, 只有60个国家将生命周期评估融入了其战略。

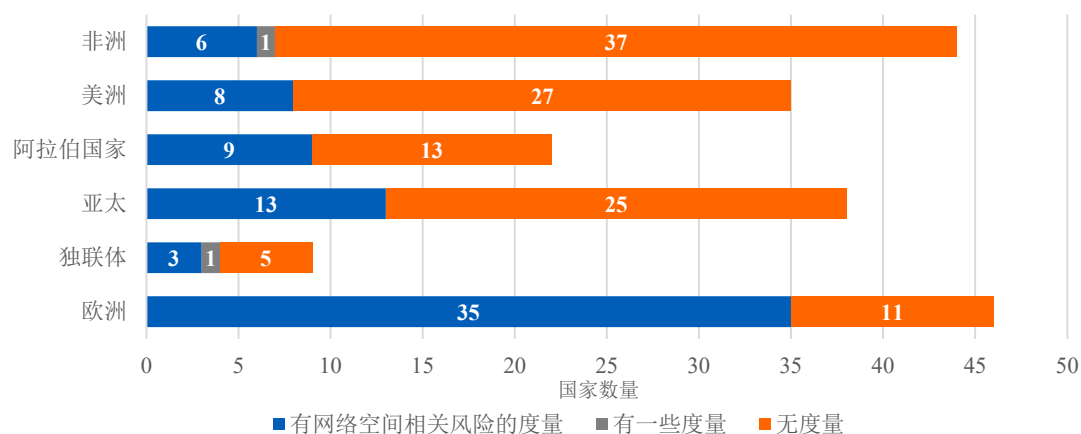
图13: 在国家层面执行的国家网络安全审计



来源: 国际电联

国家网络安全审计 (图 13) 比生命周期评估更常见。这些审计的频率没有作为本GCI迭代的一部分进行评估。

图14：在国家层面用于评估网络空间相关风险的指标



来源：国际电联

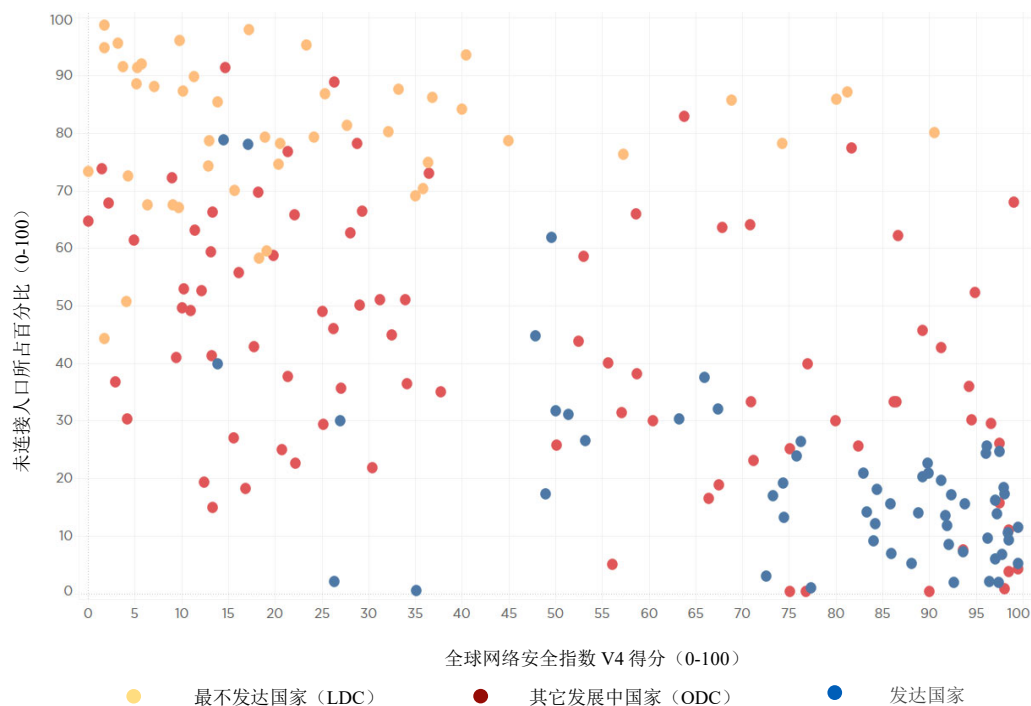
同样，大多数国家没有国家层面的、用于评估网络空间相关风险的指标。缺乏这些指标会使各国更难评估当前风险、优先考虑网络安全干预措施并对进展情况进行跟踪。

2.4 能力发展措施：发展网络安全能力

世界经济论坛估计，“每天大约有100万人第一次上网，全球三分之二的人口拥有一部移动设备。”¹⁶ 虽然数字技术的优势带来了巨大的经济和社会效益，但网络风险可以抵消数字化的好处。通过网络安全能力建设活动来保护网络领域的安全至关重要，因为它有助于减少诸如数字鸿沟和网络风险等问题。

¹⁶ <https://reports.weforum.org/global-risks-report-2020/executive-summary/>

图15: 全球网络安全指数和未连接人口



来源：全球网络安全指数、国际电联世界电信/ICT指标

如图15所示，在全球网络安全指数中表现较差的国家更有可能是最不发达国家，并且其人口中未连接的比例很高。随着这些人开始变得更多连接，他们需要支持来发展网络安全能力，以更好地应对威胁。然而，许多国家、尤其是最不发达国家，在弥合网络能力差距方面更可能面临资源方面的挑战，包括缺乏制度知识、政策限制、技能短缺等，以便在物理上和虚拟上保护其ICT系统的安全。

孟加拉国、贝宁、卢旺达和坦桑尼亚等最不发达国家中，有几个国家表现出强烈的网络安全承诺。值得注意的是，这些国家都报告说有国家网络安全产业，这是能力发展措施的一个关键特征。

图16: 可持续发展目标（8、9、10）



来源：联合国 (<https://sdgs.un.org/goals>)

为了促进体面工作和经济增长、建设有弹性的基础设施、促进包容性和可持续的工业化以及促进创新，并缩小国家内和国家间的差距，网络安全能力发展对加强旨在增强国家能力的流程、技能、资源以及研究与开发而言是必要的。网络安全能力还加强了集

能力的发展以及促进了国际合作与合作伙伴关系，以有效应对数字安全方面的网络相关挑战。

能力发展工具和措施有助于管理与网络相关的风险，保护公民、基础设施、企业，并建立更强大的网络社区。

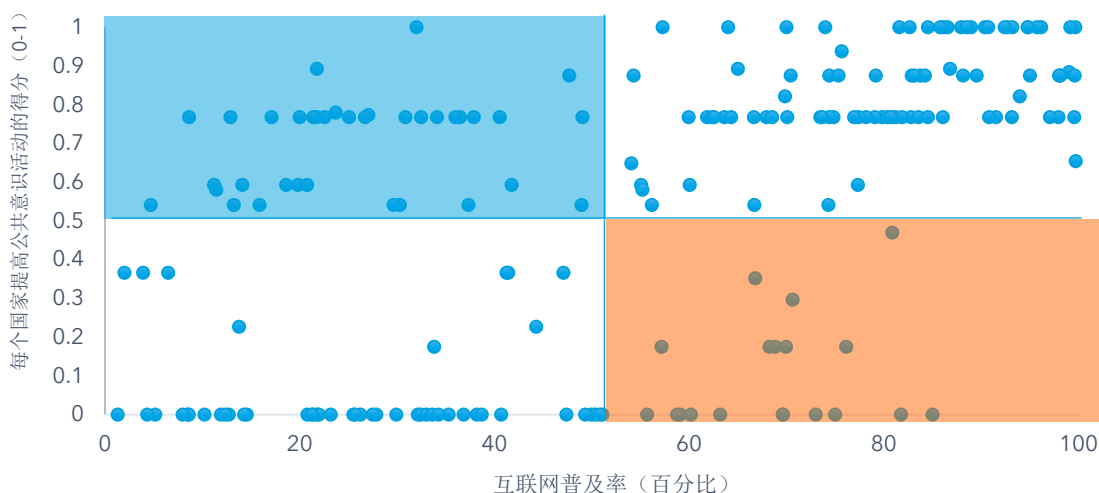
提高公众对网络安全问题的认识

有效提高对网络安全问题的认识对保持公民、企业、政府、青年和组织的警觉而言至关重要。随着当前向数字服务的转变，政府需要确保所有用户都了解其在开展数字活动过程中可能面临的风险。

当将提高公众对网络安全问题认识的活动与互联网普及率进行对比时，国家分为四大类：

- 1) 互联网普及率低/提升对网络安全问题的认识（图17中的蓝色框）：这些国家准备更好地连接未连接的人，并为人们提供上网所需的安全知识。
- 2) 互联网普及率低/不提升对网络安全问题的认识：这些国家尚未连接未连接的人，未为人们提供网络安全方面的宣传资源。
- 3) 互联网普及率高/提升对网络安全问题的认识：这些国家已实现数字连接，并参与提升网络安全意识的活动，以帮助促进安全的上网行为。
- 4) 互联网普及率高/不提升对网络安全问题的认识（图17中的橙色框）：这些国家已实现数字连接，但其民众可能并未意识到网络风险。

图17：（与互联网普及率相比，每个国家的）提高公共网络安全认识活动得分



来源：国际电联

针对残疾人和老年人的提高公众认识活动

尽管互联网和数字世界带来了前所未有的机会，但在实施决策和技术方案时，通常不会考虑残疾人和老年人。到2021年，估计有7.52亿65岁或65岁以上的人¹⁷。通过将这一数字与有针对残疾人和老年人开展提高认识活动的国家数量进行比较，结果明显偏低。在194个国家中，只有18%的国家在提高残疾人对该问题的认识，只有25%的国家开展了针对老年人的活动。有针对这两个特定人群的提高认识活动的国家数量少得令人震惊，这造成了巨大的数字鸿沟和差距，因为正在敦促残疾人和老年人使用数字服务，例如，COVID-19接触者追踪应用程序（APP）。

更加关注中小企业 (SME)、私营部门和政府的网络意识

在COVID-19大流行期间，业务运营进一步转向网络，这对私营部门网络安全做法提出了更高的要求。中小企业通常是一个国家内最常见的企业规模，因为90%的企业是中小企业，50%的就业来自中小企业，正规的中小企业对新兴经济体GDP的贡献高达40%¹⁸。中小企业通常也最不能应对网络安全问题。这使得中小企业需要提高对网络安全问题认识的活动。

图18：针对中小企业、私营部门和政府机构开展提高网络安全认识活动的国家数量



来源：国际电联

GCI的结果显示，约60%的国家正在或在过去两年中已经致力于提高中小企业、私营部门公司或政府机构的网络意识，而38%的国家未报告有任何有关网络安全的宣传活动。它们通过向目标群体通报网络安全和网络安全基线、通过诸如国家CIRT等来提供资源或者通过提供保护网络安全的工具等形式来参与。2%的国家正处于针对中小企业、私营部门公司和政府机构开展活动的早期阶段。

各国政府认识到需要针对特定部门的教育计划和针对网络安全专业人员的培训

提供培训计划以满足不同部门的需求变得越来越重要。网络安全分析师预测，到2021年，全球将有350万¹⁹到多达400万²⁰个的网络安全工作岗位空缺。尽管存在这一预计缺口，但仍有大量国家尚未开展针对特定部门的培训，超过50%的国家缺乏针对特定部门或专业的计划，例如，执法、法律行为者、中小企业、私营公司和政府官员。

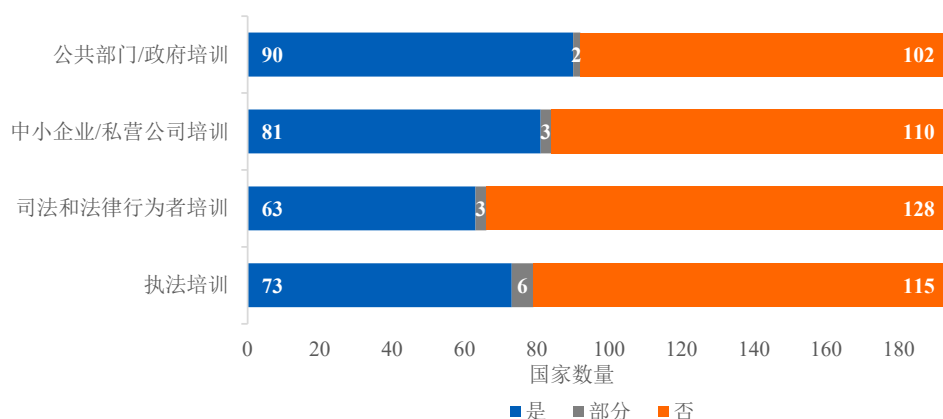
¹⁷ <https://population.un.org/wpp/DataQuery/>

¹⁸ <https://www.worldbank.org/en/topic/sme/finance>

¹⁹ <https://cybersecurityventures.com/jobs/>

²⁰ ESG研究报告：2019年数字工作调查（esg-global.com）

图19: 为专业人士提供特定网络安全教育计划/培训的国家数量



来源: 国际电联

如图19所示, 46% (90个) 国家报告为公共部门和政府官员提供了国家部门特定的网络安全培训, 41% (81个) 国家正在为包括中小企业和私营部门在内的IT专业人员提供关于网络安全问题的能力建设练习, 37% (73个) 国家正在为执法人员提供关于网络安全问题的能力建设练习, 32% (63个) 国家确保司法和其他法律行为者在确保弹性和安全方面不落伍。

各国报告称, 这些网络安全培训是通过其国家CIRT、国家网络安全中心以及政府批准或认可之其他区域和国际机构提供的培训来提供的。一些国家寻求增加网络安全专业人员的数量, 但无法提供基于国家的培训, 以及由网络安全认证机构 (例如, SANS²¹、ISC²、ICSPA²²、ISACA²³等) 提供的、经认可的国际培训。

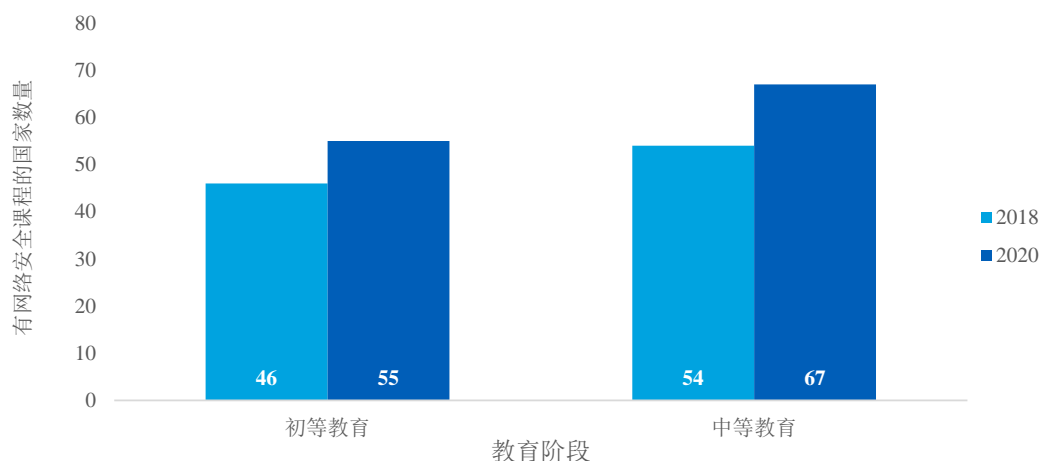
中小学网络安全课程正变得越来越普遍

随着各国转向提供网络教育, 网络安全和网络安全课程不仅在高等教育中教授, 也在中小学中教授。

²¹ <https://www.sans.org/>

²² <https://icspa.org/about-us/>

²³ <https://www.isaca.org/>

图20：将网络安全课程纳入国家学术课程的国家数量（按教育阶段分列）

来源：国际电联

如图20所示，自2018年全球网络安全指数发布以来，各国正在将更多的网络安全课程纳入国家教育课程。5%以上的国家（46-55）在小学教育中提供了关于保护儿童上网安全的入门课程，7%以上的国家（54-67）在中学学术课程中为有志于将网络安全作为一种职业的学生提供了资源，以便在很小的时候就能开始学习它。

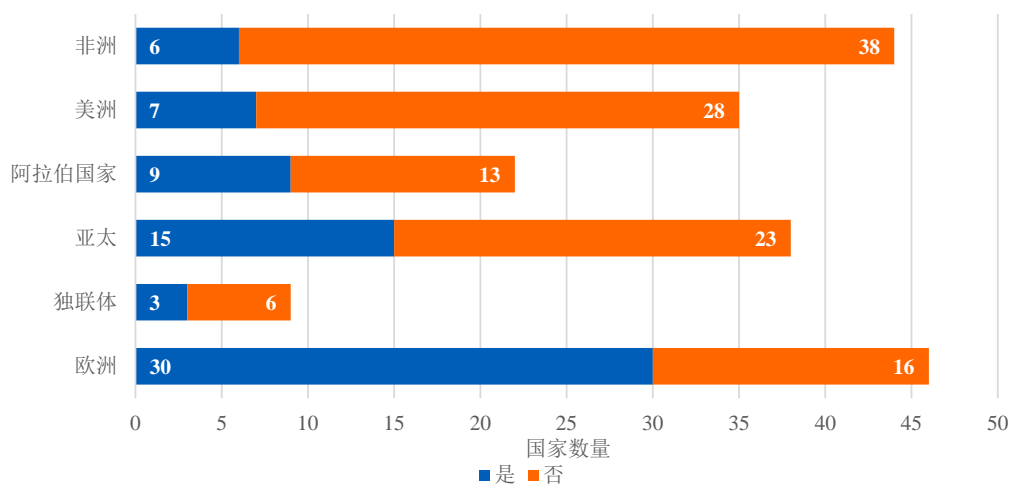
政府对网络安全发展的激励措施存在滞后现象

在国家层面促进网络安全需要同时促进网络安全文化、鼓励商业领袖转变态度、从网络安全作为一个与信息技术相关的问题转向一个更全面的观点，重视网络安全在改善整体业务效率和性能方面的作用。在组织中优先考虑网络安全问题是一个需要保证基础设施和机制可用性以鼓励采用网络安全措施的过程。促进私营部门网络安全发展和鼓励网络安全相关公司发展的国家体现在将激励措施纳入其网络安全框架中。

各国可通过激励机制来促进私营部门采用网络安全，例如，基于网络安全参数的税收激励、免税期或将网络安全标准作为合同的一部分。这些将鼓励私营部门参与者在运营结构和流程中优先考虑网络安全，从而在短期、中期和长期改善一个国家的网络安全态势。

然而，本版GCI显示，124个国家没有提供任何网络安全激励措施，反映出成员国需要采取此类激励措施来快速跟踪网络安全措施。

图21: 有网络安全能力发展激励机制的国家数量



来源: 国际电联

2.5 合作措施: 解决集体网络安全行动

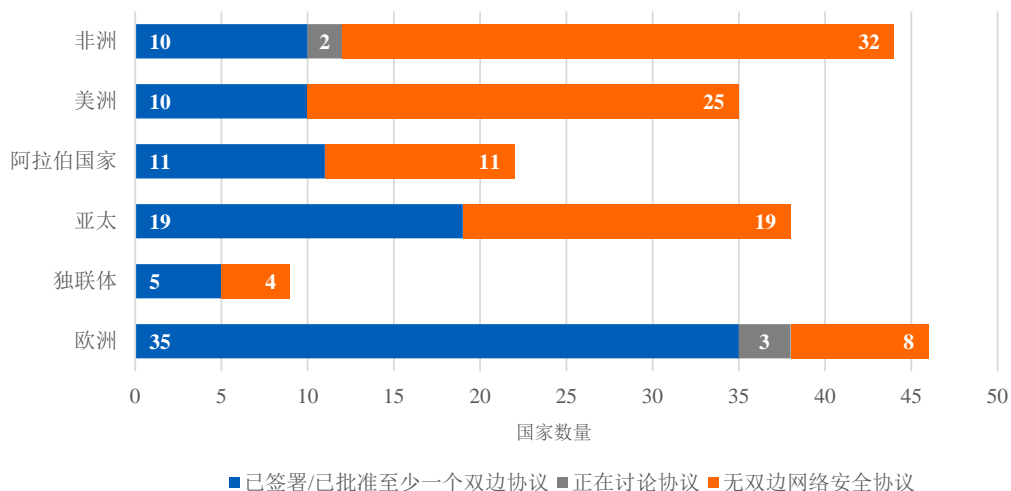
网络安全风险越来越无国界²⁴, 协作仍然是应对网络安全挑战的重要工具。由于互连和相关基础设施的增加, 网络安全仍然是一个跨国问题。全球网络生态系统的安全不能由任何单个的利益攸关方来保证或管理, 它需要国家、区域和国际合作来扩大影响力。在本合作支柱中, 问卷调查表收集了有双边和多边协议的国家以及参与机构间和公私合作伙伴关系的国家。网络安全合作的典型目标包括最低安全措施的协调、信息和良好做法的共享以及行为规范的编纂。

双边和多边协议

双边和多边协议对编纂规范和行为以及加强网络安全国际合作而言至关重要。

²⁴ <https://risk.lexisnexis.com/global/en/insights-resources/infographic/cybercrime-report-infographic-july-december-2019>

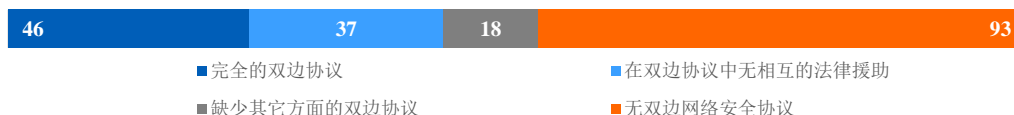
图22：参与双边网络安全协议的国家数量



来源：国际电联

提取的数据显示，有90个国家在网络安全方面达成了双边协议。对于GCI中跟踪的协议，一些国家正在签署能力发展领域的网络安全协议。在某些情况下，该协议仅涉及共享信息，网络安全并不总是协议的核心项目，而是作为其他主题的一部分。37个国家的双边协议包括信息共享和能力发展措施，但不涉及相互法律援助。

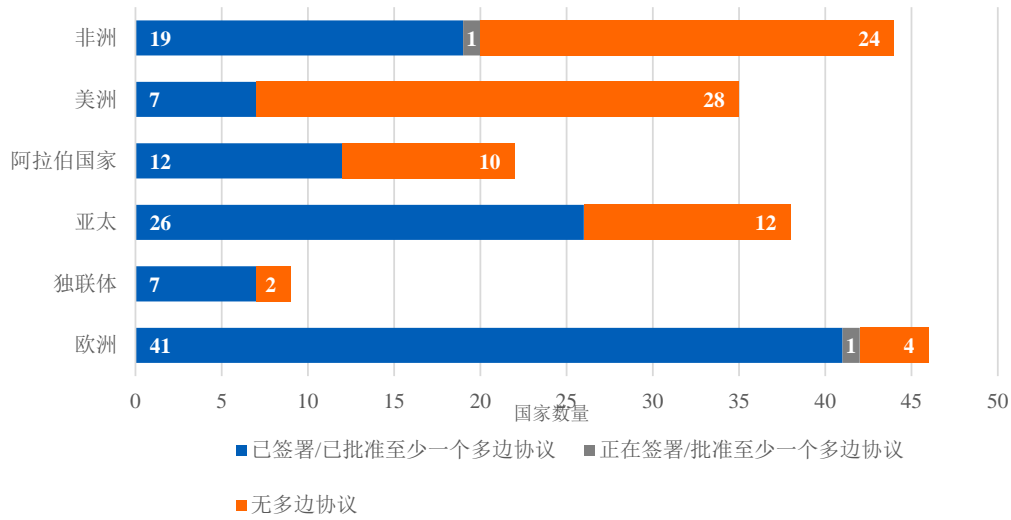
图23：有双边网络安全协议的国家数量（按涵盖的主题分列）



来源：国际电联

鉴于网络安全的集体行动问题，一些国家不仅致力于确保签署双边协议，而且确保签署多边协议。对于全球网络安全指数的本次迭代，多边协议是三方或更多方之间的协议，包括政府和区域组织，但不包括《布达佩斯网络犯罪公约》等国际公约。

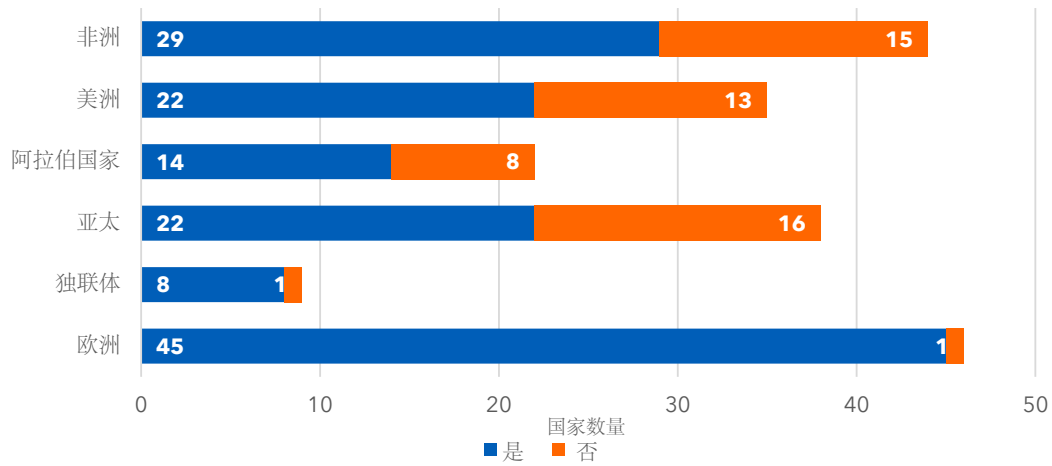
图24: 参与多边网络安全协议（已签署和已批准）的国家数量



来源: 国际电联

相比双边协议, 各国更有可能达成多边协议, 近57%的国家签署了多边协议, 而签署双边协议的国家为46%。此外, 许多国家(99个)签署或批准了关于信息共享和能力发展的多边协议。

图25: 国际活动参与情况



来源: 国际电联

除了两国或多个国家之间的正式合作外, 参与国际活动为各国提供了了解应对网络安全威胁良好做法和新方法的机会。过去两年间, 140个国家参加了诸如网络安全会议、讲习班、合作伙伴关系以及与其他国家的公约等国际活动。

公私合作伙伴关系

除了与其他国家开展合作外，各国还与私营部门的参与者开展合作。公私合作伙伴关系（PPP）对网络安全工作而言至关重要，从共享可操作的情报、交流良好做法，到交流研发需求和优先事项。表2列出了参与国际和/或国内PPP的国家数量。

表2：参与国际和/或国内PPP的国家数量

	有国际PPP	正在建设国际PPP	无国际PPP
有国内PPP	62	0	14
正在建设国内PPP	1	0	0
无国内PPP	12	1	104

来源：国际电联

为了参与更广泛的网络安全生态系统，一些国家组织了会议和讲习班，而另一些国家则与私营部门公司签约，为公共部门开展培训。越来越多的国家报告称，它们正在开发科技园区以加强其网络安全生态系统。这些平台可以作为私营和公共部门开会、提供培训、举办讲习班、协助初创企业和举办竞赛的场所。这种跨部门的举措旨在发展一种网络安全生态系统，分享来自研究人员、学生、网络安全专家、初创企业、政府机构和外国公司等各种各样利益攸关方的知识和技能。收集的数据显示，几乎一半的国家拥有至少一种类型的合作伙伴关系，86个国家参与或即将参与国际或国内PPP，其中60个国家同时参与国内和国际合作伙伴关系。

2.6 儿童上网保护

图26：国际电联儿童上网保护系列报告



来源：国际电联

正如国际电联儿童上网保护指南中所指出的，保护上网儿童是一项全球挑战，需要采取全球方法²⁵。该指南出台之际，远程学习意味着儿童比以往任何时候都更频繁地上网，而且儿童在COVID-19大流行期间面临更多风险。与前几代人因大流行而被迫通过广播进行远程学习不同²⁶，数字技术实现了交互式的双向教育体验，不仅促进了学生与学习材料之间的联系，而且促进了彼此之间的联系。

国际电联儿童上网保护指南旨在帮助儿童、家长和教育工作者管理网络风险，同时也受益于数字技术的潜力并增强其数字技能。此外，该指南还向政策制定者提供建议，以加快制定和采用完善的国家儿童上网保护战略和行动计划，并促进私营部门参与此类政策的制定。

在这方面，与儿童上网保护相关的问题通过若干项目来衡量各国为数字一代做好准备的程度，例如，保护上网儿童的现行法律、网络问题的报告机制、提高认识的活动和学校课程以及制定并遵循保护上网儿童战略的国家数量。

图27：有儿童上网保护战略的国家



来源：国际电联

根据问卷调查表，在194个国家中，有86个国家报告已采取措施来保护上网儿童。然而，收集的数据显示，在194个国家中，只有13%的国家制定了专门用于保护上网儿童的独立战略。另一方面，只有30%的国家将保护上网儿童的举措纳入更广泛的网络犯罪战略、立法或举措中。

调查结果进一步表明，欧洲区域在与上网儿童保护相关的事务上表现良好，89%的国家已全面实施与上网儿童保护相关的法律。此外，全球记录了101个报告机制，包括热线、网站、电子邮件地址和社交媒体，81个国家走得更远，分享了其上网儿童保护战略和更广泛的举措。

2.7 结论

网络安全、行为和做法都在不断演进中。无论是全球卫生紧急情况、气候变化、人口老龄化还是其他的未来挑战，数字技术都提供了一种诱人的工具来帮助推动世界向前发展。当可持续发展目标（SDG）在2030年成熟时，预计世界人口的90%，即75亿人将

²⁵ <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx>

²⁶ <https://www.washingtonpost.com/education/2020/04/03/chicago-schools-closed-during-1937-polio-epidemic-kids-learned-home-over-radio/>

在线²⁷，估计将有241亿²⁸至1250亿²⁹个IoT（物联网）设备实现连接。如果想为可持续发展目标（SDG）投入的工作得以持续，就需要网络安全来确保数字解决方案的安全、可靠和值得信赖。

COVID-19的教训之一是，需要采用跨学科和整体方法来解决诸如健康或网络安全之类的集体行动问题。处置GCI的所有支柱—法律、技术、组织、能力发展和合作措施—将需要人们相互联系并建立信任。除了在国内开展合作外，各国可能还需要支持其他应对网络安全挑战能力较弱的国家，例如，最不发达国家、小岛屿发展中国家和内陆发展中国家。

为了向前发展，各国需要解决其在网络安全方面的优势和劣势问题，并利用其竞争优势来促进总体网络能力和健康。全球网络安全指数可以帮助各国开始这一进程。为了继续下去，各国可能需要考虑：

- 定期评估其网络安全承诺，包括有意义的指标；
- 继续发展国家CIRT并进一步建立特定部门的CIRT；
- 通过明确的实施计划来监测和更新国家网络安全战略；
- 网络安全劳动力中的包容性和多样性，尤其是诸如女性和青年等代表性不足的群体；
- 定期参与国际活动，以分享良好做法、案例研究，并提高准备和响应能力；
- 提高中小微企业（MSME）的网络安全能力；以及
- 网络安全所有相关利益攸关方的定期参与，包括私营部门、学术界和民间社会。

²⁷ <https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/>

²⁸ <https://www.prnewswire.com/news-releases/global-iot-market-will-grow-to-24-1-billion-devices-in-2030-generating-1-5-trillion-annual-revenue-301061873.html>

²⁹ https://cdn.ihs.com/www/pdf/IoT_ebook.pdf

3 GCI结果：得分和排名

3.1 全球得分和国家排名

下表列出了参与问卷调查的各个国家的得分和排名。

表3：GCI结果：全球得分和排名

国家名称	得分	排名	国家名称	得分	排名
美国**	100	1	越南	94.59	25
英国	99.54	2	瑞典	94.55	26
沙特阿拉伯	99.54	2	卡塔尔	94.5	27
爱沙尼亚	99.48	3	希腊	93.98	28
大韩民国	98.52	4	奥地利	93.89	29
新加坡	98.52	4	波兰	93.86	30
西班牙	98.52	4	哈萨克斯坦	93.15	31
俄罗斯联邦	98.06	5	丹麦	92.6	32
阿拉伯联合酋长国	98.06	5	中国	92.53	33
马来西亚	98.06	5	克罗地亚	92.53	33
立陶宛	97.93	6	斯洛伐克	92.36	34
日本	97.82	7	匈牙利	91.28	35
加拿大**	97.67	8	以色列**	90.93	36
法国	97.6	9	坦桑尼亚	90.58	37
印度	97.5	10	北马其顿	89.92	38
土耳其	97.49	11	塞尔维亚	89.8	39
澳大利亚	97.47	12	阿塞拜疆	89.31	40
卢森堡	97.41	13	塞浦路斯	88.82	41
德国	97.41	13	瑞士**	86.97	42
葡萄牙	97.32	14	加纳	86.69	43
拉脱维亚	97.28	15	泰国	86.5	44
荷兰**	97.05	16	突尼斯	86.23	45
挪威**	96.89	17	爱尔兰	85.86	46
毛里求斯	96.89	17	尼日利亚	84.76	47
巴西	96.6	18	新西兰**	84.04	48
比利时	96.25	19	马耳他	83.65	49
意大利	96.13	20	摩洛哥	82.41	50
阿曼	96.04	21	肯尼亚	81.7	51
芬兰	95.78	22	墨西哥	81.68	52
埃及	95.48	23	孟加拉国	81.27	53
印度尼西亚	94.88	24	伊朗伊斯兰共和国	81.07	54

(续)

国家名称	得分	排名
格鲁吉亚	81.06	55
贝宁	80.06	56
卢旺达	79.95	57
冰岛	79.81	58
南非**	78.46	59
巴林	77.86	60
菲律宾	77	61
罗马尼亚	76.29	62
摩尔多瓦	75.78	63
乌拉圭	75.15	64
科威特	75.07	65
多米尼加共和国	75.05	66
斯洛文尼亚	74.93	67
捷克共和国	74.37	68
摩纳哥	72.57	69
乌兹别克斯坦	71.11	70
约旦	70.96	71
乌干达	69.98	72
赞比亚	68.88	73
智利	68.83	74
科特迪瓦	67.82	75
哥斯达黎加	67.45	76
保加利亚	67.38	77
乌克兰	65.93	78
巴基斯坦	64.88	79
阿尔巴尼亚	64.32	80
哥伦比亚	63.72	81
古巴	58.76	82
斯里兰卡	58.65	83
巴拉圭	57.09	84
文莱达鲁萨兰国	56.07	85
秘鲁	55.67	86
黑山	53.23	87
博茨瓦纳	53.06	88
白俄罗斯	50.57	89
亚美尼亚**	50.47	90
阿根廷	50.12	91
吉尔吉斯斯坦	49.64	92
喀麦隆	45.63	93

国家名称	得分	排名
尼泊尔共和国	44.99	94
乍得	40.44	95
布基纳法索**	39.98	96
马拉维	36.83	97
津巴布韦	36.49	98
缅甸	36.41	99
塞内加尔	35.85	100
列支敦士登**	35.15	101
苏丹	35.03	102
巴拿马	34.11	103
阿尔及利亚	33.95	104
多哥	33.19	105
牙买加**	32.53	106
冈比亚	32.12	107
苏里南	31.2	108
黎巴嫩**	30.44	109
波斯尼亚和黑塞哥维那	29.44	110
萨摩亚	29.33	111
斐济	29.08	112
利比亚	28.78	113
圭亚那	28.11	114
埃塞俄比亚	27.74	115
委内瑞拉	27.06	116
安道尔**	26.38	117
巴布亚新几内亚**	26.33	118
厄瓜多尔	26.3	119
蒙古	26.2	120
塞拉利昂	25.31	121
巴勒斯坦国	25.18	122
莫桑比克	24.18	123
马达加斯加**	23.33	124
特立尼达和多巴哥	22.18	125
阿拉伯叙利亚共和国**	22.14	126
瑙鲁**	21.42	127
汤加**	20.95	128
伊拉克**	20.71	129
几内亚**	20.53	130
老挝人民民主共和国	20.34	131
柬埔寨**	19.12	132
毛里塔尼亚	18.94	133

(续)

国家名称	得分	排名
不丹	18.34	134
斯威士兰	18.23	135
佛得角	17.74	136
索马里	17.25	137
塔吉克斯坦**	17.1	138
巴巴多斯	16.89	139
多民族玻利维亚国	16.14	140
圣多美和普林西比	15.64	141
安提瓜和巴布达	15.62	142
刚果共和国**	14.72	143
土库曼斯坦**	14.48	144
基里巴斯	13.84	145
圣马力诺	13.83	146
巴哈马	13.37	147
萨尔瓦多**	13.3	148
塞舌尔**	13.23	149
危地马拉	13.13	150
安哥拉	12.99	151
瓦努阿图	12.88	152
圣基茨和尼维斯**	12.44	153
圣文森特和格林纳丁斯**	12.18	154
纳米比亚	11.47	155
尼日尔	11.38	156
加蓬	11.36	157
圣卢西亚**	10.96	158
伯利兹	10.29	159
马里**	10.14	160
几内亚比绍	9.85	161
利比里亚	9.72	162
格林纳达	9.41	163
莱索托	9.08	164
尼加拉瓜**	9	165
所罗门群岛	7.08	166
海地	6.4	167
图瓦卢**	5.78	168
南苏丹**	5.75	169
刚果民主共和国	5.3	170
阿富汗	5.2	171

国家名称	得分	排名
马绍尔群岛**	4.9	172
东帝汶**	4.26	173
多米尼加	4.2	174
科摩罗**	3.72	175
中非共和国**	3.24	176
马尔代夫**	2.95	177
洪都拉斯**	2.2	178
吉布提	1.73	179
布隆迪	1.73	179
厄立特里亚**	1.73	179
赤道几内亚**	1.46	180
朝鲜民主主义人民共和国**	1.35	181
密克罗尼西亚*	0	182
梵蒂冈*	0	182
也门*	0	182

* 未收集数据

** 未响应问卷调查

3.2 区域得分和国家排名

表4: GCI结果: 非洲区域

国家名称	总分	区域排名
毛里求斯	96.89	1
坦桑尼亚	90.58	2
加纳	86.69	3
尼日利亚	84.76	4
肯尼亚	81.7	5
贝宁	80.06	6
卢旺达	79.95	7
南非**	78.46	8
乌干达	69.98	9
赞比亚	68.88	10
科特迪瓦	67.82	11
博茨瓦纳	53.06	12
喀麦隆	45.63	13
乍得	40.44	14
布基纳法索**	39.98	15
马拉维	36.83	16
津巴布韦	36.49	17
塞内加尔	35.85	18
多哥	33.19	19
冈比亚	32.12	20
埃塞俄比亚	27.74	21
塞拉利昂	25.31	22
莫桑比克	24.18	23
马达加斯加	23.33	24
几内亚**	20.53	25
斯威士兰	18.23	26
佛得角	17.74	27
圣多美和普林西比	15.64	28
刚果共和国**	14.72	29
塞舌尔**	13.23	30
安哥拉	12.99	31
纳米比亚	11.47	32
尼日尔	11.36	33
加蓬	11.38	34
马里**	10.14	35
几内亚比绍	9.85	36

国家名称	总分	区域排名
利比里亚	9.72	37
莱索托	9.08	38
南苏丹**	5.75	39
刚果民主共和国	5.3	40
中非共和国**	3.24	41
布隆迪	1.73	42
厄立特里亚**	1.73	42
赤道几内亚**	1.46	43

* 无数据

** 未响应问卷调查/GCI小组收集的数据

表5: GCI结果: 美洲区域

国家名称	总分	区域排名
美利坚合众国**	100	1
加拿大**	97.67	2
巴西	96.6	3
墨西哥	81.68	4
乌拉圭	75.15	5
多米尼加共和国	75.07	6
智利	68.83	7
哥斯达黎加	67.45	8
哥伦比亚	63.72	9
古巴	58.76	10
巴拉圭	57.09	11
秘鲁	55.67	12
阿根廷	50.12	13
巴拿马	34.11	14
牙买加**	32.53	15
苏里南	31.2	16
圭亚那	28.11	17
委内瑞拉	27.06	18
厄瓜多尔	26.3	19
特立尼达和多巴哥	22.18	20
巴巴多斯	16.89	21
多民族玻利维亚国	16.14	22
安提瓜和巴布达	15.62	23

表5: GCI结果: 美洲区域 (续)

国家名称	总分	区域排名
巴哈马	13.37	24
萨尔瓦多**	13.3	25
危地马拉	13.13	26
圣基茨和尼维斯	12.44	27
圣文森特和格林纳丁斯**	12.18	28
圣卢西亚**	10.96	29
伯利兹	10.29	30
格林纳达	9.41	31
尼加拉瓜	9	32
海地	6.4	33
多米尼加	4.2	34
洪都拉斯**	2.2	35

* 无数据

** 未响应问卷调查/GCI小组收集的数据

表6: GCI结果: 阿拉伯国家区域

国家名称	总分	区域排名
沙特阿拉伯	99.54	1
阿拉伯联合酋长国	98.06	2
阿曼	96.04	3
埃及	95.48	4
卡塔尔	94.5	5
突尼斯	86.23	6
摩洛哥	82.41	7
巴林	77.86	8
科威特	75.05	9
约旦	70.96	10
苏丹	35.03	11
阿尔及利亚	33.95	12
黎巴嫩**	30.44	13
利比亚	28.78	14
巴勒斯坦国	25.18	15
阿拉伯叙利亚共和国**	22.14	16
伊拉克**	20.71	17
毛里塔尼亚	18.94	18
索马里	17.25	19
科摩罗**	3.72	20

国家名称	总分	区域排名
吉布提	1.73	21
也门*	0	22

* 无数据

** 未响应问卷调查/GCI小组收集的数据

表7: GCI结果: 亚太区域

国家名称	总分	区域排名
大韩民国	98.52	1
新加坡	98.52	1
马来西亚	98.06	2
日本	97.82	3
印度	97.49	4
澳大利亚	97.47	5
印度尼西亚	94.88	6
越南	94.55	7
中国	92.53	8
泰国	86.5	9
新西兰**	84.04	10
孟加拉国	81.27	11
伊朗伊斯兰共和国	81.06	12
菲律宾	77	13
巴基斯坦	64.88	14
斯里兰卡	58.65	15
文莱达鲁萨兰国	56.07	16
尼泊尔共和国	44.99	17
缅甸	36.41	18
萨摩亚	29.33	19
斐济	29.08	20
巴布亚新几内亚**	26.33	21
蒙古	26.2	22
瑙鲁**	21.42	23
汤加**	20.95	24
老挝人民民主共和国	20.34	25
柬埔寨**	19.12	26
不丹	18.34	27
基里巴斯	13.84	28
瓦努阿图	12.88	29
所罗门群岛	7.08	30
图瓦卢**	5.78	31
阿富汗	5.2	32

表7: GCI结果: 亚太区域 (续)

国家名称	总分	区域排名
马绍尔群岛**	4.9	33
东帝汶**	4.26	34
马尔代夫**	2.95	35
朝鲜民主主义人民共和国**	1.35	36
密克罗尼西亚*	0	37

* 无数据

** 未响应问卷调查/GCI小组收集的数据

表8: GCI结果: 独联体区域

国家名称	总分	区域排名
俄罗斯联邦	98.06	1
哈萨克斯坦	93.15	2
阿塞拜疆	89.31	3
乌兹别克斯坦	71.11	4
白俄罗斯	50.57	5
亚美尼亚**	50.47	6
吉尔吉斯斯坦	49.64	7
塔吉克斯坦**	17.1	8
土库曼斯坦**	14.48	9

* 无数据

** 未响应问卷调查/GCI小组收集的数据

表9: GCI结果: 欧洲区域

国家名称	总分	区域排名
英国	99.54	1
爱沙尼亚	99.48	2
西班牙	98.52	3
立陶宛	97.93	4
法国	97.6	5
土耳其	97.5	6
卢森堡	97.41	7
德国	97.41	7
葡萄牙	97.32	8
拉脱维亚	97.28	9
荷兰**	97.05	10
挪威**	96.89	11
比利时	96.25	12

国家名称	总分	区域排名
意大利	96.13	13
芬兰	95.78	14
瑞典	94.59	15
希腊	93.98	16
奥地利	93.89	17
波兰	93.86	18
丹麦	92.6	19
克罗地亚	92.53	20
斯洛伐克	92.36	21
匈牙利	91.28	22
以色列**	90.93	23
北马其顿共和国	89.92	24
塞尔维亚	89.8	25
塞浦路斯	88.82	26
瑞士**	86.97	27
爱尔兰	85.86	28
马耳他	83.65	29
格鲁吉亚	81.07	30
冰岛	79.81	31
罗马尼亚	76.29	32
摩尔多瓦	75.78	33
斯洛文尼亚	74.93	34
捷克共和国	74.37	35
摩纳哥	72.57	36
保加利亚	67.38	37
乌克兰	65.93	39
阿尔巴尼亚	64.32	40
黑山	53.23	41
列支敦士登**	35.15	42
波斯尼亚和黑塞哥维那	29.44	43
安道尔**	26.38	44
圣马力诺	13.83	45
梵蒂冈*	0	46

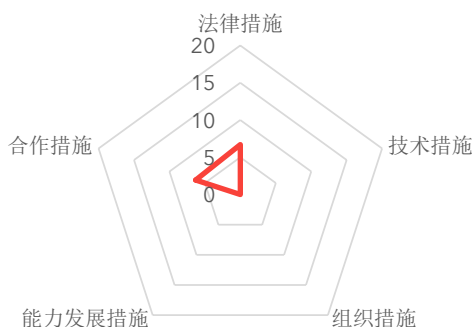
* 无数据

** 未响应问卷调查/GCI小组收集的数据

4 2020年全球网络安全指数：国家概况

非洲

安哥拉共和国



发展水平：
发展中国家、最不发达国家（LDC）

相对强的领域

法律措施

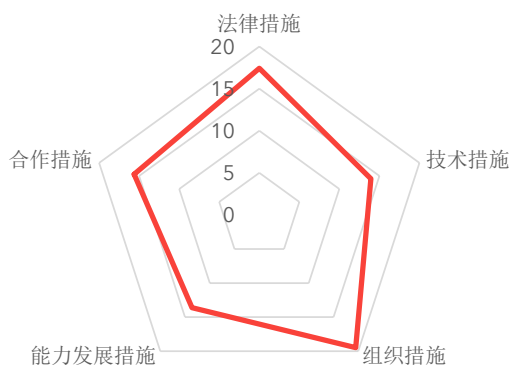
潜在增长领域

技术措施、组织措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
12.99	6.70	0.00	0.00	0.00	6.30

来源：国际电联全球网络安全指数 v4，2020 年

贝宁共和国



发展水平：
发展中国家、最不发达国家（LDC）

相对强的领域

组织措施

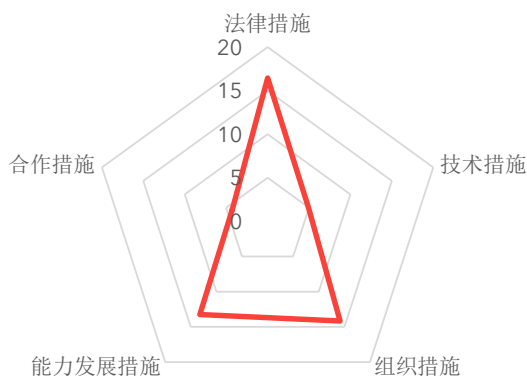
潜在增长领域

能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
80.06	17.42	13.94	19.48	13.60	15.63

来源：国际电联全球网络安全指数 v4，2020 年

博茨瓦纳共和国



发展水平:
发展中国家、内陆国家

相对强的领域

法律措施

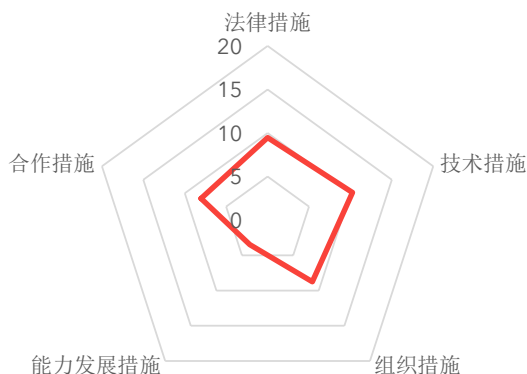
潜在增长领域

合作措施、技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
53.06	16.44	4.95	14.16	13.23	4.26

来源：国际电联全球网络安全指数 v4，2020 年

布基纳法索**



发展水平:
发展中国家、最不发达国家 (LDC)、内陆国家

相对强的领域

技术措施

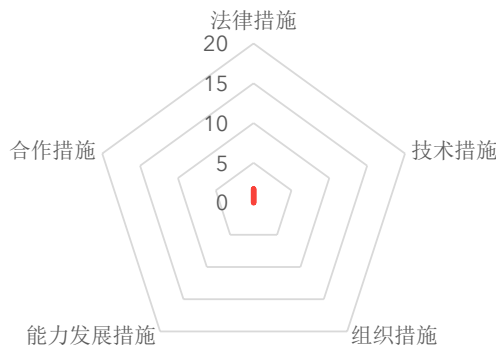
潜在增长领域

能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
39.98	9.47	10.25	8.75	3.47	8.04

来源：国际电联全球网络安全指数 v4，2020 年

布隆迪共和国



发展水平:

发展中国家、最不发达国家 (LDC)、内陆国家

相对强的领域

法律措施

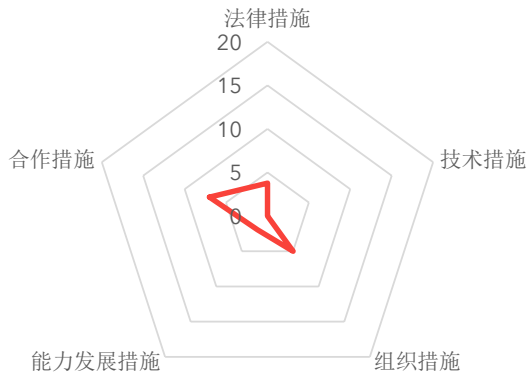
潜在增长领域

技术措施、组织措施、合作措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
1.73	1.73	0.00	0.00	0.00	0.00

来源: 国际电联全球网络安全指数 v4, 2020 年

佛得角共和国



发展水平:

发展中国家、小岛屿发展中国家 (SIDS)

相对强的领域

合作措施

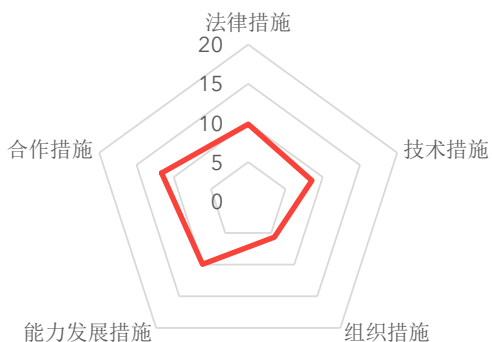
潜在增长领域

技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
17.74	3.77	0.00	5.00	1.96	7.00

来源: 国际电联全球网络安全指数 v4, 2020 年

喀麦隆共和国



发展水平:
发展中国家

相对强的领域

合作措施

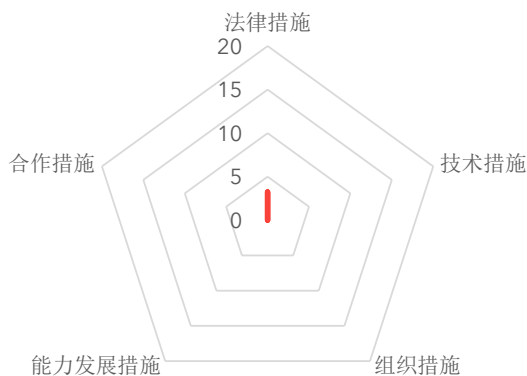
潜在增长领域

组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
45.63	9.84	8.54	5.67	9.95	11.63

来源：国际电联全球网络安全指数 v4，2020 年

中非共和国**



发展水平:

发展中国家、最不发达国家 (LDC)、内陆国家

相对强的领域

法律措施

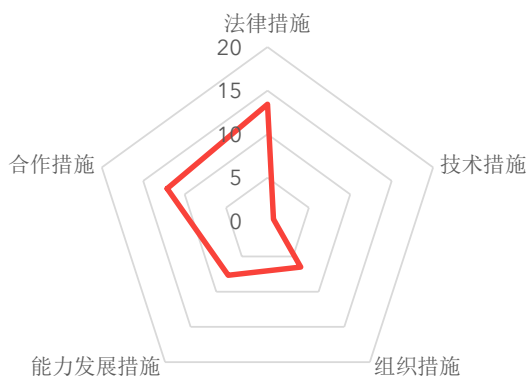
潜在增长领域

技术措施、组织措施、能力发展措施、合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
3.24	3.24	0.00	0.00	0.00	0.00

来源：国际电联全球网络安全指数 v4，2020 年

乍得共和国



发展水平:
发展中国家、最不发达国家 (LDC)、内陆国家

相对强的领域

法律措施

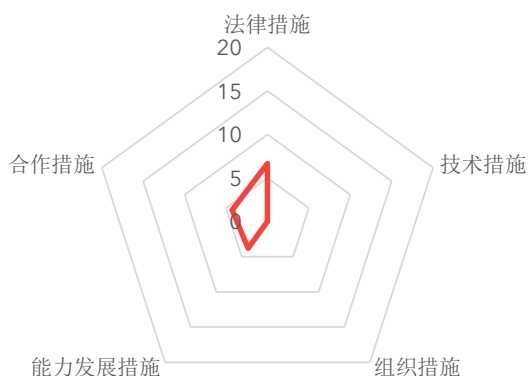
潜在增长领域

技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
40.44	13.43	0.73	6.50	7.67	12.11

来源：国际电联全球网络安全指数 v4, 2020 年

刚果共和国**



发展水平:

发展中国家

相对强的领域

法律措施

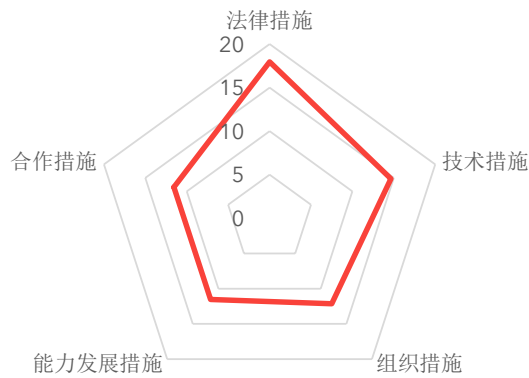
潜在增长领域

技术措施、组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
14.72	6.66	0.00	0.00	3.80	4.26

来源：国际电联全球网络安全指数 v4, 2020 年

科特迪瓦共和国



发展水平：
发展中国家

相对强的领域

法律措施

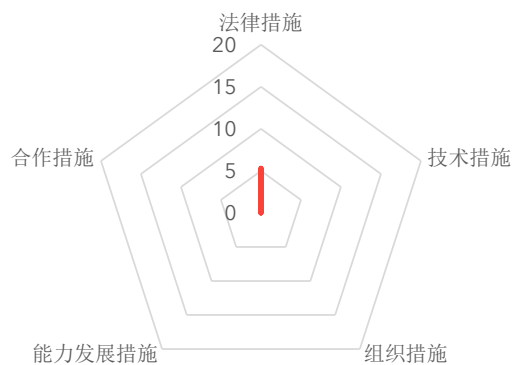
潜在增长领域

能力发展措施、合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
67.82	17.95	14.65	12.14	11.53	11.55

来源：国际电联全球网络安全指数 v4，2020 年

刚果民主共和国



发展水平：

发展中国家、最不发达国家（LDC）

相对强的领域

法律措施

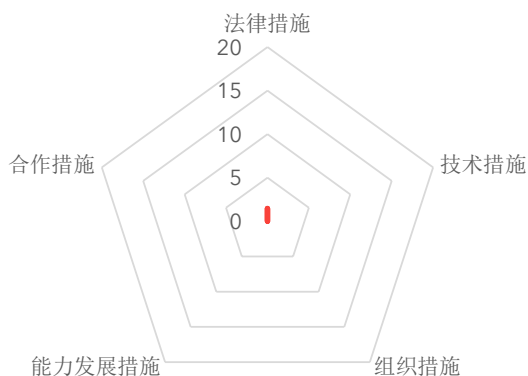
潜在增长领域

技术措施、组织措施、合作措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
5.30	5.30	0.00	0.00	0.00	0.00

来源：国际电联全球网络安全指数 v4，2020 年

赤道几内亚共和国**



发展水平:
发展中国家

相对强的领域

法律措施

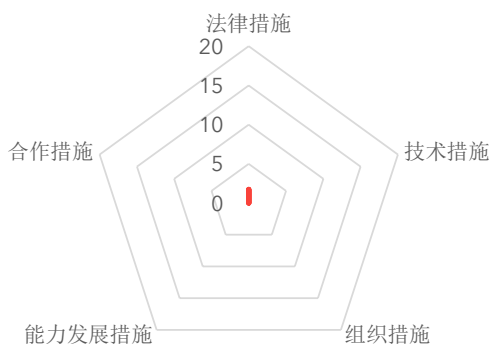
潜在增长领域

技术措施、组织措施、合作措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
1.46	1.46	0.00	0.00	0.00	0.00

来源：国际电联全球网络安全指数 v4，2020 年

厄立特里亚**



发展水平:

发展中国家、最不发达国家（LDC）

相对强的领域

法律措施

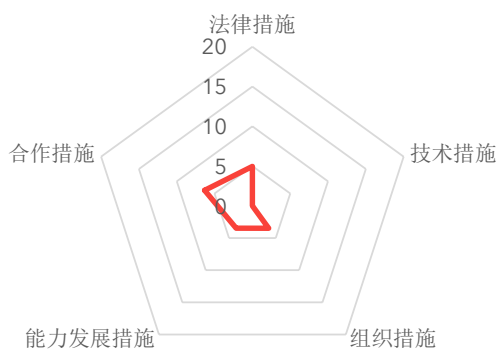
潜在增长领域

技术措施、组织措施、合作措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
1.73	1.73	0.00	0.00	0.00	0.00

来源：国际电联全球网络安全指数 v4，2020 年

斯威士兰王国



发展水平:
发展中国家、内陆国家

相对强的领域

合作措施

潜在增长领域

技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
18.23	4.96	0.00	3.49	3.47	6.31

来源：国际电联全球网络安全指数 v4，2020 年

埃塞俄比亚联邦民主共和国



发展水平:

发展中国家、最不发达国家 (LDC)、内陆国家

相对强的领域

法律措施

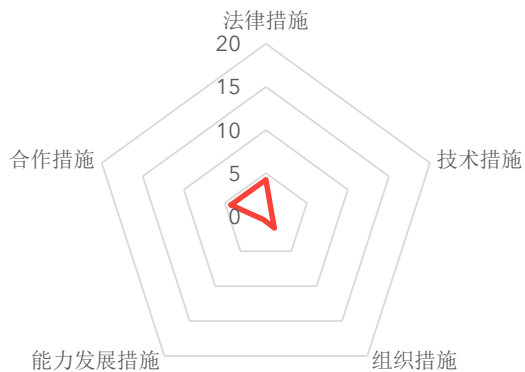
潜在增长领域

合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
27.74	11.56	4.46	8.03	3.69	0.00

来源：国际电联全球网络安全指数 v4，2020 年

加蓬共和国



发展水平：
发展中国家

相对强的领域

合作措施

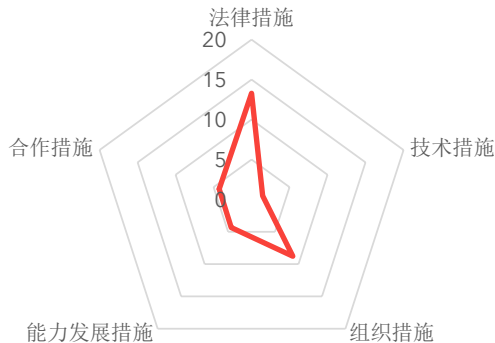
潜在增长领域

技术措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
11.38	4.24	0.73	1.69	0.46	4.26

来源：国际电联全球网络安全指数 v4，2020 年

冈比亚共和国



发展水平：

发展中国家、最不发达国家（LDC）

相对强的领域

法律措施

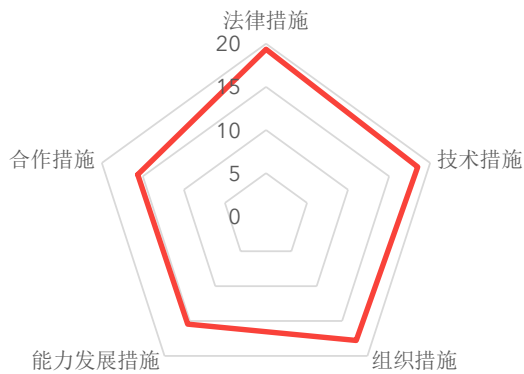
潜在增长领域

技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
32.12	13.28	1.46	8.78	4.34	4.26

来源：国际电联全球网络安全指数 v4，2020 年

加纳



发展水平:
发展中国家

相对强的领域

法律措施、技术措施

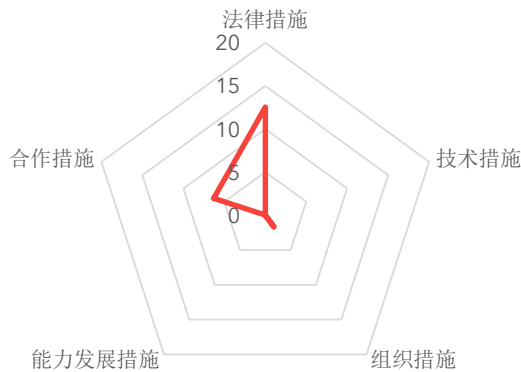
潜在增长领域

能力发展措施、合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
86.69	19.35	18.48	17.78	15.44	15.63

来源：国际电联全球网络安全指数 v4，2020 年

几内亚共和国**



发展水平:
发展中国家、最不发达国家 (LDC)

相对强的领域

法律措施

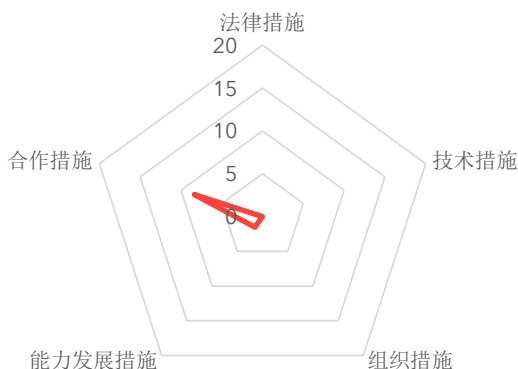
潜在增长领域

技术措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
20.53	12.54	0.00	1.69	0.00	6.30

来源：国际电联全球网络安全指数 v4，2020 年

几内亚比绍共和国



发展水平:
发展中国家、最不发达国家 (LDC)
小岛屿发展中国家 (SIDS)

相对强的领域

合作措施

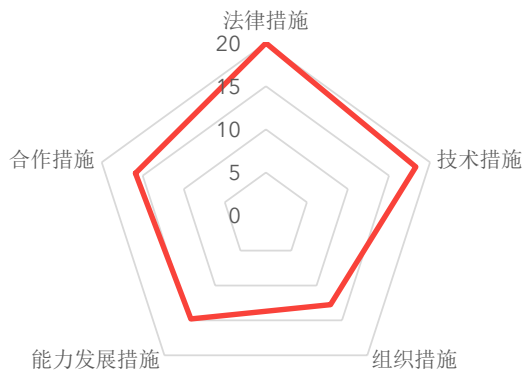
潜在增长领域

法律措施、技术措施、组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
9.85	0.00	0.00	0.00	1.52	8.33

来源：国际电联全球网络安全指数 v4, 2020 年

肯尼亚共和国



发展水平:
发展中国家

相对强的领域

法律措施、技术措施

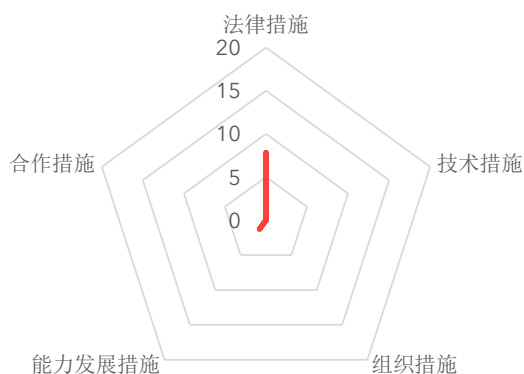
潜在增长领域

组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
81.70	20.00	18.27	12.75	14.79	15.89

来源：国际电联全球网络安全指数 v4, 2020 年

莱索托王国



发展水平:

发展中国家、最不发达国家 (LDC)、内陆国家

相对强的领域

法律措施

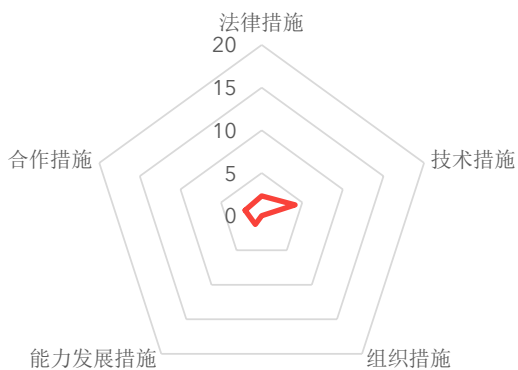
潜在增长领域

技术措施、组织措施、合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
9.08	7.82	0.00	0.00	1.26	0.00

来源：国际电联全球网络安全指数 v4，2020 年

利比里亚共和国



发展水平:

发展中国家、最不发达国家 (LDC)

相对强的领域

技术措施

潜在增长领域

组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
9.72	2.31	4.11	0.00	1.26	2.04

来源：国际电联全球网络安全指数 v4，2020 年

马达加斯加共和国**



发展水平:
发展中国家、最不发达国家 (LDC)

相对强的领域

法律措施

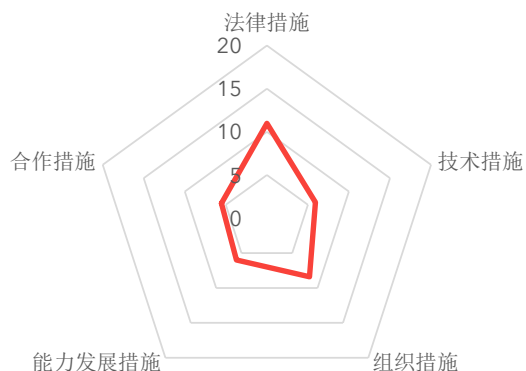
潜在增长领域

组织措施、合作措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
23.33	8.96	4.11	3.00	3.47	3.78

来源：国际电联全球网络安全指数 v4, 2020 年

马拉维



发展水平:
发展中国家、最不发达国家 (LDC)、内陆国家

相对强的领域

法律措施、组织措施

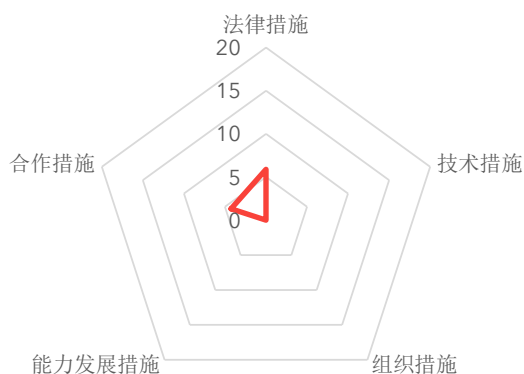
潜在增长领域

合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
36.83	10.98	5.92	8.40	6.00	5.54

来源：国际电联全球网络安全指数 v4, 2020 年

马里共和国**



发展水平:
发展中国家、最不发达国家 (LDC)、内陆国家

相对强的领域

法律措施

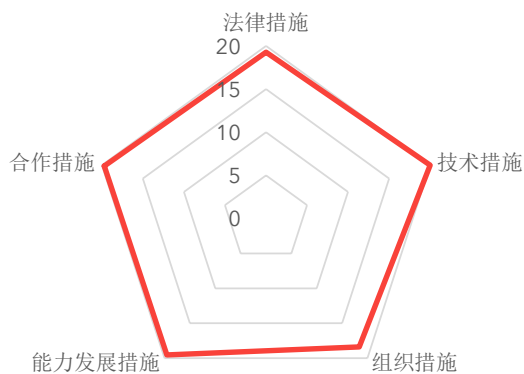
潜在增长领域

技术措施、组织措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
10.14	5.89	0.00	0.00	0.00	4.26

来源：国际电联全球网络安全指数 v4, 2020 年

毛里求斯共和国



发展水平:

发展中国家、小岛屿发展中国家 (SIDS)

相对强的领域

技术措施、合作措施、能力发展措施

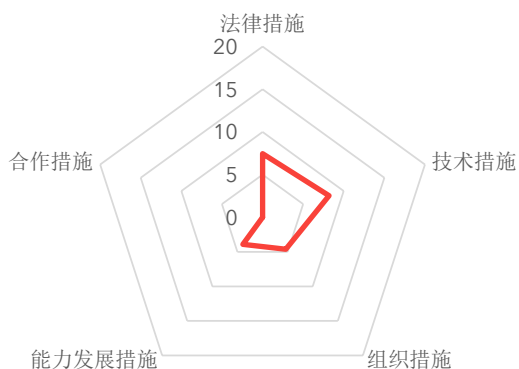
潜在增长领域

组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
96.89	19.27	20.00	18.38	19.54	19.70

来源：国际电联全球网络安全指数 v4, 2020 年

莫桑比克共和国



发展水平:
发展中国家、最不发达国家 (LDC)

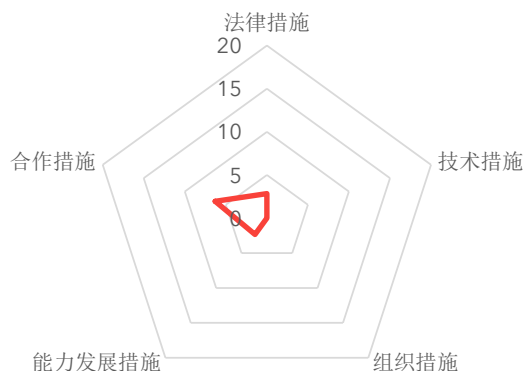
相对强的领域
技术措施、法律措施

潜在增长领域
合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
24.181	7.46	8.19	4.62	3.92	0.00

来源：国际电联全球网络安全指数 v4，2020 年

纳米比亚共和国



发展水平:
发展中国家

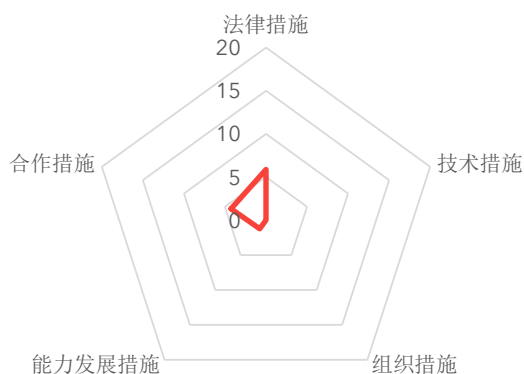
相对强的领域
技术措施

潜在增长领域
技术措施、组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
11.47	2.84	0.00	0.00	2.34	6.30

来源：国际电联全球网络安全指数 v4，2020 年

尼日尔共和国



发展水平:
发展中国家、最不发达国家 (LDC)、内陆国家

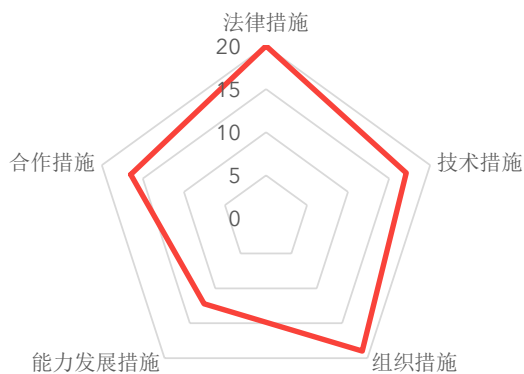
相对强的领域
法律措施、合作措施

潜在增长领域
技术措施、组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
11.36	5.87	0.00	0.00	1.23	4.26

来源：国际电联全球网络安全指数 v4, 2020 年

尼日利亚联邦共和国



发展水平:
发展中国家

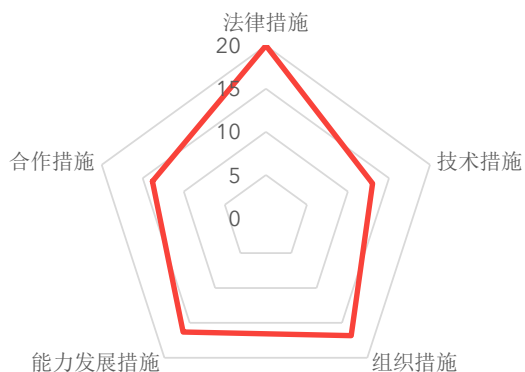
相对强的领域
法律措施

潜在增长领域
能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
84.76	20.00	17.09	18.98	12.21	16.48

来源：国际电联全球网络安全指数 v4, 2020 年

卢旺达共和国



发展水平:
发展中国家、最不发达国家 (LDC)、内陆国家

相对强的领域

法律措施

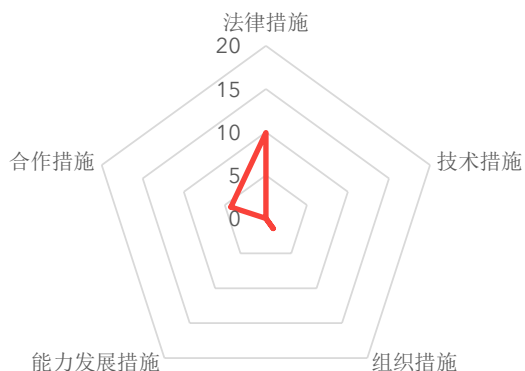
潜在增长领域

技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
79.95	20.00	13.00	16.83	16.30	13.82

来源：国际电联全球网络安全指数 v4，2020 年

圣多美和普林西比民主共和国



发展水平:
发展中国家、最不发达国家 (LDC)、小岛屿发展中国家 (SIDS)

相对强的领域

法律措施

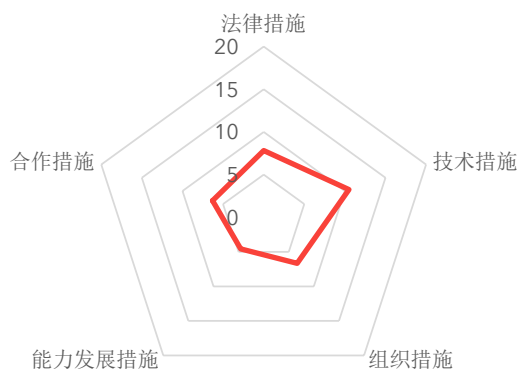
潜在增长领域

技术措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
15.64	9.94	0.00	1.44	0.00	4.26

来源：国际电联全球网络安全指数 v4，2020 年

塞内加尔共和国



发展水平:
发展中国家、最不发达国家 (LDC)

相对强的领域

技术措施

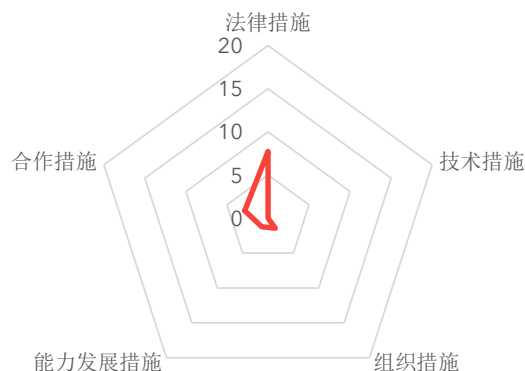
潜在增长领域

能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
35.85	7.82	10.50	6.66	4.58	6.30

来源：国际电联全球网络安全指数 v4, 2020 年

塞舌尔共和国**



发展水平:
发展中国家、小岛屿发展中国家 (SIDS)

相对强的领域

法律措施

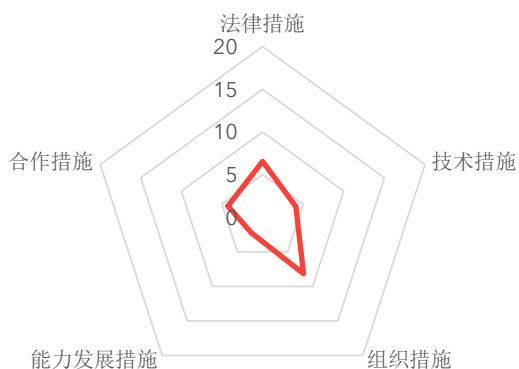
潜在增长领域

技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
13.23	7.73	0.00	1.44	1.23	2.83

来源：国际电联全球网络安全指数 v4, 2020 年

塞拉利昂



发展水平:
发展中国家、最不发达国家 (LDC)

相对强的领域

组织措施

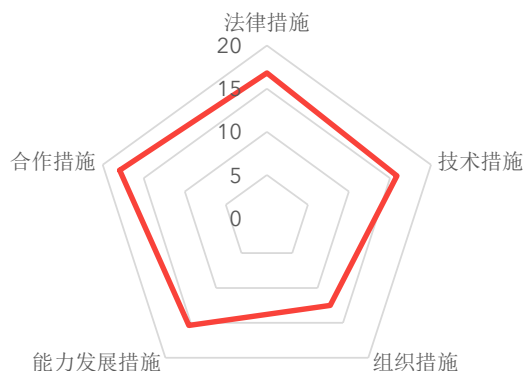
潜在增长领域

能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
25.31	6.54	4.11	8.16	2.24	4.26

来源：国际电联全球网络安全指数 v4，2020 年

南非共和国**



发展水平:

发展中国家

相对强的领域

合作措施

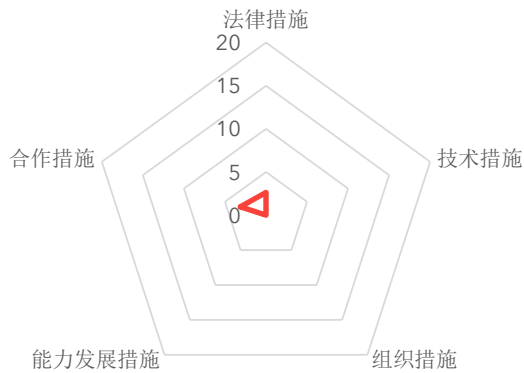
潜在增长领域

组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
78.46	16.82	15.85	12.50	15.37	17.93

来源：国际电联全球网络安全指数 v4，2020 年

南苏丹共和国**



发展水平:

发展中国家、最不发达国家 (LDC)、内陆国家

相对强的领域

合作措施

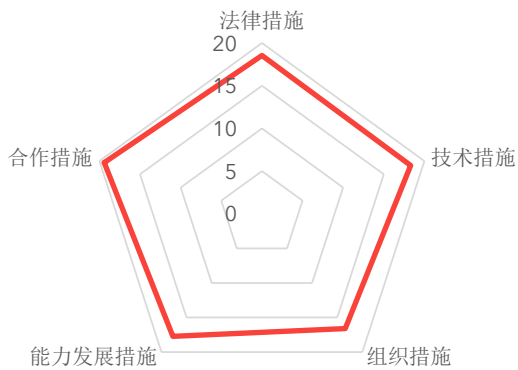
潜在增长领域

技术措施、组织措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
5.75	2.63	0.00	0.00	0.00	3.12

来源：国际电联全球网络安全指数 v4，2020 年

坦桑尼亚联合共和国



发展水平:

发展中国家、最不发达国家 (LDC)

相对强的领域

合作措施

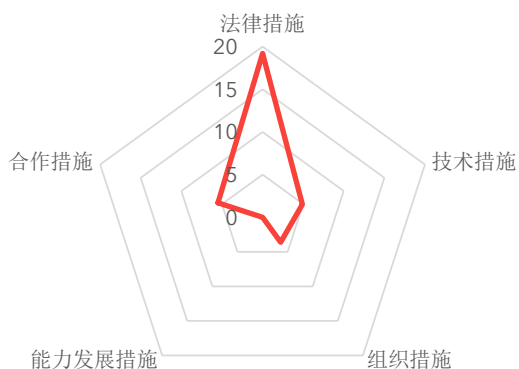
潜在增长领域

组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
90.58	18.54	18.31	16.60	17.72	19.41

来源：国际电联全球网络安全指数 v4，2020 年

多哥共和国



发展水平:
发展中国家、最不发达国家 (LDC)

相对强的领域

法律措施

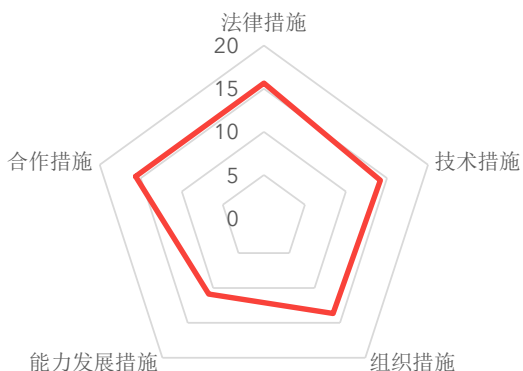
潜在增长领域

能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
33.19	19.19	4.90	3.61	0.00	5.49

来源：国际电联全球网络安全指数 v4，2020 年

乌干达共和国



发展水平:
发展中国家、最不发达国家 (LDC)、内陆国家

相对强的领域

法律措施

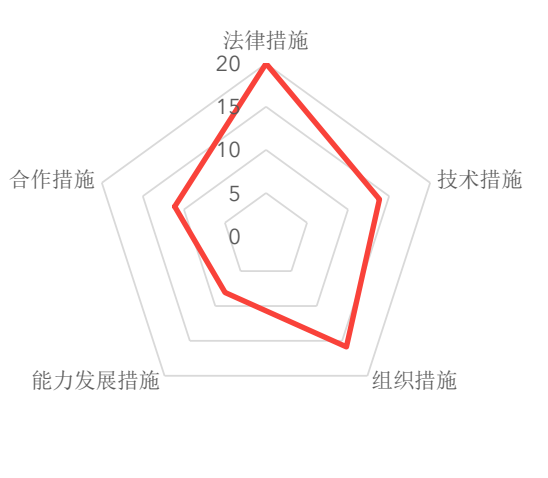
潜在增长领域

能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
69.98	15.64	14.19	13.65	10.87	15.63

来源：国际电联全球网络安全指数 v4，2020 年

赞比亚共和国



发展水平:
发展中国家、最不发达国家 (LDC)、内陆国家

相对强的领域

法律措施

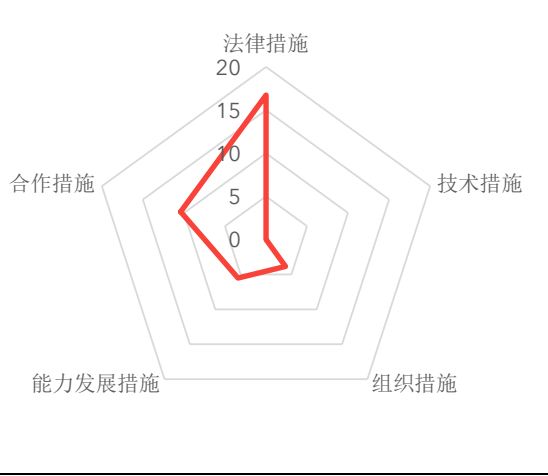
潜在增长领域

能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
68.88	20.00	13.82	15.86	8.07	11.12

来源：国际电联全球网络安全指数 v4，2020 年

津巴布韦共和国



发展水平:
发展中国家、内陆国家

相对强的领域

法律措施

潜在增长领域

技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
36.49	16.73	0.00	3.84	5.52	10.40

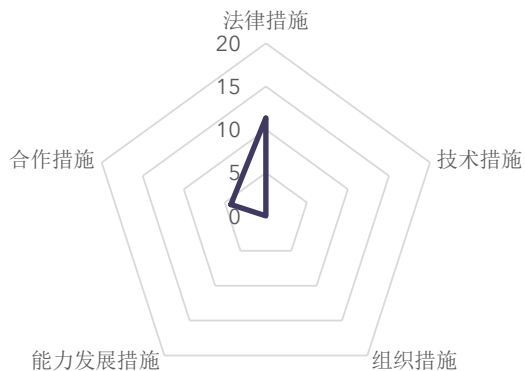
来源：国际电联全球网络安全指数 v4，2020 年

** 未响应问卷调查/GCI小组收集的数据

* 无数据

美洲区域

安提瓜和巴布达



发展水平:
发展中国家、小岛屿发展中国家 (SIDS)

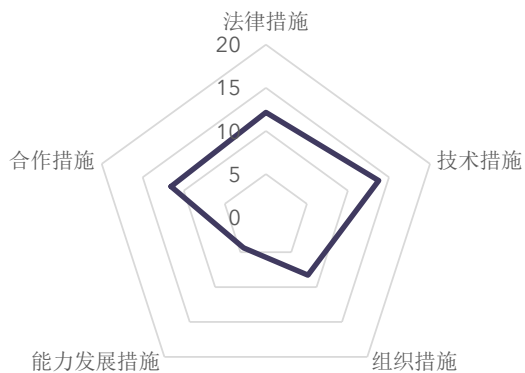
相对强的领域
法律措施

潜在增长领域
技术措施、组织措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
15.62	11.36	0.00	0.00	0.00	4.26

来源：国际电联全球网络安全指数 v4, 2020 年

阿根廷共和国



发展水平:
发展中国家

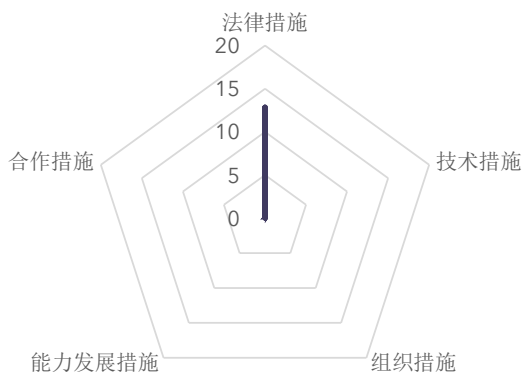
相对强的领域
技术措施

潜在增长领域
能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
50.12	12.15	13.75	8.29	4.38	11.55

来源：国际电联全球网络安全指数 v4, 2020 年

巴哈马联邦



发展水平:
发展中国家、小岛屿发展中国家 (SIDS)

相对强的领域

法律措施

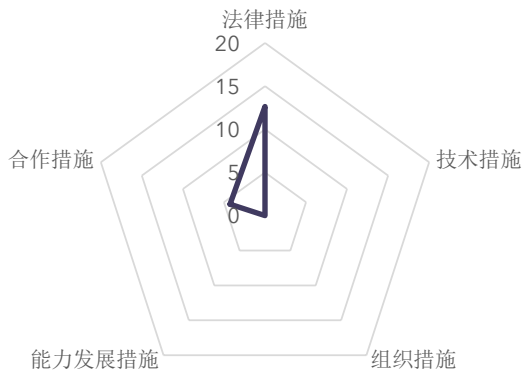
潜在增长领域

技术措施、组织措施、合作措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
13.37	12.85	0.00	0.00	0.52	0.00

来源：国际电联全球网络安全指数 v4, 2020 年

巴巴多斯



发展水平:
发展中国家、小岛屿发展中国家 (SIDS)

相对强的领域

法律措施

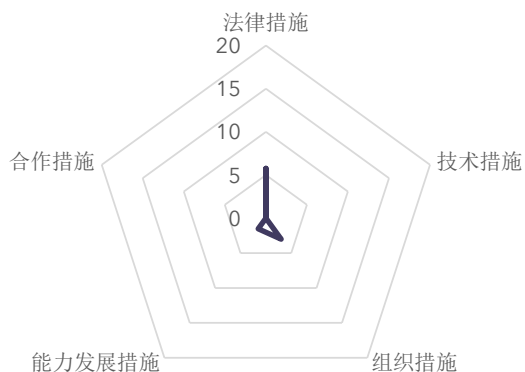
潜在增长领域

技术措施、组织措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
16.89	12.63	0.00	0.00	0.00	4.26

来源：国际电联全球网络安全指数 v4, 2020 年

伯利兹



发展水平:
发展中国家、小岛屿发展中国家 (SIDS)

相对强的领域

法律措施

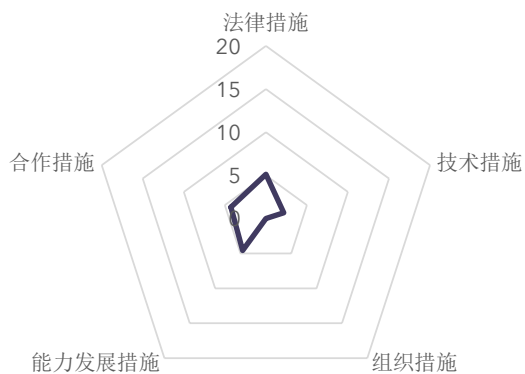
潜在增长领域

技术措施、合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
10.29	5.77	0.00	3.01	1.52	0.00

来源：国际电联全球网络安全指数 v4, 2020 年

多民族玻利维亚国



发展水平:

发展中国家、内陆国家

相对强的领域

法律措施

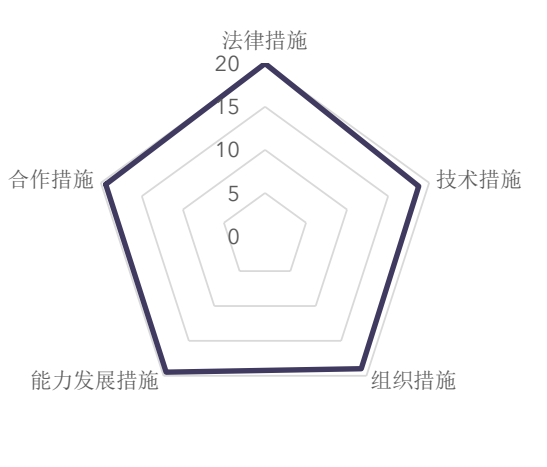
潜在增长领域

组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
16.14	5.13	2.18	0.00	4.58	4.26

来源：国际电联全球网络安全指数 v4, 2020 年

巴西联邦共和国



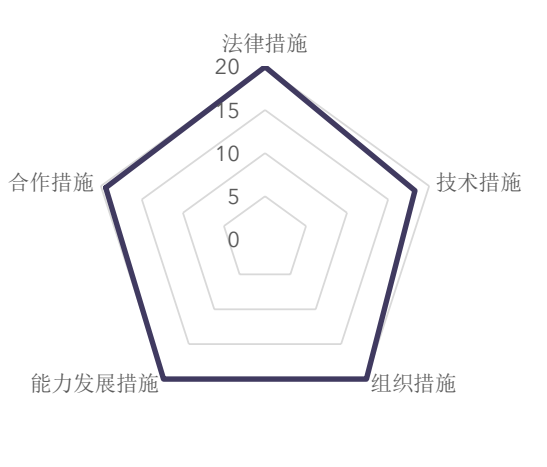
发展水平:
发展中国家

相对强的领域
法律措施
潜在增长领域
技术措施、组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
96.60	20.00	18.73	18.98	19.48	19.41

来源：国际电联全球网络安全指数 v4，2020 年

加拿大**



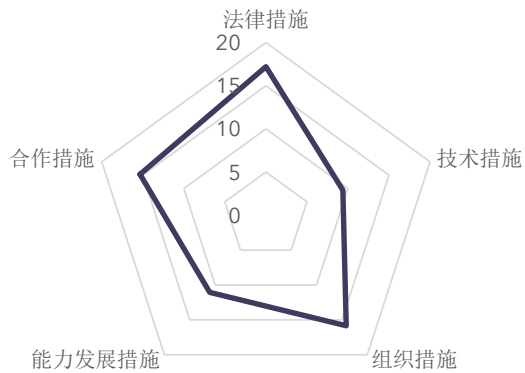
发展水平:
发达国家

相对强的领域
法律措施、组织措施、能力措施
潜在增长领域
技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
97.67	20.00	18.27	20.00	20.00	19.41

来源：国际电联全球网络安全指数 v4，2020 年

智利



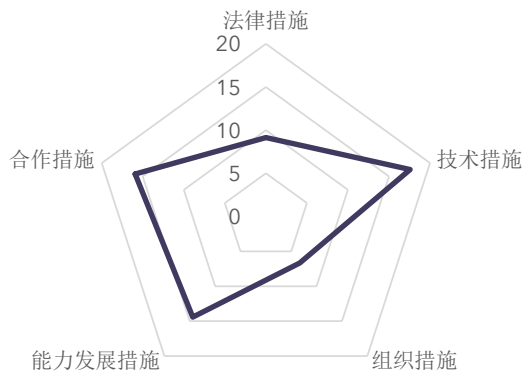
发展水平:
发展中国家

相对强的领域
法律措施
潜在增长领域
技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
68.83	17.20	9.39	15.84	11.07	15.33

来源：国际电联全球网络安全指数 v4, 2020 年

哥伦比亚共和国



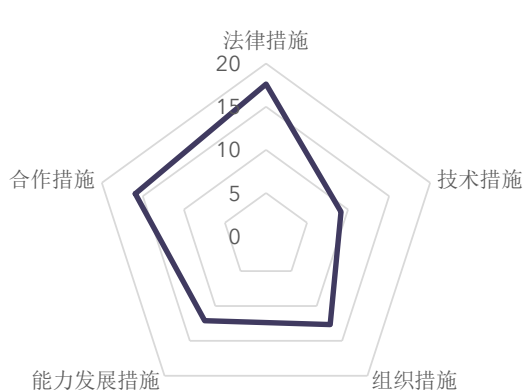
发展水平:
发展中国家

相对强的领域
技术措施
潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
63.72	9.14	17.58	6.67	14.42	15.93

来源：国际电联全球网络安全指数 v4, 2020 年

哥斯达黎加



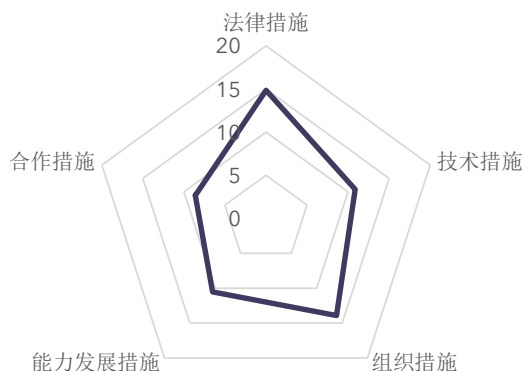
发展水平:
发展中国家

相对强的领域
法律措施
潜在增长领域
技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
67.45	17.62	9.14	12.66	12.11	15.93

来源：国际电联全球网络安全指数 v4，2020 年

古巴



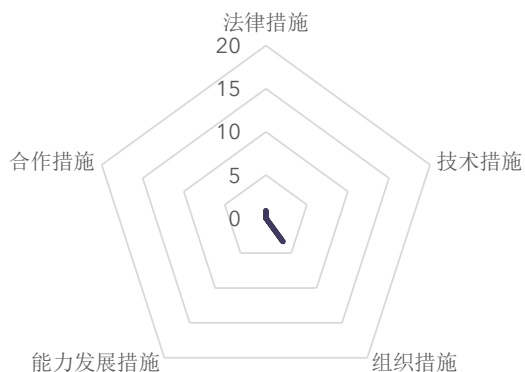
发展水平:
发展中国家、小岛屿发展中国家 (SIDS)

相对强的领域
法律措施
潜在增长领域
合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
58.76	14.85	10.87	13.91	10.52	8.61

来源：国际电联全球网络安全指数 v4，2020 年

多米尼加联邦



发展水平:
发展中国家、小岛屿发展中国家 (SIDS)

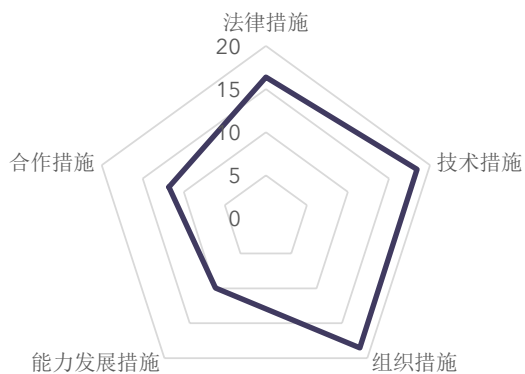
相对强的领域
组织措施

潜在增长领域
技术措施、合作措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
4.20	0.85	0.00	3.35	0.00	0.00

来源：国际电联全球网络安全指数 v4, 2020 年

多米尼加共和国



发展水平:
发展中国家、小岛屿发展中国家 (SIDS)

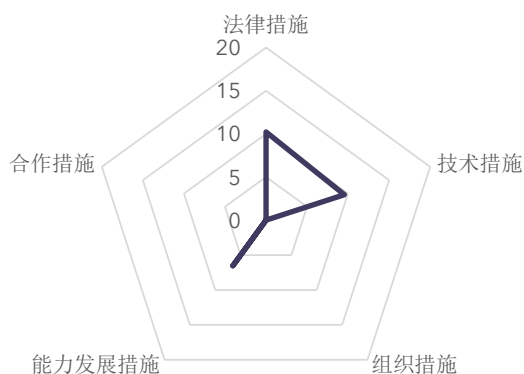
相对强的领域
组织措施

潜在增长领域
能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
75.07	16.38	18.42	18.52	9.94	11.81

来源：国际电联全球网络安全指数 v4, 2020 年

厄瓜多尔



发展水平:
发展中国家

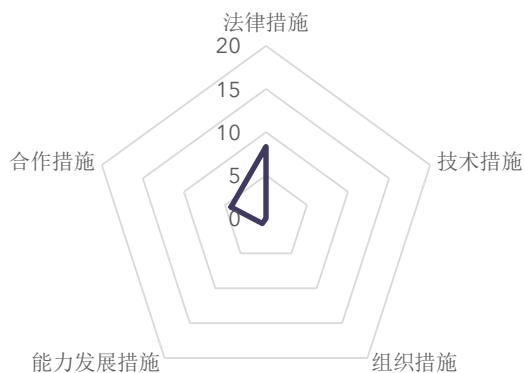
相对强的领域
法律措施

潜在增长领域
组织措施、合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
26.30	10.22	9.55	0.00	6.53	0.00

来源：国际电联全球网络安全指数 v4，2020 年

萨尔瓦多共和国**



发展水平:
发展中国家

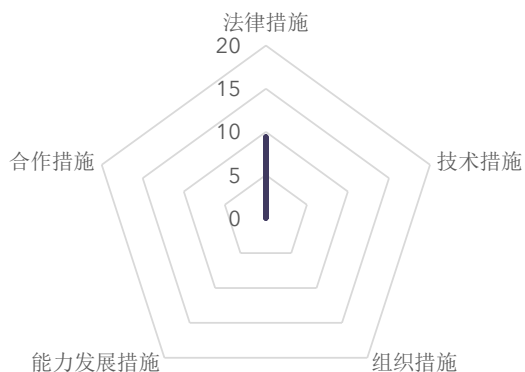
相对强的领域
法律措施

潜在增长领域
技术措施、组织措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
13.30	8.32	0.00	0.00	0.72	4.26

来源：国际电联全球网络安全指数 v4，2020 年

格林纳达



发展水平:
发展中国家、小岛屿发展中国家 (SIDS)

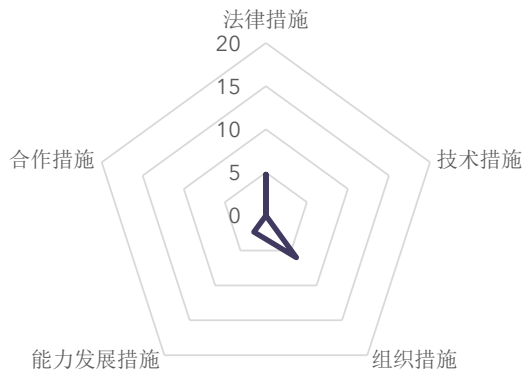
相对强的领域
法律措施

潜在增长领域
技术措施、组织措施、合作措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
9.41	9.41	0.00	0.00	0.00	0.00

来源：国际电联全球网络安全指数 v4, 2020 年

危地马拉共和国



发展水平:
发展中国家

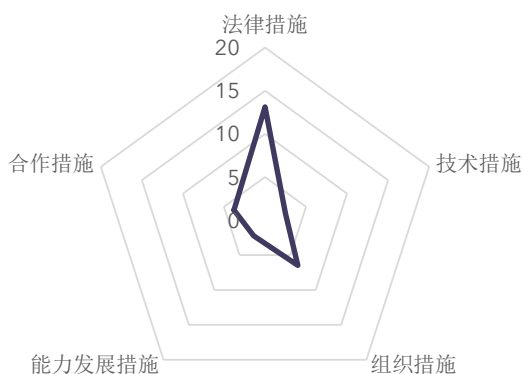
相对强的领域
组织措施

潜在增长领域
技术措施、合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
13.13	4.76	0.00	6.01	2.36	0.00

来源：国际电联全球网络安全指数 v4, 2020 年

圭亚那



发展水平:
发展中国家、小岛屿发展中国家 (SIDS)

相对强的领域

法律措施

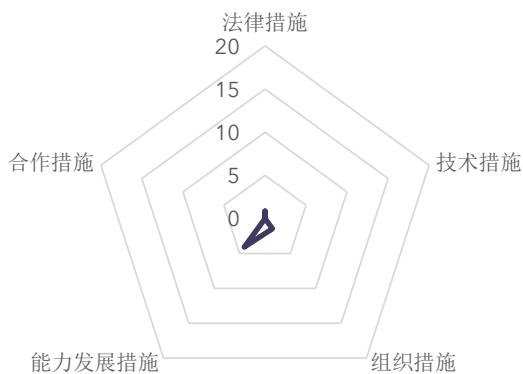
潜在增长领域

能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
28.11	13.12	2.50	6.47	2.24	3.78

来源：国际电联全球网络安全指数 v4，2020 年

海地共和国



发展水平:
发展中国家、最不发达国家 (LDC)、小岛屿发展中国家 (SIDS)

相对强的领域

能力发展措施

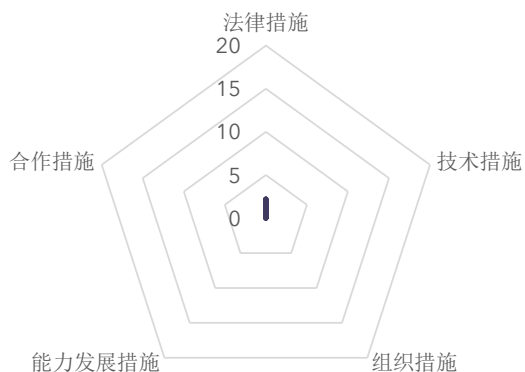
潜在增长领域

技术措施、合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
6.40	0.85	0.00	1.46	4.09	0.00

来源：国际电联全球网络安全指数 v4，2020 年

洪都拉斯共和国**



发展水平:
发展中国家

相对强的领域

法律措施

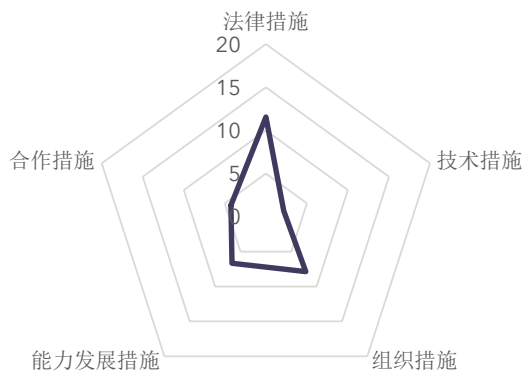
潜在增长领域

技术措施、组织措施、合作措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
2.20	2.20	0.00	0.00	0.00	0.00

来源：国际电联全球网络安全指数 v4, 2020 年

牙买加**



发展水平:

发展中国家、小岛屿发展中国家 (SIDS)

相对强的领域

法律措施

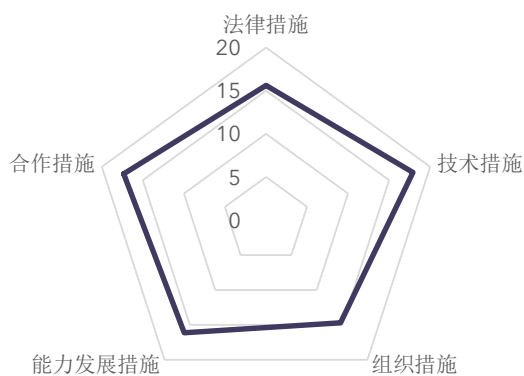
潜在增长领域

技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
32.53	11.54	2.18	7.87	6.68	4.26

来源：国际电联全球网络安全指数 v4, 2020 年

墨西哥



发展水平:
发展中国家

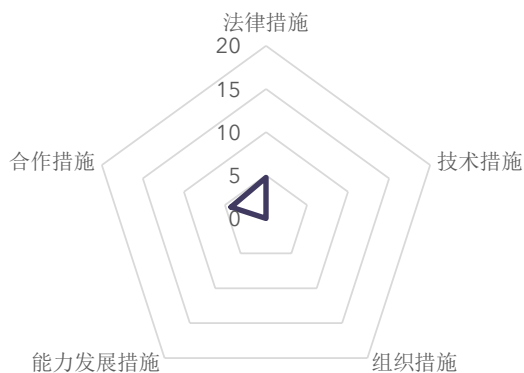
相对强的领域
技术措施、合作措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
81.68	15.61	17.90	14.70	16.13	17.34

来源：国际电联全球网络安全指数 v4, 2020 年

尼加拉瓜**



发展水平:
发展中国家

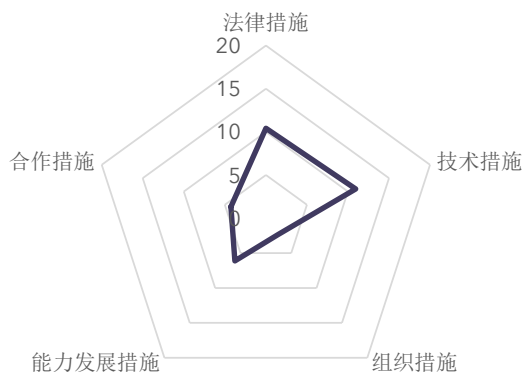
相对强的领域
法律措施

潜在增长领域
技术措施、组织措施、能力发展措施,

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
9.00	4.74	0.00	0.00	0.00	4.26

来源：国际电联全球网络安全指数 v4, 2020 年

巴拿马共和国



发展水平:
发展中国家

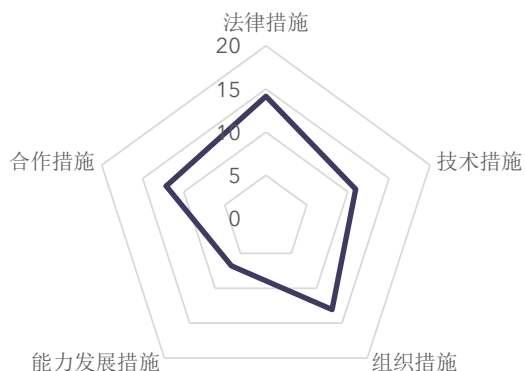
相对强的领域
技术措施、法律措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
34.11	10.41	10.94	2.37	6.12	4.26

来源：国际电联全球网络安全指数 v4, 2020 年

巴拉圭共和国



发展水平:
发展中国家、内陆国家

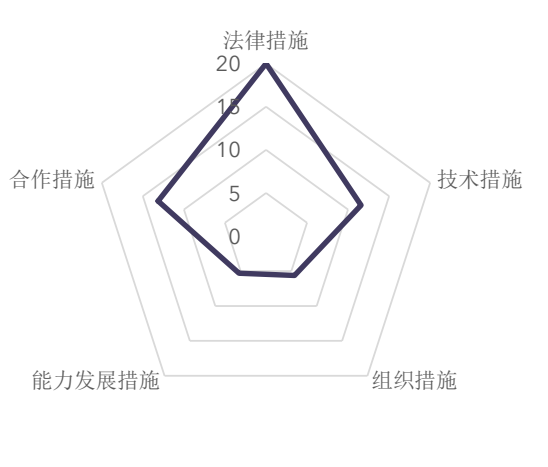
相对强的领域
法律措施

潜在增长领域
能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
57.09	14.15	10.94	13.06	6.79	12.14

来源：国际电联全球网络安全指数 v4, 2020 年

秘鲁



发展水平:
发展中国家

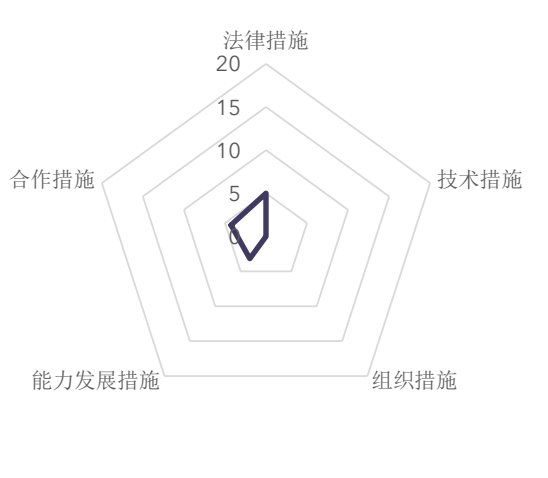
相对强的领域
法律措施

潜在增长领域
组织措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
55.67	20.00	11.58	5.63	5.32	13.15

来源：国际电联全球网络安全指数 v4，2020 年

圣基茨和尼维斯联邦



发展水平:
发展中国家、小岛屿发展中国家 (SIDS)

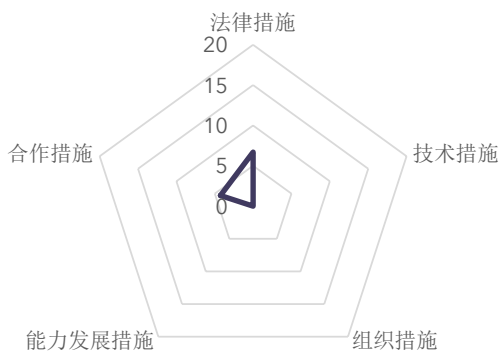
相对强的领域
法律措施

潜在增长领域
技术措施、组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
12.44	5.00	0.00	0.00	3.18	4.26

来源：国际电联全球网络安全指数 v4，2020 年

圣卢西亚**



发展水平:
发展中国家、小岛屿发展中国家 (SIDS)

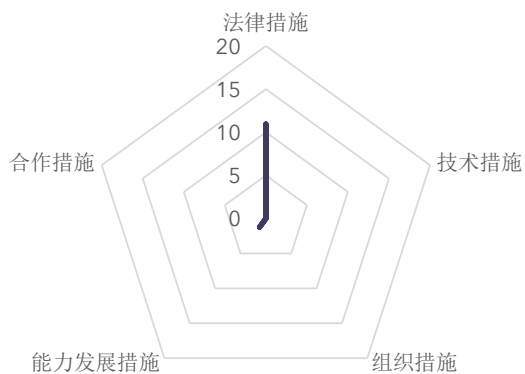
相对强的领域
法律措施

潜在增长领域
技术措施、组织措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
10.96	6.70	0.00	0.00	0.00	4.26

来源：国际电联全球网络安全指数 v4, 2020 年

圣文森特和格林纳丁斯**



发展水平:
发展中国家、小岛屿发展中国家 (SIDS)

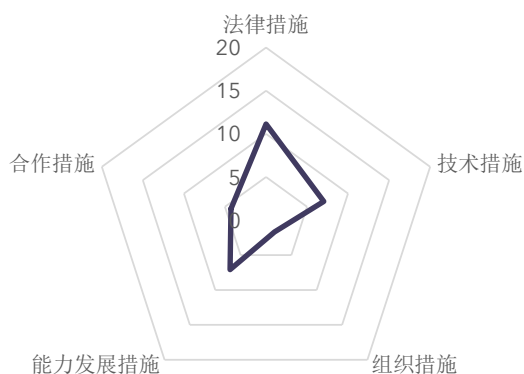
相对强的领域
法律措施

潜在增长领域
技术措施、组织措施、合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
12.18	10.95	0.00	0.00	1.23	0.00

来源：国际电联全球网络安全指数 v4, 2020 年

苏里南共和国



发展水平:
发展中国家、小岛屿发展中国家 (SIDS)

相对强的领域

法律措施

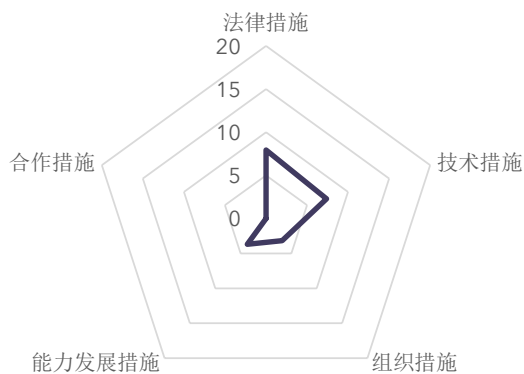
潜在增长领域

组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
31.20	11.13	7.04	1.69	7.08	4.26

来源：国际电联全球网络安全指数 v4，2020 年

特立尼达和多巴哥



发展水平:
发展中国家、小岛屿发展中国家 (SIDS)

相对强的领域

法律措施

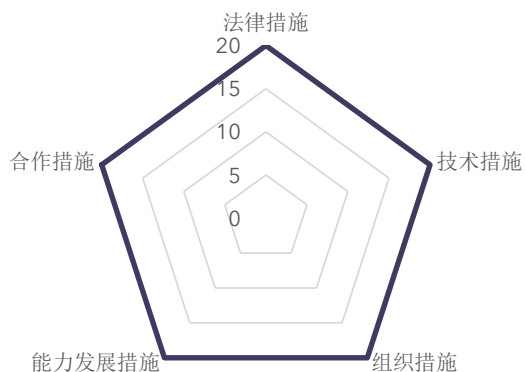
潜在增长领域

合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
22.18	7.94	7.38	3.18	3.69	0.00

来源：国际电联全球网络安全指数 v4，2020 年

美利坚合众国**



发展水平:
发达国家

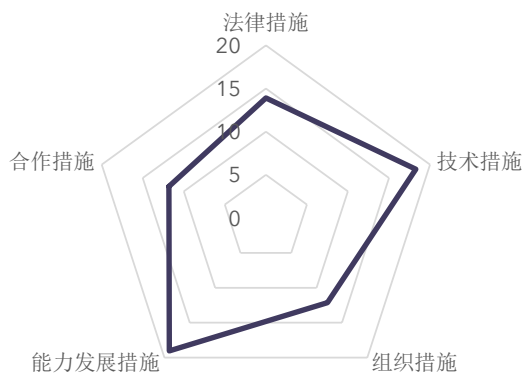
相对强的领域
法律措施、技术措施、组织措施、合作措施、能力发展措施

潜在增长领域
N/A

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
100.00	20.00	20.00	20.00	20.00	20.00

来源：国际电联全球网络安全指数 v4, 2020 年

乌拉圭东部共和国



发展水平:
发展中国家

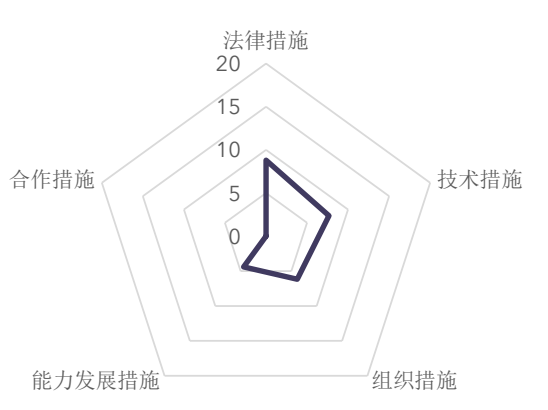
相对强的领域
能力发展措施

潜在增长领域
合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
75.15	13.90	18.27	12.13	19.04	11.81

来源：国际电联全球网络安全指数 v4, 2020 年

委内瑞拉玻利瓦尔共和国



发展水平:
发展中国家

相对强的领域
法律措施
潜在增长领域
合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
27.06	8.80	7.67	6.17	4.41	0.00

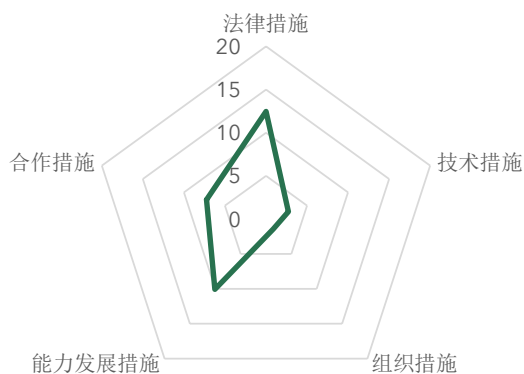
来源：国际电联全球网络安全指数 v4，2020 年

** 未响应问卷调查/GCI小组收集的数据

* 无数据

阿拉伯国家区域

阿尔及利亚人民共和国



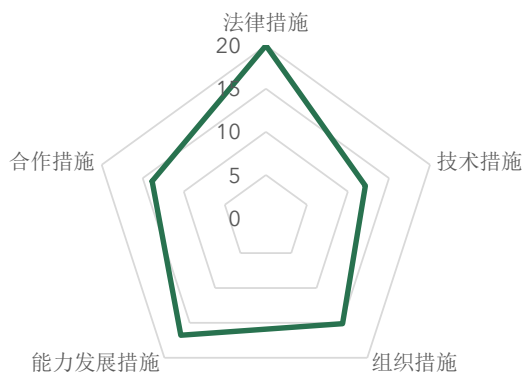
发展水平:
发展中国家

相对强的领域
法律措施
潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
33.95	12.46	2.73	1.44	10.07	7.25

来源：国际电联全球网络安全指数 v4，2020 年

巴林王国



发展水平：
发展中国家

相对强的领域

法律措施

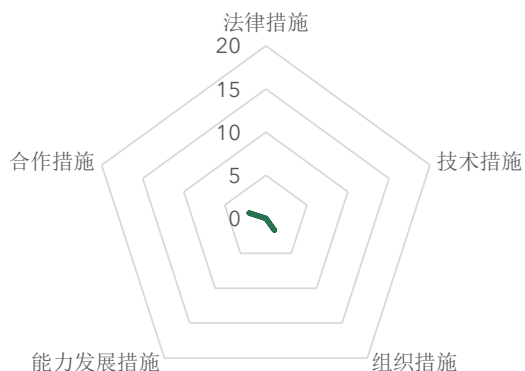
潜在增长领域

技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
77.86	20.00	12.12	15.11	16.77	13.86

来源：国际电联全球网络安全指数 v4，2020 年

科摩罗联盟**



发展水平：

发展中国家、最不发达国家 (LDC)、小岛屿发展中国家 (SIDS)

相对强的领域

合作措施

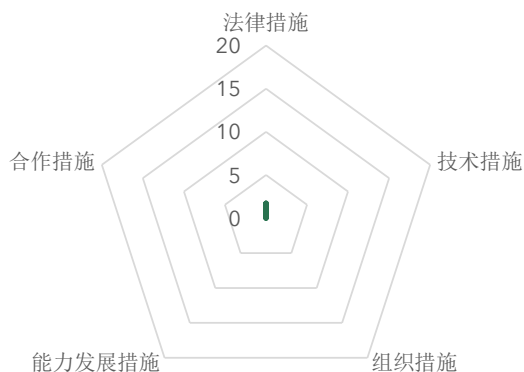
潜在增长领域

法律措施、技术措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
3.72	0.00	0.00	1.69	0.00	2.04

来源：国际电联全球网络安全指数 v4，2020 年

吉布提共和国



发展水平:
发展中国家、最不发达国家 (LDC)

相对强的领域

法律措施

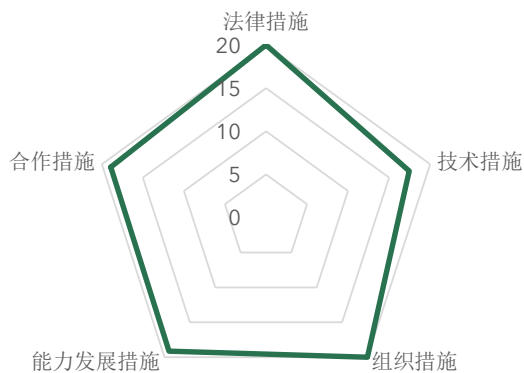
潜在增长领域

技术措施、组织措施、合作措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
1.73	1.73	0.00	0.00	0.00	0.00

来源：国际电联全球网络安全指数 v4, 2020 年

埃及阿拉伯共和国



发展水平:

发展中国家

相对强的领域

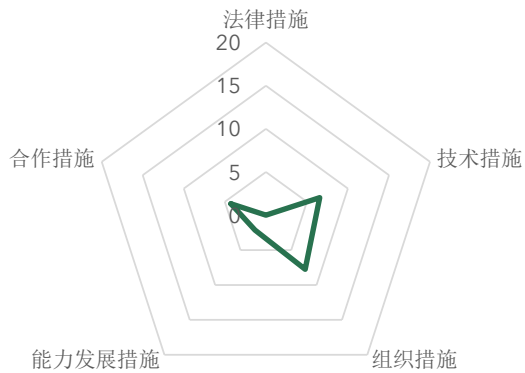
法律措施、组织措施

潜在增长领域

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
95.48	20.00	17.45	20.00	19.12	18.91

来源：国际电联全球网络安全指数 v4, 2020 年

伊拉克共和国**



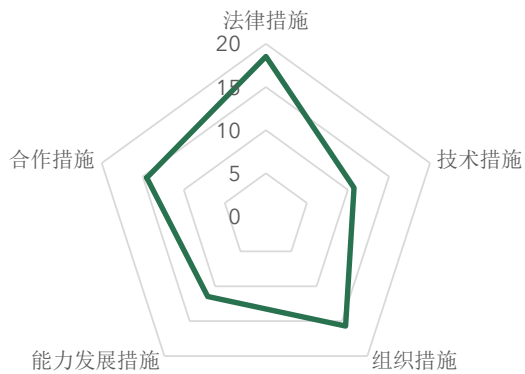
发展水平：
发展中国家

相对强的领域
组织措施
潜在增长领域
法律措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
20.71	0.00	6.56	7.75	2.14	4.26

来源：国际电联全球网络安全指数 v4, 2020 年

约旦哈希姆王国



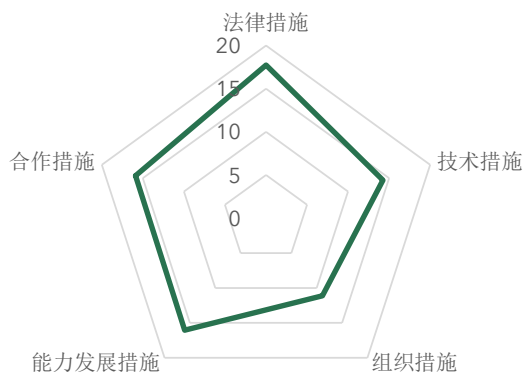
发展水平：
发展中国家

相对强的领域
法律措施
潜在增长领域
技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
70.96	18.53	10.74	15.70	11.47	14.51

来源：国际电联全球网络安全指数 v4, 2020 年

科威特国



发展水平:
发展中国家

相对强的领域

法律措施

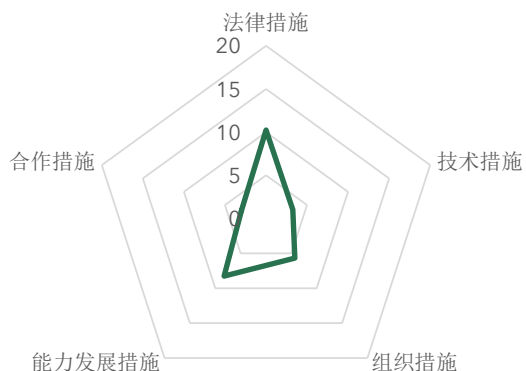
潜在增长领域

组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
75.05	17.74	14.25	11.13	16.05	15.90

来源：国际电联全球网络安全指数 v4，2020 年

黎巴嫩**



发展水平:
发展中国家

相对强的领域

法律措施

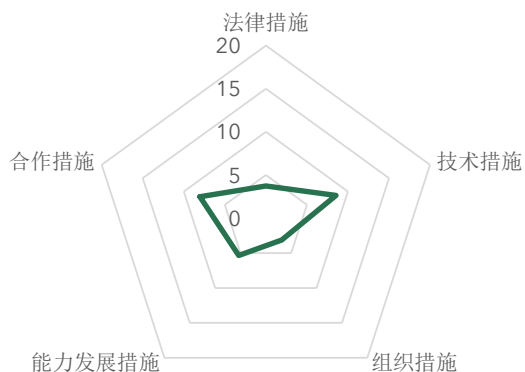
潜在增长领域

合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
30.44	10.24	3.27	5.69	8.26	2.99

来源：国际电联全球网络安全指数 v4，2020 年

利比亚国



发展水平：
发展中国家

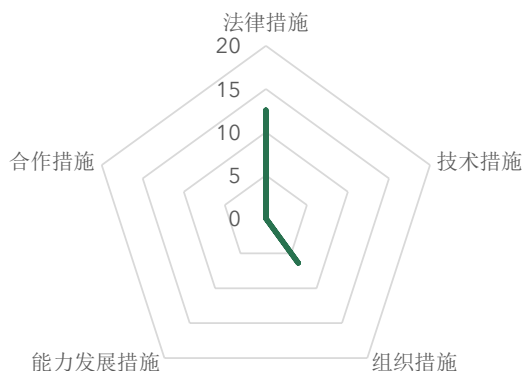
相对强的领域
技术措施、合作措施

潜在增长领域
法律措施、组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
28.78	3.73	8.54	3.13	5.34	8.04

来源：国际电联全球网络安全指数 v4，2020 年

毛里塔尼亚伊斯兰共和国



发展水平：
发展中国家、最不发达国家 (LDC)

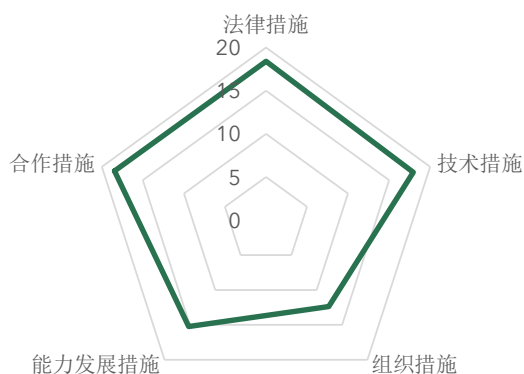
相对强的领域
法律措施

潜在增长领域
技术措施、合作措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
18.94	12.55	0.00	6.39	0.00	0.00

来源：国际电联全球网络安全指数 v4，2020 年

摩洛哥王国



发展水平:
发展中国家

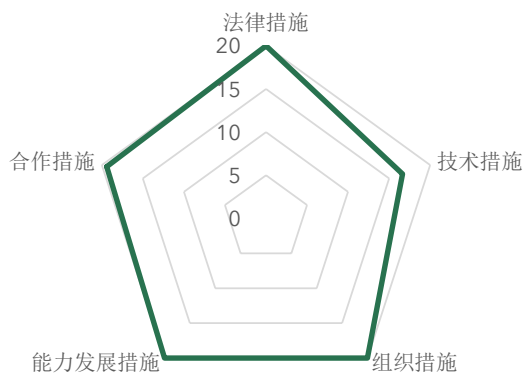
相对强的领域
法律措施、合作措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
82.41	18.40	17.94	12.37	15.24	18.46

来源：国际电联全球网络安全指数 v4，2020 年

阿曼苏丹国



发展水平:
发展中国家

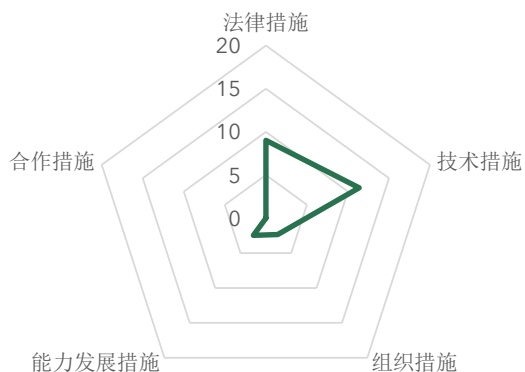
相对强的领域
法律措施、组织措施、能力发展措施

潜在增长领域
技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
96.04	20.00	16.64	20.00	20.00	19.41

来源：国际电联全球网络安全指数 v4，2020 年

巴勒斯坦国



发展水平：
发展中国家

相对强的领域

技术措施

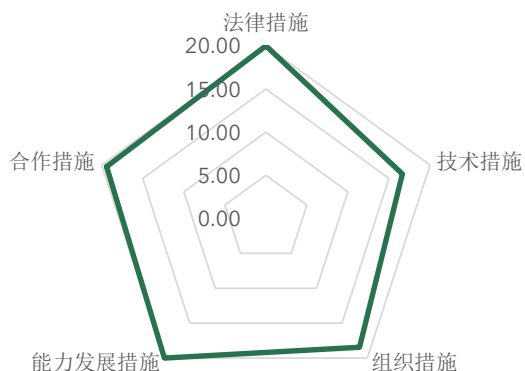
潜在增长领域

合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
25.18	9.02	11.36	2.34	2.46	0.00

来源：国际电联全球网络安全指数 v4, 2020 年

卡塔尔国



发展水平：
发展中国家

相对强的领域

法律措施、能力发展措施

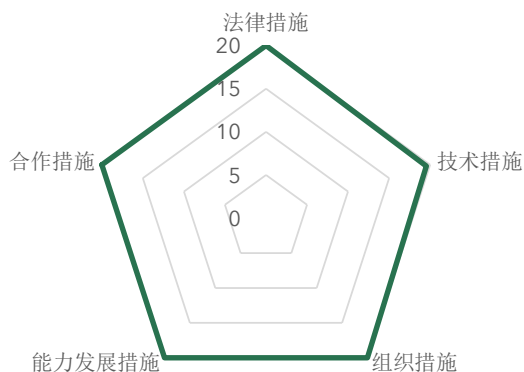
潜在增长领域

技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
94.50	20.00	16.64	18.46	20.00	19.41

来源：国际电联全球网络安全指数 v4, 2020 年

沙特阿拉伯王国



发展水平:
发展中国家

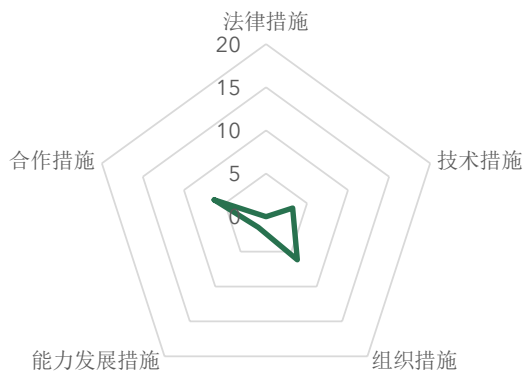
相对强的领域
法律措施、组织措施、合作措施、能力发展措施

潜在增长领域
技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
99.54	20.00	19.54	20.00	20.00	20.00

来源：国际电联全球网络安全指数 v4，2020 年

索马里联邦共和国



发展水平:

发展中国家、最不发达国家 (LDC)

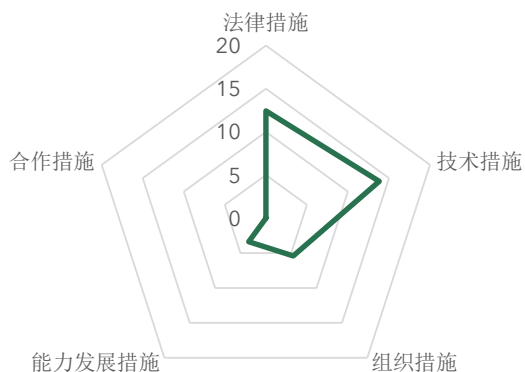
相对强的领域
组织措施、合作措施

潜在增长领域
法律措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
17.25	0.00	3.25	6.17	1.52	6.31

来源：国际电联全球网络安全指数 v4，2020 年

苏丹共和国



发展水平:
发展中国家、最不发达国家 (LDC)

相对强的领域

技术措施

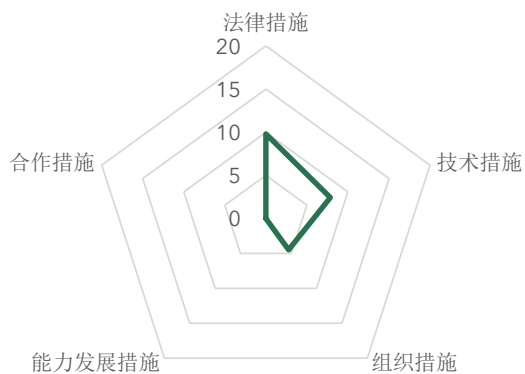
潜在增长领域

合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
35.03	12.43	13.81	5.41	3.38	0.00

来源：国际电联全球网络安全指数 v4，2020 年

阿拉伯叙利亚共和国**



发展水平:

发展中国家

相对强的领域

法律措施

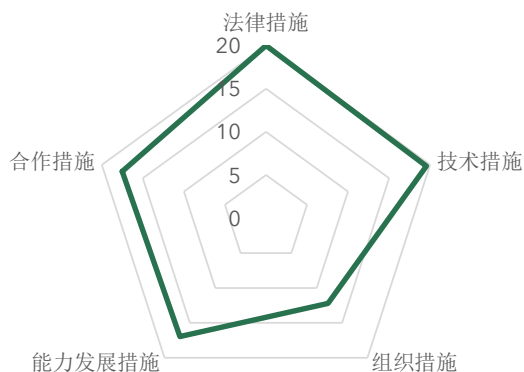
潜在增长领域

能力发展措施、合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
22.14	9.80	7.85	4.49	0.00	0.00

来源：国际电联全球网络安全指数 v4，2020 年

突尼斯



发展水平:
发展中国家

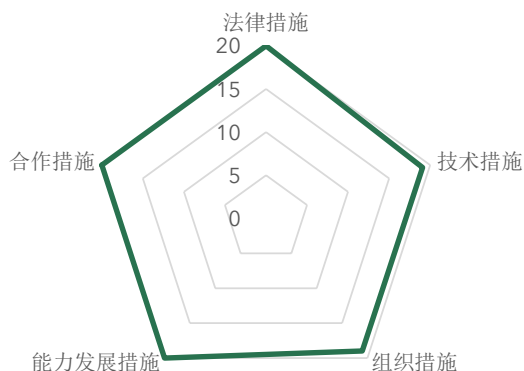
相对强的领域
法律措施、技术措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
86.23	20.00	19.54	12.21	16.96	17.52

来源：国际电联全球网络安全指数 v4，2020 年

阿拉伯联合酋长国



发展水平:
发展中国家

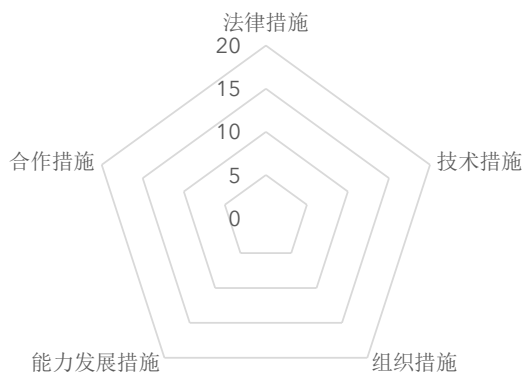
相对强的领域
法律措施、合作措施、能力发展措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
98.06	20.00	19.08	18.98	20.00	20.00

来源：国际电联全球网络安全指数 v4，2020 年

也门共和国*



发展水平:
发展中国家、最不发达国家 (LDC)

相对强的领域
N/A

潜在增长领域
N/A

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
0	0	0	0	0	0

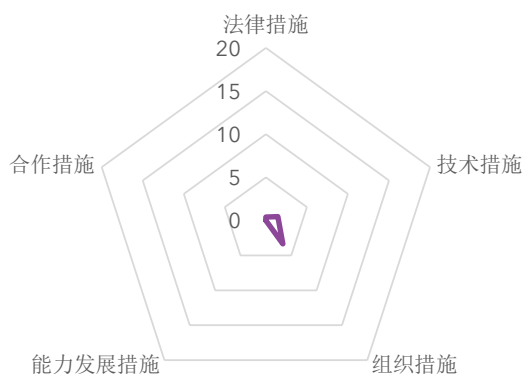
来源：国际电联全球网络安全指数 v4, 2020 年

** 未响应问卷调查/GCI小组收集的数据

* 无数据

亚太区域

阿富汗



发展水平:
发展中国家、最不发达国家 (LDC)、内陆国家

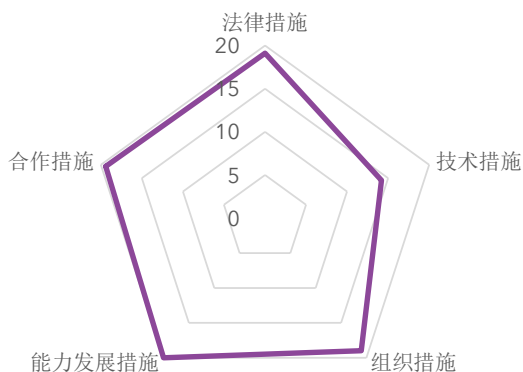
相对强的领域
组织措施

潜在增长领域
能力发展措施、合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
5.20	0.40	1.46	3.35	0.00	0.00

来源：国际电联全球网络安全指数 v4, 2020 年

澳大利亚



发展水平:

发达国家

相对强的领域

法律措施、能力发展措施

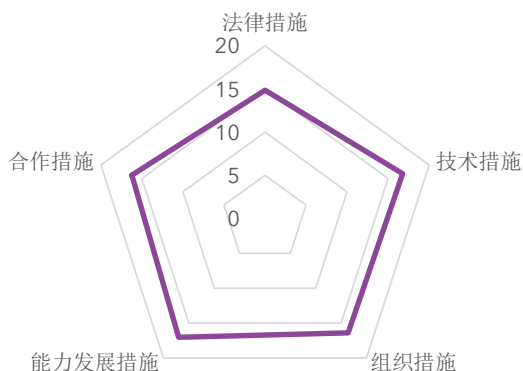
潜在增长领域

组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
97.47	20.00	19.08	18.98	20.00	19.41

来源：国际电联全球网络安全指数 v4，2020 年

孟加拉人民共和国



发展水平:

发展中国家、最不发达国家 (LDC)

相对强的领域

能力发展措施、技术措施

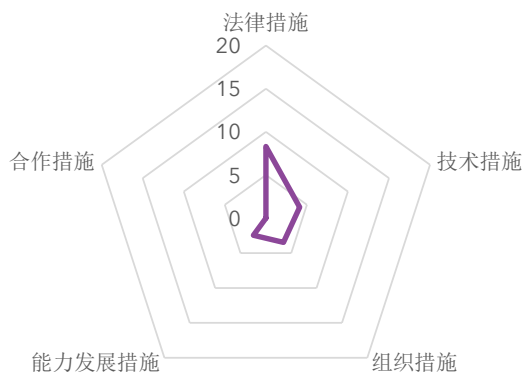
潜在增长领域

法律措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
81.27	14.86	16.77	16.39	17.03	16.22

来源：国际电联全球网络安全指数 v4，2020 年

不丹王国



发展水平:
发展中国家、最不发达国家 (LDC)、内陆国家

相对强的领域

法律措施

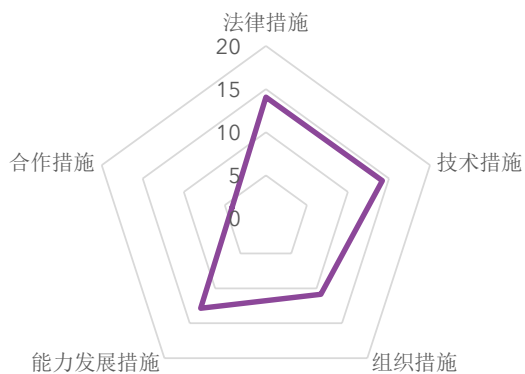
潜在增长领域

合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
18.34	8.30	4.12	3.47	2.45	0.00

来源：国际电联全球网络安全指数 v4, 2020 年

文莱达鲁萨兰国



发展水平:

发展中国家

相对强的领域

法律措施、技术措施

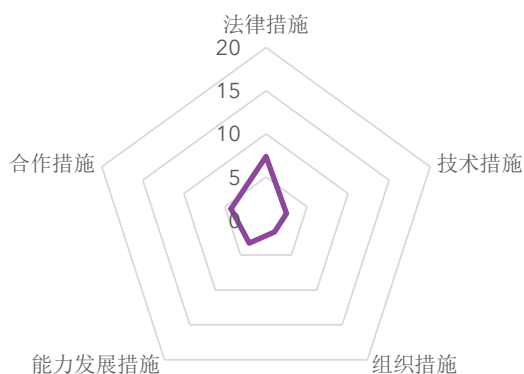
潜在增长领域

合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
56.07	14.06	14.19	10.84	12.85	4.12

来源：国际电联全球网络安全指数 v4, 2020 年

柬埔寨王国**



发展水平:
发展中国家、最不发达国家 (LDC)

相对强的领域

法律措施

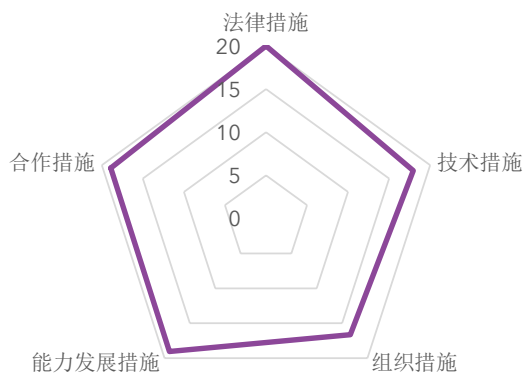
潜在增长领域

组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
19.12	7.38	2.50	1.69	3.29	4.26

来源：国际电联全球网络安全指数 v4，2020 年

中华人民共和国



发展水平:

发展中国家

相对强的领域

法律措施

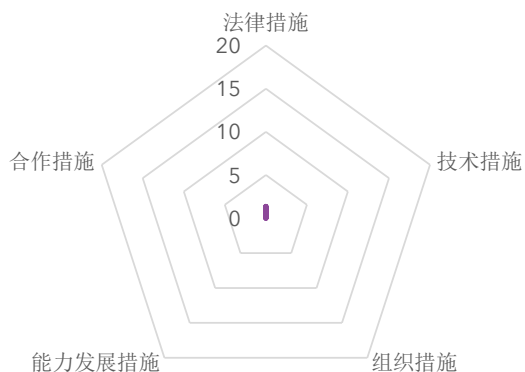
潜在增长领域

组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
92.53	20.00	17.94	16.63	19.04	18.91

来源：国际电联全球网络安全指数 v4，2020 年

朝鲜民主主义人民共和国**



发展水平:
发展中国家

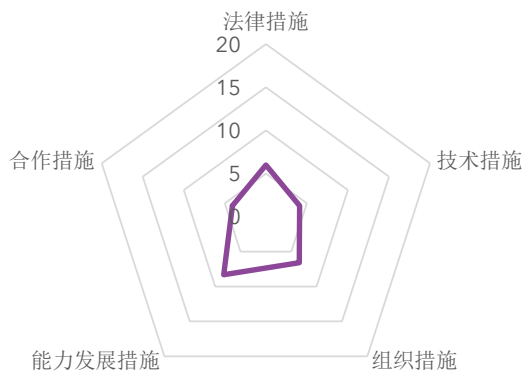
相对强的领域
法律措施

潜在增长领域
技术措施、组织措施、合作措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
1.35	1.35	0.00	0.00	0.00	0.00

来源：国际电联全球网络安全指数 v4, 2020 年

斐济共和国



发展水平:
发展中国家、小岛屿发展中国家 (SIDS)

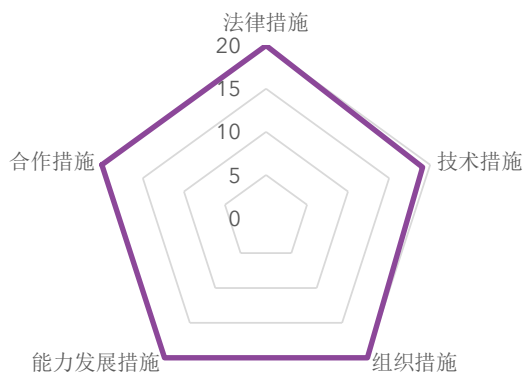
相对强的领域
能力发展措施

潜在增长领域
技术措施、合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
29.08	5.99	4.11	6.59	8.31	4.07

来源：国际电联全球网络安全指数 v4, 2020 年

印度共和国



发展水平:
发展中国家

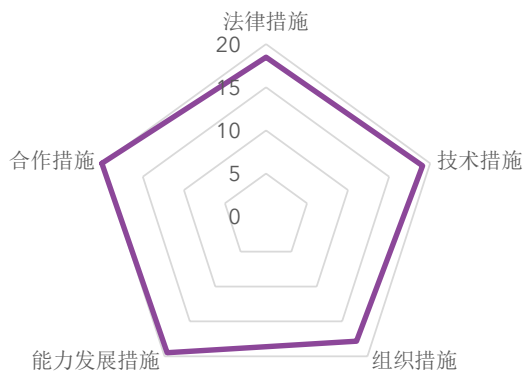
相对强的领域
法律措施、合作措施、能力发展措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
97.49	20.00	19.08	18.41	20.00	20.00

来源：国际电联全球网络安全指数 v4，2020 年

印度尼西亚共和国



发展水平:
发展中国家

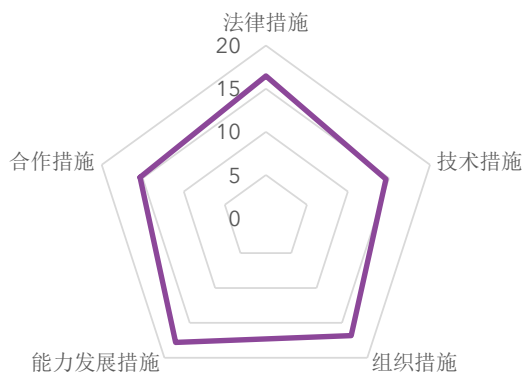
相对强的领域
合作措施、能力发展措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
94.88	18.48	19.08	17.84	19.48	20.00

来源：国际电联全球网络安全指数 v4，2020 年

伊朗伊斯兰共和国



发展水平:
发展中国家

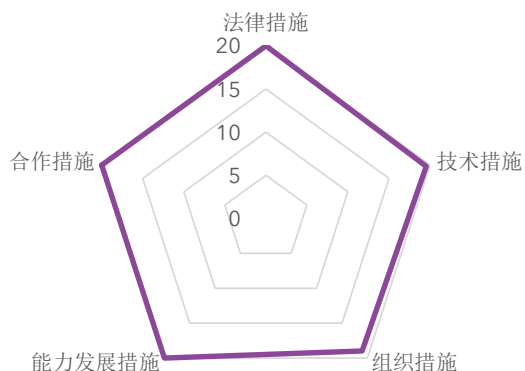
相对强的领域
能力发展措施、组织措施

潜在增长领域
技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
81.06	16.48	14.63	16.82	17.80	15.33

来源：国际电联全球网络安全指数 v4，2020 年

大韩民国



发展水平:
发展中国家

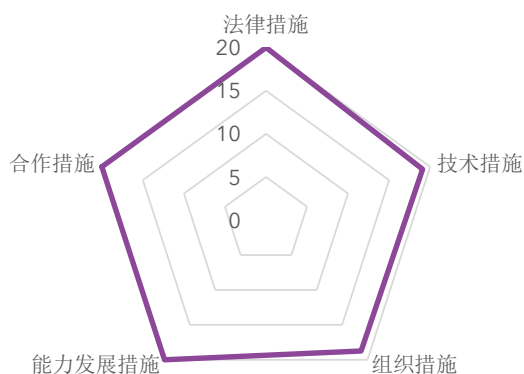
相对强的领域
法律措施、合作措施、能力发展措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
98.52	20.00	19.54	18.98	20.00	20.00

来源：国际电联全球网络安全指数 v4，2020 年

日本



发展水平:

发达国家

相对强的领域

法律措施、合作措施、能力发展措施

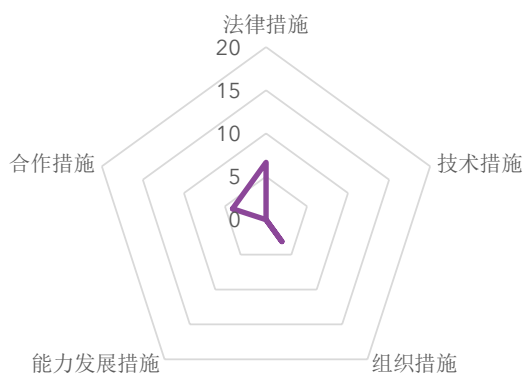
潜在增长领域

组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
97.82	20.00	19.08	18.74	20.00	20.00

来源：国际电联全球网络安全指数 v4，2020 年

基里巴斯共和国



发展水平:

发展中国家、最不发达国家 (LDC)、小岛屿发展中国家 (SIDS)

相对强的领域

法律措施

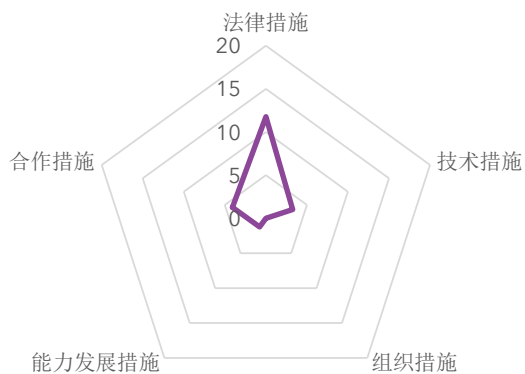
潜在增长领域

技术措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
13.84	6.64	0.00	3.13	0.00	4.07

来源：国际电联全球网络安全指数 v4，2020 年

老挝人民民主共和国



发展水平:
发展中国家、最不发达国家 (LDC)、内陆国家

相对强的领域

法律措施

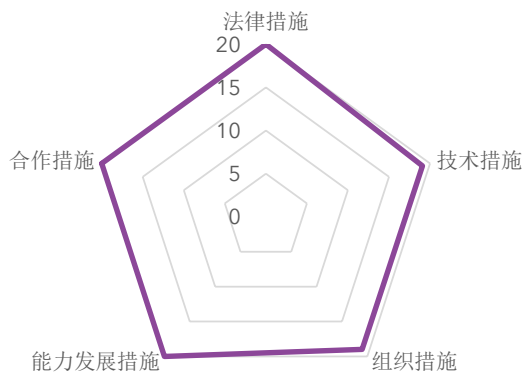
潜在增长领域

组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
20.34	11.77	3.27	0.00	1.23	4.07

来源：国际电联全球网络安全指数 v4, 2020 年

马来西亚



发展水平:

发展中国家

相对强的领域

法律措施、合作措施、能力发展措施

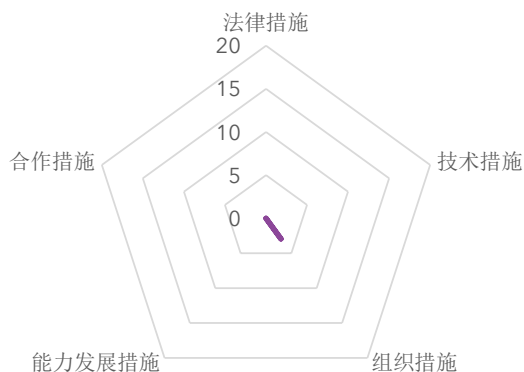
潜在增长领域

组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
98.06	20.00	19.08	18.98	20.00	20.00

来源：国际电联全球网络安全指数 v4, 2020 年

马尔代夫共和国**



发展水平:
发展中国家、小岛屿发展中国家 (SIDS)

相对强的领域

组织措施

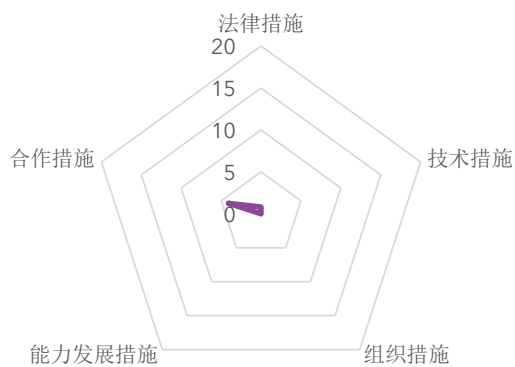
潜在增长领域

法律措施、技术措施、合作措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
2.95	0.00	0.00	2.95	0.00	0.00

来源：国际电联全球网络安全指数 v4, 2020 年

马绍尔群岛共和国**



发展水平:
发展中国家、小岛屿发展中国家 (SIDS)

相对强的领域

合作措施

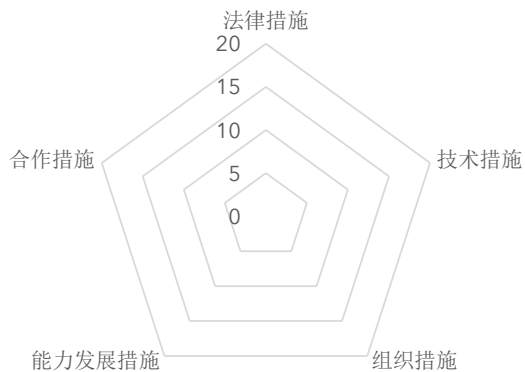
潜在增长领域

技术措施、组织措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
4.90	0.83	0.00	0.00	0.00	4.07

来源：国际电联全球网络安全指数 v4, 2020 年

密克罗尼西亚联邦*



发展水平:
发展中国家、小岛屿发展中国家 (SIDS)

相对强的领域

N/A

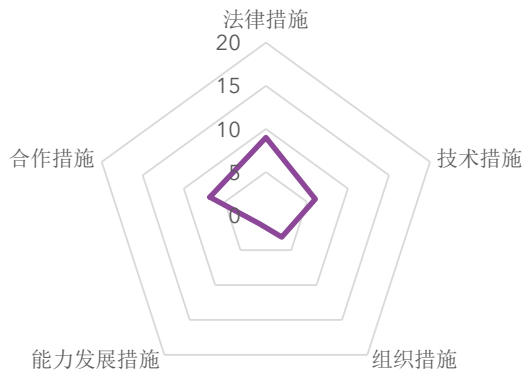
潜在增长领域

N/A

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
0	0	0	0	0	0

来源：国际电联全球网络安全指数 v4, 2020 年

蒙古



发展水平:
发展中国家、内陆国家

相对强的领域

法律措施

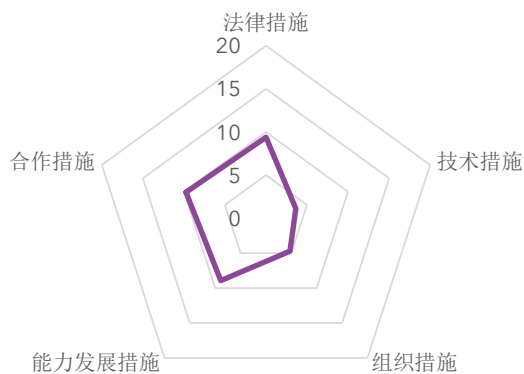
潜在增长领域

能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
26.20	9.00	6.02	3.13	1.23	6.82

来源：国际电联全球网络安全指数 v4, 2020 年

缅甸联邦共和国



发展水平:
发展中国家、最不发达国家 (LDC)

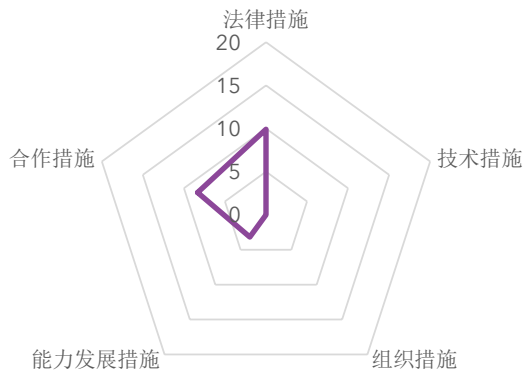
相对强的领域
合作措施、法律措施

潜在增长领域
技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
36.41	9.39	3.64	4.71	8.92	9.75

来源：国际电联全球网络安全指数 v4, 2020 年

瑙鲁共和国**



发展水平:
发展中国家、小岛屿发展中国家 (SIDS)

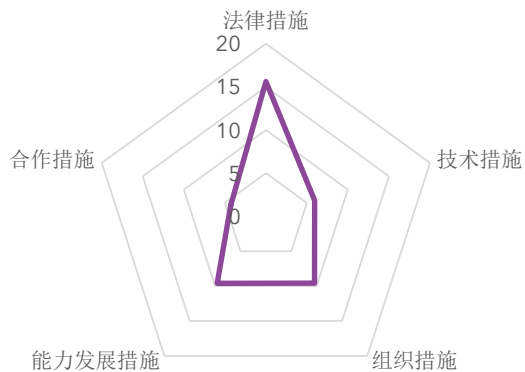
相对强的领域
法律措施

潜在增长领域
技术措施、组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
21.42	9.91	0.00	0.00	3.18	8.33

来源：国际电联全球网络安全指数 v4, 2020 年

尼泊尔联邦民主共和国**



发展水平：
发展中国家、最不发达国家
(LDC)、内陆国家

相对强的领域

法律措施

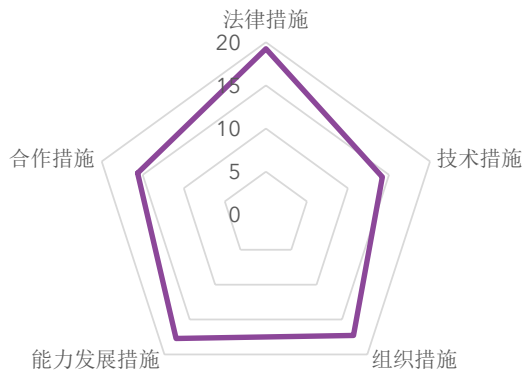
潜在增长领域

合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
44.99	15.61	5.94	9.58	9.60	4.26

来源：国际电联全球网络安全指数 v4, 2020 年

新西兰**



发展水平：

发达国家

相对强的领域

法律措施

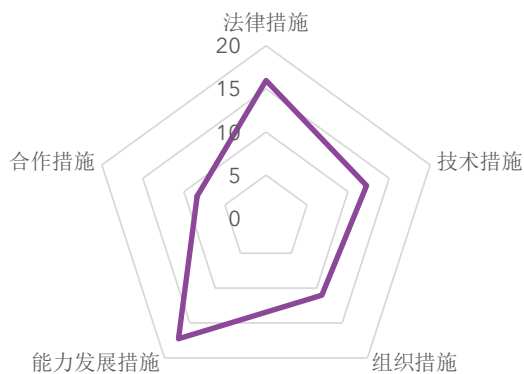
潜在增长领域

技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
84.04	19.24	14.19	17.27	17.71	15.63

来源：国际电联全球网络安全指数 v4, 2020 年

巴基斯坦伊斯兰共和国



发展水平：
发展中国家

相对强的领域

能力发展措施

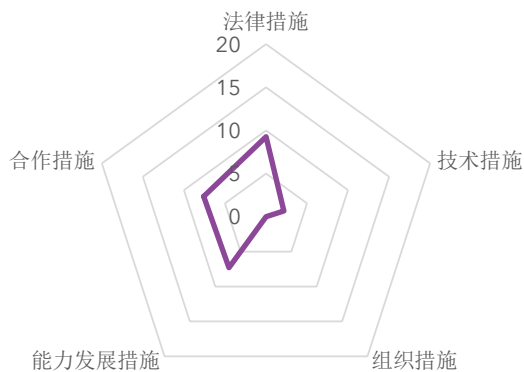
潜在增长领域

合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
64.88	15.97	12.26	11.01	17.25	8.38

来源：国际电联全球网络安全指数 v4，2020 年

巴布亚新几内亚**



发展水平：

发展中国家、小岛屿发展中国家 (SIDS)

相对强的领域

法律措施

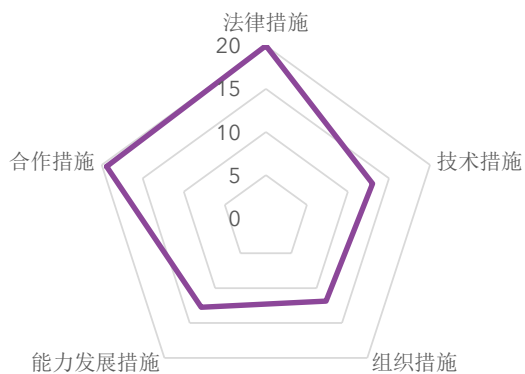
潜在增长领域

组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
26.33	9.26	2.18	0.00	7.30	7.59

来源：国际电联全球网络安全指数 v4，2020 年

菲律宾共和国



发展水平：
发展中国家

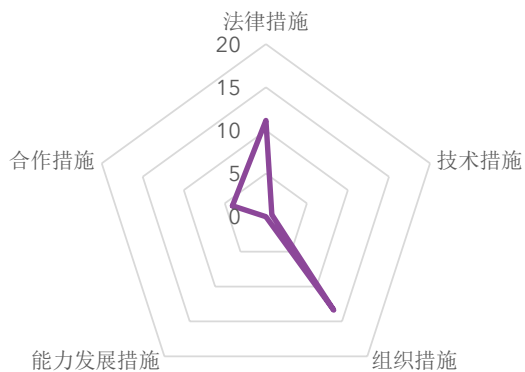
相对强的领域
法律措施、合作措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
77.00	20.00	13.00	11.85	12.74	19.41

来源：国际电联全球网络安全指数 v4，2020 年

萨摩亚独立国



发展水平：
发展中国家、小岛屿发展中国家 (SIDS)

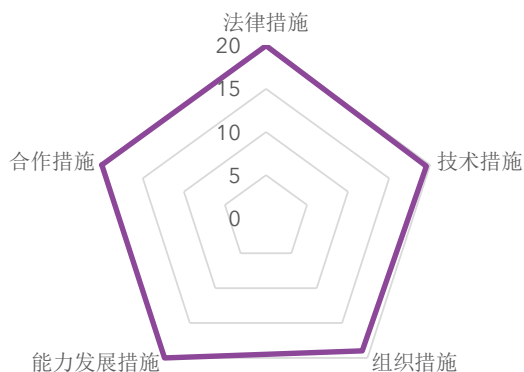
相对强的领域
组织措施

潜在增长领域
能力发展措施、技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
29.33	11.15	0.73	13.37	0.00	4.07

来源：国际电联全球网络安全指数 v4，2020 年

新加坡共和国



发展水平:
发展中国家、小岛屿发展中国家 (SIDS)

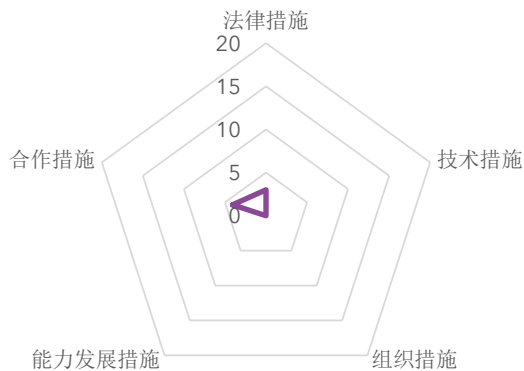
相对强的领域
法律措施、合作措施、能力发展措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
98.52	20.00	19.54	18.98	20.00	20.00

来源：国际电联全球网络安全指数 v4, 2020 年

所罗门群岛



发展水平:
发展中国家、最不发达国家 (LDC)、小岛屿发展中国家 (SIDS)

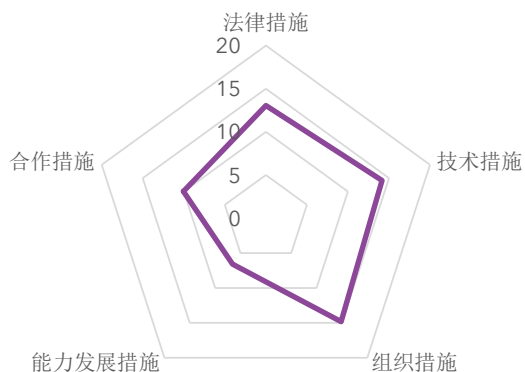
相对强的领域
合作措施、法律措施

潜在增长领域
技术措施、组织措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
7.08	3.00	0.00	0.00	0.00	4.07

来源：国际电联全球网络安全指数 v4, 2020 年

斯里兰卡民主社会主义共和国



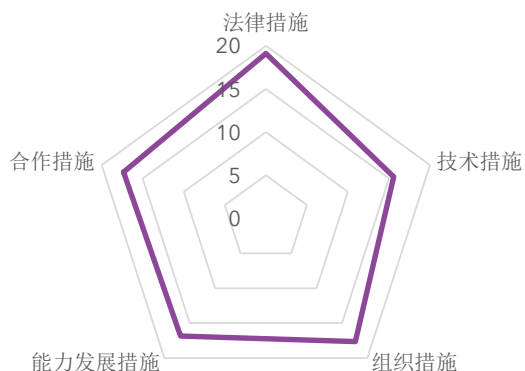
发展水平:
发展中国家

相对强的领域
组织措施、技术措施
潜在增长领域
能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
58.65	13.05	14.15	14.82	6.58	10.04

来源：国际电联全球网络安全指数 v4, 2020 年

泰国



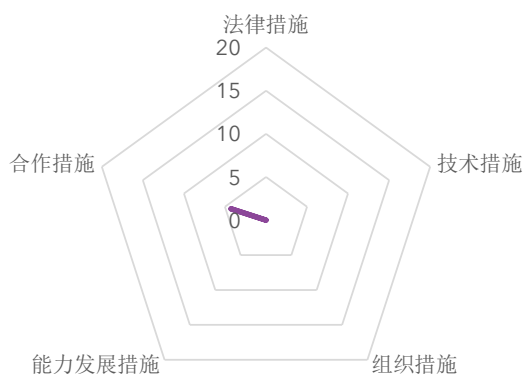
发展水平:
发展中国家

相对强的领域
法律措施
潜在增长领域
技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
86.50	19.11	15.57	17.64	16.84	17.34

来源：国际电联全球网络安全指数 v4, 2020 年

东帝汶民主共和国**



发展水平:

发展中国家、最不发达国家 (LDC)、小岛屿发展中国家 (SIDS)

相对强的领域

合作措施

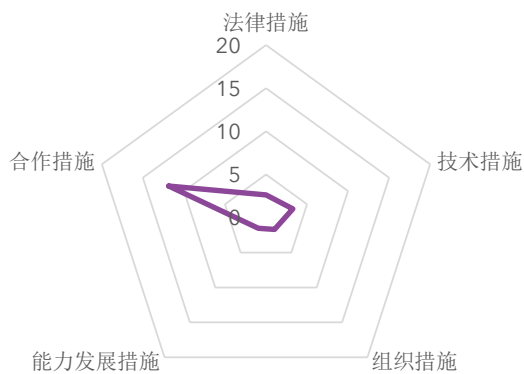
潜在增长领域

法律措施、技术措施、组织措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
4.26	0.00	0.00	0.00	0.00	4.26

来源：国际电联全球网络安全指数 v4, 2020 年

汤加王国**



发展水平:

发展中国家、小岛屿发展中国家 (SIDS)

相对强的领域

合作措施

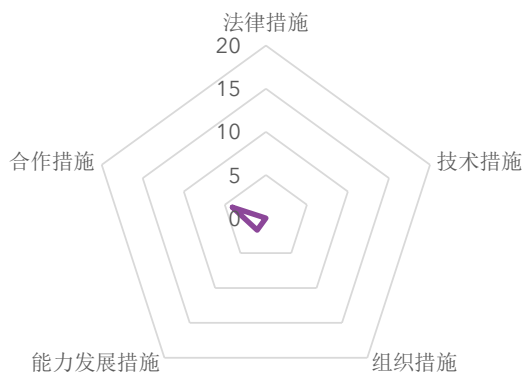
潜在增长领域

组织措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
20.95	2.63	3.27	1.69	1.52	11.85

来源：国际电联全球网络安全指数 v4, 2020 年

图瓦卢**



发展水平：

发展中国家、最不发达国家（LDC）、小岛屿发展中国家（SIDS）

相对强的领域

合作措施

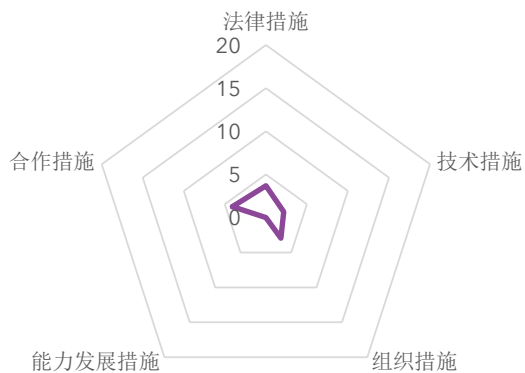
潜在增长领域

法律措施、技术措施、组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
5.78	0.00	0.00	0.00	1.71	4.07

来源：国际电联全球网络安全指数 v4, 2020 年

瓦努阿图共和国



发展水平：

发展中国家、小岛屿发展中国家（SIDS）

相对强的领域

合作措施

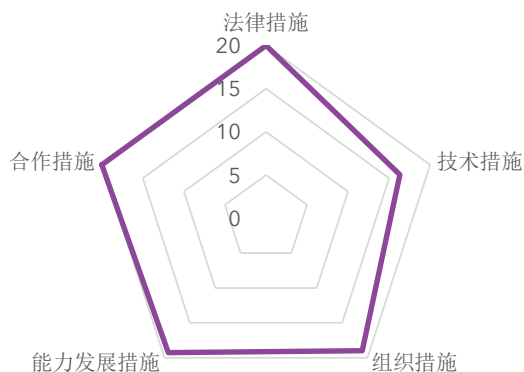
潜在增长领域

能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
12.88	3.69	2.18	2.95	0.00	4.07

来源：国际电联全球网络安全指数 v4, 2020 年

越南社会主义共和国



发展水平:
发展中国家

相对强的领域
法律措施、合作措施

潜在增长领域
技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
94.55	20.00	16.31	18.98	19.26	20.00

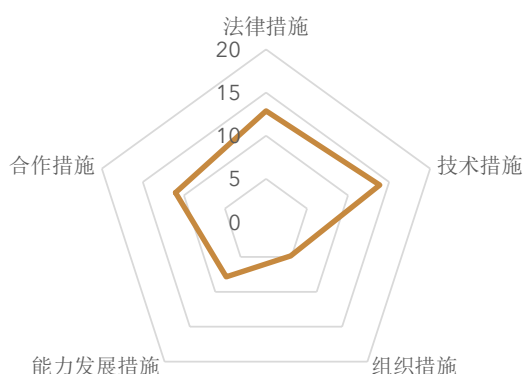
来源：国际电联全球网络安全指数 v4，2020 年

** 未响应问卷调查/GCI小组收集的数据

* 无数据

独联体区域

亚美尼亚共和国**



发展水平:
发展中国家、内陆国家

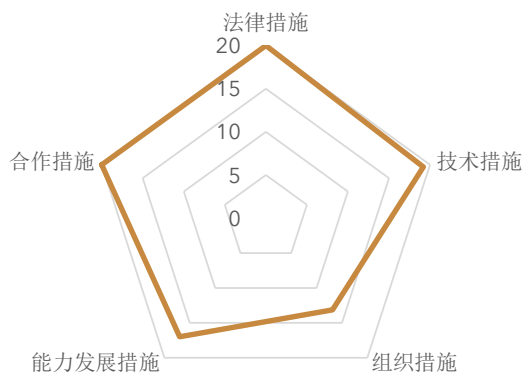
相对强的领域
技术措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
50.47	12.87	13.86	4.87	7.85	11.02

来源：国际电联全球网络安全指数 v4，2020 年

阿塞拜疆共和国



发展水平:
发展中国家、内陆国家

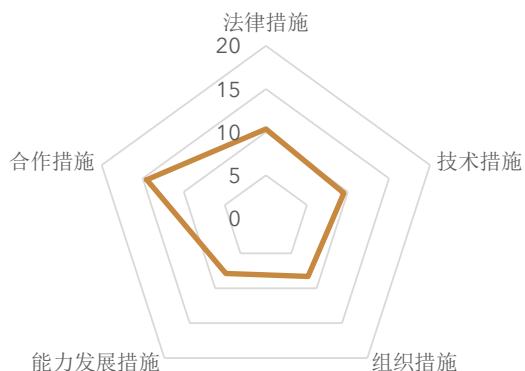
相对强的领域
法律措施、合作措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
89.31	20.00	19.19	13.14	16.99	20.00

来源：国际电联全球网络安全指数 v4, 2020 年

白俄罗斯共和国



发展水平:
发达国家

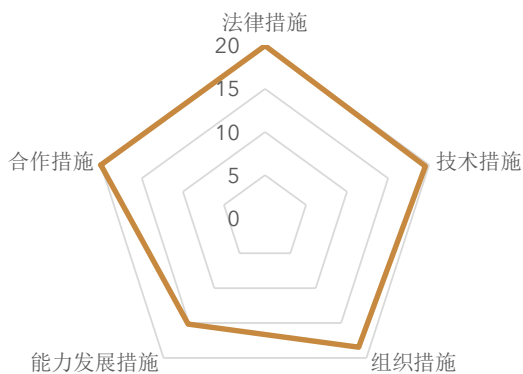
相对强的领域
合作措施

潜在增长领域
组织措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
50.57	10.36	9.50	8.31	7.88	14.51

来源：国际电联全球网络安全指数 v4, 2020 年

哈萨克斯坦共和国



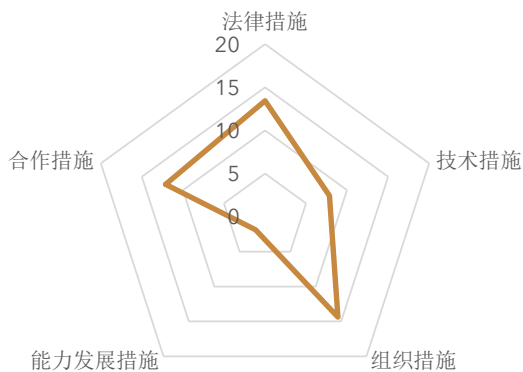
发展水平:
发展中国家

相对强的领域
法律措施、合作措施
潜在增长领域
能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
93.15	20.00	19.54	18.46	15.15	20.00

来源：国际电联全球网络安全指数 v4，2020 年

吉尔吉斯斯坦共和国



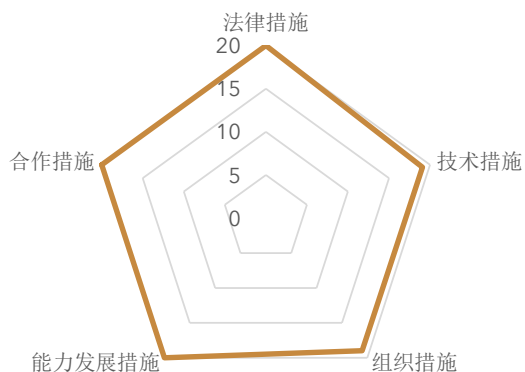
发展水平:
发展中国家、内陆国家

相对强的领域
组织措施、法律措施
潜在增长领域
能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
49.64	13.43	7.85	14.37	1.87	12.11

来源：国际电联全球网络安全指数 v4，2020 年

俄罗斯联邦



发展水平：
发达国家

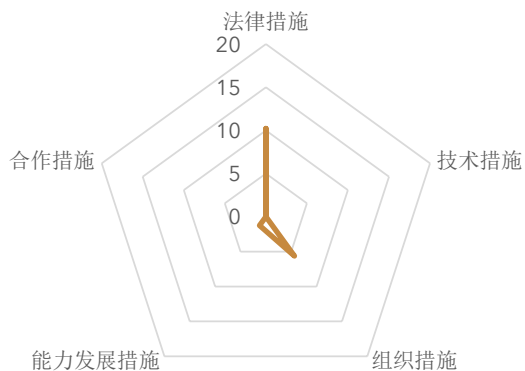
相对强的领域
法律措施、合作措施、能力发展措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
98.06	20.00	19.08	18.98	20.00	20.00

来源：国际电联全球网络安全指数 v4, 2020 年

塔吉克斯坦共和国**



发展水平：
发展中国家、内陆国家

相对强的领域
法律措施

潜在增长领域
技术措施、合作措施

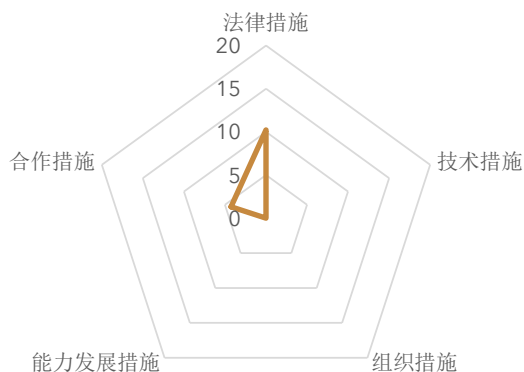
总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
17.10	10.22	0.00	5.63	1.25	0.00

来源：国际电联全球网络安全指数 v4, 2020 年

** 未响应问卷调查/GCI小组收集的数据

* 无数据

土库曼斯坦**



发展水平：
发展中国家、内陆国家

相对强的领域

法律措施

潜在增长领域

技术措施、组织措施、能力发展措施

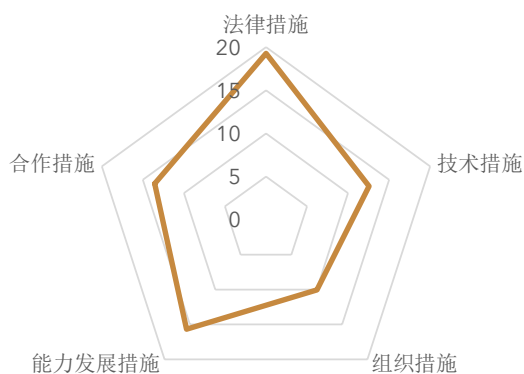
总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
14.48	10.22	0.00	0.00	0.00	4.26

来源：国际电联全球网络安全指数 v4，2020 年

** 未响应问卷调查/GCI小组收集的数据

* 无数据

乌兹别克斯坦共和国



发展水平：
发展中国家、内陆国家

相对强的领域

法律措施

潜在增长领域

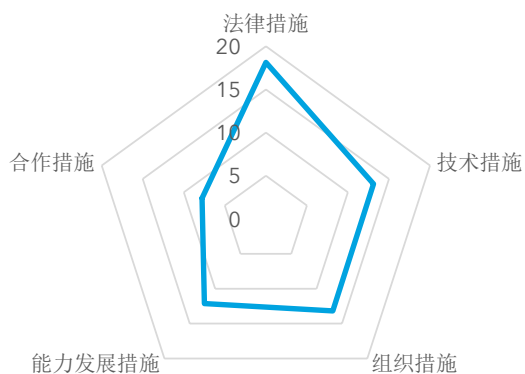
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
71.11	19.27	12.56	10.05	15.68	13.56

来源：国际电联全球网络安全指数 v4，2020 年

欧洲

阿尔巴尼亚共和国



发展水平:
发达国家

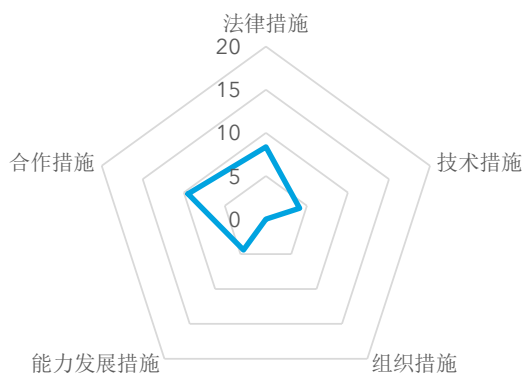
相对强的领域
法律措施

潜在增长领域
合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
64.32	18.13	13.12	13.18	12.12	7.78

来源：国际电联全球网络安全指数 v4, 2020 年

安道尔公国**



发展水平:
发达国家

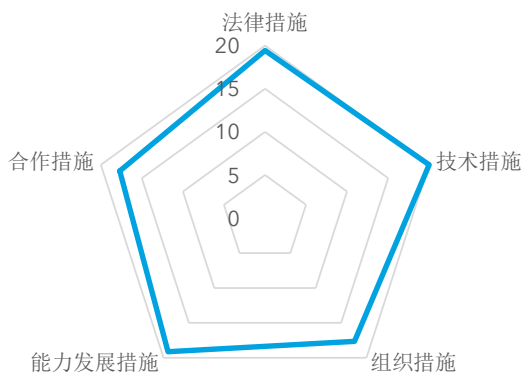
相对强的领域
合作措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
26.38	8.37	4.11	0.00	4.41	9.49

来源：国际电联全球网络安全指数 v4, 2020 年

奥地利



发展水平:
发达国家

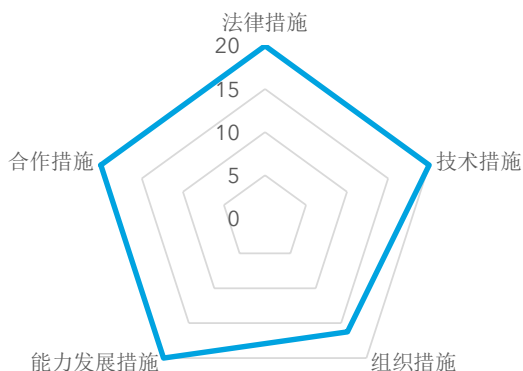
相对强的领域
技术措施

潜在增长领域
组织措施、合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
93.89	19.43	20.00	17.64	19.13	17.70

来源：国际电联全球网络安全指数 v4，2020 年

比利时



发展水平:
发达国家

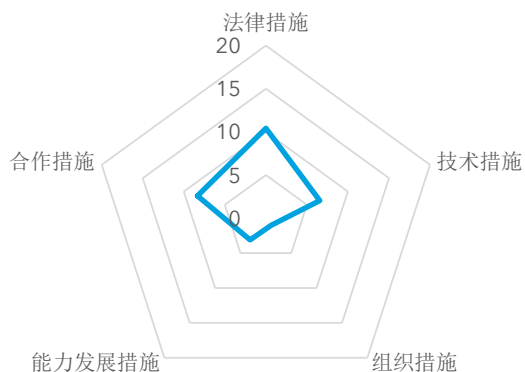
相对强的领域
法律措施、技术措施、合作措施、能力发展措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
96.25	20.00	20.00	16.25	20.00	20.00

来源：国际电联全球网络安全指数 v4，2020 年

波斯尼亚和黑塞哥维那



发展水平:
发达国家

相对强的领域

法律措施

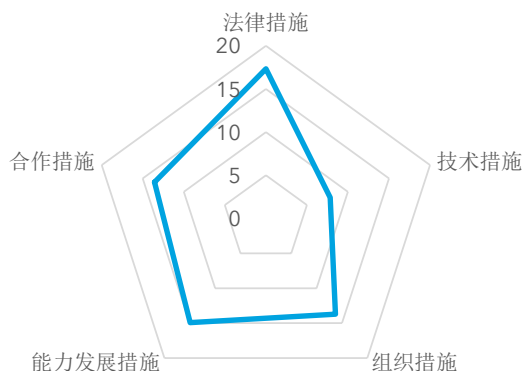
潜在增长领域

组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
29.44	10.41	6.56	1.02	3.12	8.33

来源：国际电联全球网络安全指数 v4, 2020 年

保加利亚共和国



发展水平:
发达国家

相对强的领域

法律措施

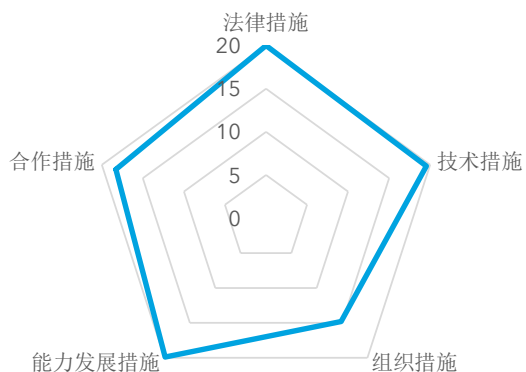
潜在增长领域

技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
67.38	17.34	7.84	13.72	14.92	13.57

来源：国际电联全球网络安全指数 v4, 2020 年

克罗地亚共和国



发展水平：
发达国家

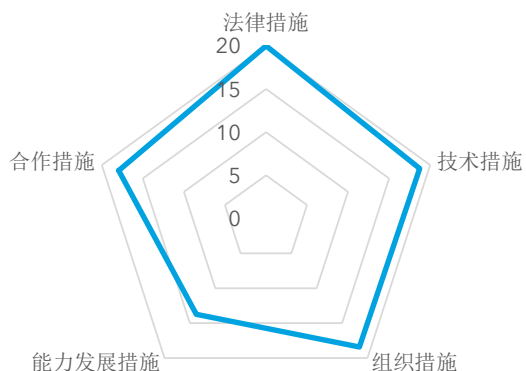
相对强的领域
法律措施、能力发展措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
92.53	20.00	19.54	14.80	19.89	18.29

来源：国际电联全球网络安全指数 v4，2020 年

塞浦路斯共和国



发展水平：
发达国家

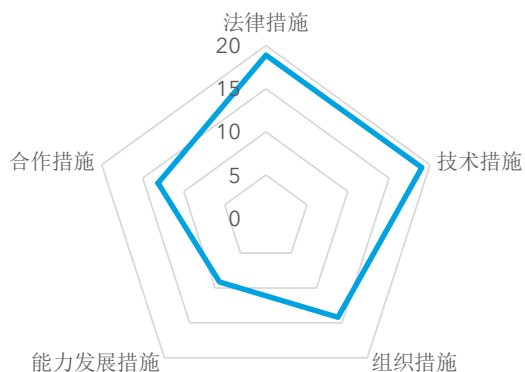
相对强的领域
法律措施

潜在增长领域
能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
88.82	20.00	18.73	18.41	13.73	17.94

来源：国际电联全球网络安全指数 v4，2020 年

捷克共和国



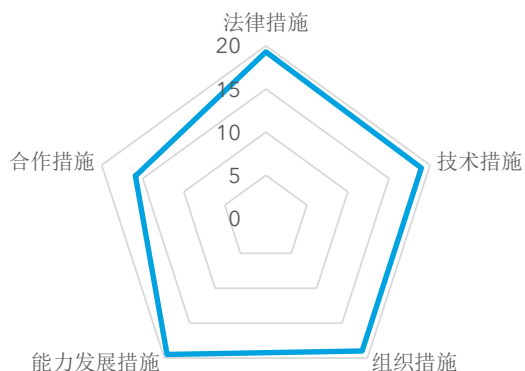
发展水平:
发达国家

相对强的领域
技术措施、法律措施
潜在增长领域
能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
74.37	18.89	19.00	14.20	9.14	13.14

来源：国际电联全球网络安全指数 v4, 2020 年

丹麦



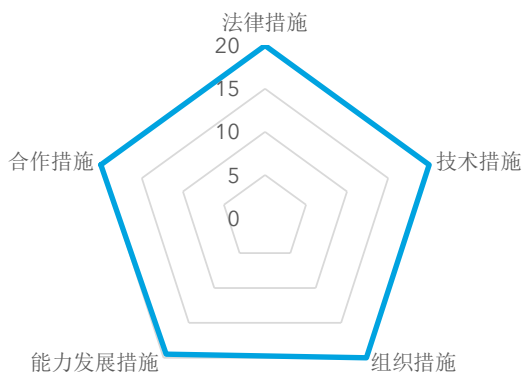
发展水平:
发达国家

相对强的领域
能力发展措施、法律措施
潜在增长领域
合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
92.60	19.30	18.94	18.98	19.48	15.89

来源：国际电联全球网络安全指数 v4, 2020 年

爱沙尼亚共和国



发展水平:
发达国家

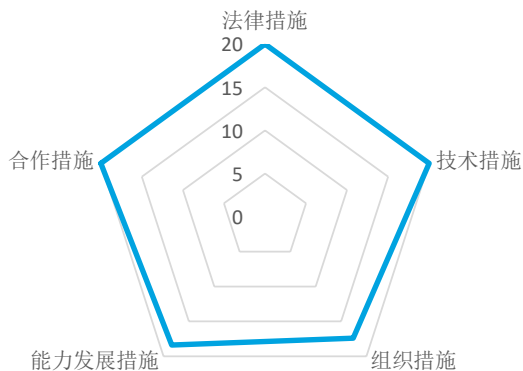
相对强的领域
法律措施、技术措施、组织措施、合作措施

潜在增长领域
能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
99.48	20.00	20.00	20.00	19.48	20.00

来源：国际电联全球网络安全指数 v4，2020 年

芬兰



发展水平:
发达国家

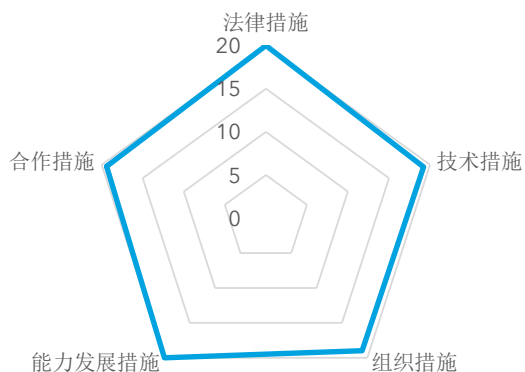
相对强的领域
法律措施、技术措施、合作措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
92.07	20.00	20.00	14.33	17.74	20.00

来源：国际电联全球网络安全指数 v4，2020 年

法国



发展水平:
发达国家

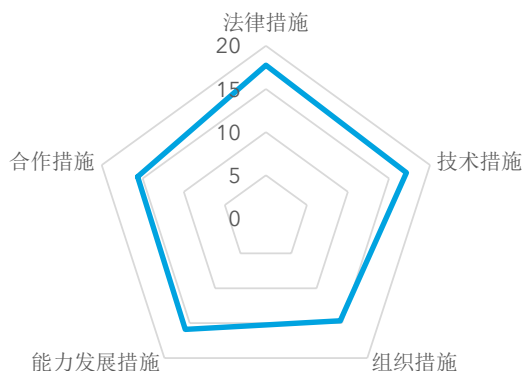
相对强的领域
法律措施、能力发展措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
97.60	20.00	19.21	18.98	20.00	19.41

来源：国际电联全球网络安全指数 v4, 2020 年

格鲁吉亚



发展水平:
发展中国家

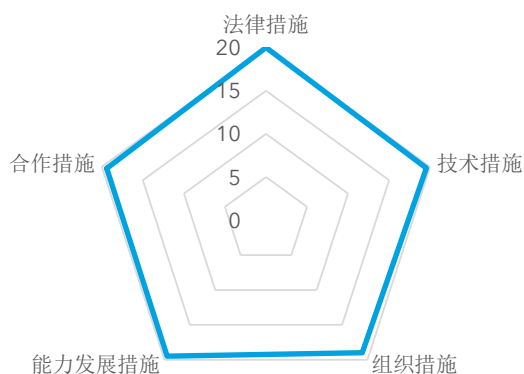
相对强的领域
法律措施

潜在增长领域
组织措施、合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
81.07	17.75	17.13	14.67	15.89	15.63

来源：国际电联全球网络安全指数 v4, 2020 年

德意志联邦共和国



发展水平:
发达国家

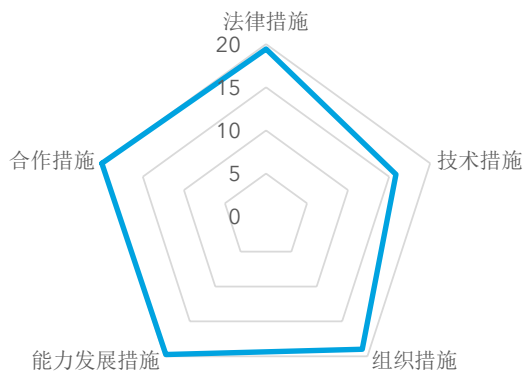
相对强的领域
法律措施、技术措施、能力发展措施、合作措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
97.41	20.00	19.54	18.98	19.48	19.41

来源：国际电联全球网络安全指数 v4，2020 年

希腊



发展水平:
发达国家

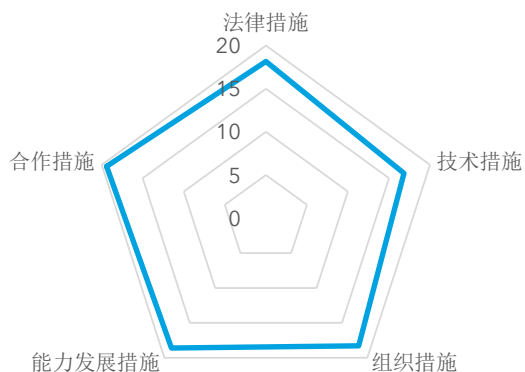
相对强的领域
合作措施、能力发展措施、法律措施

潜在增长领域
技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
93.98	19.43	15.83	18.98	19.74	20.00

来源：国际电联全球网络安全指数 v4，2020 年

匈牙利



发展水平:
发达国家

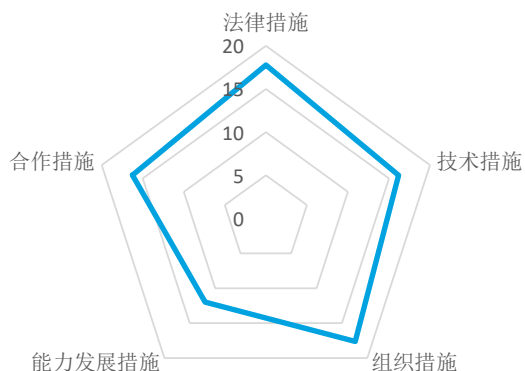
相对强的领域
合作措施、能力发展措施

潜在增长领域
技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
91.28	18.16	16.82	18.29	18.60	19.41

来源：国际电联全球网络安全指数 v4, 2020 年

冰岛



发展水平:
发达国家

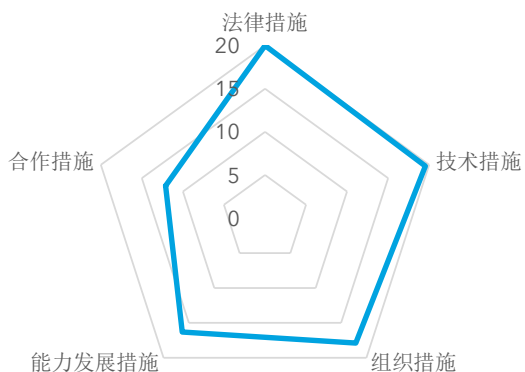
相对强的领域
法律措施、组织措施

潜在增长领域
能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
79.81	17.78	16.17	17.62	11.99	16.25

来源：国际电联全球网络安全指数 v4, 2020 年

爱尔兰



发展水平:
发达国家

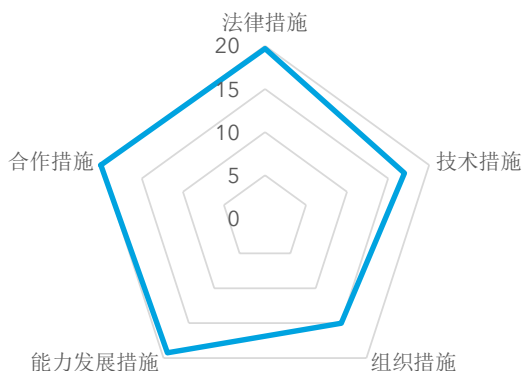
相对强的领域
法律措施、技术措施

潜在增长领域
合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
85.86	20.00	19.54	17.89	16.32	12.11

来源：国际电联全球网络安全指数 v4，2020 年

以色列**



发展水平:
发达国家

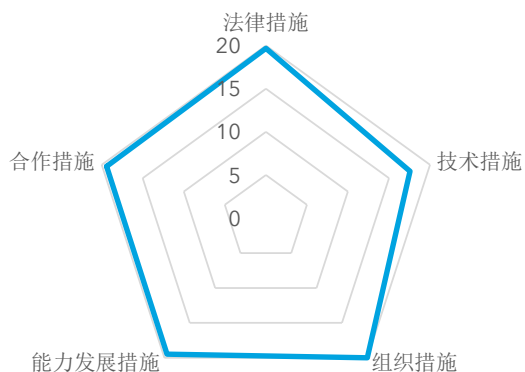
相对强的领域
合作措施、法律措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
90.93	19.68	16.99	15.02	19.24	20.00

来源：国际电联全球网络安全指数 v4，2020 年

意大利



发展水平：
发达国家

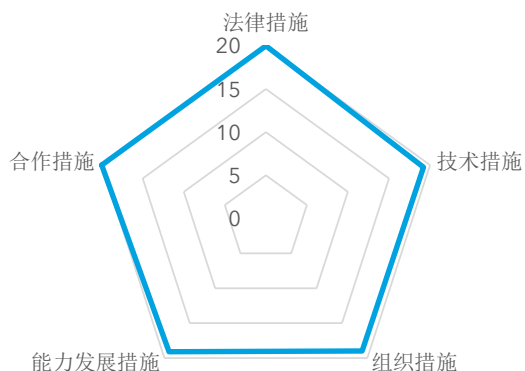
相对强的领域
组织措施

潜在增长领域
技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
96.13	19.68	17.56	20.00	19.48	19.41

来源：国际电联全球网络安全指数 v4，2020 年

拉脱维亚共和国



发展水平：
发达国家

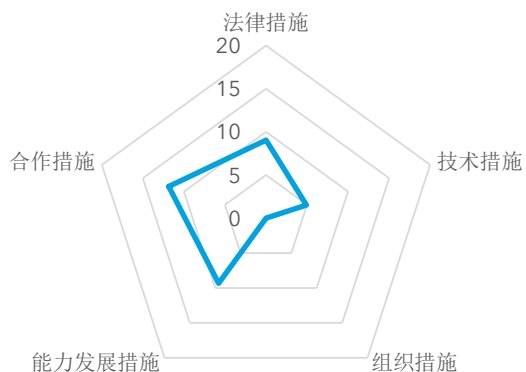
相对强的领域
法律措施、合作措施、技术措施、能力发展措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
97.28	20.00	19.21	18.98	19.09	20.00

来源：国际电联全球网络安全指数 v4，2020 年

列支敦士登公国**



发展水平:
发达国家、内陆国家

相对强的领域

合作措施

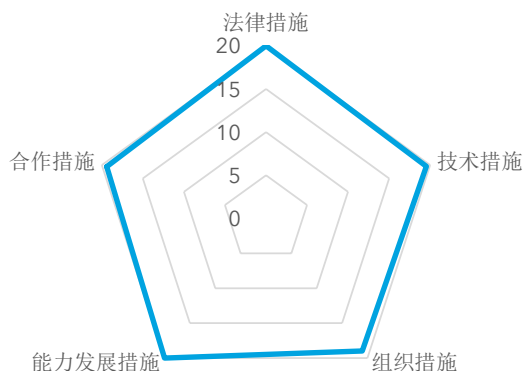
潜在增长领域

组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
35.15	9.04	4.93	0.00	9.34	11.85

来源：国际电联全球网络安全指数 v4，2020 年

立陶宛共和国



发展水平:

发达国家

相对强的领域

法律措施、能力发展措施、技术措施、合作措施

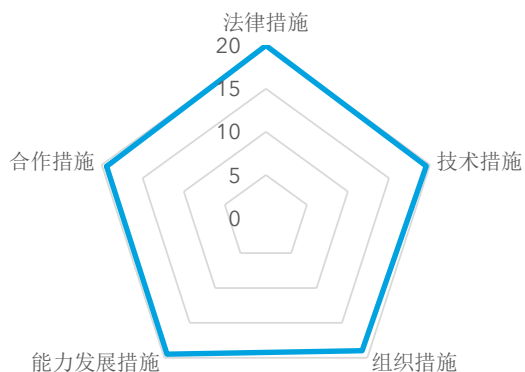
潜在增长领域

组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
97.93	20.00	19.54	18.98	20.00	19.41

来源：国际电联全球网络安全指数 v4，2020 年

卢森堡



发展水平:
发达国家、内陆国家

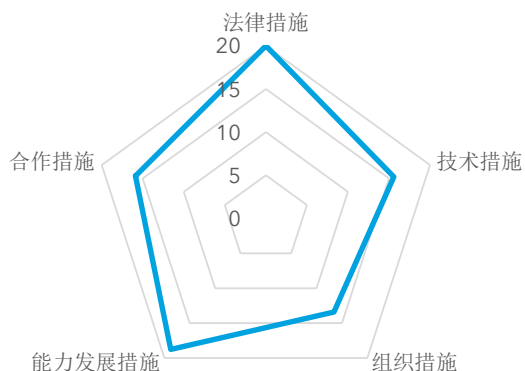
相对强的领域
法律措施、技术措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
97.41	20.00	19.54	18.98	19.48	19.41

来源：国际电联全球网络安全指数 v4, 2020 年

马耳他



发展水平:
发达国家

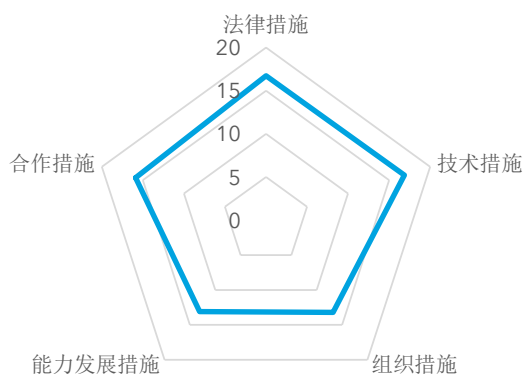
相对强的领域
法律措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
83.65	20.00	15.59	13.41	18.76	15.89

来源：国际电联全球网络安全指数 v4, 2020 年

摩尔多瓦共和国



发展水平：
发达国家、内陆国家

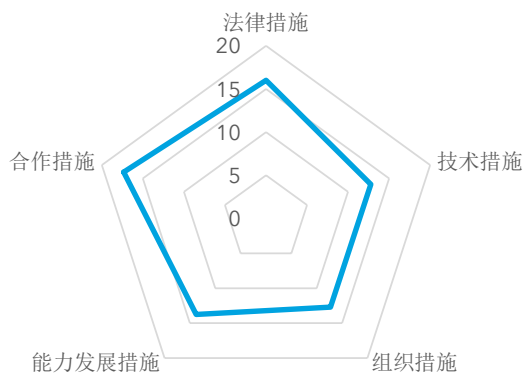
相对强的领域
法律措施、技术措施

潜在增长领域
组织措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
75.78	16.73	16.86	13.21	13.09	15.89

来源：国际电联全球网络安全指数 v4，2020 年

摩纳哥公国



发展水平：
发达国家

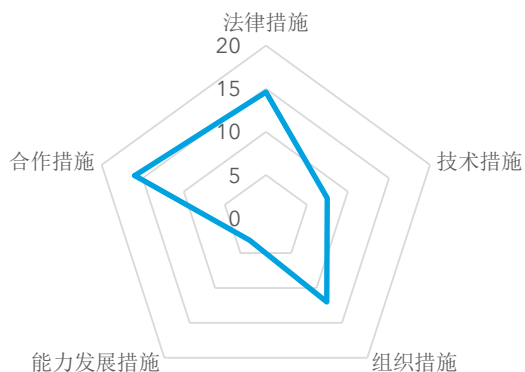
相对强的领域
合作措施

潜在增长领域
技术措施、组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
72.57	16.00	12.77	12.70	13.75	17.34

来源：国际电联全球网络安全指数 v4，2020 年

黑山共和国



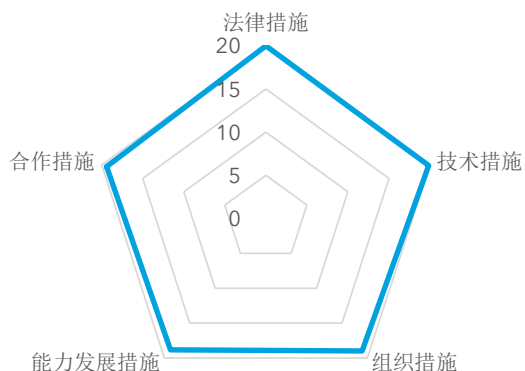
发展水平：
发达国家

相对强的领域
合作措施
潜在增长领域
能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
53.23	14.61	7.48	12.00	3.18	15.97

来源：国际电联全球网络安全指数 v4, 2020 年

荷兰王国**



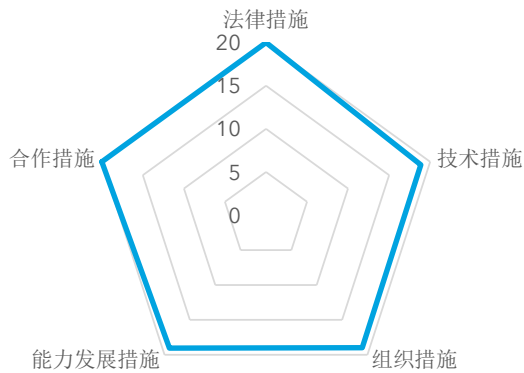
发展水平：
发达国家

相对强的领域
法律措施、技术措施、合作措施
潜在增长领域
组织措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
97.05	20.00	19.84	18.98	18.82	19.41

来源：国际电联全球网络安全指数 v4, 2020 年

挪威**



发展水平:
发达国家

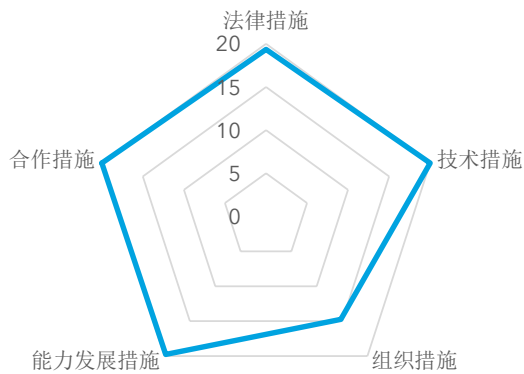
相对强的领域
法律措施、合作措施

潜在增长领域
技术措施、组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
96.89	20.00	18.86	18.98	19.04	20.00

来源：国际电联全球网络安全指数 v4，2020 年

波兰共和国



发展水平:
发达国家

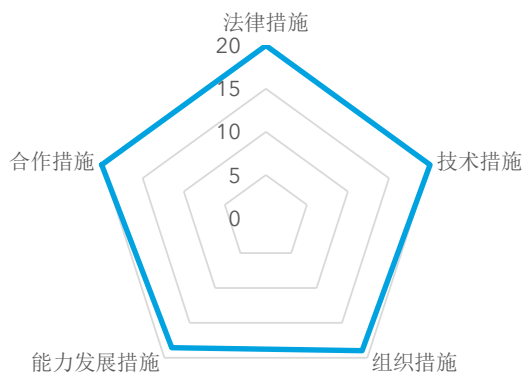
相对强的领域
技术措施、合作措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
93.86	19.35	20.00	14.74	19.77	20.00

来源：国际电联全球网络安全指数 v4，2020 年

葡萄牙



发展水平:
发达国家

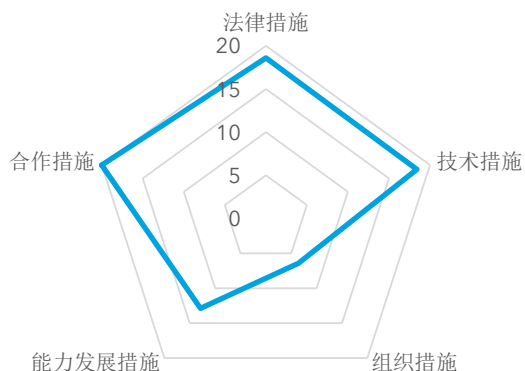
相对强的领域
法律措施、技术措施、合作措施

潜在增长领域
组织措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
97.32	20.00	20.00	18.98	18.34	20.00

来源：国际电联全球网络安全指数 v4，2020 年

罗马尼亚



发展水平:
发达国家

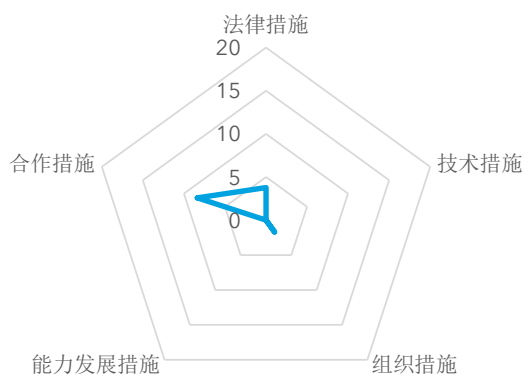
相对强的领域
合作措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
76.29	18.60	18.40	6.42	12.88	20.00

来源：国际电联全球网络安全指数 v4，2020 年

圣马力诺共和国



发展水平:
发达国家、内陆国家

相对强的领域

合作措施

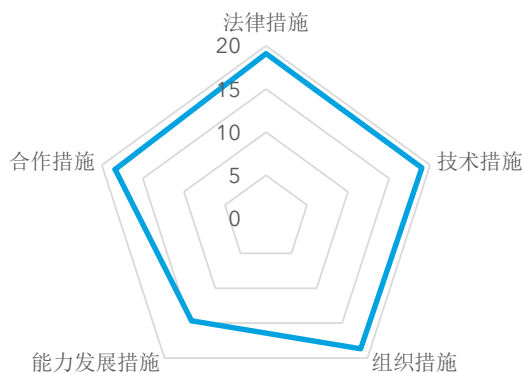
潜在增长领域

技术措施、能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
13.83	3.77	0.00	1.69	0.00	8.37

来源：国际电联全球网络安全指数 v4, 2020 年

塞尔维亚共和国



发展水平:
发达国家、内陆国家

相对强的领域

法律措施、技术措施

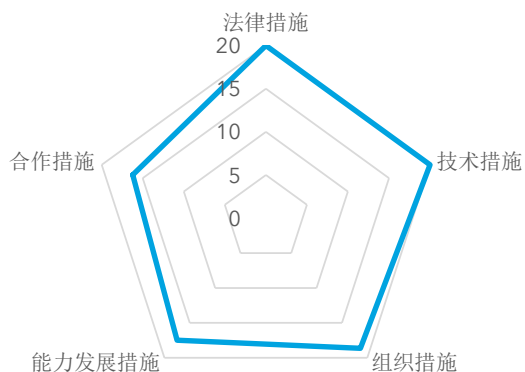
潜在增长领域

能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
89.80	19.10	18.99	18.67	14.66	18.38

来源：国际电联全球网络安全指数 v4, 2020 年

斯洛伐克共和国



发展水平:
发达国家、内陆国家

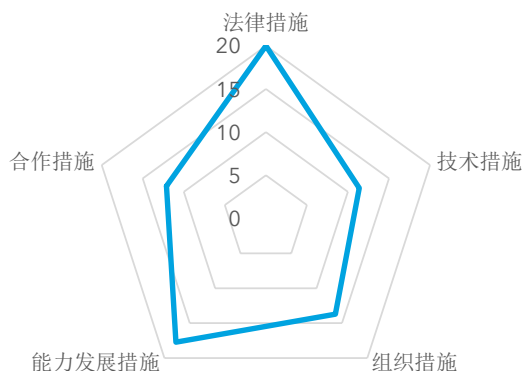
相对强的领域
法律措施、技术措施

潜在增长领域
合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
92.36	20.00	20.00	18.64	17.50	16.22

来源：国际电联全球网络安全指数 v4, 2020 年

斯洛文尼亚共和国



发展水平:
发达国家

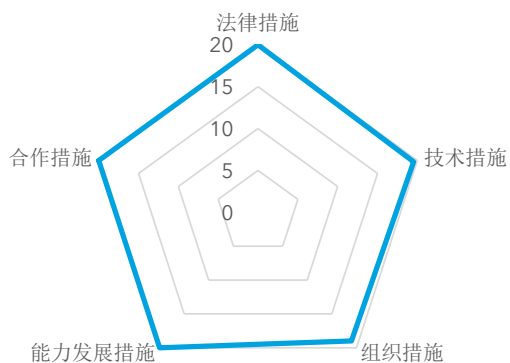
相对强的领域
法律措施

潜在增长领域
技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
74.93	20.00	11.38	13.71	17.72	12.11

来源：国际电联全球网络安全指数 v4, 2020 年

西班牙



发展水平:

发达国家

相对强的领域

法律措施、合作措施、能力发展措施、技术措施

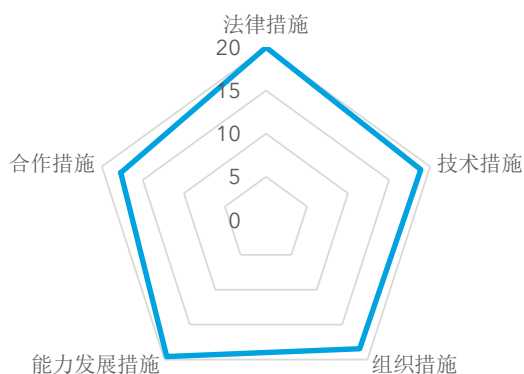
潜在增长领域

组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
98.52	20.00	19.54	18.98	20.00	20.00

来源：国际电联全球网络安全指数 v4，2020 年

瑞典



发展水平:

发达国家

相对强的领域

法律措施、能力发展措施

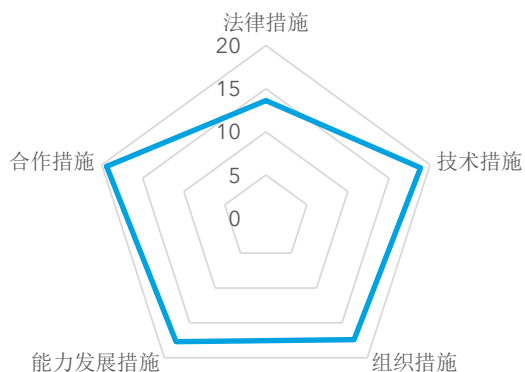
潜在增长领域

合作措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
94.59	20.00	18.86	18.46	19.57	17.70

来源：国际电联全球网络安全指数 v4，2020 年

瑞士联邦**



发展水平：
发达国家、内陆国家

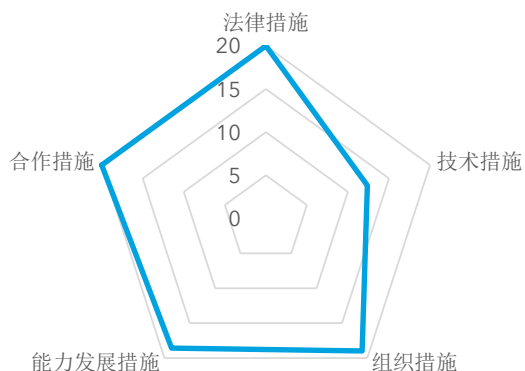
相对强的领域
合作措施、技术措施

潜在增长领域
法律措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
86.97	13.62	18.85	17.40	17.69	19.41

来源：国际电联全球网络安全指数 v4, 2020 年

北马其顿共和国



发展水平：
发达国家、内陆国家

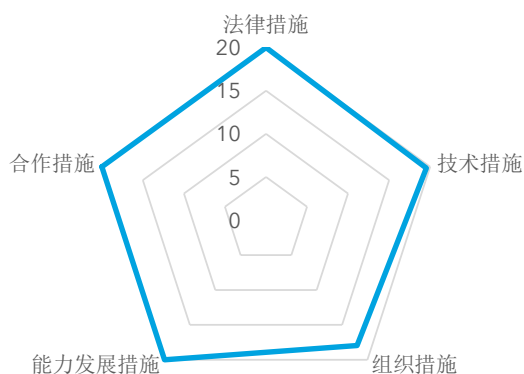
相对强的领域
法律措施、合作措施

潜在增长领域
技术措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
89.92	20.00	12.37	18.98	18.57	20.00

来源：国际电联全球网络安全指数 v4, 2020 年

土耳其



发展水平：
发展中国家

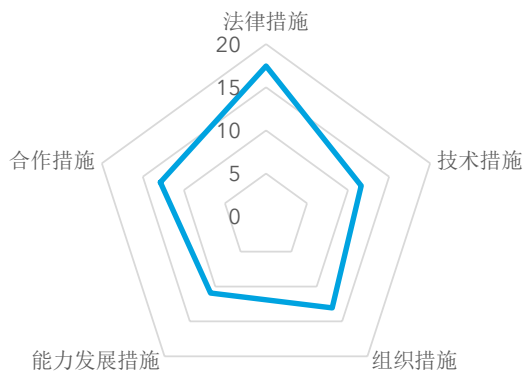
相对强的领域
法律措施、合作措施、技术措施、能力发展措施

潜在增长领域
组织措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
97.50	20.00	19.54	17.96	20.00	20.00

来源：国际电联全球网络安全指数 v4，2020 年

乌克兰



发展水平：
发达国家

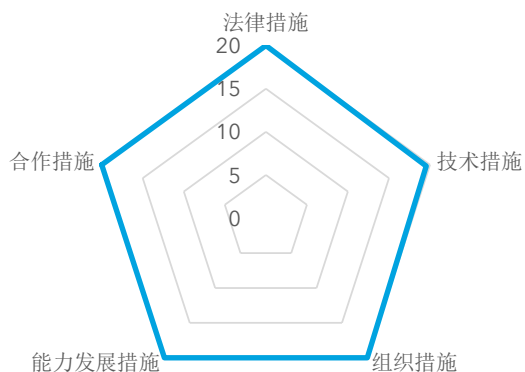
相对强的领域
法律措施

潜在增长领域
能力发展措施

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
65.93	17.46	11.60	13.06	10.94	12.87

来源：国际电联全球网络安全指数 v4，2020 年

大不列颠及北爱尔兰联合王国



发展水平:
发达国家

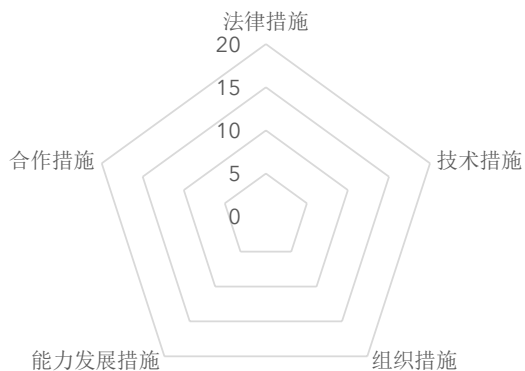
相对强的领域
法律措施、组织措施、合作措施、能力发展措施

潜在增长领域
技术措施

总分	法律措施	技术措施	组织措施	合作措施	能力发展措施
99.54	20.00	19.54	20.00	20.00	20.00

来源：国际电联全球网络安全指数 v4, 2020 年

梵蒂冈*



发展水平:
发达国家、内陆国家

相对强的领域
N/A

潜在增长领域
N/A

总分	法律措施	技术措施	组织措施	能力发展措施	合作措施
0	0	0	0	0	0

来源：国际电联全球网络安全指数 v4, 2020 年

** 未响应问卷调查/GCI小组收集的数据

* 无数据

词汇表

缩写词	定义
CERT	计算机应急响应小组，卡内基梅隆大学注册商标
CI	关键基础设施
CIRT*	计算机事件响应小组，请参阅相关术语CSIRT、CERT
CSIRT	计算机安全事件响应小组
DPP	数据和隐私保护
EU	欧洲联盟
GCI-1/2/3/4	全球网络安全指数的迭代
GDPR	通用数据保护条例（欧盟）
ICT	信息通信技术
ITU	国际电信联盟
LDC	最不发达国家
LLDCs	内陆发达国家
MLAT	法律互助条约
MSMEs	中小微企业
NCS	国家网络安全战略
NGO	非政府组织
ODC	其他发展中国家
OT	操作技术
PPP	公私合作伙伴关系
SIDS	小岛屿发展中国家
SME	中小企业
UN	联合国

附件A：方法论

A1. GCI范围和框架

全球网络安全指数（GCI）的任务源自国际电联全权代表大会第130号决议（2018年，迪拜，修订版）“加强国际电联在树立使用信息通信技术（ICT）的信心和提高安全性方面的作用”。特别地，请各国“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，分享跨行业和跨部门工作的信息”。GCI的目标是促进全球网络安全文化及其在ICT核心上的整合。

表A1：全球网络安全指数参与情况和数据收集年份

	GCI-1	GCI-2	GCI-3	GCI-4
提供联系人的国家数量	105	136	155	169
数据收集年份	2013-2014	2016	2017-2018	2020
发布年份	2015	2017	2019	2021

GCI是围绕国际电联成员提供的数据而制定的，包括感兴趣的个人、专家和行业利益攸关方，作为与澳大利亚战略政策研究所、FIRST（事件响应和安全小组论坛）、格勒诺布尔大学（法国）、印第安纳大学、INTERPOL、在阿曼的国际电联-阿拉伯区域网络安全中心、韩国互联网和安全局、埃及NTRA、网络红队、波托马克政策研究所、UNICRI、牙买加科技大学、UNODC和世界银行有合作关系和有贡献作用的合作伙伴。

GCI范围

全球网络安全指数（GCI）是一个指标的综合指数，随着每次迭代而演变，用于监测全球网络安全议程（GCA）五个支柱中的网络安全承诺水平，其主要目标是衡量：

- 国家内以及相对于其他国家的网络安全承诺的类型、级别和随时间的演变。
- 从全球角度看各国在网络安全承诺方面的进展。
- 从区域角度看网络安全承诺方面的进展。
- 网络安全承诺鸿沟（即各国在网络安全举措参与程度方面的差异）。

GCI的目标是协助各国确定网络安全领域有待改进的领域，并鼓励它们针对这些领域采取行动。这也将是帮助提高全球网络安全承诺整体水平、协调实践和培育全球网络安全文化的机会。GCI旨在说明网络安全方面的成功范例，这些范例可以作为具有相似国家环境的国家的良好实践和指南。

A2. 国际电联网络安全合作框架

网络安全是一个多学科领域，其应用涉及纵向和横向的所有部门、行业和利益攸关方。为了加速发展国家能力，需要政治、经济和社会力量的共同努力。这可以由执法部

门、司法部门、教育机构、部委、私营部门运营商、技术开发商、公私合作伙伴关系和国家内合作等来完成。

国际电联网络安全国际多利益攸关方合作框架旨在形成当前与未来举措之间的协同，重点关注以下五个支柱，这些支柱塑造了国家网络安全文化的内在基石。

表A2: GCI 2020支柱描述

法律措施
<p>基于处理网络安全和网络犯罪问题的现有法律框架的措施。</p> <p>法律措施（包括立法、监管和遏制垃圾邮件立法）授权国家通过调查和起诉犯罪以及对不遵守或违法行为实施制裁来建立基本的响应机制。立法框架设定了可以建立进一步网络安全能力的最低行为基础。从根本上说，目标是制定足够的法律，以协调区域/国际层面的做法并简化国际打击网络犯罪的斗争。</p>
技术措施
<p>基于处理网络安全问题的现有技术机构和框架的措施。</p> <p>只有在信任和安全的的环境中，高效的ICT开发和使用才能得到蓬勃发展。因此，各国需要为软件应用程序和系统建立与安装公认的最低安全标准和认证方案。这些工作需要由负责处理网络事件的国家机构、权威的政府实体和国家框架的实施方案来补充，以观察、警告和响应事件。</p>
组织措施
<p>基于国家层面现有网络安全发展协调机构、政策和战略的措施。</p> <p>组织措施包括确定网络安全目标和战略计划，以及对机构角色、责任和问责制的正式定义，以确保其实施。这些措施对于支持制定和实施有效的网络安全态势必不可少。国家需要制定广泛的战略目标，并在实施、交付和衡量方面制定全面的计划。国家机构必须参与实施该战略并评估结果。如果没有国家战略、治理模式和监管机构，不同部门的工作就会相互冲突，有碍在网络安全发展过程中的有效协调。</p>
能力建设措施
<p>基于促进能力建设的现有研究和开发、教育和培训计划、认证专业人员和公共部门机构的措施。</p> <p>能力建设包括提高公众认识活动、网络安全专业人员认证和鉴定框架、网络安全专业课程、教育计划或学术课程等。该支柱是前三个支柱（法律、技术和组织）的内在支柱。尽管存在许多社会经济和政治影响，但最常见的作法是从技术角度来解决网络安全问题。人力和机构能力建设对提高跨部门的认识、知识和技能、系统和适当的解决方案以及促进合格专业人员的发展而言至关重要。</p>
合作措施
<p>基于现有合作伙伴关系、合作框架和信息共享网络的措施。</p> <p>由于国家之间前所未有的互联程度，网络安全是一项共同的责任，也是一项跨国挑战。加强合作可以发展更强大的网络安全能力，有助于降低网络风险，并能够更好地调查、逮捕和起诉恶意代理。</p>

A3. 按支柱分列的关键变化

法律措施

法律措施衡量在网络安全方面的法律干预，已做更新，以更好地反映与网络安全有关的国家实体法。

- 根据BDT管理咨询小组的建议，全球网络安全指数不再衡量程序法。取而代之的是，在包括身份盗窃、网络骚扰、种族主义在内的几个领域都更加明确了。
- 法律措施下的问题最初是根据《布达佩斯网络犯罪公约》等公约的建议而制定的。然而，现在的答案仅侧重于强调已实施的国家法律，不再收集此类公约的批准情况。尽管如此，鉴于国际公约的影响及其在创造具有约束力的承诺方面的作用，《布达佩斯公约》等国际公约现在被纳入有关合作措施的国际活动下进行衡量。
- 随着人们越来越多地上网，一个同样促进多样性和包容性的、值得信赖的网络空间需要审查诸如隐私以及骚扰、欺凌、儿童诱骗、儿童色情和种族主义等问题。全球网络安全指数的本次迭代增加了有关这些事项的问题。

技术措施

技术支柱已做重组，以更好地反映CIRT的运作方式，包括：

- 计算机事件响应小组 – 政府和国家CIRT已合并为一个指标。
- CIRT认证是提供有关处理网络事件能力之见解的重要元素。为评估国家CIRT¹成熟度水平，添加了SIM3认证计划。TF-CSIRT/可信的介绍人使用SIM3作为评估和具有最高成熟度阶段的“经认证”成员的基础。全球网络安全指数的未来迭代将更深入地探索CIRT的安全成熟度模型。

组织措施

- 由于网络安全是一个持续的过程，因此鼓励各国定期重新审视和修订国家网络安全战略（至少每五年一次），以评估NCS是否在不断变化的风险环境下仍然具有相关性，它是否仍然反映国家目标并了解需要什么样的调整。根据这一建议，在过去五年中未重申或更新其NCS的国家在NCS指标上获得了部分得分。
- 制定保护上网儿童的机制应成为各国的重要优先事项之一，尤其在COVID-19大流行迫使儿童在线学习的情况下。互联网在为儿童教育和成长带来巨大好处的同时，也让他们面临网络风险。大多数国家已采取措施来支持儿童上网保护，例如，通过创建网站和社交媒体等工作，为儿童、家长和教育工作者提供专门的教育材料、信息游戏和指南。为了区分临时的干预措施和在更大、更明确战略内构建的干预措施，后者将获得满分，而只有一次性或零星举措的国家仅获得部分得分。

能力发展措施

自GCI的第二次迭代以来，该支柱的指标一直保持稳定。在本次迭代中，范围扩大到包括提高政府对支持中小企业（SME）的认识，因为它们在数字经济和供应链中发挥着重要作用，而这是一个向电子商务转变的时期，中小企业需要网络风险管理方面的支持。

¹ 也被称为CSIRT/CERT，CIRT是组织实体，在国家层面负责协调和支持对计算机安全事件或事故的响应。

合作措施

本支柱反映了协议是否已签署或已批准，无论它们是否具有法律约束力。哪些协议符合双边和多边协议的条件已得到澄清。《布达佩斯公约》之前是被计入多边协议下的，现在被计为国际活动。

A4. 计算方法

用于GCI的问卷调查表为通过82个问题构建的20个指标提供了一个值。这实现了所需的粒度级别，并提高了答案的准确性和质量。各指标可以在GCI问卷调查表中找到（附件B）。

用于计算GCI的指标的选择基于的是：

- 与五个GCA支柱的相关性；
- 与主要GCI目标和概念框架的相关性；
- 数据可用性和质量；以及
- 通过二手数据进行交叉验证的可能性。

GCI基于网络安全发展图，一个国家在改进其网络安全承诺时可能会考虑到该图。问卷调查表建立在由五种特定颜色区分的五个不同支柱上。在本报告的图表中，路径的深度表明了更高的发展水平。

本报告提供了区域和世界趋势。为确保准确性，各国需要通过上传支持文件和URL的功能来支持其答复。对每个支柱都添加了一个评论部分，以允许各国提供良好的做法，讲述其网络安全演变的影响故事。

对5个支柱20个指标的82个问题，为各国提供了二元或三元答案，如果某个项目处于草案或实施阶段，则评论部分用于详细说明实施阶段。

问卷调查表返回后，接受两个不同的验证者做两次验证，如果答案涉及草案或正在实施阶段/或者如果它不具体回答问题的所有项目，则提供部分得分。通过一个包含特定项目的表格来呈现正面和部分答案，这种三元评估模式避免了基于意见的评估和主观偏见。

为此，BDT秘书处于2019年10月向第2研究组问题3报告人组会议提交了第四版全球网络安全指数问卷调查表和任何相关的文件，该问卷调查表在发布前获得批准。2020年3月，在SG2会议期间，BDT更新了Q3的状态，并与各国磋商以任命网络安全领域的专家，来参与权重分配过程。

总的GCI处理流程

1. 向所有国际电联成员国和巴勒斯坦国发出邀请函，通知它们该倡议并要求有一个负责收集所有相关数据和完成网络GCI问卷调查表的联系人。在网络调查期间，国际电联正式邀请获准的联系人回答问卷调查表。
2. 主数据收集（针对对问卷调查表无答复的国家）：

- 国际电联利用公开可用的数据和网络研究，草拟问卷调查表的初步答复。
 - 将问卷调查表草稿发送给联系人进行评审。
 - 联系人改善准确性并返回问卷调查表草稿。
 - 将更正后的问卷调查表草稿发送给每个联系人以供最终批准。
 - 验证后的问卷调查表用于分析、评分和排名。
3. 次数据收集（针对对问卷调查表有答复的国家）：
- 国际电联确定任何缺失的答复、支持文件、链接等。
 - 联系人在必要时改善答复的准确性。
 - 将更正后的问卷调查表草稿发送给每个联系人以供最终批准。
 - 验证后的问卷调查表用于分析、评分和排名。

注：如果一个国家没有为GCI问卷调查表提供联系人，国际电联将与国际电联全球目录中的机构联系人建立联系。

权重

与之前迭代的尺度为0到1不同，本次GCI迭代的尺度为0到100，每个支柱的权重为20分。

作为一个综合加权指数，每个指标、子指标和微指标都被赋予一个权重，给定对指标组的相对重要性。权重会对最终得分产生重大影响，不同的技术将产生不同的排名。

GCI采用参与式方法，使用了预算分配流程（BAP）。它认为权重从根本上说是价值判断，需要广泛听取专家的意见。

在预算分配方法中，专家有一个给定的“预算”，他们可以在一个指标组内分配该预算，为被评估为更重要的指标分配更多的资金。要求专家为其所专长的支柱提供权重建议。

由于数据所依据的所有国家答复都是报告的调查数据，并由国际电联小组核实，因此加权并未考虑数据的统计质量。

由于作为数据基础的所有国家答复都是报告的调查数据，并经国际电联团队核实，因此权重没有考虑到数据的统计质量。

权重专家组的参与

2020年10月，通过通函邀请国际电联成员国和私营部门成员提名专家参与此次全球网络安全指数的迭代。被提名的专家隶属于学术界、智囊团、ICT部委、监管机构和标准组织。

也邀请为全球网络安全指数的先前迭代做出贡献的专家提供权重建议。

共有 84 名专家参与，要求他们提供与其专业领域相关的、各支柱的权重建议。

集总

对指标组使用加权算术平均值来集总。这意味着一个国家在某一方面得分不佳，可以通过在其他方面表现出色来弥补部分得分。

正如经合组织（OECD）综合指数手册中所指出的，“在几何集总下，低绝对分数增加的边际效用将远高于高绝对分数。因此，如果集总是几何的而非线性的，那么一个国家将有很大的动力去解决那些得分低的部门/活动/备选方案中存在的问题”（33）。然而，出于清晰和理解的目的，认为线性方法更易理解和操作。

敏感性分析

鉴于权重对最终国家得分的重要性，进行了敏感性分析，其中包括：

- 包含/排除个别指标；
- 不同的加权方案（同等加权、预算分配方法、专家建议的极端方案）；
- 不同的集总系统（加权平均、累积式）。

排名

使用“密集”排名方法，按其最终得分对国家进行排名。相同的得分导致相同的排名。两个或更多个排名相同的国家之后的下一个国家获得下一个序数。

附件B：全球网络安全指数问卷调查表（第4版）

本问卷调查表已经ITU-D第3/2号课题报告人研究组会议详细拟定并审查：确保信息和通信网络的安全：培育网络安全文化的最佳做法。在会议上征求成员国的批准，以启动国际电联全球网络安全指数第4版进程。

问卷调查表由五个部分组成，所有部分的问题都希望得到是/否（伴有勾号框）的回答。问卷调查表设计为在线完成。（通过国际电联的官方邮件）为每个答卷者提供一个唯一的URL和登录信息，用于答卷。它还允许答卷者上传有关每个问题的相关文档（和URL）作为支持信息。本问卷调查表的答卷者所提供的信息应为非机密性信息。

表B1：GCI问卷调查表：法律措施

1. 网络犯罪实体法

说明：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。

1.1 贵国是否有关于非法在线行为的实体法？

- 是
 否

上传链接/URL

上传文件

1.1.1 贵国是否有关于非法访问设备、计算机系统和数据的实体法？

说明：访问 – 与某个系统进行通信或以其他方式与之交互、使用系统资源来处理信息、获得系统所含信息或控制系统组件和功能的能力和手段（NICCS）；

计算机系统或系统 – 一个设备或一组互连的或相关的设备，其中一个或多个设备根据程序执行数据的自动处理（欧洲理事会-网络犯罪公约）；

计算机数据 – 以适于在计算机系统内进行处理的形式对事实、信息或概念的任何再现，包括适于使计算机系统执行功能的程序（欧洲理事会-网络犯罪公约）；

- 是
 否

上传链接/URL

上传文件

1.1.2 贵国是否有关于对设备、数据和计算机系统的非法干扰（通过输入、更改和限制数据）的实体法？

说明：干扰计算机系统 – 既包括故意的，也包括未经授权的严重妨碍计算机系统功能的行为。它可能包括输入、传输、损坏、删除、恶化、更改或限制计算机数据。

干扰数据 – 既包括故意的，也包括未经授权的破坏、删除、恶化、更改或限制计算机数据。

- 是
 否

上传链接/URL

上传文件

表B1: GCI问卷调查表: 法律措施 (续)

1.1.3 贵国是否有关于非法拦截设备、计算机系统和数据的实体法律?

说明: 非法拦截 – 既包括故意的, 也包括未经授权的, 通过技术手段获得非公开传输的计算机数据, 既包括传向计算机或其他电子系统的数据, 也包括从计算机或其他电子系统传出的数据, 以及在计算机或其他电子系统内部传输的数据。

是

否

上传链接/URL

上传文件

1.1.4 贵国是否有关于盗窃在线身份和数据的实体法律?

说明: 盗窃在线身份 – 窃取个人信息, 例如姓名、地址、出生日期、联系信息或银行帐户信息。可能是网络钓鱼、黑客侵入在线帐户、从社交媒体非法获取信息或非法访问数据库的结果。

是

否

上传链接/URL

上传文件

1.2 贵国是否对与计算机有关的伪造(盗版/侵犯版权)进行处置?

说明: 未经授权的输入、更改或删除计算机数据会导致虚假数据, 目的是使其看起来像是合法的, 或者可将其用于合法目的, 从而使欺诈行为或虚假设计持续下去。

是

否

上传链接/URL

上传文件

1.3 贵国是否有关于网络安全的实体法?

说明: 网络安全 – 关于互联网上针对与私人以及个人或产权有关的信息的各种安全风险, 尽力克服这些风险, 以及增强用户的自我保护免受网络犯罪的侵害。

1.3.1 贵国对与网络种族主义和仇外行为有关的犯罪是否有处置/法律措施?

说明: 采取处置/措施防止各种形式的网上仇恨言论和其他形式的不宽容, 无论这种不宽容是基于种族、肤色、宗教、血统、民族或种族出身、性取向或性别认同、残疾、社会地位引起的, 还是基于其他特征而引起的。

是

否

上传链接/URL

上传文件

1.3.2 贵国是否有关于对个人的尊严/诚信进行网上骚扰和虐待的行为的处理/法律措施?

说明: 网络骚扰或欺凌 – 通过电子邮件、直接信息或贬损网站发送的消息, 目的是通过个性化的攻击来欺凌或骚扰个人或一群人。

是

否

上传链接/URL

上传文件

表B1: GCI问卷调查表: 法律措施 (续)

1.3.3 贵国是否有与儿童上网保护有关的处置/法律措施?

说明: 法律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于犯罪行为。也有必要制定新的法律或通过已有的法律, 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, 或以性为目的诱骗儿童在现实世界中相识(《国际电联儿童上网保护决策者指南》)。

- 是
 否

上传链接/URL

上传文件

2. 贵国是否有关于以下各项的网络安全立法或规定?

说明: 监管基于一定的规则, 旨在执行具体的法律。通常由为执行法律目标或规定而成立或授权的监管机构执行法规。

网络安全法规规定各利益攸关方应遵循的原则。法规源自相关法律, 并是其一部分, 主要针对数据保护、入侵通知、网络安全认证/标准化要求、网络安全措施的实施、网络安全审计要求、隐私保护、儿童上网保护、数字签名和电子交易、以及互联网供应商的义务。

2.1 保护个人数据/隐私?

说明: 有关保护个人数据免受未经授权访问、改变、破坏或使用的有关法规。本条含义宽泛, 包括各种与保护敏感和私人数据、通信和偏好数据的各种因素、技巧和技术。此类立法例如《数据保护法》。

- 是
 否

上传链接/URL

上传文件

2.2 数据泄露/事故的通知?

说明: 泄露通知法律或规定要求被入侵的实体向管理当局、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识别信息的消费者数据库的入侵行为。

- 是
 否

上传链接/URL

上传文件

2.3 网络安全审计要求?

说明: 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信息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。

- 是
 否

上传链接/URL

上传文件

表B1: GCI问卷调查表: 法律措施 (续)

2.4 实施标准?

说明: 有经政府批准 (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、ITU、IETF、IEEE、ATIS、OASIS、3GPP、3GPP2、IAB、ISOC、ISG、ISI、ETSI、ISF、RFC、ISA、IEC、NERC、NIST、FIPS、PCI DSS等。

是

否

上传链接/URL

上传文件

2.7 识别和保护国家关键信息基础设施?

说明: 关键基础设施是一国安全、安防、经济安全和公共卫生的关键系统, 包括但不限于国防系统、银行和金融、电信、能源及其他系统等。请提供任何定义关键基础设施的链接或文档或用于确认这些定义的文档或新闻。

是

否

上传链接/URL

上传文件

请提供贵国在合作措施方面已经/正在参与的网络安全行动的一些最佳做法/成就/进展。

请在评论栏中提供有关做法的详情, 并提供有关证明的链接,

或者提供文件/包括有关证明的链接。

表B2: GCI问卷调查表: 技术措施

1.国家/政府计算机事件响应小组 (CIRT) /计算机安全事件响应小组 (CSIRT) /计算机应急响应小组 (CERT)。

说明: CIRT-CSIRT-CERT: 计算机事件响应小组 (CIRT), 是配备人员的具体组织实体, 在全国层面或政府层面负责协调和支持对计算机安全事情或事件的响应。

注: 有时, 政府的和国家的计算机事件响应小组 (CIRT) 作为单独/不同的实体有所区别-政府计算机事件响应小组为政府机构提供服务, 而国家计算机事件响应小组为国家机构包括私营部门和公民提供服务。有时, 也会把它们当作同一实体。

1.1 贵国是否有国家/政府的CIRT/CSIRT/CERT?

说明: 由政府的决定支持或是政府或国家机构的一部分。

是

否

上传链接/URL

上传文件

1.2 贵国国家的或政府的CIRT/CSIRT/CERT是否...

表B2: GCI问卷调查表: 技术措施 (续)

1.2.1 制定并执行网络安全宣传活动?

说明: 努力开展广泛的宣传活动, 以使有关安全上网的网络行为的信息传播到全国。

是

否

上传链接/URL

上传文件

1.2.2 定期进行网络安全演习, 例如网络演习 (Cyber Drills) ?

说明: 有计划地开展演习活动, 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、缓和、响应或恢复等能力。这种演习是否定期或重复举行?

是

否

上传链接/URL

上传文件

1.2.3 向公众开放咨询?

说明: 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措施。

是

否

上传链接/URL

上传文件

1.2.4 对保护儿童上网问题有贡献吗?

说明: CIRT/CSIRT/CERT所提供的支持, 例如提高认识的宣传活动、报告与儿童有关的事件、提供有关“儿童上网保护”及其他内容的教育材料等。

是

否

上传链接/URL

上传文件

1.3 上述CIRT (CSIRT或CERT) 是否加入了事件响应与安全小组论坛 (FIRST) ?

说明: 是事件响应与安全小组论坛的正式成员还是联络成员。论坛网址: www.first.org

是

否

上传链接/URL

上传文件

1.4 上述CIRT (CSIRT或CERT) 是否加入了某个区域的CERT?

说明: 与国内或国外的其他CERT有正式关系还是非正式关系, 是否是任何一个区域CERT的成员。区域性的CERT举例, 例如APCERT、AFRICACERT、EGC、OIC、和OAS。

是

否

上传链接/URL

上传文件

表B2: GCI问卷调查表: 技术措施 (续)

1.5 上述CIRT、CSIRT或CERT业务的成熟度是否通过了TI认证计划的TF-CSIRT-SIM3认证?
说明: SIM3是CIRT认证的基础认证。

是

否

上传链接/URL

上传文件

2.行业的CIRT/CSIRT/CERT

说明: 行业的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的CERT。行业的CERT仅向某一行业的机构提供服务。

2.1 贵国是否有行业的CIRT/CSIRT/CERT?

是

否

上传链接/URL

上传文件

2.2. 贵国的行业CIRT/CSIRT/CERT是否:

2.2.1 制定并执行关于某个行业的网络安全宣传活动?

是

否

上传链接/URL

上传文件

2.2.2 积极参与国家的网络演习?

是

否

上传链接/URL

上传文件

2.2.3 在其成员中分享与行业有关的事件?

说明: 分享有关新兴网络威胁的信息以及建议采取的措施。

是

否

上传链接/URL

上传文件

3.实施网络安全标准的国家框架

说明: 有一个(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。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。

表B2: GCI问卷调查表: 技术措施 (续)

3.1 是否有实施/采用网络安全标准的框架?

- 是
 否

上传链接/URL

上传文件

3.2 框架是否包括国际或其他相关标准?

说明: ITU-T、ISO/IEC、NIST、ANSI/ISA和其他标准。

- 是
 否

上传链接/URL

上传文件

4. 儿童上网保护

说明: 该指标用于衡量是否有专门负责儿童上网保护 (COP) 的国家机构, 是否有用于报告与儿童上网有关的问题的国内电话号码, 是否部署了用于帮助保护儿童上网的任何技术制度或力量, 是否有政府或非政府机构通过开展活动向利益攸关方提供关于如何保护儿童上网的知识和支持, 如提供电话号码、电子邮件地址、网络表格以及其他支持等, 有关方面可以利用这些支持汇报与儿童上网保护 (COP) 有关的事件或关切。

4.1 是否部署了任何报告机制和力量来帮助保护儿童上网?

说明: 如热线, 求助热线等。

- 是
 否

上传链接/URL

上传文件

请提供贵国在合作措施方面已经/正在参与的网络安全行动的一些最佳做法/成就/进展。

请在评论栏中提供有关做法的详情, 并提供有关证明的链接,

或者提供文件/包括有关证明的链接。

表B3: GCI问卷调查表: 组织措施

1. 国家网络安全战略

说明: 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、组织和国家的物质和知识资产; 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。

1.1 贵国是否有国家网络安全战略/政策?

- 是
 否

上传链接/URL

上传文件

表B3: GCI问卷调查表: 组织措施 (续)

它是否涉及了对国家关键信息基础设施（包括电信行业）的保护？

说明：国家关键信息基础设施指以任何方式控制、处理、传输、接收或存储任何形式（包括数据、声音或视频）的电子信息的物理的或虚拟的信息系统，其对关键基础设施的正常运行具有至关重要的作用；它们的重要作用体现在，此类系统的功能丧失或遭到破坏将会对国家安全、国家经济安全或国家公共卫生与安全造成破坏性影响。

是

否

上传链接/URL

上传文件

它是否涉及了国家网络安全的弹性？

说明：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职能。

是

否

上传链接/URL

上传文件

国家网络安全战略是否持续进行修订和更新？

说明：战略的生命周期管理的定义，根据可能影响国家网络安全的国内的、技术的、社会的、经济的和政治的发展对战略进行更新。

是

否

上传链接/URL

上传文件

是否就网络安全战略向国内的网络安全专家进行任何形式的咨询？

说明：所有利益攸关方，包括关键基础设施运营商、ISP、学术界和其他领域等，都可参与讨论战略。

是

否

上传链接/URL

上传文件

1.2 是否有实施网络安全治理的明确的行动计划/路线图？

说明：战略计划定义了国家网络安全的成果，也包括了实施该计划所需的步骤和阶段。

是

否

上传链接/URL

上传文件

1.3 是否有保护儿童上网的国家战略？

是

否

上传链接/URL

上传文件

表B3：GCI问卷调查表：组织措施（续）

2. 负责机构

说明：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。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执行政策和采纳标准。

2.1 在国家层面是否有负责协调网络安全的机构？

- 是
 否

上传链接/URL

上传文件

2.1.1 该机构是否负责保护国家关键信息基础设施？

- 是
 否

上传链接/URL

上传文件

2.2 是否有负责国家网络安全能力建设的国家机构？

- 是
 否

上传链接/URL

上传文件

2.3 在国家层面是否有监管儿童上网保护举措的机构？

说明：有专门监督和促进儿童上网保护的国家机构。

- 是
 否

上传链接/URL

上传文件

3. 网络安全指标

说明：有官方认可的国家的或具体到行业的标杆或参考，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。

3.1 在国家层面是否进行网络安全审计？

说明：安全审计是根据一套已成型的标准衡量信息系统的符合程度，从而系统地评估信息系统安全。全面的审计通常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。监管机构有可能要求私营机构管理的关键基础设施定期进行安全态势评估并报告评估结果。

- 是
 否

上传链接/URL

上传文件

表B3: GCI问卷调查表: 组织措施 (续)

3.2 在国家层面是否有评估网络空间相关风险的指标?

说明: 这是一个包括风险识别、风险分析和风险评估的程序。

是

否

上传链接/URL

上传文件

3.3 在国家层面是否存在评估国家网络安全发展水平的措施?

说明: 这是衡量国家网络安全发展水平的一个方法。

是

否

上传链接/URL

上传文件

请提供贵国在合作措施方面已经/正在参与的网络安全行动的一些最佳做法/成就/进展。

请在评论栏中提供有关做法的详情, 并提供有关证明的链接,

或者提供文件/包括有关证明的链接。

表B4: GCI问卷调查表: 能力发展建设

1. 公众网络安全宣传活动

说明: 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。此类活动包括建设提高公众认识的门户和网站, 传播支持材料, 以及其他有关活动。

1.1 是否有针对特定行业, 例如中小企业、私营企业和政府机构的公众宣传活动?

是

否

上传链接/URL

上传文件

1.2 是否有针对民间社会的公众宣传活动?

说明: 针对非政府组织和社区基层组织。

是

否

上传链接/URL

上传文件

1.3 是否有针对公民的公众宣传活动?

是

否

上传链接/URL

上传文件

表B4：GCI问卷调查表：能力发展建设（续）

1.4 是否有针对老年人的公众宣传活动？

- 是
 否

上传链接/URL

上传文件

1.5 是否有针对有特殊需要的人群的公众宣传活动？

- 是
 否

上传链接/URL

上传文件

1.6 是否有针对父母、教育者和儿童（与COP相关）的公众宣传活动？

- 是
 否

上传链接/URL

上传文件

2. 培训网络安全专业人员

说明：有针对特定行业的专业培训计划，以提高公众认识（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）的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。

它还包括对执法人员、司法人员和其他法律人士的网络安全培训，设计的专业和技术培训还可重复用于对警察、执法人员、法官、讼状律师、出庭律师、代理人、律师、律师助理和其他从事法律和执法职业人士的培训。这个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。

2.1 贵国政府是否开发了/支持网络安全专业培训课程？

说明：在（技术、社会科学等领域的）劳动力队伍中推动网络安全课程，推动公共或私营部门的专业人士获得证书。

- 是
 否

上传链接/URL

上传文件

2.2 贵国是否有针对网络安全专业人员的认证计划？

说明：对网络安全专业人员进行认证的机构或任何其他的相关机制。

- 是
 否

上传链接/URL

上传文件

表B4: GCI问卷调查表: 能力发展建设 (续)

2.3 是否有针对网络安全专业人员的关于国内各个具体行业的教育计划/培训/课程?

- 是
 否

上传链接/URL

上传文件

2.3.1 是否有针对执法部门的国内具体行业的教育计划/培训/课程?

说明: 网络安全正式程序, 用于对从事法律工作的人员 (警察和执法人员) 进行计算机安全教育

- 是
 否

上传链接/URL

上传文件

2.3.2 是否有针对司法和其他从事法律工作的人员的国内具体行业的教育计划/培训/课程?

说明: 网络安全培训或技术培训还可重复用于对警察、执法人员、法官、讼状律师、出庭律师、代理人、律师、律师助理和其他从事法律和执法职业人士的培训。

- 是
 否

上传链接/URL

上传文件

2.3.3 是否有针对中小企业/私营公司的国内具体行业的教育计划/培训/课程?

说明: 通过正确使用在线服务进行有关网络安全的良好实践培训/能力开发, 以保护其业务。

- 是
 否

上传链接/URL

上传文件

2.3.4 是否有针对其他公共部门/政府官员的国内具体行业的教育计划/培训/课程?

- 是
 否

上传链接/URL

上传文件

3. 贵政府/组织是否开发了或支持网络安全教育项目或学术课程

说明: 在学校、大专、大学或其他教学机构有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。

3.1 小学教育中有吗?

- 是
 否

上传链接/URL

上传文件

表B4: GCI问卷调查表: 能力发展建设 (续)

3.2 中学教育中有吗?

- 是
- 否

上传链接/URL

上传文件

3.3 高等教育中有吗?

- 是
- 否

上传链接/URL

上传文件

4. 是否有网络安全研发项目?

说明: 这个指标衡量的是私有、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入。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。网络安全研究计划包括但不限于恶意软件分析、密码学研究、系统脆弱性研究以及安全模型和概念研究。网络安全开发计划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改善不同机构之间的协调和必要的资源共享。

4.1 在国家层面是否有网络安全研发活动?

- 是
- 否

上传链接/URL

上传文件

4.1.1 私营部门是否有网络安全研发计划?

- 是
- 否

上传链接/URL

上传文件

4.1.2 公共部门是否有网络安全研发计划?

- 是
- 否

上传链接/URL

上传文件

4.1.3 学术界和大学等高等教育机构是否从事研发活动?

- 是
- 否

上传链接/URL

上传文件

表B4: GCI问卷调查表: 能力发展建设 (续)

5. 国家网络安全产业

说明: 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。提高公众认识的活动、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。

5.1 国内是否有网络安全产业? 是 否

上传链接/URL

上传文件

6. 政府是否有激励机制?

说明: 这个指标考察政府是否有任何激励措施, 用于鼓励在网络安全领域进行能力建设, 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。激励措施增加了对网络安全相关服务和产品的需求, 提高了防范网络威胁的能力。

6.1 是否在网络安全领域鼓励能力建设? 是 否

上传链接/URL

上传文件

6.2 是否支持网络安全产业的发展?

说明: 支持学术界和其他领域的初创企业提供网络安全服务

 是 否

上传链接/URL

上传文件

请提供贵国在合作措施方面已经/正在参与的网络安全行动的一些最佳做法/成就/进展。
请在评论栏中提供有关做法的详情, 并提供有关证明的链接,
或者提供文件/包括有关证明的链接。

表B5: GCI问卷调查表: 合作措施

1. 与其他国家是否有关于网络安全合作的双边协议

说明: 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, 由政府与外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)。这个指标还衡量是否分享威胁情报信息。能力建设指的是分享专业工具、先进的专家包络和其他等。

表B5: GCI问卷调查表: 合作措施 (续)

1.1 贵国是否与其他国家签订了有关网络安全合作的双边协议?

- 是
 否

上传链接/URL

上传文件

协议中包括信息共享吗?

说明: 信息共享指的是共享非敏感信息的做法。

- 是
 否

上传链接/URL

上传文件

协议中包括能力建设吗?

说明: 鼓励开展培训, 以增强国家网络安全专业人员的技能、能力和水平, 从而通过合作确保共同努力应对网络威胁。

- 是
 否

上传链接/URL

上传文件

协议中包括司法协助吗?

说明: 两个或多个国家之间的互助, 目的是收集和交换信息, 用于执行公法或刑法。

- 是
 否

上传链接/URL

上传文件

2. 政府参与与网络安全活动有关的国际机制

说明: 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》和其他等。

2.1 贵国政府/组织是否参加了与网络安全活动有关的国际机制?

- 是
 否

上传链接/URL

上传文件

3. 网络安全多边协议

说明: 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)。

表B5: GCI问卷调查表: 合作措施 (续)

3.1 贵国政府是否有关于网络安全合作的多边协议?

- 是
 否

上传链接/URL

上传文件

3.1.1 协议中包括信息共享吗?

说明: 信息共享指的是共享非敏感信息的做法。

- 是
 否

上传链接/URL

上传文件

3.1.2 协议中包括能力建设吗?

说明: 鼓励开展培训, 以增强国家网络安全专业人员的技能、能力和水平, 从而通过合作确保共同努力应对网络威胁。

- 是
 否

上传链接/URL

上传文件

4. 是否存在公私合作伙伴关系 (PPP)

说明: 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, 无论公共部门是与国内的私营部门, 还是与国际上的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)。

4.1 贵国政府是否与当地公司进行PPP合作?

- 是
 否

上传链接/URL

上传文件

4.2 贵国政府是否与在贵国运营的外资公司进行PPP合作?

- 是
 否

上传链接/URL

上传文件

5. 跨机构合作伙伴关系

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

表B5: GCI问卷调查表: 合作措施 (续)

5.1 不同政府机构之间在网络安全领域是否存在跨机构的合作伙伴关系/协议?

说明: 部委或专业机构之间的合作

是

否

上传链接/URL

上传文件

请提供贵国在合作措施方面已经/正在参与的网络安全行动的一些最佳做法/成就/进展。

请在评论栏中提供有关做法的详情, 并提供有关证明的链接,

或者提供文件/包括有关证明的链接。

**国际电信联盟 (ITU)
电信发展局 (BDT)
主任办公室**

Place des Nations
CH-1211 Geneva 20
Switzerland

电子邮件: bdtdirector@itu.int
电话: +41 22 730 5035/5435
传真: +41 22 730 5484

数字网络和社会部 (DNS)

电子邮件: bdt-dns@itu.int
电话: +41 22 730 5421
传真: +41 22 730 5484

非洲

埃塞俄比亚

**国际电联
区域代表处**

Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Addis Ababa
Ethiopia

电子邮件: itu-ro-africa@itu.int
电话: +251 11 551 4977
电话: +251 11 551 4855
电话: +251 11 551 8328
传真: +251 11 551 7299

美洲

巴西

**国际电联
区域代表处**

SAUS Quadra 6 Ed. Luis Eduardo
Magalhães,
Bloco "E", 10º andar, Ala Sul
(Anatel)
CEP 70070-940 Brasília - DF
Brazil

电子邮件: itubrasilia@itu.int
电话: +55 61 2312 2730-1
电话: +55 61 2312 2733-5
传真: +55 61 2312 2738

阿拉伯国家

埃及

**国际电联
区域代表处**

Smart Village, Building B 147,
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo
Egypt

电子邮件: itu-ro-arabstates@itu.int
电话: +202 3537 1777
传真: +202 3537 1888

欧洲

瑞士

**国际电联
欧洲处**

Place des Nations
CH-1211 Geneva 20
Switzerland

电子邮件: eurregion@itu.int
电话: +41 22 730 5467
传真: +41 22 730 5484

**副主任兼行政和运营
协调部负责人 (DDR)**

Place des Nations
CH-1211 Geneva 20
Switzerland

电子邮件: bdtdeputydir@itu.int
电话: +41 22 730 5131
传真: +41 22 730 5484

数字化发展合作伙伴部 (PDD)

电子邮件: bdt-pdd@itu.int
电话: +41 22 730 5447
传真: +41 22 730 5484

数字知识中心部 (DKH)

电子邮件: bdt-dkh@itu.int
电话: +41 22 730 5900
传真: +41 22 730 5484

喀麦隆

**国际电联
地区办事处**

Immeuble CAMPOST, 3^e étage
Boulevard du 20 mai
Boite postale 11017
Yaoundé
Cameroon

电子邮件: itu-yaounde@itu.int
电话: +237 22 22 9292
电话: +237 22 22 9291
传真: +237 22 22 9297

巴巴多斯

**国际电联
地区办事处**

United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown
Barbados

电子邮件: itubridgetown@itu.int
电话: +1 246 431 0343
传真: +1 246 437 7403

亚太

泰国

**国际电联
区域代表处**

4th floor NBTC Region 1 Building
101 Chaengwattana Road
Laksi,
Bangkok 10210,
Thailand

邮寄地址:

P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Thailand

电子邮件: itu-ro-asiapacific@itu.int
电话: +66 2 574 9326 - 8
+66 2 575 0055

塞内加尔

**国际电联
地区办事处**

8, Route des Almadies
Immeuble Rokhaya, 3^e étage
Boite postale 29471
Dakar - Yoff
Senegal

电子邮件: itu-dakar@itu.int
电话: +221 33 859 7010
电话: +221 33 859 7021
传真: +221 33 868 6386

智利

**国际电联
地区办事处**

Merced 753, Piso 4
Santiago de Chile
Chile

电子邮件: itusantiago@itu.int
电话: +56 2 632 6134/6147
传真: +56 2 632 6154

印度尼西亚

**国际电联
地区办事处**

Sapta Pesona Building
13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10110
Indonesia

电子邮件: itu-ro-asiapacific@itu.int
电话: +62 21 381 3572
电话: +62 21 380 2322/2324
传真: +62 21 389 5521

津巴布韦

**国际电联
地区办事处**

TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792
Belvedere Harare
Zimbabwe

电子邮件: itu-harare@itu.int
电话: +263 4 77 5939
电话: +263 4 77 5941
传真: +263 4 77 1257

洪都拉斯

**国际电联
地区办事处**

Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa
Honduras

电子邮件: itutegucigalpa@itu.int
电话: +504 2235 5470
传真: +504 2235 5471

独联体国家

俄罗斯联邦

**国际电联
区域代表处**

4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

电子邮件: itumoscw@itu.int
电话: +7 495 926 6070

国际电信联盟
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN 978-92-61-33925-8



9 789261 339258

瑞士出版
2021年,日内瓦

图片鸣谢: Shutterstock