5G网络安全

2022-2025年
研究期

第3/2号课题

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

2024年
中期可交付成果

内容提要

本中期可交付成果强调了全球网络威胁日益加剧的情况下5G网络安全的关键问题以及电信基础设施的关键性质。凭借其先进的软件、基于云的架构和广泛的连接性，5G技术引入了**新的安全范式**。它带来了显著的好处，但也带来了新的风险，需要采取强大的网络安全措施来防范威胁。

5G网络的复杂性要求先进的安全策略和不同利益攸关方之间的协作。**标准制定组织**（SDO）已开始对5G网络的网络安全问题进行标准化，但需要持续开展合作和沟通，以避免重复工作。

积极主动的网络安全措施在网络部署的各个阶段均至关重要，供应商和运营商有责任管理网络安全风险。

各种5G网络安全的国家政策和法规正在制定中。许多国家已经采取了缓解安全风险的方法，现在正专注于其实施和合规制度。

投资教育和培训对于满足对熟练网络安全专业人员日益增长的需求至关重要。

展望未来，**6G规划**从一开始就强调增强的网络安全和弹性。国际电联的IMT-2030框架体现了整合稳健安全措施以支持未来技术进步的承诺。

引言

在2022年6月在卢旺达基加利举行的最新一届世界电信发展大会期间，审议了ITU-D第2研究组第3/2号研究课题“确保信息通信网络的安全：培育网络安全文化的最佳做法”的职责范围。确定研究的具体问题之一是“讨论5G网络安全的挑战和途径”。

经批准的第3/2号课题的职责范围承认，网络安全威胁仍然是世界各国政府、组织和个人的主要关切。根据世界经济论坛的《2024年全球风险报告》，在全球范围内，网络安全被列为第四位最严重短期风险。[1] 在许多司法管辖区，电信网络被视为关键国家基础设施或基本服务的重要组成部分，容易受到网络攻击，这可能会扰乱基本服务和公共安全。

5G技术的引入标志着电信业的重大变化，它提供了更快的速度和更好的连接，有可能改善行业，扩展物联网（IoT）应用，并为数字通信带来新的方法。然而，促成这些进步的复杂架构也带来了复杂的网络安全挑战，需要全面的了解和强有力的保护措施。

认识到保护5G基础设施和服务的至关重要性，研究第3/2号课题的第2研究组于2024年5月2日组织了一场专门的全天讲习班，汇集了电信行业决策机构、监管机构、运营商和其他成员，讨论5G网络安全的复杂性，分享现有做法，并探索应对新出现的威胁的创新解决方案。随着5G网络在全球部署，建立一个安全的生态系统对于确保信息的完整性、可用性和保密性以及保护已成为数字经济支柱的基础设施至关重要。

本报告反映了讲习班的讨论情况以及本研究期收到的文稿。这不是一份关于5G网络安全的技术报告；而是旨在分享在该研究课题背景下收集的观点和优秀做法，国际电联成员可以在其国家背景下予以考虑和实施。本报告的重点主要涉及公共电子网络的5G网络安全。

1. 为电信网络带来全新的安全模式

5G网络安全概述

5G的特点是其先进的软件系统，能够实现更灵活的配置以及用户和设备的大规模连接。该技术支持增强现实、远程手术和综合互联网服务等低时延应用，这些均依赖于稳健可靠的网络。5G的主要用例之一是物联网（IoT），它利用了5G连接大量端点的能力。5G技术即将彻底改变连通性，但这也带来了动态网络安全的新风险和挑战。

[1] 《2024年全球风险报告》

与前几代无线技术不同，5G引入了向基于云的架构、软件定义网络（SDN）和网络功能虚拟化（NFV）的重大转变。这一转变创造了一个更加复杂和动态的网络安全格局。

随着5G的日益普及，电信基础设施有望成为恶意网络活动更具吸引力的目标，因此需要采取先进的安全措施来适应不断变化的威胁。5G的网络安全应侧重于提高整个生态系统的弹性，包括基础设施和应用。这包括保护连接设备、数据和网络免受网络威胁的影响。

认识到不同的组织采用不同的网络安全定义[2]，应铭记本报告中的“5G网络安全”一词是指5G背景下的网络安全，需要对其新参数、标准和技术功能进行适当管理，以保护整个数字生态系统并确保网络复原力。

> 在国际电联，电信标准化部门（ITU-T）X.1205建议书将网络安全定义为“用以保护网络环境和机构及用户资产的各种工具、政策、安全理念、安全保障、指导原则、风险管理方式、行动、培训、最佳做法、保证和技术。机构和用户的资产包括相互连接的计算装置、人员、基础设施、应用、服务、电信系统以及在网络环境中全部传送和/或存储的信息。网络安全工作旨在确保防范网络环境中的各种安全风险，实现并维护机构和用户资产的安全特性。网络安全的总体目标包括以下内容：
>
> - 可用性
> - 完整性（其中可能包括真实性和不可否认性）
> - 机密性”[3]

传统网络部署

运营商最初倾向于在非独立（NSA）基础上部署5G网络，在部署独立（SA）的端到端5G网络之前利用现有的4G基础设施[4]。5G NSA网络继承了4G或甚至2G/3G的传统漏洞，需要对其进行相应的管理。对一些运营商而言，这相当于一种“技术债务”：管理老旧系统意味着需要开发一套标准化的安全控制措施来衡量不同世代成熟度的基础设施组件的安全状况[5]。

需要强调的是，与过去几代移动技术相比，5G SA提供了提高网络安全性的机会：它被设计为比4G更安

[2] https://www.enisa.europa.eu/publications/definition-of-cybersecurity
[3] https://www.itu.int/rec/T-REC-X.1205-200804-I
[4] 当在NSA 5G网络上运营的设备需要更大的带宽和更低的延迟（例如智能汽车之间的通信）时，这些设备通常将连接到5G频率进行数据传输，或者减少物联网设备的功耗，但继续依赖4G甚至2G/3G网络进行语音通话和短信发送。来源：https://www.gsma.com/get-involved/gsma-membership/wp-content/uploads/2019/11/5G-Research_A4.pdf
[5] 讲习班材料 – Maxis

全。在用户安全和隐私、无线接入网（RAN）、网络核心和漫游安全等领域取得了进展。[6] [7]

2. 许多SDO正在开展保护5G的标准活动，因此SDO需要共同努力，相互沟通并避免重复工作

活跃在5G网络安全领域的SDO

由于5G技术的复杂性和涉及到的问题，没有一家标准制定组织（SDO）能独自负责5G的网络安全工作。为避免重复工作，已经建立了SDO之间共享信息和协调提案与工作项目的机制。

为帮助描述这些不同的活动并告知ITU-T中5G相关的安全标准化工作的方向，第17研究组（SG17）准备了一份技术报告，将现有标准和正在制定的标准与SDO及其在5G网络中的应用进行了对照说明[8]。该报告确定了ITU-T、第三代合作伙伴计划（3GPP）、欧洲电信标准协会（ETSI）以及电气和电子工程师学会标准协会（IEEE SA）的标准以及与5G网络安全相关的非标准资源。

该研究组已经根据运营商、供应商、智能手机制造商、内容提供商等起草的文稿发布了11份关于5G安全的建议书。这些建议书重点关注五个领域的安全问题：SDN-NFV、网络切片、移动边缘、5G网络管理和5G业务。第17研究组已与其他SDO（如3GPP和互联网工程任务组（IETF））以及从事5G网络安全标准化相关规范制定工作的行业组织建立了联络关系。

GSM协会（GSMA）即是这样一个行业组织，虽然GSMA自身并不是一个标准机构，但它编写规范，召集其成员与SDO合作，使这些规范得到改进和/或被采纳为标准。GSMA发布了一份基线安全控制清单，移动运营商可在部署5G网络时，在自愿基础上加以考虑[9]。

鉴于与5G安全相关的信息来源众多，欧洲网络安全机构ENISA发布了一个统一的5G网络技术安全控制资料库-5G安全控制矩阵[10]。该资料库目前作为电子表格发布，但该机构也在开发一个网络工具来提高可用性。

随着网络的日益复杂以及电信与IP网络的融合，越来越难以让某个SDO承担标准化工作的具体领域。这增加了工作重叠和重复的风险，使得标准制定组织之间的沟通和信息共享变得更加重要。

将标准纳入强制性监管要求中

标准有助于确保技术之间的互操作性，并减少创新进入全球市场所需的时间。网络安全可定义公认的共同安全基线，反映普世的优秀做法。标准产生于基于共识的过程。它们可以是强制性的，但在绝大多数情况下是可选的，使得厂商和运营商在做部署决定时有更大的灵活性。在某些情况下，如果国家技术法规在其安全要求中包括了特定的标准，那么这些标准可以是强制性的。国家5G网络安全战略应反映全球最佳做法与本地运作现实之间的平衡。一般而言，国家监管要求应借鉴国际公认的标准，使其适应当地环境和本地要求，以便确保5G的部署和网络的安全。

3. 在网络部署前的不同阶段，标准和规范应辅之以积极主动的网络安全措施

供货商层面的安全考虑

标准和规范只是5G网络安全的一个组成部分。厂商和运营商如何实施这些标准并对其进行配置，决定了5G网络的安全状况。爱立信对5G安全采取了一种整体方法，涉及四个层面：标准、供应商产品开发、网络部署和网络运营[11]。该公司认为，这种综合方法可以确保缓解措施的实施方式既可顾及各层之间的相互依存关系，又可满足各层的具体需求。

作为5G安全措施的一个具体示例，由GSMA和3GPP开发的网络设备安全保障方案（NESAS）[12]旨在通过提供可在全球范围内适用的保障方案来提高移动网络设备的安全水平。该方案以内部和独立专家审计为基础，即供应商流程评估和产品评估的混合体，并提供认证。该方案的目的是减轻往往在全球范围运营的网络设备提供商的安全测试负担。主要供应商已获得NESAS认证。NESAS也是欧盟5G网络安全认证方案的一个候选者[13]。该方案是欧盟级别的认证，将使欧盟各国符合要求。该认证不会取代当前的NESAS方案，而是协同存在。鉴于威胁形势在不断变化，以一种既保持灵活性又可快速更新的方式制定方案/认证计划至关重要。

---

6 https://www.cisa.gov/sites/default/files/publications/5G_Security_Evaluation_Process_Investigation_508c.pdf

7 https://www.gsma.com/solutions-and-impact/technologies/security/securing-the-5g-era

8 https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTS-2022-2-PDF-E.pdf

9 https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/fs-31-gsma-baseline-security-controls/

10 https://www.enisa.europa.eu/publications/5g-security-controls-matrix

11 https://www.ericsson.com/en/public-policy-and-government-affairs/cyber-network-security

12 https://www.gsma.com/solutions-and-impact/industry-services/certification-services/network-equipment-security-assurance-scheme-nesas/

13 https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification

在英国，国家网络安全中心（NCSC）建议使用供应商评估框架[14]，该指南帮助运营商评估与使用供应商设备相关的网络风险。

运营商层面的安全考虑

NESAS可以提供一定程度的保证，确保部署前的网络设备是安全的。随着运营商部署和运营其网络，需要纳入其他安全考虑，例如攻击检测和自动响应。此时运营商应考虑利用人工智能、威胁情报和分析来帮助支持其网络防御。5G网络安全提供了实时安全性和零信任策略等优势，可以提高系统可见性。然而，它自身面临着一些挑战：以不同的安全级别维护不同网络的连接；使用传统组件和不同的网络类型；以及将人工智能集成到安全措施中的复杂性。根据“最小特权”原则实施严格的访问控制，可确保将网络中的各种权限（如网络功能间的访问权限、网络管理员权限、虚拟化配置）最小化。有很多关于5G具体网络安全策略的文献供运营商考虑[15]。

对真实的电信网络进行测试对于确定电信网络真正的网络风险也至关重要。运营商可利用内部资源或雇用独立的外部承包商，针对自己的网络和系统进行某种形式的安全测试。在英国，TBEST是一种基于结果的渗透测试方案，它模拟资源雄厚的网络攻击者可能使用的技术和战术。它评估通信提供商如何能够检测、遏制和应对这种攻击。其总体目标是在提供商的功能、流程、政策、系统或网络中发现并解决安全漏洞或其他弱点，如果不被发现，这些漏洞或弱点可一起危害企业的关键系统。通过实施自愿性TBEST计划，通信提供商可以确定其安全方面可以提高的特定领域；监管机构Ofcom也与他们合作，协助他们及时做出适当的改变[16]。

5G网络安全强有力的商业案例至关重要。虽然运营商需要看到他们在5G业务方面的投资得到回报，但应认识到遵守基线安全措施是必不可少的，并相应地做出预算。

开放RAN是对无线接入网（RAN）进行分解，并对连接这些分解元素的接口进行标准化，从而能够使用来自不同供应商的部件来构建网络。

一方面，开放的RAN可进一步增加电信网络供应链的复杂性。这种架构鼓励RAN中供应商的多样化，需要在整个网络供应链中进一步开展集成工作，这可能会增加攻击向量。另一方面，开放RAN提高了供应链的透明度，提高了运营商的知名度并允许他们监测和检测安全风险。简而言之，它使运营商们更好地了解网络架构和设备，并可更全面地扫描和管理漏洞。O-RAN联盟（制定开放RAN规范的主要场所）正在为开放RAN架构制定安全规范，并旨在使这些规范在ETSI中实现标准化。

NTT Docomo（日本）因其设备选择的灵活性而成为采用开放RAN架构的运营商之一。这一决定从安全角度提出了质疑，因为通常认为开放性意味着有更多的攻击机会。然而，该运营商已经比较了传统RAN和开放RAN，并得出结论，两者之间的安全差异很小[17]。

4. 5G网络和网络安全是近期处于不同实施阶段的政策和监管举措的重点

保护5G网络的国家政策和法规示例

除了供应商和运营商的标准和做法之外，可在国家层面提出保护5G网络的政策和法规。这可能采取供应商评估、测试、认证、制定导则或要求等各种形式。虽然方法因国情而异，但这些举措都旨在减轻5G带来的安全风险，包括具体针对网络的风险。实施和遵守机制也应被视为总体框架的组成部分。

以下示例提供了不同行动及其当前状态的简要介绍。

- **巴西**对5G网络安全的整体方法侧重于运营商的风险管理。根据5G频谱拍卖的条款和《电信行业网络安全条例》[18]的要求，5G运营商需遵守监管框架，其中包括确保整个行业网络安全的原则、导则和事前控制。这些控制措施结合了网络安全治理、强制性事件通知、信息共享、漏洞评估周期、关键基础设施报告和其他规定。巴西国家电

[14] https://www.ncsc.gov.uk/report/vendor-security-assessment

[15] 例如见：https://www.5gamericas.org/wp-content/uploads/2020/07/Security-Considerations-for-the-5G-Era-2020-WP-Lossless.pdf和https://www.5gamericas.org/security-for-5g/

[16] https://www.itu.int/md/D22-SG02.RGQ-C-0074/

[17] 有关Open RAN安全性的更多信息，请参阅例如：https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/09/enhancing-the-security-of-communication-infrastructure_79b78b4d/bb608fe5-en.pdf

[18] https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740和 https://informacoes.anatel.gov.br/legislacao/resolucoes/2024（两者均为葡萄牙语）。

信局（Anatel）也与学术界合作，在此方面开展研究[19]。

- **英国**政府通过《2003年通信法》为公共电子通信网络或服务提供商制定了安全框架，该法案后由《2021年电信（安全）法》（TSA）予以修订）。该框架适用于5G和所有其他网络：虽然英国正在向5G和所有未来网络为全光纤网络的过渡，但许多网络提供商将旧技术纳入其基础设施。TSA规定了所有公共电信提供商[20]的新安全义务，并赋予了国务大臣制定法规和发布行为守则的新权力。这些守则已得到制定，并通过公众咨询进行了通报[21]。该法案还包括加强Ofcom监管权力的条款，以监督和强制执行提供商如何遵守其新职责。
- **韩国**的5G网络安全法规和政策是全球公认最严格的，反映了该国在采用5G技术方面的领先地位。韩国政府通过科学技术信息通信部（MSIT）和韩国互联网与安全局（KISA）实施了保护5G网络的综合框架。该框架包括对电信运营商实施严格的网络安全要求，以确保网络基础设施的安全、用户数据的保护和降低网络安全风险。这些法规强调需要安全的供应链、先进的加密标准以及在网络架构中部署安全设计原则。此外，韩国还与国际合作伙伴和标准组织合作，以确保其5G安全措施符合全球最佳做法。
- **印度**加强5G网络安全的法律和技术框架包括：
  - 电信行业的国家安全指令，确保解决电信供应链和来源中的问题和漏洞；
  - 电信设备的强制性测试和认证，确保符合每项5G网络功能的基本安全要求；和
  - 电信服务提供商的许可条件，包括对电信基础设施安全进行定期公开审计。

  为支持上述目标，印度建立了各种体制机制：成立了国家通信安全中心（NCCS），负责制定电信安全要求/标准（印度电信安全保证要求（ITSAR））及其相关的安全测试和认证实验室；为国家电信部门成立了电信计算机安全事件响应团队（CSIRT）；以及，制定多项以公民为中心的欺诈管理和消费者保护措施等。关于安全协议和3GPP等标准，印度审议了行业标准提出的合规性监测和进一步的电信许可条件（包括对服务提供商网络的定期安全审计）的规范。
- 在**阿拉伯联合酋长国**，通过多管齐下的战略确保5G网络安全，其中包括严格的国家网络演习和培训、建立国家安全运营中心（SOC）以实时了解和应对威胁，以及网络脉冲举措，以提高关键防御战略方面的意识并培训人员。强调与国际合作伙伴、供应商、学术界和其他利益攸关方的合作和信息共享，以加强网络安全措施。此外，建立了符合国际标准（如ISO和NIST发布的标准）的弹性网络安全框架，以确保整个电信部门的合规性。为了树立消费者和企业对5G安全的信心，该国制定了治理政策、程序和法律，以促进供应商之间的安全设计原则和负责任的安全实践。最后，该国采取了以人为本的网络安全方针，侧重于培训、宣传和支持，以增强个人和组织对抗网络威胁的能力，从而巩固对5G网络潜在威胁的强大防御。
- **津巴布韦**正在解决5G网络安全问题，重点关注边缘计算日益增长的重要性，并探索采用开放RAN技术以提高供应商的灵活性。虽然津巴布韦没有具体的5G安全法，但现有的数据保护立法和正在制定的AI治理文件支撑着该国的做法。津巴布韦将使其安全做法与ISO/IEC 27001和NIST标准等国际标准保持一致，确保新的5G无线电接口符合既定的安全协议。津巴布韦邮电管理局负责执行安全准则，并提高业界对维护国家电信基础设施完整性的认识。
- **肯尼亚**于2022年4月通过了其5G移动通信路线图和战略。该战略认识到安全是5G网络架构的一个重要方面。互联服务不断发展的性质以及预期互联设备数量和类型的显著增加增加了数据隐私、数据保护和网络安全对肯尼亚的重要性；其中包括检测威胁、用户认证和优秀实践做法。5G通过设计提供更好的安全性，在网络演进和根据早期技术已取得经验加以调整的基础上纳入了更高的安全要求。肯尼亚通信管理局通过了国际电联和3GPP制定的已批准国际标准，以确保移动系统的互操作性和安全性。管理局计划利用各利益攸关方的专业知识和网络安全方面的国际最佳做法来制定技术规范并实施标准化的最低安全评估清单，以确保5G网络符合最新的技术标准，并符合与5G安全相关的全球规范。
- 在对5G网络的网络安全风险进行广泛审查后，**欧盟**（EU）开发了“风险缓解措施工具箱”[22]，旨在确定一套缓解主要5G网络安全风险的通用措施，并协助确定欧盟和国家层面应对计划中相关措施的优先级。《数字十年网络安全战略》强调了保护下一代宽带移动网络的重要性，并就5G网络网络安全的下一步制定了具体附录[23]。《欧盟认证框架》包括正在制定的5G网络安全认证计划[24]。

[19] 部分结果见：https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica/estudos-e-pesquisas（葡萄牙语）。
[20] 微实体除外。
[21] https://www.legislation.gov.uk/uksi/2022/933/contents/made和https://assets.publishing.service.gov.uk/media/6384d09ed3bf7f7eba1f286c/E02781980_Telecommunications_Security_CoP_Accessible.pdf
[22] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures
[23] https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
[24] https://certification.enisa.europa.eu/index_en

实施和合规挑战

政策的制定与注重有效实施同等重要。报告机制、对相关标准的遵守以及切实可行的政策和监管执行措施对于确保5G网络强有力的网络安全至关重要。新框架对电信网络安全带来的变化将要求电信服务提供商持续进行合规，因此需要与行业密切接触。在**英国**，Ofcom在其电信安全制度下采用一种监督模式，并与电信提供商的监管和技术团队接触。监管机构认为，实施不仅涉及技术措施，还需要从文化上转变电信提供商对网络安全的思维方式，要求他们确定其外包的部分网络和服务并对其负责。与高层接触并获得政府、监管机构和业界高层的承诺和支持是取得成功的先决条件。

在**马来西亚**，政府批准了一项新的网络安全法案，该法案规定将由单一机构管理包括电信在内的所有关键基础设施。监管机构正在制定一套要求，以便运营商报告安全合规情况。该国一家运营商强调，新政策的实施可能具有挑战性，因为它涉及传达风险和阐明最低安全要求，这需要时间、成本和开展大量工作，通常还涉及股东方的考虑。对于有股东的运营商而言，安全方面的结构、政策和法规有时不一致，这可能给安全团队带来挑战。因此，在考虑新的安全框架时，有必要让所有团队，包括首席执行官参与。

5. 投资于教育和培训劳动力队伍以应对5G网络安全的复杂性仍是重点

根据Allied Market Research的数据[25]，到2031年，全球5G安全市场预计将达到378亿美元，对网络安全专业人员的需求也大幅飙升，尤其是那些拥有保护5G网络专业技能的专业人员。各国、组织和机构应优先考虑劳动力培训和招聘，以确保推进5G网络安全。目前，劳动力队伍中很难找到所需的专业技能；此外，实现招聘的性别平衡也是一项挑战。如果劳动力队伍未做好准备，将会减缓向5G的过渡步伐并使其复杂化。虽然各国应通过国家计划优先考虑培训和教育，但私营部门也可以探索培训和技能提升计划，因为需要更广泛行业的参与才能确保需求得到满足。

土耳其是正在寻找应对劳动力挑战解决方案的国家的一个例子，该国加大了对教育和培训劳动力的投资，使之能够应对复杂的5G安全。作为这一承诺的一部分，信息通信技术管理局、中东技术大学、İhsan Doğramacı Bilkent大学、Hacettepe大学和电信运营商土耳其电信（Türk Telekomünikasyon A.S.）、Turkcell İletişim Hizmetleri A.Ş.和沃达丰电信（Vodafone Telekomünikasyon A.S）等主要机构建立了一个5G谷开放测试场。该测试场作为5G及以后技术的研究、开发和测试的重要平台，为学术界和业界提供了合作的机会。由上述机构代表组成的5G谷执行委员会确保了该举措的有效实施。通过为学者、研究人员、博士生和初创企业提供一个可以参与5G及以后相关工作的平台，开放测试场不仅促进了创新，而且有助于培养高技能的劳动力。这一举措是土耳其战略不可或缺的组成部分，旨在通过持续投资于教育、培训和研究来优先考虑和增强5G网络的安全性[26]。

6. 超越5G：设定6G网络安全的方向

尽管在许多国家和地区5G仍处于规划和部署阶段，但研发和标准化进程的注意力已开始转向5G之后网络。因此，到2023年底，国际电联无线电通信部门（ITU-R）批准了2030年及之后IMT[27]未来发展的框架和总体目标，即商业上所说的6G。

> 该框架强调，IMT-2030有望成为实现增强的安全性和弹性的重要推动因素。预计设备在设计上是安全的，并有能力在破坏性事件（无论是自然事件还是人为事件）期间继续运行并从中迅速恢复。该文件还重申，IMT-2030系统的安全性和复原力是实现更广泛的社会和经济目标的基础。
>
> 在IMT-2030的背景下，该框架将安全定义为“保护信息（如用户数据和信号）的机密性、完整性和可用性，保护网络、设备和系统免受黑客攻击、分布式拒绝服务、中间人攻击等网络攻击”。弹性定义为“网络和系统在自然或人为干扰（如主电源丢失等）期间和之后继续正常运行的能力”。

很明显，人们正在设想6G，并开始其标准化过程，对安全性和弹性有着强烈的关注，这与5G技术的早期设计阶段（包括从标准化的角度来看）不同。与2015年批准的IMT-2020（商用称为5G）愿景相比[28]，令人信服地说明了思维的转变，同时亦认识到需要适当解决网络安全和网络复原力问题，将其作为数字化转型和数字经济的支撑支柱。

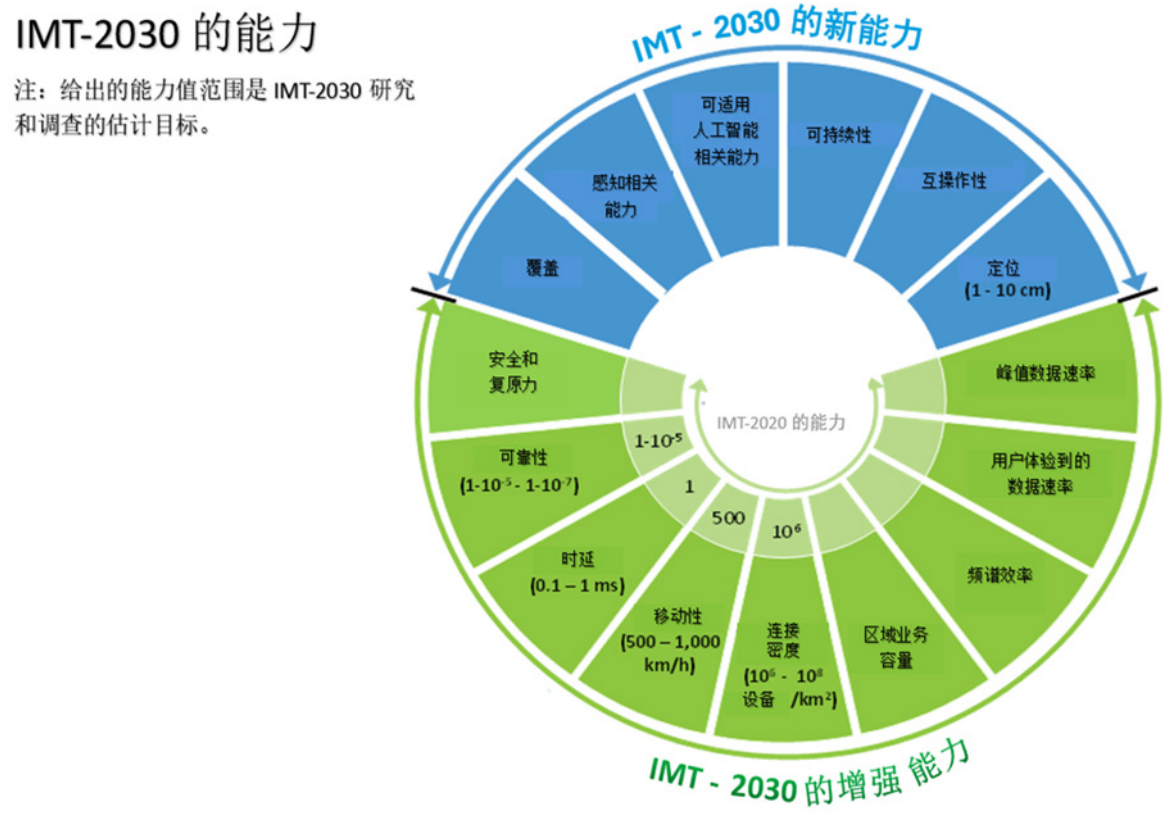
[25] https://www.alliedmarketresearch.com/5g-security-market-A12820

[26] https://5gtrforum.org.tr/en

[27] ITU-R M.2160建议书，见：https://www.itu.int/rec/R-REC-M.2160-0-202311-I/en。

[28] ITU-R M.2083建议书，见：https://www.itu.int/rec/R-REC-M.2083-0-201509-I。

图1：IMT-2030的能力



来源：ITU-R M.2160建议书

跟进**2022-2025年ITU-D第2研究组第3/2号课题**“培育网络安全文化的最佳做法”

第3/2号课题网站http://www.itu.int/en/ITU-D/Study-Groups/2022-2025/Pages/reference/SG2/questions/Question-3-2.aspx

邮件列表：d22sg3q2@lists.itu.int 请点击此处

ITU-D研究组网站：www.itu.int/itu-d/sites/studygroups/

分享您反馈，请发邮件至devSG@itu.int，电话：+41 22 730 5999

ITU出版物
瑞士出版，日内瓦，2024
ITU 免责声明: https://www.itu.int/en/publications/Pages/Disclaimer.aspx
国际电信联盟
Place des Nations, CH-1211 Geneva Switzerland