



5G 网络安全的欧盟策略与实践

郭丰, 嵇叶楠, 黄潇怡

(中国信息通信研究院, 北京 100191)

摘要: 5G 网络有望成为未来经济和社会发展的关键基础设施。当前, 5G 全球竞争升温, 领先运营商竞相加快 5G 部署。归纳总结了欧盟国家部署 5G 网络的工程技术路线, 分析了欧盟国家下一阶段部署 5G 网络的路线设计、影响因素和时间步骤, 并对如何开展中欧 5G 领域合作提出了相关建议。

关键词: 5G; 安全; 欧盟; 策略

中图分类号: TN929.54

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2020176

EU's strategy and practice of 5G network security

GUO Feng, JI Yenan, HUANG Xiaoyi

China Academy of Information and Communications Technology, Beijing 100191, China

Abstract: 5G network is expected to become a key infrastructure for future economic and social development. Nowadays, global competition for 5G has been heating up, with leading operators racing to speed up their 5G deployments. The road-map of engineering and technology for the deployment of 5G networks in EU countries were summarized, the route design, influencing factors as well as time steps for the next phase of 5G networks deployment of them were analyzed. Besides, relevant suggestions for the development of China-EU cooperation in the field of 5G were put forward.

Key words: 5G, security, EU, strategy

1 引言

随着全球新一轮科技革命和产业变革深入发展, 5G 网络有望成为未来经济和社会发展的关键基础设施, 各国围绕 5G 技术和产业的博弈加剧。2020 年 1 月 29 日, 欧盟委员会出台名为《5G 网络安全工具箱》^[1]的指导文件(以下简称“指导文件”)。指导文件是在欧盟成员国于 2019 年

10 月联合发布的《欧盟 5G 网络安全协调风险评估报告》基础上, 由欧盟委员会和欧盟网络与信息安全局(ENISA)会同各成员国共同制定的, 为的是全面梳理欧盟面临的 5G 网络安全风险, 并提出一套可行措施推动欧盟成员国采取协调一致的方法在部署 5G 网络的过程中强化网络安全。本文从指导文件出发, 结合相关信息阐述和分析欧盟在加强 5G 网络安全方面的策略与实践。



2 欧盟提升 5G 网络安全的工程策略

根据《5G 网络安全工具箱》文件，欧盟认为 5G 网络主要涉及以下 5 类安全风险。

- 安全措施不足带来的风险，例如网络配置错误、缺乏访问控制。
- 与 5G 供应链有关的风险，例如产品质量不达标、依赖单一供应商。
- 主要威胁者造成的风险，例如针对 5G 供应链实施国家干预、针对最终用户实施有组织犯罪。
- 5G 网络与其他关键系统之间相互依存导致的风险，例如严重破坏关键基础设施或服务、由于电力供应中断或其他支持系统问题造成的网络大规模故障。
- 终端用户设备带来的风险，例如使用物联网终端、手机或智能设备引发的安全问题。

指导文件针对每类风险制定了详细的缓解计划，包括 8 项战略措施和 11 项技术措施。其中，对于 5G 移动网络运营商，指导文件要求成员国提高安全要求，包括严格控制访问权限、制定安全操作和监控规则、限制特定功能外包等。对于 5G 设备供应商，要求成员国开展风险评估，限制高风险供应商参与建设欧盟重要敏感网络资产（如核心网功能、网络功能虚拟化管理和配置（MANO）等）；实施多供应商策略，避免或降低对单个供应商（尤其是高风险供应商）的过度依赖，以维持多样化和可持续的 5G 供应链等。指导文件还提出了 10 项支持行动以提高上述措施的实施效果，包括加强沟通协作，制定网络安全相关标准、实施指南、认证计划，分享最佳实践措施，强化欧盟和成员国层面的测试和审计能力，提供公共资金支持等。

通过上述对指导文件的工程实施策略可以看出，对于 5G 移动网络运营商，指导文件要求成员国提高安全要求，包括严格控制访问权限、制定

安全操作和监控规则、限制特定功能外包等。对于 5G 设备供应商，要求成员国开展风险评估，限制高风险供应商参与建设欧盟重要敏感网络资产（如核心网功能、网络功能虚拟化管理和配置（MANO）等）；实施多供应商策略，避免或降低对单个供应商（尤其是高风险供应商）的过度依赖，以维持多样化和可持续的 5G 供应链等。此外，值得注意的是，英国政府于 2020 年 1 月 28 日宣布，批准华为参与英国 5G 网络“非核心”部分的建设，其市场占有率上限为 35%。德国、法国等欧盟主要成员国也纷纷表示，不会在 5G 问题上预先排除特定国家企业。

3 5G 全球竞争升温，领先运营商竞相加快 5G 部署

5G 赋能万物互联，各国在国家数字经济战略中均将 5G 作为优先发展领域，强化产业布局，塑造竞争新优势，同时开始提前布局 6G。据 GSMA 统计，截至 2020 年 3 月，全球已有 63 家运营商在 35 个国家和地区推出 5G 商用服务^[2]；全球有 359 家运营商正在投资 5G 网络，包括 5G 网络测试、试点或已启动大规模部署。美国、欧盟和中国拥有全球主要的数字供给和消费市场，近年来围绕 5G 领域展开竞争、博弈或合作，均希望取得数字时代的最大领先优势。自 2018 年 10 月，美国各大运营商相继开启 5G 商用。截至 2019 年 10 月，美国 AT&T 公司在全美 20 个城市启动 5G 业务。Verizon 公司在美国 13 个城市推出 5G 业务，在 13 个美国橄榄球联盟（NFL）球场建设完成基于毫米波的 5G 网络；Sprint 在 9 个城市开展了 5G 业务，其网络部署在 2.6 GHz 频段。上述 3 家美国运营商当前正在加快对全美国的 5G 网络规模覆盖，以期尽早在全美国实现 5G 商用。5G 发展成为欧盟抓住新一轮科技革命重大机遇、发展数字经济、维护技术主权的重要着力点。当前，欧洲各国 5G 部署开始提速，德国、法国、奥地利、

比利时、捷克、希腊、匈牙利等国陆续开展 5G 网络建设招标。随着欧洲 5G 部署进度的提速,全球移动通信系统协会(GSMA)预计到 2025 年,全球 5G 连接数将达到 18 亿,其中欧洲将占 13.1%,约 2.3 亿元,5G 将占欧洲所有连接数的 34%^[3]。

欧盟关于 5G 的指导文件对外传达了明确信号,即欧盟地区 5G 市场虽然总体开放但门槛提高,具体开放程度和准入条件等将交由各成员国决定。各成员国将围绕 5G 产业各环节,通过提升安全管理要求、强化安全评估监测、实施多供应商策略等手段,维护技术主权,着力扭转在互联网产业与服务上对外严重依赖的不利局面。

4 提升 5G 网络安全是欧盟维护技术主权的重要方面

近年来欧盟和多数欧洲国家进一步认识到发展数字经济的重要性和紧迫性,出台一系列围绕数字经济的政策指南,例如 2015 年欧盟公布《单一数字市场》战略,提出数字产业及相关社会和安全治理的顶层设计。近期,欧洲在数字经济方面强调维护“技术主权”,法国、德国等国家领衔,同其他欧盟成员国一道致力于增强欧盟战略自主性。新当选的欧盟委员会主席乌尔苏拉·冯·德莱茵将科技政策作为其执政重点,上任 100 天初期即推出《塑造欧洲数字未来》^[4]发展战略,她指出要发展关键技术,摆脱对外国的依赖,制定符合欧洲价值观和规则的数字经济规则。

基于上述背景,欧洲开始在 5G、数据治理、数字税、网络安全、关键基础设施、人工智能伦理等领域积极实施政策举措与技术手段,而 5G 网络安全无疑是欧盟维护其技术主权的重要领域。欧洲在信息通信技术领域谋求的“技术主权”主要是指掌握核心技术或保证技术掌控力,在新一轮科技革命和产业变革浪潮中,实现技术自主,摆脱产业依赖,强化市场监管,构建数字竞争优势,进一步提升欧洲数字经济发展水平。在欧盟

追求“技术主权”的道路上,5G 领域是当前欧盟和欧洲国家决策层最为关注的重点领域之一,集中体现了欧盟的内部监管策略以及国际竞争与合作策略。

5 美国政府或将影响欧盟国家部署 5G 的工程技术路线

2019 年年初以来,美国国会发布一系列法案,显示了美国在 5G 领域的全球策略,应对现阶段在 5G 领域的竞争。从 2019 年至 2020 年 2 月,美国第 116 届国会两院共提出了超过 30 项有关应对 5G 竞争的法案以及 5 个提高美国 5G 竞争力的动议。法案内容涵盖美国国内的 5G 能力建设以及应对 5G 竞争的全球策略。

美国政府强调与盟友、战略合作伙伴开展信息共享,并强调建立共同的测试环境与研究发展计划。《5G 安全与其他法案》中有关美国与其盟友、战略合作伙伴合作的规定主要分为 4 步。

(1) 要求全面评估盟友或战略合作伙伴国内的 5G 供应商生产和供给水平,促进这些供应商发展,最终为美国 5G 行业提供充足资源。

(2) 评估美国盟友和战略合作伙伴的通信设备供应链中存在的安全差距并制定措施缩小差距。

(3) 建立外交互动机制与它们共享 5G 安全风险信息和合作应对风险,同时在 5G 标准方面加强合作最大程度提高互操作性、竞争力、开放性和平台安全。

(4) 制定能够共同参与的测试环境、研究与发展的计划。《提高美国在 5G 的国际领导力法案》提出制定关于 5G 及下一代移动通信系统和基础设施所使用设备的外交战略,该战略将促进美国政府与盟友、战略合作伙伴共享相关设备的安全风险信息和相关进展情况并携手共同应对风险。

美国政府和企业的 5G 发展策略或将影响欧盟国家围绕部署 5G 的工程技术路线。目前,美国



政府和企业对 5G 技术、产业、安全等方面的重视程度日益提升，以苹果、高通公司为代表的美国科技公司在全球 5G 产业链上占据重要位置，美国市场又是全球最大的 5G 市场之一，美国政府和企业发展、部署 5G 网络的策略具有很强的示范效应。因此，作为美国信息通信企业的重点目标市场，欧洲国家下一阶段部署 5G 网络的工程技术路线在很大程度上将受到美国高通等公司的带动。

6 欧盟及成员国建设 5G 网络的政策走向

从指导文件所涉及的相关主体来看，欧盟层面（即欧盟委员会）预计将继续加强对各个成员国 5G 发展的统筹协调，组织各国各方研究制定欧盟层面的与 5G 网络安全相关的政策及认证标准并推动相关规则在各成员国层面执行，强化安全评估与监测手段，依托欧盟计划和项目进一步提高 5G 及后 5G 技术研发和商用推广投入等。欧盟各国主管部门将参照指导文件，完善本国法律法规、制定实施细则，结合本国 5G 发展规划和网络安全管理要求，参与制定欧盟相关政策及认证标准，强化本国行业监管、设备入网、安全防护等手段建设等。移动网络运营商将严格落实欧盟及本国政府要求，重点实施多供应商策略，参与制定并执行欧盟相关政策及认证标准，在设备采购环节提出更高的安全管理要求等。5G 设备供应商需要符合更高标准的网络安全要求并接受相应评估与监测，欧盟以外的供应商预计将面临更严格的市场准入要求，也就是说欧盟以外的设备供应商将付出更多的合规成本，而欧盟本土供应商则将拥有更多的市场空间和机遇。

根据工作计划，欧盟委员会呼吁各成员国于 2020 年 4 月 30 日前采取措施落实指导文件要求，并于 6 月 30 日前将相关实施情况提交欧盟委员会；10 月 1 日前，欧盟委员会将联合各成员国评估上述措施的实施效果，并确定是否有必要采取下一步行动。

7 结束语

作为新一代移动通信技术，5G 引领了跨行业数字融合、全场景应用及商业模式革新。长期看，开展 5G 信息基础设施建设将构建数字经济时代的关键支撑^[5]。5G 网络安全是关系到世界各国和人民的全球性新挑战，只能通过国际社会合作应对，要避免将网络安全政治化。总的来说，我国电信设备企业一方面要正视和尊重欧洲对于 5G 安全的诉求，努力符合欧洲关于 5G 网络建设的要求，另一方面，要利用好中欧各种沟通渠道，通过对话与协商，呼吁欧盟为中国企业投资和经营提供公平、公开、公正和非歧视性的环境。建议我国相关政府部门和企业从以下 3 方面继续开展好全球范围内、特别是中欧 5G 交流与合作。

（1）跟踪进展，开展国别研究

考虑到欧盟委员会在统筹协调欧盟成员国开展 5G 网络安全工作方面已步入实质阶段，建议我国信息通信行业企业及时关注、跟踪欧盟方面相关工作进展，开展欧盟及其主要成员国市场准入和监管政策跟踪研究，并持续关注美国及全球其他主要大国和区域市场（如金砖国家、中东等）动向，评估英国政府表态对全球 5G 市场发展政策产生的作用，对于有类似要求的，及时分析其对我国电信设备厂商带来的影响。

（2）保持沟通，提供合规服务

通过产业交流等渠道与欧盟方面保持顺畅沟通，及时了解欧盟 5G 发展与管理工作的进展，就关键问题进行对话，进行必要的澄清与解释，呼吁欧盟方面给予中国企业公平、公正、无偏见待遇。同时，建议华为、中兴等设备厂商自行研究指导文件相关要求对企业的影响及应对方案，积极关注欧盟相关政策及认证标准制定工作，将自查与第三方评估相结合，确保产品和服务符合欧盟及其成员国相关规定。建议我国电信设备厂商不断深化与欧盟运营商合作抢占价值高地，创新 5G 商

业模式^[6]。

(3) 借鉴思路, 做好安全防护

欧盟关于强化管理、降低 5G 网络安全风险的做法值得各国各方借鉴。建议我国相关政府部门加紧制定出台关键信息基础设施保护、数据保护等国内管理政策, 统筹推进国际国内 5G 相关网络安全标准规范, 加强网络监测、风险感知、主动防御与数据保护能力, 提升我国在信息科技领域的总体安全保障水平。

参考文献:

- [1] 欧盟委员会. 5G 网络安全工具箱[Z]. 2019.
European Commission. Cybersecurity of 5G networks-EU Toolbox of risk mitigating measures[Z]. 2019.
- [2] 赵子骏. 5G 商用之后是 6G 竞争的开始[J]. 网信军民融合, 2020(2): 40-42.
ZHAO Z J. 6G competition starts from 5G business deployment[J]. Civil-Military Integration on Cyberspace, 2020(2): 40-42.
- [3] 陈骞. 欧盟 5G 网络安全建议报告解读[J]. 上海信息化, 2019(5): 80-82.
CHEN J. Analysis on EU 5G network security report[J]. Shanghai Informatization, 2019(5): 80-82.
- [4] 欧盟委员会. 欧盟发布《欧洲工业战略》塑造欧洲数字未来[EB]. 2019.

European Commission. EV releases “European Industrial Strategy” to shape Europe’s digit future[EB]. 2019.

- [5] 曾剑秋, 吕可可. 5G 赋能未来智慧社会[J]. 张江科技评论, 2020(1): 27-29.
ZENG J Q, LV K K. 5G enable future intelligent society[J]. Zhang Jiang Technology Review, 2020(1): 27-29.
- [6] 孟海华. 5G 技术发展趋势、瓶颈及攻关重点[J]. 张江科技评论, 2020(1): 66-70.
MENG H H. The technology trend, bottleneck and research key areas of 5G[J]. Zhang Jiang Technology Review, 2020(1): 66-70.

[作者简介]



郭丰 (1981—), 男, 中国信息通信研究院政策与经济研究所高级工程师、互联网治理研究中心副主任, GAC 章程工作组主席, 主要从事信息通信技术与政策、互联网资源管理、互联网治理、网络安全、网络空间战略等方面的研究工作。

嵇叶楠 (1985—), 女, 中国信息通信研究院政策与经济研究所高级工程师, 主要从事网络空间治理、信息通信政策、网络基础资源等方面的研究工作。

黄潇怡 (1984—), 女, 中国信息通信研究院政策与经济研究所工程师, 主要从事网络安全战略、网络基础资源等方面的研究工作。