群策群力 应对5G安全挑战

本报记者 高 博

世界5G大会21日开幕，在北京亦庄的展馆内，5G安全板块成为吸引观众驻足的一个点。观众可近距离观看工业机器人破解、NFC隐私信息窃取、手机远程窃听偷拍、智能门锁破解等场景，由此意识到智能网络风险的普遍存在。

比如工程师演示了一种常见的手机窃听方法：黑客控制免费WiFi，或自己搭建WiFi，当用户连接，并使用未经过安全检测的APP时，黑客就可以悄悄控制手机的前置摄像头和麦克风，还可以随意读取和发送信息，窃取用户所有隐私。不仅是手机，一些家用智能音箱也会被黑，成了“间谍”。

许多仓库和办公室门口配备了门禁或密码锁，一些安全性能不过关的门禁，可以被“电磁振荡特斯拉线圈”轻而易举地刷开。

携带具有RFID读卡功能的设备，在不打开对方钱包的情况下，可以读到钱包里的银行卡信息，包括卡号、持卡人姓名、身份证号码和近期10条交易记录，这些都会在黑客的屏幕中展现。

“在一个案例中，某顶级团队发现，一个城市的智能路灯存在漏洞，它允许上传恶意代码，让黑客能控制城市大部分路灯。”网络安全专家苗春雨说。

5G大会现场还演示了一台工业机械臂，本来正小心地书写毛笔字，而在黑客发动攻击、更改指令后，机械臂行为紊乱，开始书写预料之外的笔划。工厂再发送指令也无法修复。“一台机械臂可以重启恢复；但如果是在生产线上，上千台的机械臂重启，损失不可估量。”奇安信集团的工程师讲解说。

在关键展位的中央大屏幕上，论坛展示了5G时代下的数字城市内生安全系统。技术供应商试图展示，在5G时代设备互联互通的复杂情况下，保障一切顺利需要新的体系。

5G本身的安全问题并不复杂，但由于5G涉及物联网和人工智能，运行差异极大的各种业务，便可能带来严峻的网络安全挑战，一些风险或许尚未浮现。

3G、4G互联网时代的安全问题就是解决网民上网安全问题，相对简单。随着5G时代的到来，要解决的不仅是5G通讯安全问题，更重要的是解决5G应用在不同行业场景的安全问题，其中工业、城市、基础设施等领域尤为重要。由5G带来的物联网应用，让暴露面已经从网络空间转移到广大的实体空间，网络边界即将消失，所以网络风险即将实体化为物理空间的风险，对此不可小觑。

在21日的世界5G大会·5G安全高峰论坛上，工信部网络安全管理局局长赵志国表示，5G通过采用统一的认证框架、差异化的身份管理和各类应用场景按需保护等相关安全机制，提高了网络的整体安全水平。但5G引用的网络功能虚拟化，网络切片技术以及网络边缘计算等相关技术，在进一步增强网络连接性、服务弹性和个性化能力的同时，也带来了新的安全风险和不确定性。

“一方面基础设施向云端转移，被攻击的网络风险点明显增多，从封闭的平台扩展到开放的平台，用户隐私泄露的信息的风险增大，也给网络安全监管工作提出了更大的挑战。”

赵志国说：“网络安全与工业、能源、交通、医疗等实体经济生产安全问题交织。5G引入了更多的主体，各类主体之间的安全截面和责任更为模糊，对保障5G安全提出了新的挑战。”

中国网络空间安全协会理事长王秀军表示，5G技术发展以及应用场景更具广泛性、开放性和挑战性，需要设备制造企业、行业应用和网络安全企业，还有网络研究机构，去探索与5G相适应的安全体系，共同应对网络安全风险。

“世界各国发展数字经济的愿望是相同的。应对5G的安全挑战，也需要各国携手并肩。”王秀军说，“我们应该就5G安全治理问题积极研究，积极参与国际交流与合作，共同应对网络安全的挑战和风险，为网络安全发挥自己应有的作用。”

- 中国特别希望能够跟世界各国一起构建一个平台，共同探讨5G相关的规则和标准。我想中国会坚持推动开放、包容、多边的讨论，这样能够真正推动5G的广泛应用和发展。
- 我们要构建安全生态体系。加强网络安全攻关突破，加强产品研发和成果转化，加强安全服务和解决方案的推广力度，提升网络安全技术的防护能力，积极引导重点机构、企业提升网络安全保护力度，带动网络安全技术产业能力的提升，形成相互促进、互动发展的良好局面。
- 中国三大运营商的5G商用在全球有着里程碑式的意义，因为它会推动5G基站规模扩大。预计到2020年，5G用户规模将会达到16亿，仅中国就会有6亿，占全球40%。
- 产业链上的所有“玩家”应该加强沟通对话，将各自对安全的诉求直接加入到标准里面，甚至向网络运营商、设备商去提交，他们才能把安全系统设计得更加合理、可靠，这是未来我们应对5G安全挑战的必由之路。

现场回放

薛澜
清华大学教授

安全规则需各国合作共建

5G应用场景下可能带来的安全挑战大概分四方面。首先是对工控系统防护挑战。随着工业互联网时代到来，海量的工控系统和业务系统有可能成为黑客攻击对象，这种“网络安全直逼生产一线”可能是我们没有碰到过的情况。5G核心是超大带宽和超低延时，这带来一系列新问题，对系统的维护提出新的要求。另外，海量连接可能引发各种攻击。这些方面都有可能对工业控制系统构成压力。专家们也提出了很多防护措施。

第二个挑战是信息安全监测方面的。比如边缘计算技术等，绕过了现有的信息安全监测体系，对网络治理提出了挑战。

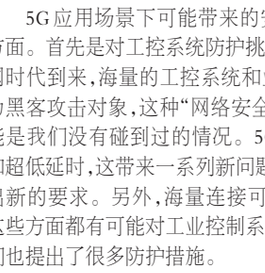
第三个挑战是针对信息安全传输的。首先是对内容的篡改，可能恶意植入某些东西；另外是身份的仿冒（没有授权，我潜入到你系统里面来窃听数据信息）；还有数据管理系统的篡改；以及越权的访问。

第四个是对供应商重度依赖存在潜在的风险。

2019年5月份，欧盟就未来5G网络达成了一致，应该说也是到目前为止最高级别的会议，从政策安全、数字经济等四个方面对5G进行了阐述，强调了5G安全。

中国特别希望能够跟世界各国一起构建一个平台，共同探讨5G相关的规则和标准。我想中国会坚持推动开放、包容、多边的讨论，这样能够真正推动5G的广泛应用和发展。

数据治理规则的制定需要我们尽快推动。有时候为了让技术健康发展，出台的规则不一定那么全面，可能先有一个大方向，再不断调整。我感觉除了技术手段以外，在治理规则方面大家要形成一定的共识。在国家层面还应该去建立一种交流机制，促进互信，不要影响到国家创新发展。



赵志国
工信部网络安全管理局局长

中国高度重视5G安全

5G作为信息技术演进升级的重要方向，是实现万物互联的关键基础，是数字化转型的重要驱动力量。随着5G与经济社会各领域的深度融合和广泛应用，数字经济发展的新空间不断拓展。中国高度重视5G发展，已于今年6月正式发放了5G的商用牌照。与此同时，我们也必须面对5G网络安全问题。

安全是发展的基础和保障。5G通过采用统一的认证框架、差异化的身份管理，各类应用场景按需保护等相关的安全机制，提高了网络的整体安全水平。但5G引用的网络功能虚拟化、网络切片技术以及网络边缘计算等相关技术，在进一步增强网络的连接性、网络服务的弹性和个性化等能力的同时，也带来了新的安全风险和不确定性。向云转移的基础设施，使得网络被攻击的风险点明显增多；从封闭的平台扩展到开放的平台，用户隐私泄露信息的风险增大，也给网络安全监管工作也提出了更大的挑战。

网络安全与工业、能源、交通、医疗等实体经济生产安全问题交织，5G引入了更多的主体，各类主体之间的安全截面和责任更为模糊，对保障5G安全提出了新的挑战。

在5G安全方面，我们坚持前瞻布局，试点应用，着力推进我国5G网络安全体系和能力建设：一是建立了5G网络安全保障体系，从多角度系统性地规划了5G安全体系建设；二是通过建设国家网络安全产业园区和开展网络安全学习，进一步推进试点示范和资源整合、资源配置工作，推动5G安全技术创新应用，提升5G安全技术保障的水平；三是着力推进与俄罗斯、欧盟、东盟等国家和地区的科研机构和企业在网络安全方面的技术交流合作，营造更加开放、公正、透明的国际网络安全发展环境。

我们要构建安全生态体系。加强网络安全攻关突破，加强产品研发和成果转化，加强安全服务和解决方案的推广力度，提升网络安全技术的防护能力，积极引导重点机构、企业提升网络安全保护力度，带动网络安全技术产业能力的提升，形成相互促进、互动发展的良好局面。瞄准5G产业链各环节，加强龙头企业，促进中小企业的发展，打造产业链、关键技术、产品和服务的一体化生态体系。

一方面，我们要加强能力建设，不断提升网络安全的保障水平。做好分析态势感知和应急处置等机制建设，统筹做好5G网络设施安全、应用系统安全、数据安全等相关工作，全面提升5G网络自身安全的保障水平。另一方面，着眼5G应用带来的安全风险，聚焦5G新技术安全风险的隐患，开展试点验证，围绕车联网、工业互联网、智慧能源等5G热门领域，积极探索网络安全的解决方案。

我们要打造协调联动的网络安全体系，推动跨部门、跨系统的合作。

陈华平
奇安信集团
副总裁

5G开启真正的个性化安全时代

5G通信网络安全性是可接受的，其安全风险集中在应用场景和接入设备上，核心是要保证数据安全，需要构建与业务融合的多重、多维度内生安全防御体系。

5G通信网络秉承了4G网络的协议、安全性设计。5G的网络切片和核心网下沉，能实现不同业务场景的需求并满足剧增的数据吞吐量，在带来飞速发展的同时也带来了安全挑战。

5G应用面临三大安全挑战：一是物联网安全，由于终端接入更简单、成本更低、数量更大，带来了认证难、审查难、控制难等安全问题；二是大数据安全，5G时代的边缘计算在用户侧，每个边缘计算中心都是大数据中心，数据实时吞吐量很大，容易被篡改和窃取；三是场景安全，5G应用和场景的关联非常紧密，要针对行业的差异化需求进行匹配，因此5G开启了真正的个性化安全时代。

面对这三大挑战，传统围墙式的安全防护手段已经失效。需要构建5G的“内生安全”，把单一的围墙式防护，变成与业务系统融合的多重、多维度防御。内生安全要求信息系统自我免疫、内外兼修、自我进化。首先安全系统必须像人体免疫系统一样自适应，对网络攻击做出反应；内外兼修是指安全体系必须同时具有内外两种能力，“外”能及时感知威胁、发现风险，“内”能与业务系统深度融合；自我进化是指安全体系能随着业务的成长，在抵抗网络攻击中不断完善自我。内生安全是“一个中心五张滤网”，能对网络、身份、应用、数据和行为进行动态审查和控制，最大程度降低网络攻击风险。

与业务融合，解决5G安全挑战：一是不再将安全能力与硬件绑定，而是用软件让规则变得极其容易编排，做到自动化、灵活化扩展，即使单个终端被攻击，也难以对全局造成巨大威胁；二是“零信任”动态访问控制机制，数据在不同的业务应用和平台之间流动，改变网络安全架构，“零信任”改变了以往在数据中心网络边界上进行防护的策略，引导安全体系架构从网络中心化走向身份中心化，以保护“虚拟化”的数据中心；三是端到端全局掌控，基于网络切片，通过安全网络管控平台，定制安全功能，对资源进行动态调度，灵活组合满足垂直行业的个性化需求，让安全没有死角，构建感知、分析、执行的闭环，实现端到端的全局掌控。

斯寒
全球移动通信系统协会大中华区总裁

5G安全守护美好未来

我们今天谈到的5G安全问题，在全球移动通信系统协会（GSMA）中主要是由一个工作组来处理：3GPP，他们的标准已经有了非常确切的5G商用机会。全球有24个运营商已经将其投入商用。中国三大运营商的5G商用在全球有着里程碑式的意义，因为它会推动5G基站规模扩大。预计到2020年，5G用户规模将会达到16亿，仅中国就会有6亿，占全球40%。

我们在看5G安全问题的时候，认为它主要来自两个增长，一个是业务需求的增长，一个是5G赋能千行百业需求的增长。5G安全对于一些领域非常重要，比如智能驾驶、远程手术等等，它们对安全等级要求非常高，因为这关系到人们的生命。可以说，5G的安全超越了前面任何一代移动通信技术的安全等级。

另一方面，新的技术和5G技术相结合，使得5G网络的复杂性、使用场景的复杂性、架构的复杂性和技术创新的复杂性都在增长，风险也随之增长。大家担心5G安全，我认为是合理的，但我觉得也没什么必要。你可以想一想，5G时代一定会有端到端的加密和容灾能力，因为安全问题不仅仅是网络问题，所以需要根据不同需求进行各种完备的、端到端的安全设计。当然我也认为，运营商和厂商在建5G网络时，还是应该保证或者提升5G网络安全水平。

新技术的使用会给5G时代带来新风险，比如网络虚拟化、资源耗尽，云服务也会遇到挑战。如果没有很好的保护，会导致信息泄露或者恶意软件的传播。如何正确保护、管理用户和终端在不同切片之间的迁移也是一个难点。物联网会有很多低成本的接入，如果不给予足够的重视，海量的终端接入会放大它的安全问题。5G初期还有“回落攻击”问题：刚开始5G覆盖不那么好，很多时候需要回落到2G、3G，用户是不是能得到及时的警告是一个非常重要的问题。恶意软件可能会利用这一点。物联网等网络攻击会导致出现更多的故障点、风险点，所以我们要避免攻击者对于设备的接管。

另外是关于技能问题，安全技术人员需要适应这种网络转型。虚拟化网络的安全和人工智能安全的技能缺乏，会导致风险。

GSMA从2012年开始就一直在研究5G安全标准的制定。其安全机制大概分为四个方面：隔离、加固、保护和预防。GSMA的漏洞报告项目会组织运营商、厂商及相关方面治理漏洞，我们对其中特别有建设性的漏洞报告公司或者工作人员，设立了名人堂。第一个进入GSMA名人堂的，就是中国团队。

我们还有一个信息分享和分析中心来讨论移动通信领域安全发展的方向，前瞻性地讨论人工智能的安全、量子密码等领域。GSMA的特别工作组，则主要研究5G信任模型和网络切片。

GSMA一直在努力促进网络安全方面的多方合作和创新。今年9月份，我们成立了一个5G创新投资平台，在这个投资平台中，我们主要关注了十个领域，安全便是其中非常重要的一个领域。我们非常鼓励和欢迎安全领域的初创企业和投资者入驻5G创新投资平台。5G改变社会，安全属于全社会，GSMA将与行业伙伴们共同维护5G美好的未来。

胡华东
华为公司安全专家

5G安全标准比以往更优秀

大家非常关注5G安全标准化。4G时代已经形成了非常统一的全球标准，在5G时代，统一标准又进一步变得更加坚实。它的整个技术标准和安全标准是在前面三代的基础上演进过来。5G时代的标准，我们可以认为是最安全的一代标准。

5G安全分成不同的层次，第一个层次是网络安全，也就是加密本身的安全特性设计。这个标准是由3GPP、W3C设计的，而且也是在5G网络一开始就嵌入系统里面的，这个技术也非常成熟。我们发现其中的漏洞都会不断做弥补，包括GSMA学术圈或者工业界发现了4G或者5G的漏洞，都可以进行相应的改进。4G或者5G的安全是不断迭代的演进过程，确保我们的通信系统是安全的。

第二个层次是对于设备的安全认证和安全评估标准。这个标准在4G时代已经起步了，是由GSMA和3GPP联合助其起步的，为了回应大家对于网络安全方面的担心，这个标准在今年10月份已经基本上就位了，GSMA已经正式发布了该标准。这个标准现在已经可以用在产业里面，包括对于设备商端到端的整个生命周期以及产品开发周期是否安全，都可以做评估，还可以对设备进行安全攻防。这套标准涵盖了整个设备生产流程的安全领域，包括设备本身的物理安全或者软硬件安全。

这套标准能为我们持续构建更安全的系统打下一个基础，但是这样的标准还不够。我们需要有安全的实验室、安全评估机构，去做出安全评估资质的认定。

我们还要考虑相关法律法规的健全。因为将来需要发证，必然会涉及到政府在这方面的要求。整个安全标准体系是一个非常大的生态系统，需要我们从方方面面去构建。安全生态、安全实验室、安全法律法规的建设还在进行当中，我们在向欧盟推荐相关标准，希望未来能有可公开、可对比的安全标准体系，构建一个全连接的智慧世界。

我觉得大家一直在谈论5G安全所面临的挑战，从我个人的理解来看，最大的挑战是5G要进入到千行万业，尤其是eMbb（增强移动宽带）业务，因为医院、电网等等很多垂直行业都会加入进来。5G的产业链也会发生一些变化，虚拟化领域的IP比较少，整个核心网会采纳更多的云化技术，给产业链上带来了一些新的“玩家”，这些都给5G安全方面的协同带来了复杂度。

产业链上的所有“玩家”应该加强沟通对话，将各自对安全的诉求直接加入到标准里面，甚至向网络运营商、设备商去提交，他们才能把安全系统设计得更加合理、可靠，这是未来我们应对5G安全挑战的必由之路。在加强不同产业链之间的协同方面，标准在其中可以起到关键作用。

（发言摘要由本报记者高博整理
本版照片由王友民 本报记者周维海摄）