2018年中国网络安全发展形势展望

【内容提要】 展望2018年，全球网络安全形势仍然严峻，勒索软件继续肆虐，针对关键信息基础设施的网络攻击进一步加强，各国在网络空间的“军备竞赛”将持续加剧，全球局部网络战有随时爆发的风险。面对新情况，如何加强网络安全建设？更好地应对网络安全威胁？更有力地保障国家安全？赛迪智库提出了加快完善《网络安全法》的配套法规体系；提升自主研发实力，构建核心技术生态圈；推进网络可信身份建设，构建可信网络空间；优化体制机制，全面保护关键信息基础设施；完善网络安全人才培养机制，建设网络安全人才队伍等对策建议。

【关键词】 网络安全 发展形势 展望

2017年，我国网络安全技术产品研发取得新成就，人才队伍建设不断加强，网络安全产业发展势头强劲，网络安全形势整体向好。展望2018年，全球网络攻击呈现出新的趋势，局部爆发网络战的风险一触即发，各国将采取有效措施强化网络空间的治理能力。我国网络安全能力建设将继续加强，但需要处理好网络安全法规体系不完善、信息技术产品自主可控生态尚未形成、网络可信身份体系建设滞后、关键信息基础设施安全问题突出、网络安全人才匮乏等问题，以提升我国网络安全保障能力。

一、对2018年形势的基本判断

（一）全球网络攻击将呈现出新的特点

蜜蜂内参

让您深入洞察整个商业世界

每天精挑细选3份最值得关注的学习资料

关注公众号：mifengMBA

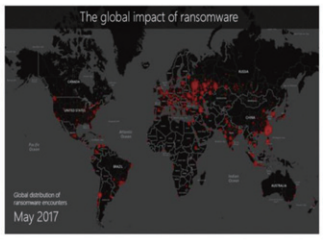
回复“入群”加入“蜜蜂内参”城市群

（不需要转发哦……）

扫一扫

回复“入群”

全球网络攻击呈现出新的特点



勒索软件肆虐全球

选举系统成为攻击新目标

关键信息基础设施屡遭黑客攻击

2017年，全球网络攻击态势依然严峻，并且呈现出新的特点。**一是勒索软件肆虐全球。**5月，全球150个国家和地区被勒索病毒攻击，被攻击电脑文件被病毒加密，只有支付赎金才能恢复，教育、企业、医疗、电力、能源、银行、交通等多个行业受到影响。6月，韩国网络托管公司Nayana旗下153台Linux服务器和3400个网站感染Erebus勒索软件，并向黑客支付了赎金。10月，俄罗斯、乌克兰和其它国家的组织机构遭遇etya勒索软件的新变种“坏兔子”勒索软件的网络攻击。**二是关键信息基础设施屡遭黑客攻击。**3月，俄罗斯第一大私人商业银行阿尔法银行(Alfa)发布公告称，阿尔法的网络基础设施遭遇大规模DNS僵尸网络攻击。7月，英国政府通讯总部称，英国工控系统与服务机构遭受黑客攻击。10月，瑞典三家交通机构的IT系统遭到黑客DDoS攻击，导致官网服务掉线、列车运行延误。**三是选举系统成为黑客攻击的新目标。**6月，国外媒体报道，俄罗斯入侵了美国39个州的选民数据库和软件系统，对

美国选举系统发动的网络攻击数量大约是之前报道的2倍。网络安全公司ThreatConnect发布报告指出，巴勒斯坦民族权力机构（Palestinian Authority）选举活动被新型恶意软件Kasperagent攻击。9月，德国保守派基督教民主联盟副主席发表声明称，在电视竞选辩论之前，德国竞选网站遭受了3000余次网络攻击，其中多数IP地址来自俄罗斯。

2018年，随着技术的进步，全球网络攻击的方式将会更多，黑客针对关键信息基础设施的攻击次数更多、范围更广。

（二）全球局部爆发网络战的风险将进一步增加

网络空间已成为国家、地区之间安全博弈的新战场，各国为了维护本国在网络空间的核心利益，持续加大网络空间的军事投入，国家级网络冲突爆发的风险不断增加。一**是网络空间“军备竞赛”持续升级。**2

月，美国国防部高级研究计划局启动SHARE项目，试图创建一种新的数据共享技术，使美军可以在世界各地安全地发出或者接收远程敏感信息。4月，韩国国防部公布《2018-2022年国防中期计划》，计划5年间将投入2500亿韩元加强网络安全建设。6月，美国国防部计划5年投资10亿美元，支持雷神公司开发、操作与维护“DOMino”项目。**二是有政府背景的网络攻击行为日益猖獗。**8月，印度黑客入侵巴基斯坦政府官网，将网站页面设为纯黑色，并播放印度国歌，以庆祝印度独立日。8月，美国网络安全公司FireEye研究人员发现伊朗黑客组织APT33瞄准多国航空、国防与能源设施展开新一轮网络攻击活动。9月，网络安全公司Palo Alto Networks发现黑客组织利用恶意软件Babar操控刚果民主共和国常设理事会官方网站，窃取国家重要信息。上述三个黑客组织都被怀疑有政府背景。**三是国际社会不断强化网络安全军事演习。**7月，美国网络司令部举行年度夺旗军事演习，将关键设施遭受攻击应对作为演习目标。7月，新加坡举办“网络星”网络安全演习，模拟网页篡改、数据渗透攻击、勒索软件攻击、分布式拒绝服务攻击及物理层网络攻击等多种情境。9月，欧盟多国国防部长参加大规模网络防御演习，模拟欧盟军队在受到网络攻击时所能作出的反应。

2018年，全球各国将会继续加强网络“军备竞赛”投入，提高本国网络战的能力，全球局部地区爆发网络冲突的风险进一步提高。

（三）各国将采取有效措施强化网络空间治理能力

2017年，全球网络事件频发，各国为了保护本国网络安全，从两个方面采取措施，提高网络空间的治理能力。**一方面，纷纷制定出台网络安全法律法规。**7月，俄罗斯杜马通过《俄罗斯联邦关键信息基础设施安全法》，明确关键信息基础设施定义范围，包括国防工业自动控制系统、医疗、通信、交通、银行、金融、能源等领域。新加坡发布《网络安全法案》草案，明确关键信息基础设施范围，包括政府、医疗、信息通信等11类。**另一方面，强化对网络犯罪的打击力度。**7月，美欧执法部门联手捣毁“阿尔法湾”和“汉萨”等暗网黑市交易网站，其中仅“阿尔法湾”中失窃或伪造的身份证件与设备、恶意软件及其他黑客工具的商品条目就超过10万条。8月，美国国家反情报与安全中心、FBI及NSA内部警务小组联合对“影子经纪人”（Shadow Brokers）的身份展开调查。

2018年，各国将会更加重视网络空间安全，继续出台相关的法律法规，同时加大对网络犯罪，尤其是网络恐怖主义的打击力度。

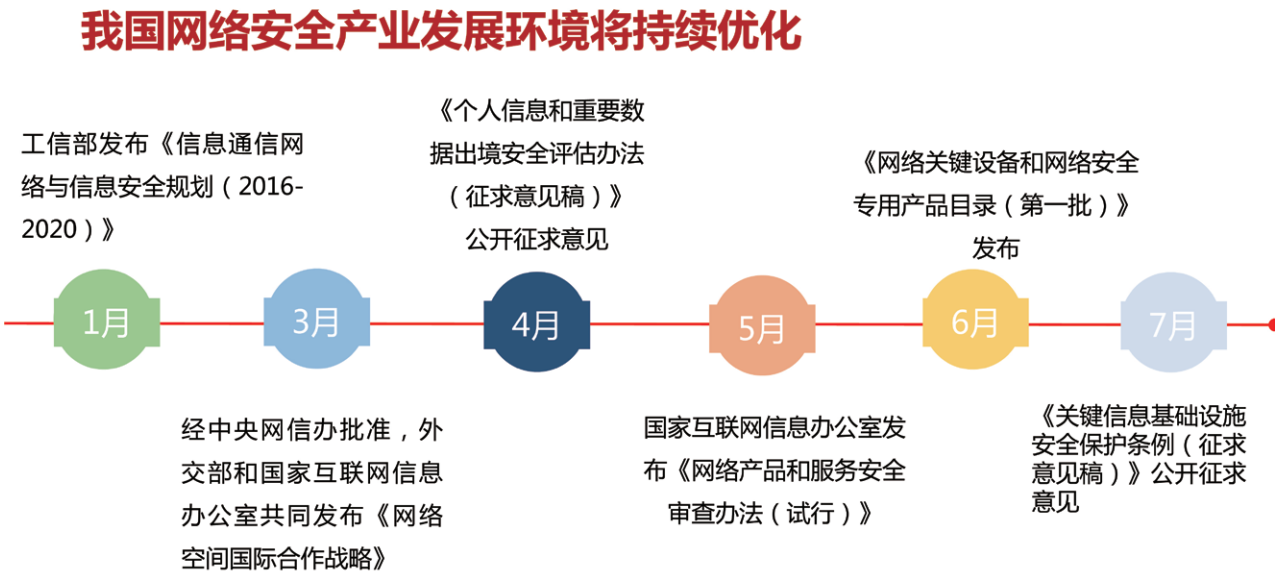
（四）我国网络安全能力建设不断加强

为了应对日益复杂的网络安全形势，确立网络空间优势，我国不断从技术研发、人才培养等方面加强网络安全能力建设。**一是不断推出网络安全新技术新产品。**2月，华为发布业界首款T级云综合安全网关，为客户提供高性能、易管理的全面软件化虚拟网络安全防护。4月，盘古实验室推出我国首个移动应用威胁数据平台——Janus移动安全威胁数据平台，深度挖掘分析应用的安全性及可靠性。9月，360企业安全集团发布

天御云网络威胁感知中心（云镜）、智慧管理与分析系统、高级威胁检测工具箱等产品，实现威胁发现、攻击溯源、流量取证和可视化展现。**二是不断加强网络安全人才培养力度。**4月，贵州师范大学联合中科院计算所、阿里巴巴、匡恩网络、梆梆安全、安恒信息等企业共同建立我国首个大数据安全重点实验室，旨在深入研究大数据安全基础理论和共性关键技术，完善大数据安全人才培养的产学研体系。8月，武汉临空港经济技术开发区管委会与杭州安恒信息签署战略合作协议，共同建设国家网络安全人才与创新基地。9月，在国家网络安全宣传周上，首批一流网络安全学院建设示范项目正式对外公布，包括西安电子科技大学、东南大学、武汉大学等7所高校。**三是网络安全企业通过多渠道合作优化网络安全生态环境。**6月，360联合SecurityInnovation打造自动驾驶安全实验室，在自动驾驶网络安全、V2X信息安全等方面进行深入合作，共同推进V2X的行业安全标准以及智能网联汽车信息安全防护产品。8月，亚信安全与腾讯云在政企客户云计算安全合规、云计算项目建设、产业互联网等领域的多个层面展开深入合作，打造一体化云安全服务。

2018年，我国将继续加强网络安全核心技术的研发，强化网络安全复合型人才的培养力度，鼓励企业通过多种方式开展合作，进一步提高我国的网络安全能力。

（五）我国网络安全产业发展环境将持续优化



2017年，我国对网络安全的重视程度日益提高，不断出台法规政策，网络安全产业发展环境不断优化。1月，工信部发布《信息通信网络与信息安全规划（2016-2020）》，提出全面提升网络与信息安全技术保障水平、推动网络安全服务市场发展等9大任务。3月，经中央网络安全和信息化领导小组批准，外交部和国家互联网信息办公室共同发布《网络空间国际合作战略》，以和平发展、合作共赢为主题，以构建网络空间命运共同体为目标，首次全面系统的提出了推动网络空间国际交流合作的中国主张。4月，为保障个人信息和重要数据安全，维护网络空间主权和国家安全、社会公共利益，国家互联网信息办公室会同相关部门起草了《个人信息和重要数据出境安全评估办法（征求意见稿）》，并向

社会公开征求意见。5月，国家互联网信息办公室发布了《网络产品和服务安全审查办法（试行）》，明确了审查对象、流程、机制等，为推动开展网络安全审查、提升网络产品和服务安全可控水平提供依据。6月，国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会等部门制定了《网络关键设备和网络安全专用产品目录（第一批）》，涉及路由器、交换机、服务器、防火墙等15类产品。7月，为保障关键信息基础设施安全，国家互联网信息办公室关于会同相关部门起草了《关键信息基础设施安全保护条例（征求意见稿）》，并向社会公开征求意见。

2018年，我国将会继续完善网络安全相关法律法规，出台系列网络安全标准体系，进一步优化网络安全产业发展的环境。

二、需要关注的几个问题

（一）《网络安全法》的配套法规尚不完善

2017年6月1日，《网络安全法》正式实施，作为我国网络空间安全管理的基本法，它框架性地构建了多项法律制度和要求。目前，一部分《网络安全法》的配套法规已开始生效，例如《网络产品和服务安全审查办法（试行）》等；但是仍有大量相关的法规尚未出台，例如个人信息安全保护方面的法律法规、数据安全管理办法、关键信息基础设施安全保护条例、个人信息和重要数据出境安全评估办法等。因此，2018年我国相关部门应继续加大力度，尽快完善网络安全领域的相关法律规范。

（二）信息技术产品自主可控生态尚未形成

长期以来，我国网络安全核心技术一直受制于人，重要信息系统和基础信息网络大量使用国外基础软件与核心关键设备，为我国网络安全带来严重威胁。2017年，欧美跨国企业对核心技术的开放程度继续提升，国内信息技术产业出现新一轮引进式创新热潮。相关专家学者对此持有不同观点，一种表示赞同，另一种认为应该走独立自主发展的道路。由于各界认识不统一，政府尚未集中优势资源对某一条具体实现路径进行扶持，尚未构建真正自主的产业生态体系。此外，信息技术产品安全可控的相关配套政策标准尚不健全，评价标准尚未发布，难以对相关信息技术产品和服务的安全性、可控性进行管控。

（三）网络可信身份体系建设仍需强化

我国网络信任体系建设滞后，网络身份管理存在缺漏，难以确保网络身份真实性、数据保密性，无法有效解决身份盗用等安全问题，导致网络欺诈、网络谣言等行为十分猖獗，给公众造成经济损失的同时，也严重扰乱了网络空间秩序。《网络安全法》明确提出，“国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。”然而目前，我国网络可信身份体系建设存在缺乏顶层设计，统筹规划和布局尚不明晰；身份基础资源尚未实现互联互通，重复建设现象严重；标准体系更新滞后，资金投入等保障措施不健全的一系列问题。因此，亟需开展针对性的研究，尽快制定国家

网络可信身份战略，建设网络身份体系，创建可信网络空间。

（四）关键信息基础设施安全问题日益突出

万物互联时代，关键信息基础设施互联互通的发展趋势愈发明显，在实现数据高效交互、信息资源共享的同时，也为针对关键信息基础设施的网络攻击提供了可能。目前，随着信息化与工业化的不断融合，网络攻击路径不断增多，工业控制系统的采集执行层、现场控制层、集中监控层、管理调度层以及企业内网和互联网等都成为潜在攻击发起点。此外，我国的关键信息基础设施安全保障还存在着标准缺失、网络安全检查评估机制不健全等问题。因此，面对日益严峻的网络安全挑战，我国应尽快完善关键信息基础设施安全保障体系。

（五）网络安全领域人才缺口较大

加强网络安全保障能力建设，人才队伍是关键，尤其是既懂技术、又懂管理的复合型人才。调查显示，我国网络安全人才需求高达90万，并以每年11%左右的需求增长，到2020年我国网络安全人才需求数量将达到140万。然而，目前我国网络安全专业毕业生仅维持在1万人/年的水平。这意味着我国网络安全岗位配备的人员大部分并非来源于网络安全专业，网络安全人才缺口巨大。究其原因是我国尚未形成专业、完整的网络安全人才培养机制。网络安全学科建设、资源投入、教学科研能力、人才培养模式等方面的体系不够完善，导致网络安全人才供需严重不平衡，且毕业生在科学素养、综合分析素养和创新精神方面与先进国家存在较大差距。此

外，人才待遇和薪酬激励机制不合理造成人才流失严重，优秀的网络安全人才或流失到欧美等发达国家的企业，或流向黑色产业链。

三、应采取的对策建议

（一）加强统筹协调，完善《网络安全法》的配套法规

一是加快出台关键信息基础设施网络安全保护条例，明确我国关键信息基础设施的范围、保护主体及职责、保护措施等，加大对关键信息基础设施安全保障共性技术和核心技术的研发。二是加强《网络产品和服务安全审查办法》的实施，采购关系国家安全的网络和信息系统与重要网络产品和服务，应经过网络安全审查。三是推动完善个人信息保护立法，健全网络数据和用户信息安全防护措施，保护公民个人信息及隐私。

（二）提升自主研发实力，构建核心技术生态圈

一是统一信息领域核心技术发展思路。统一自主可控、安全可控、安全可靠、安全可信等概念，摒弃自主创新和引进消化吸收之间的路线之争，改变以出身论安全的思路，形成信息技术产品安全可控评价标准，组织开展评价工作，引导厂商提升自主创新能力和产业生态掌控能力。二是优化核心技术自主创新环境。强化企业的创新主体地位，着力构建以企业为主体、市场为导向、产学研相结合的技术创新体系，提高企业创新积极性，继续以基金等形式支持企业通过技术合作、资本运作等手段争取国际先进技术和人才等，为企业充分利用国际资源提升自主创新能力提供支撑。三是构建核心技术生态圈。依托政府、军队等安全

要求较高的应用领域，结合应用单位基本需求，制定自主生态技术标准，统一相关技术产品的关键功能模块、技术接口等，依托安全可控评价等手段，引导企业协同创新，推动产业上下游企业团结协作，打造安全可控生态圈。

（三）推进网络可信身份建设，构建可信网络空间

一是做好网络可信身份体系的顶层设计。借鉴国外做法，结合我国国情，明确我国网络可信身份体系框架、各参与方在其中的角色和职责，并细化网络可信身份体系建设的路径，建立实施机制，明确组织、资金等各方面保障，从法律法规、标准规范、技术研发、试点示范、产业发展等多方面推进体系建设。二是按照包容并蓄原则，支持发展包括电子认证、用户行为分析等多种网络可信身份的技术和服务。三是组织开展网络可信身份法律法规、标准规范制定和应用示范等工作。根据网络身份体系建设需求，修订现有法律法规或制定新法，明确网络身份凭证的法律效力，完善相关配套规定；研究确定网络身份体系标准框架，加快制定和完善相关标准；开展网络可信身份相关试点示范，评估示范成效，并逐步大规模推广应用。

（四）优化体制机制，全面保护关键信息基础设施

一是着力加强关键信息基础设施安全保障工作的统筹协调。构建由国家网信部门统筹协调、行业主管部门各自负责的协调机制，加强各部门间的沟通协调，形成合力。二是建立健全关键信息基础设施保护制

度。明确保障关键信息基础设施安全保障的基本要求和主要目标，提出工作任务和措施。三是研究制定关键信息基础设施网络安全标准规范。研制关键信息基础设施的基础性标准，推动关键信息基础设施分类分级、安全评估等标准的研制和发布。四是建立健全关键信息基础设施安全监管机制。一方面，健全关键信息基础设施安全检查评估机制，面向重点行业开展网络安全检查和风险评估，指导并监督地方开展安全自查，组织专业队伍对重点系统开展安全抽查，形成自查与重点抽查相结合的长效机制；另一方面，完善关键信息基础设施安全风险信息共享机制，理顺信息报送渠道，完善监测技术手段和监测网络，加快形成关键信息基础设施网络安全风险信息共享的长效机制。

（五）完善网络安全人才机培养制，建设网络安全人才队伍

一是完善网络安全人才培养机制，继续加强网络安全学科、专业建设，完善网络安全教材体系，强化对网络安全专业人才和复合型人才培养力度。二是健全网络安全人才选拔、评价和激励机制，拓宽复合型人才选拔途径，采取符合网络安全人才特点的评价和激励措施。三是强化网络安全专项基金工作，继续实施网络安全优秀人才奖，优秀教师奖和奖学金等高等级、高奖金、高规格的奖项。四是加强网络安全人才国际交流，通过派出访问学者、参加国际会议或黑客大会等方式提升我国网络安全人才国际竞争力。五是改变金融资本价值取向，提升国家、企业等社会各界对发明、专利、新产品等技术成果的认可程度，营造尊重知识、崇尚技术、鼓励创新的人才成长环境。

本文作者：网络安全形势分析课题组　13601152007　liuquan@ccidthinktank.com