

“互联网+”对网络空间安全影响及未来发展趋势

袁得崙¹, 王小娟², 万建超³

(1. 中国人民公安大学信息技术与网络安全学院, 北京 102623;

2. 北京邮电大学电子工程学院, 北京 100876;

3. 普天信息技术有限公司, 北京 100080)

摘要: 网络信息技术的飞速发展深刻改变了人类的生活、工作和思维方式。与技术发展和用户增长形成鲜明对比的是, 全球网络空间安全形势日趋复杂。“互联网+”时代更应强调网络空间安全的重要性, 构建安全、稳定的网络空间意义重大。“互联网+”时代, 网络规模的不断扩大, 应用模式的不断创新, 以及应用环境的复杂化, 带来了许多新的安全问题。基于此, 分析了“互联网+”提出的对于网络空间安全的影响, 阐述了“互联网+”时代网络空间安全的发展趋势, 并给出了对策与建议。

关键词: 互联网+; 网络空间安全; 云计算; 大数据

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00145

Influence of Internet plus on cyberspace security and the technology development trend in Internet plus era

YUAN De-yu¹, WANG Xiao-juan², WAN Jian-chao³

(1. School of Information Technology and Security, People's Public Security University of China, Beijing 102623, China;

2. School of Electronic Science and Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China;

3. Potevio Information Technology Co. Ltd., Beijing 100080, China)

Abstract: The rapid development of network and information technology have profoundly changed the way of human life, work and thinking. However, in sharp contrast to technological development and subscriber growth, the global cyberspace security situation is becoming increasingly complex. Therefore, the importance of cyberspace security should be emphasized, and building safe and stable cyberspace is of great significance in the Internet plus era. The fact that the scale of the network continues to expand, the application model becomes more and more innovative, and the application environment becomes more and more complex brings a lot of new security issues. Based on this consideration, the influence of Internet plus on cyberspace security and the technology development trend was analyzed, and the countermeasures and suggestions were given.

Key words: Internet plus, cyberspace security, cloud computing, big data

1 引言

当今世界, 随着网络信息技术的飞速发展和全面普及, 人类生活、工作、思维方式都在发生

深刻变革, 以互联网基础设施为载体的网络空间和现实世界不断融合, 互联网不断地把自己编织进人们的生活、工作中^[1]。正如普适计算之父马克·韦泽所说: “最高深的技术总是令人无法察

收稿日期: 2017-01-04; 修回日期: 2017-02-05。通信作者: 袁得崙, yuandeyu@gmail.com

基金项目: 中国人民公安大学基本科研业务基金资助项目 (No.2016JKF01317)

Foundation Item: The Basic Scientific Research Item of People's Public Security University of China (No.2016JKF01317)

觉,却又不断融入生活。”而互联网正是这样的技术。中国高度重视互联网的发展,于2015年提出了推进“互联网+”行动的指导意见^[2,3],旨在促进互联网的创新成果与经济、社会各领域的深度融合,提升经济社会、经济实体的创造力,最终形成以互联网为基础设施和实现工具的经济发展新形态。“互联网+”代表了一种新的经济形态,“互联网+”的提出是对互联网的进一步升华和发展^[4]。截止到2016年1月,中国网民规模已经达到6.88亿,中国已经成为全球网民最多的国家^[5],更拥有一批具有世界影响力的互联网公司,具备了发展“互联网+”的深厚基础。

与技术创新、用户增长和经济繁荣形成鲜明对比的是,全球网络空间安全形势日趋复杂严峻,不仅体现在博弈主体更加多元错综,国际组织、主权国家、非政府组织、企业乃至普通公众均涉及其中,全球网络空间成为继陆、海、空、太空之外人类赖以生存的“第五空间”^[6]。在“互联网+”时代,安全风险边界不断扩展泛化,超越了传统的技术风险范畴。技术边界越来越模糊,安全环境越来越复杂,将对各国政治、经济、军事、文化等构成威胁。

当前,已有学者针对“互联网+”的内涵以及网络技术的发展趋势展开研究。其中,文献[4]讨论了适合“互联网+”发展需要的网络范型以及网络在规模、异构、性能、安全、应用等方面所面临的挑战。文献[7]分析了中国网络空间在互联互通、“工业4.0”等方面的安全需求和挑战,并对网络空间安全的发展趋势进行了阐述。文献[8]提出了基于网络空间安全层次模型的网络空间安全技术体系。本文专注于研究“互联网+”的提出对网络空间安全的影响,并阐述分析了“互联网+”时代网络空间安全发展的趋势以及对策建议。

2 “互联网+”对网络空间安全的影响

网络空间安全技术具有显著的伴随性,基于信息技术的演进,“互联网+”的提出将对信息技术变革与服务模式创新带来短期难以规避的高安全风险。在中国,网络空间安全已成为维稳、反恐、社会服务与治理之基,面临诸多安全风险与发展机遇,我国从“网络大国”向“网络强国”

转变的道路异常艰巨^[9]。当前我国核心信息技术受制于人,无法确保网络基础设施和重要信息系统完全自主安全可控,国家网络空间的安全威胁日趋凸显^[10]。“互联网+”的提出对网络空间安全产生的影响颇多,具体表现为以下方面。

2.1 “互联网+”实现方式向范围经济转变,模糊了网络空间安全技术边界

“互联网+”时代多链路接入、多网系融合、多服务接口开放、多认知交互的特点拓展了不同应用领域的网络攻击面,带来了更大的安全风险。特别是随着网络规模的不断扩大,以及诸如下一代互联网、云计算、物联网、大规模移动应用等应用模式的不断创新,应用环境越来越复杂,应用服务越来越多样^[11],因此带来了许多新的安全问题。

1) 经济模式的转变模糊了网络空间安全技术边界

作为工业革命后又一次重大的技术革命,互联网技术的发展速度和影响力大大超过了工业革命时代。在“互联网+”时代,随着互联网技术逐步发展,行业的增值空间将由规模经济向范围经济转变^[12]。互联网的高速发展确立了消费者的主体地位,从而改变了规模经济的市场基调。“互联网+”的提出进一步改变了企业利用规模优势来提高收益的方式。一方面,“互联网+”时代消费者的需求更加多元,互联网尤其是在线社交网络为满足不同用户的个性化需求提供了可能,用户开始追求能够反映个人诉求的商品和服务。另一方面,范围经济成为管理中的新热点,企业边际成本不断下降,产品组合丰富的经济性不断提高,“分布式”的综合管理迅猛发展。

因此,随着移动互联网、物联网、云计算、大数据等网络信息技术的普及应用,以及在此基础上的即时通信、社交网络、电子商务、互联网金融等网络应用模式的持续创新,网络空间技术生态环境更加复杂,商业价值不断凸显^[13],一系列的安全事件影响重大并呈现出全球传导的趋势。特别是“互联网+”时代多网络融合、开放、交互的特点,拓展了不同应用领域的网络攻击面,终端的衍化则扩充了对边界的定义,也模糊了网络安全技术的作用领域,因此,“互联网+”时代的安全挑战更加严峻。

2) 云计算的应用拓宽了网络攻击面

云计算的普及和应用提高了运行效率，同时也伴随产生了现实的安全风险，云服务日益成为网络攻击的潜在重点目标。传统针对单机机器进行数据获取和控制的攻击方式得到升级，黑客逐渐把攻击目标聚焦在云节点上，一旦控制云节点，就能利用云端和用户之间的信任关系，并以云端作为跳板，获取大量数据，批量控制用户机器^[14]。

无论是公有云、私有云还是混合云，都无限放大了单个系统、服务或应用程序接口存在的脆弱性带来的影响。另外，针对云平台上某一目标的攻击，还可能导致其他业务受到牵连，影响整体业务的可用性和连续性，造成大面积用户无法访问或使用。例如，据2013年《纽约时报》报道，黑客利用云技术，通过远程劫持亚马逊和google云计算服务，利用庞大的云资源，发起了针对美国金融机构进行的大规模分布式拒绝服务攻击。在我国，2014年仅由国家计算机网络应急技术处理中心协助处置的对云平台的大规模攻击事件就达10余起^[15]。

另一方面，资源共享带来了新的多租户安全问题，云服务商的出现则对用户数据以及用户隐私的保护提出了新的挑战，云计算的用户是否有能力监督、审计云计算服务商是另一个值得思考的问题。总之，云计算系统将成为“互联网+”的基础IT架构，一旦出现安全问题将会影响与之相关的多个行业。

3) 终端的衍化泛化了安全风险边界

从个人计算机到智能手机、移动设备，再到智能手表、智能眼镜等可穿戴设备，甚至到工业、农业基础设施中的传感器，联网的终端不断快速演进，终端的演进反过来也在不断推动着互联网的发展。云计算、大数据、物联网等技术打破了传统的安全风险边界，云安全、数据跨境流动、工控系统^[16]渗透等成为安全领域新的关注点。

互联网通过计算机、手机等终端的连接，部分实现了人与人、人与信息的连接。“互联网+”把水利、电力基础设施、家具、冰箱，可穿戴设备等各种各样的设备都连接起来，实现了人与人、人与物、人与服务、人与场景以及人与未来的连接^[17]。然而，我国当前尚未全面掌握新的信息革命的核心技术和规则标准，我国的网络空间面临巨大的系统性风险，安全保障能力存在巨大的不确定性。现有的以国家、组织或系统为对象的安全保障思想、方法和技术都面临新一轮重构。

2.2 “互联网+”生产要素向用户资源集中，加大了网络空间数据定罪难度

“互联网+”将用户资源集中，用户信息被细化为数据，对大数据的掌握程度实现了经济价值的转换。信息化的量变向数据化的质变已经撼动了商业、医疗、政府、教育、经济、人文及社会各个领域，大数据推动着传统行业从“+互联网”向“互联网+”的转换。从图1可以看出，与用户

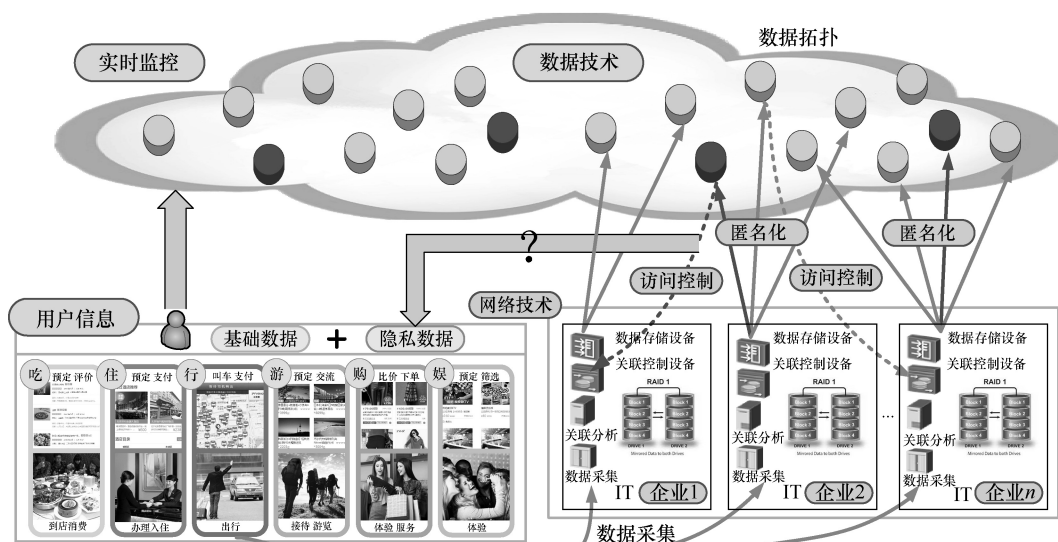


图1 数据化的“互联网+”需求

相关的吃、住、行、游、购、娱等数据皆可量化,大数据揭示了粗粒度样本无法揭示的细节信息。这种从信息粗粒度向数据细粒度的转变,使网络空间的各种攻击行为都隐藏在了大数据中^[8],如何应对数据增值过程中的安全问题,从技术层面来看,主要面临3个方面的挑战。

1) 实时计算海量存储,如何保证安全管控需求

在大数据时代,可以分析更多更杂的数据,有时候甚至可以得到和某个特定事件相关的所有数据,而不再依赖于随机采样。针对小数据量和特定的事情,追求精确性依然是可行的。但在大数据时代,由于数据纷繁多样、优劣掺杂,且分布在全球不同的服务器上,摒弃对于小数据量和特定事件的精确性追求,追求宏观上更优的洞察力变得具有特殊的吸引力。然而如何保证在一个安全的框架下进行数据之间的共享共通,是首要解决的问题^[18]。

2) 频繁数据流转交换,如何防止敏感数据泄露

当前是数据为王的时代,海量数据将成为未来创造社会经济价值的核心资产,而数据的集中处理和运算也将成为未来网络潜在的脆弱点,云平台的自身安全(特别是对海量数据的安全防护)将面临严峻的挑战。例如,存储在云端的国家机密、商业机密、社会保障数据等遭到窃取或无法提供正常服务,将会给国家、军队、企业带来不可估量的损失,直接影响国家安全和社会稳定^[19]。

3) 虚拟现实全息投射,如何防止社会工程学攻击

社会工程学攻击主要是指利用网络环境中“人的漏洞”实施攻击的行为,传统的安全防御手段通常很难起到保护作用^[20]。“互联网+”渗透了生活的各个角落,带来便利的同时也使黑客能够通过大量渠道获得用户的各类数据,综合分析用户的行为习惯以及个人隐私,使用社会工程学的方式发起精确攻击。例如,黑客可根据用户平时的上网习惯,分析出用户兴趣,定制专门的挂马邮件,增大攻击成功率;甚至可以直接根据海量数据,对用户的社交平台、邮箱密码、交易和支付密码等进行猜解,用户的个人隐私和财产安全面临着重大安全隐患。

2.3 “互联网+”作用领域向传统行业渗透,逆转了现实虚拟空间映射关系

“互联网+”的提出,标志着移动互联网、云计算、物联网、大数据等正在从简单的工具演变为社会的基础设施和核心理念,互联网将成为新的创新主体,经济运行模式将完成重构。移动互联网和物联网的普及让一切在线、虚拟和现实的边界变得越来越模糊。融合云计算、大数据、物联网、移动互联网等技术的“互联网+”满足了应用“突破时间和空间的全连接和零距离”和“基于数据的智能和智慧”的需求,实现了用户实时(real time)、按需(on-demand)、在线(all on-line)、社交化(social)的个性化请求^[21]，“互联网+”构建在万物互联的基础上,新产品、新服务、与新应用层出不穷。一方面,现实世界向网络空间延伸,国家安全问题延伸到虚拟网络空间;另一方面,网络空间向现实世界渗透,网络攻击、网络犯罪向传统行业渗透。

德国政府在所提的“工业4.0”中提出发展的3个阶段,即纵向集成—传统工厂边界内发生的技术革新、端到端集成—对供应链的集成、横向集成—跨越多条价值链的集成。其中,纵向集成将导致机器人、人工智能的大量应用,生产的高度自动化以及真正的信息物理融合系统(CPS, cyber physical system)^[22],可以预见,虚拟网络空间上安全威胁将会变成物理上的威胁。例如工控系统安全,由于使用周期长、更新成本高、设计阶段攻击威胁考虑不周全等因素导致当前对工控系统的防护基本还处于“攻击检测”阶段。然而工控系统安全关乎国家、民生、经济命脉,因此更具紧迫性。

3 “互联网+”时代网络空间安全发展的趋势

“互联网+”时代,信息技术从工具转变为关键基础设施,互联网为用户提供了像水、电、公路一样的基本服务,用户可以利用快捷、低成本的计算资源提升生产效率,创新业务模式。如图2所示,“互联网+”时代的信息基础设施可以概括为“云、网、端”这3个部分。云是指云计算、大数据基础设施;“网”包括传统互联网、移动互联网以及物联网等;“端”则包括个人计算机、移

动终端、可穿戴设备、工控系统中的传感器以及软件形式的应用。

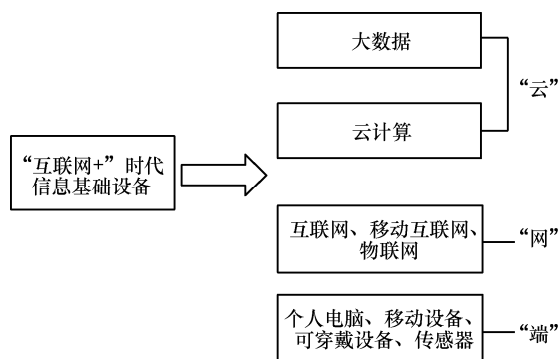


图2 “互联网+”时代的新基础设施

以智能终端为代表的各种“端”设备，在互联网、云计算、大数据设施构成的“云网”助力下，提供了数据的来源和服务器的界面。其信息基础设施承载能力不断得到提高，新增价值持续得到挖掘，此类“端”设备将在原有的工业、农业基础设施之上，发挥越来越重要的作用。

3.1 “端”安全向“云网”安全转变

快速发展的互联网技术在提高生产、生活效率的同时也为黑客攻击提供了可乘之机。“互联网+”时代，随着大数据以及云计算应用的快速普及，技术边界越来越模糊，安全环境越来越复杂，除了系统、应用程序漏洞之外，网络攻击的方法和来源越来越多样。物联网、工控系统、智能摄像头、家用无线路由器、智能家居设备等不断被破解，物联网、虚拟化系统、云计算平台成为不法分子的潜在攻击目标，大量的物联网设备被黑客控制用以实施拒绝服务攻击^[23]。云网安全将和终端安全一起构成未来的安全体系架构，网络空间安全将逐步从“端”安全向“云网”安全演变。

对于“端”安全，由于终端是网络攻击的源头，所有的攻击都是从攻陷终端开始，因此，对于终端的防护至关重要。杀毒软件可以解决传统桌面操作系统的安全问题，但在万物互联时代显然远远不够。一方面，物联网、可穿戴设备、智能汽车等新型移动终端不断涌现，另一方面，操作系统碎片化趋势明显，潜在安全威胁不断提升。对于“云网”安全，由于越来越多的服务和应用延伸到开放的云平台，安全防护也随之向“云网”

转移。传统安全解决方案无法满足“云网”安全中对大数据业务的要求，如实时在线计算要求运算效率，而传统加解密技术则成为性能提升的瓶颈；海量数据的访问控制需要动态的数据权限以满足数据管控需求^[24]；分布式的计算节点易被伪装攻击等。本节将从云平台中数据资源的存储、传输和共享这3个方面展开阐述。

1) 数据资源的存储安全

本地存储数据的加密：当云计算成为新的IT基础设施后，传统的基于加密算法来保证数据的完整性和私密性，并提供加密数据的细粒度访问控制的方法不再适用，这是因为云无法对加密的数据进行操作。隐私同态加密（PHE，privacy homomorphism encryption）则能够解决这一问题，一旦新的加密数据被创建，操作结果便如同纯文本文件一样，云无需知道底层数据就能对加密数据进行操作。

不同存储介质的数据移动：持续以指数形式爆炸性增长的数据集，对大数据存储的灵活性与高效性提出了越来越高的要求。自动存储分层（AST，automated storage tier）则能够将数据安全地迁移到较低的存储层中以削减存储成本，因此可以使大多数随机密集的环境受益^[25]。自动存储分层能够在不同存储之间建立分层，并可根据实际使用情况自动进行数据调度，以迁移到最佳存储层和磁盘阵列（RAID，redundant arrays of independent disks）级。然而，由于自动存储分层并不记录数据在哪里存储，为安全数据存储带来了新的挑战。

2) 数据资源的传输安全技术

访问控制技术：为了确保最敏感的私人数据端到端的传输安全，数据必须基于访问控制策略加密。为了确保认证、协议和分布式实体的公平，必须实现基于加密的安全通信框架。基于属性的加密方案则通过利用公共密码机制来缓解这个问题，相关属性数据加密提供解锁服务。另外，对于未加密的敏感数据，同样需要在一个安全和一致的方式下基于加密安全通信框架进行传递。

端点输入验证：在企业数据的许多大数据应用实例中，要求从许多来源中收集数据。例如，一个安全信息和事件管理系统可能从百万的硬件

和企业网络的应用软件中收集事件日志。在企业数据收集过程中的一个主要挑战是输入验证,即如何确保输入数据的来源是可靠的并从收集的数据中过滤掉恶意输入。由不信任输入源带来的输入验证和过滤问题是一个艰巨的挑战。

3) 数据资源的云端共享安全技术

分布式编程框架中的安全计算: 分布式编程框架利用计算和存储的并行性来处理大量数据。当前有 2 种主要的攻击防护手段: 检查映射机和检查不被信任的映射机中的数据。其中, 不被信任的映射机会返回错误的结果, 因此会产生不正确的结果。这些任务涉及对于大数据集的高度细化计算, 并且十分适用于分布式编程框架。然而, 数据映射程序可能包含有意或无意的泄露, 如一个数据映射程序可能通过分析一个私人的数据发出一个十分独特的值, 破坏用户的隐私。

无关联数据云存储安全: 由 NoSQL 数据库推广的无关联数据存储仍然涉及安全基础设施。NoSQL 数据库的聚类方面对于安全实践方面的顽健性提出了额外挑战。处理大型无结构化数据集的企业在处理庞大数据时可能由传统数据库转化为 NoSQL 数据库中受益。一般情况下, NoSQL 数据库的安全依赖于外部机制。为了减少安全事故, 公司必须检查中间设备的安全策略将条目添加到它的安全引擎, 同时在不影响其操作功能的情况下强化 NoSQL 数据库本身来匹配其对应的关系数据库^[26]。

3.2 “点”防护向“面”防护发展

在新一代技术革命的浪潮下, 伴随着云计算、大数据、自携的设备办公 (BYOD, bring your own device) 以及可穿戴设备的普及应用, 信息资源已经成为基础性社会资源, 融入到社会生活的各个领域, 颠覆性地改变着人类的生活、生产方式。与之伴生的物联网设备、云服务商成为黑客攻击的对象, 网络安全威胁如“细胞分裂”般扩散。在这个全新的时代, 传统的网络安全“点”防护模式如开关式防火墙产品、打补丁式的技术演进已远不能满足新形势对信息安全的要求。

一方面, 云计算的发展使云服务成为网络攻

击的潜在目标, 云计算放大了单点系统、服务、应用程序的脆弱性所带来的影响。传统针对单点机器进行数据获取和控制的攻击方式得到升级, 攻击者通过控制网络中的云节点, 利用云端和用户之间的信任关系, 以云端作为跳板, 可以批量控制用户机器, 从而获取大量的用户数据, 造成“面”毁伤的严重后果。同时, 对云平台中某一特定目标的攻击, 也可能造成大面积的其他业务无法使用。

另一方面, 早期的安全防护, 人们专注于在网络边界上实施诸多安全防护措施, 如在内外网出入口部署防火墙、入侵检测系统等防攻击设备, 旨在把攻击者挡在“墙外”。但在“互联网+”时代, 终端的移动化打破了网络的物理边界, 移动互联网、物联网等打破了传统网络安全架构, 旧有的互联网安全体系在万物互联的“互联网+”时代已经崩溃。当前, 对于“面”防护的迫切需求将对传统的互联网体系造成颠覆性的改变, 传统的安全防护措施需走出“象牙塔”, 创新固有模式, 转型创造“互联网+”式的信息安全解决方案。此外, 在“互联网+”时代, 大数据的广泛应用还带来了高级持续性威胁 (APT, advanced persistent threat) 攻击、基于隐私数据的社会工程学攻击这 2 个方面的隐患。

1) 基于大数据的 APT 攻击, 大数据为防护者制造的明显障碍就是如何从价值低密度性的海量数据中去识别攻击行为, 传统的安全架构是通过单个时间点上单个行为的特征进行识别, 如果和恶意行为库中的特征匹配, 就视为攻击行为, 但在“互联网+”时代, 黑客完全可以通过拆分攻击步骤, 将每一步行为隐藏在海量的正常用户数据行为中, 规避安全系统的检测, 实施隐蔽性更高, 破坏性更大的 APT 攻击^[27]。

2) 基于隐私数据的社会工程学攻击, 黑客能够通过大量渠道获得用户的各类数据, 综合分析用户的隐私, 从而使用社会工程学的方式发起精确攻击, 如根据用户平时网上订餐的习惯, 分析用户的饮食兴趣, 定制专门的挂马邮件, 会大大提高用户单击的概率, 增大攻击成功率, 甚至可以直接根据数据对用户的社交平台、邮箱密码进行猜解, 获得控制权^[28,29]。

4 “互联网+”网络空间安全的对策建议

4.1 坚持自主可控和安全可控

“互联网+”时代万物互联，短板效应突出，接入点、汇聚点、处理点、存储点、应用点等各个方面都存在安全隐患。在当前的国际竞争格局下，做不到自主可控便会处处受制于人。因此，在对策及应用上应当注意以下2个方面。

1) 推进“体系化”安全理念，在国家牵头下筹划全产业链布局，打破既有利益结构，发展产业联盟，构建利益共同体。加大核心设备、核心技术的自主化研发，提高对核心技术的掌控力，同时明确“自主不等于安全”，在技术成熟、落地之前，不盲目、强制推行自主。

2) 加强供应链审查，提高安全产品的来源审查^[7]，从源头上控制网络安全风险隐患。在安全产品入市前，对用户安全进行技术审查、风险评估，确保安全可控。同时对产品是否对国家安全、公共安全造成影响，是否会引起技术垄断等进行评估。

4.2 责任与自由并举的数据管理

“互联网+”时代需要建立全新的数据管理模式，在共享互通的数据技术(DT, data technology)安全思维引导下，更要着重强调数据使用者的责任，对涉及个人数据再利用的行为进行评测。因此，在对策及应用上应该注意以下2个方面。

1) 在数据价值的挖掘过程中要防止触碰隐私的高压线。缩短数据存储周期，降低历史数据遭到损害的风险；有选择性地发布原始数据、不发布或者发布精度较低的敏感数据；使用数据匿名、数据扰乱安全多方计算等对隐私披露风险和精度进行折中，保证对敏感、隐私数据的披露风险在可容忍范围之内；谨慎处理针对性强的数据，如交通监管和定位信息等^[30]。

2) 在数据责任实践中要提供安全可靠的保护措施。对云服务提供商进行定期的安全审计，确保其有足够的安全保护机制；建立完善的访问控制策略，避免非授权用户的非法访问；定期评估数据在传输、存储和处理过程中存在的系统风险，使用数据加密技术保障数据存储安全。

4.3 实时合法的数据全链条监控

挖掘隐藏在海量数据中的经济价值是“互联网+”思维的核心要素。但是，云服务和大数据也给隐蔽攻击提供了可乘之机，因此，在对策及应用上应当注意以下2个方面。

1) 监管者要对数据产生、传输和利用的过程进行监控，保证用户敏感、隐私信息切实得到保护。建立大数据的应用管理框架，引导大数据的收集、使用方向，为用户隐私保护提供法律依据，完成衍生数据的敏感度管理，建立防止用户隐私被无意泄露的准则。这种细粒度的数据全链条监控就要求企业在信息的一致性与用户隐私之间找到平衡，并提供审计记录。

2) 要对全量数据进行收集、监控，实现对于数据未知安全事件的快速侦测和响应。对于终端、主机、应用、网络设备、安全设备、开放云平台上的数据，进行统一的存储、分析和呈现。基于数据关联分析发现未知的、潜在的安全威胁，监控未授权访问数据以及云平台中的脆弱部分，做好异常检测以及电子取证。

5 结束语

网络空间安全不仅包括传统信息安全所研究的信息保密性、完整性和可用性，同时还包括构成网络空间基础设施的安全和可信。“互联网+”时代，虚拟和现实的边界越来越模糊，网络攻击的方法和来源越来越多样，信息安全本身也更立体和更宽域。网络空间安全已成为我国维稳、反恐、社会服务与治理之基，面临诸多安全风险与发展机遇，然而，我国从“网络大国”向“网络强国”转变的道路依然异常艰巨。当前我国核心信息技术受制于人，无法确保网络基础设施和重要信息系统完全自主安全可控，国家网络空间的安全威胁日趋凸显。“互联网+”时代更要坚持自主可控和安全可控，提高核心技术的掌控力，强调责任与自由并举的数据管控。唯此才能当前的国际竞争格局下避免受制于人，立于不败之地。

参考文献：

- [1] SCHÖNWÄLDER J, FOUQUET M, RODOSEK G D, et al. Future Internet = content + services + management[J]. IEEE Communica-

- tions Magazine, 2009, 47(7):27-33.
- [2] 国务院. 国务院关于积极推进“互联网+”行动的指导意见[J]. 中华人民共和国国务院公报, 2015(20): 20-22.
- State Council of the People's Republic of China. Opinions of the State Council on actively promoting the "Internet +" action[J]. Bulletin of the State Council of the People's Republic of China, 2015(20): 20-22.
- [3] 工业和信息化部. 工业和信息化部关于印发贯彻落实《国务院关于积极推进“互联网+”行动的指导意见》行动计划(2015-2018年)的通知[Z].
- Ministry of Industry and Information Technology. Notice on the implementation of the action plan of the State Council on actively promoting the guidance of the "Internet +" action (2015-2018)[Z].
- [4] 王兴伟, 李婕, 谭振华, 等. 面向“互联网+”的网络技术发展现状与未来趋势[J]. 计算机研究与发展, 2016, 53(4):729-741.
- WANG X W, LI J, TAN Z H, et al. The current situation and future trend of network technology for "Internet+"[J]. Computer Research and Development, 2016, 53(4):729-741.
- [5] 中国互联网络信息中心. 第36次中国互联网络发展状况统计报告[R]. 2015.
- CNNIC. The 36th annual statistics report of China Internet development[R]. 2015.
- [6] 中国新闻网. 中国应以军队为主体整合国家网络空间安全力量[EB/OL]. <http://www.chinanews.com/gn/2015/04-27/7235700.shtml>.
- China News Network. China should use the army as the main body to integrate national cyberspace security forces[EB/OL]. <http://www.chinanews.com/gn/2015/04-27/7235700.shtml>.
- [7] 李风华. 信息技术与网络空间安全发展趋势[J]. 网络与信息安全学报, 2015, 1(1):8-17.
- LI F H. Information technology and network space security development trend[J]. Chinese Journal of Network and Information Security, 2015, 1(1):8-17.
- [8] 方滨兴. 从层次角度看网络空间安全技术的覆盖领域[J]. 网络与信息安全学报, 2015, 1(1):2-7.
- FANG B X. Study on the coverage of cyberspace security technology from the perspective of hierarchy[J]. Chinese Journal of Network and Information Security, 2015, 1(1):2-7.
- [9] 丁禹, 逯志安, 焦建伟. 2014年网络空间安全问题综述与展望[J]. 信息安全与通信保密, 2015(2):16-21.
- DING Y, LU Z A, JIAO J W. Summary and prospect of cyberspace security in 2014[J]. Information Security and Communication Confidentiality, 2015(2):16-21.
- [10] 李翊. 维护国家网络空间主权势在必行[J]. 信息安全与通信保密, 2015(8):27.
- LI N. Maintaining national cyberspace dominance is imperative[J]. Information Security and Communication Confidentiality, 2015(8): 27.
- [11] MENDYK-KRAJEWSKA T, MAZUR Z. Problem of network security threats[C]//The 3rd Conference on Human System Interactions. 2010:436-443.
- [12] 阿里研究院. 互联网+: 从IT到DT[M]. 北京: 机械工业出版社, 2015.
- Alibaba Research Institute. Internet+: from IT to DT[M]. Beijing: Machinery Industry Press, 2015.
- [13] FURDEK M, WOSINSKA L, GOŚCIEŃ R, et al. An overview of security challenges in communication networks[C]//Resilient Networks Design and Modeling. 2016.
- [14] HASHIZUME K, ROSADO D G, FERNÁNDEZ-MEDINA E, et al. An analysis of security issues for cloud computing[J]. Journal of Internet Services and Applications, 2013, 4(1):1-13.
- [15] 国家计算机网络应急技术处理协调中心. 2014年中国互联网络网络安全报告[M]. 北京: 人民邮电出版社, 2015.
- CNCERT/CC. China Internet network security report 2014[M]. Beijing: Posts and Telecommunications Press, 2015.
- [16] DRIAS Z, SERHROUCHNI A, VOGEL O. Analysis of cyber security for industrial control systems[C]//The International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications. 2015.
- [17] 陶耀东, 李宁, 曾广圣. 工业控制系统安全综述[J]. 计算机工程与应用, 2016, 52(13):8-18.
- TAO Y D, LI N, ZENG G S. Safety of industrial control system[J]. Computer Engineering and Applications, 2016, 52(13):8-18.
- [18] 维克托·迈尔-舍恩伯格, 肯尼斯·库克耶. 大数据时代[M]. 杭州: 浙江人民出版社, 2012: 27-60.
- MEYER-SCHOENBERG V, COOKE K. Big data era[M]. Hangzhou: Zhejiang People's Publishing House, 2012: 27-60.
- [19] 苏鹏冲, 马丁, 袁得崧. “互联网+”时代网络安全与执法专业人才培养研究[J]. 中国人民公安大学学报: 自然科学版, 2016(1):79-82.
- SU P C, MA D, YUAN D Y. Research on the training of network security and law enforcement professional talents in Internet plus era[J]. Journal of People's Public Security University of China: Natural Science Edition, 2016(1):79-82.
- [20] 马明阳. 针对社会工程学攻击的防御技术研究[D]. 北京: 北京邮电大学, 2015.
- MA M Y. Research on defense technology for social engineering attack[D]. Beijing: Beijing University of Posts and Telecommunications, 2015.
- [21] ROADS of storage[EB/OL]. http://wenku.it168.com/d_001656415.shtml, 2017.
- [22] 杨帅. 工业4.0与工业互联网: 比较、启示与应对策略[J]. 当代财经, 2015(8):99-107.
- YANG S. Industrial 4.0 and industrial Internet: comparison, revelation and coping strategies[J]. Contemporary Finance and Economics, 2015(8):99-107.
- [23] GAN G, LU Z, JIANG J. Internet of things security analysis[C]//The International Conference on Internet Technology and Applications. 2011:1-4.
- [24] 郑斌. 大数据下的数据安全[EB/OL]. <http://www.doc88.com/p-7095219096470.html>, 2016.
- ZHENG B. Data security under big data[EB/OL]. <http://www.doc88.com/p-7095219096470.html>, 2016.

- [25] 杨洁冰. 自动分层存储技术及其应用[D]. 北京: 北京邮电大学, 2011.
YANG J B. Automatic tiered storage technology and its application[D]. Beijing: Beijing University of Posts and Telecommunications, 2011.
- [26] BANDARI G M, CHANDRA N S, KRISHNA V. Secure cloud storage through public auditing and cryptographic primitives[J]. International Journal of Computer Trends & Technology, 2014, 15(2):36-48.
- [27] YU S, LIU M, DOU W, et al. Networking for big data: a survey[J]. IEEE Communications Surveys & Tutorials, 2016, 99:1.
- [28] WANG J, LUO Y, ZHAO Y, et al. A survey on privacy preserving data mining[C]//The International Workshop on Database Technology & Applications. 2009:111-114.
- [29] WU F, XU L, KUMARI S, et al. A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security[J]. Journal of Ambient Intelligence & Humanized Computing, 2016:1-16.
- [30] 黄刘生, 田苗苗, 黄河. 大数据隐私保护密码技术研究综述[J]. 软件学报, 2015, 26(4):945-959.
HUANG L S, TIAN M M, HUANG H. A survey on big data privacy protection[J]. Journal of Software, 2015, 26(4):945-959.

作者简介:



袁得崙 (1986-), 男, 河北承德人, 博士, 中国人民公安大学讲师, 主要研究方向为无线网络、网络安全、复杂网络、网络犯罪侦查与取证。



王小娟 (1985-), 女, 河北保定人, 博士, 北京邮电大学讲师, 主要研究方向为 SDN、认知无线网络、网络安全。

万建超 (1974-), 男, 湖北武汉人, 普天信息技术有限公司工程师, 主要研究方向为移动通信、网络信息安全、物联网技术。