

信息技术与网络空间安全发展趋势

李风华

(中国科学院信息工程研究所 信息安全国家重点实验室, 北京 100093)

摘要: 首先剖析了互联网、移动互联网、物联网、云计算、大数据等技术的基本特征、相互间差异及其内在关系, 深层次梳理了信息技术和信息服务模式的演化规律, 从宏观上探讨了信息技术螺旋式上升的发展态势和我国后发式赶超的机遇, 并指出了下一代信息技术的革新关键在于能耗。在此基础上, 详细分析了我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, 提出了安全技术的研究应与信息技术的发展同步。最后凝练了我国网络空间安全的发展机遇与对策, 并对网络空间安全的发展趋势进行了展望。

关键词: 信息技术; 网络空间安全; 信息保护; 服务模式

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2015.00002

Development trends of the information technology and cyberspace security

LI Feng-hua

(The State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)

Abstract: The basic characteristics, mutual differences and intrinsic relationships of the internet, mobile internet, internet of things, cloud computing and big data technologies were analyzed, and the evolutions of the information technology and information service mode were deeply studied, the spiraling development trends of information technology and our catching up opportunities were explored, and that the major problem in next generation of information technology was energy consumption was pointed out. Based on the analysis, the security requirements and challenges of the network connections, Industrie 4.0 issues in our cyberspace were analyzed, and that the research on security technology should be synchronized with the development of information technology was presented. Finally, the development opportunities and strategies of our cyberspace security were concluded, and an outlook of the development trends of the cyberspace security was given.

Key words: information technology; cyberspace security; information protection; service mode

1 引言

随着移动通信技术、网络技术、信息技术的

持续快速发展和普及, 使得“通过网络之网络访问系统之系统的信息化发展趋势”更容易实现, 深刻地改变了人们的工作、学习和生活方式, 如

收稿日期: 2015-10-26; 修回日期: 2015-11-28。通信作者: 李风华, lfh@iie.ac.cn

基金项目: 国家自然科学基金资助项目(61170251); 国家高技术研究发展计划(“863”计划)基金资助项目(2015AA016007)

Foundation Items: The National Natural Science Foundation of China(61170251); The National High Technology Research and Development Program of China(863 Program)(2015AA016007)

网上购物、社交网络等。在科技改变生活，网络引领未来的新时代，技术日新月异，移动互联网、云计算、物联网、大数据等新技术对信息产业产生颠覆性、革命性的创新效应，促进爆炸式增长的信息消费，新业态、新商业模式的不断涌现正在重塑着全球电子信息产业发展的新格局，在此过程中信息化和经济全球化相互促进，“互联网+”更推动我国发展分享经济。然而，我国虽然已经成了“网络大国”，但并不是“网络强国”，在互联网和信息技术上，我国目前仍然是“跟跑者”，核心技术将持续受制于人，我国作为“信息技术消费大国”天然地受制于“信息技术生产大国”。

洞察信息技术的演化规律对制定相关发展战略规划和确立研究方向有着深远的影响。例如，20世纪80年代，个人计算机性价比相对较低，苹果和王安个人电脑因坚持个性化的“不兼容”技术发展路线而导致失败，成就了今天微软和Intel公司的霸主地位；但随着信息技术快速发展，移动终端广泛普及，苹果采取版权保护和精品战略，使其短期获得大量应用程序、数字作品支持，再结合良好的个性化用户体验，终于获得重生，再现辉煌成就。由于安全技术伴随于信息技术，如果不能准确把握信息技术的发展脉络，将很难在战略层面做出准确判断，因此必须紧跟不断演进的信息技术，变革与完善国家网络空间安全技术体系及能力建设是关键。

纵观信息技术不断螺旋式上升的演化规律，当前信息技术进入到更新换代时期，处于不同发展阶段的国家又获得同一起跑线的发展机遇。然而，主导变革的国家势必会在技术发展前期通过制定相关技术标准、治理规则等，以图再次获得领先优势，并实现对其他国家的有效约束与控制。面对这一现状，我国应主动迎接技术变革，利用后发优势和广阔市场，以市场换取国际主流标准的平等参与权和决策权。

在从“网络大国”走向“网络强国”发展过程中，网络空间安全是维稳、反恐、社会服务与治理之基，我国网络空间面临诸多安全风险与发展机遇。本文不对某一具体的信息技术演化进行

过多总结，而是着眼于对信息技术与网络空间安全的重大宏观态势进行概括。

2 信息技术与服务模式

2.1 信息技术演进

2.1.1 互联网

互联网自1968年诞生至今，其开放和广泛互联互通促进了以互联网为代表的信息技术日新月异的螺旋式革新，将传统文化与现代科技不断融合，推动了经济全球化、文化多样化、社会信息化的深入发展，并不断拓展人类生活空间。互联网的本质是提供信息广泛传播和共享平台，“互联、互通”是根本，因而公益性、政策宣传、广告类等需要广泛传播的信息，是传播人类文化、弘扬正能量的重要载体，是各国人民交流的通道。

既然互联网是一个公共的平台，敏感信息、隐私信息以及需要付费才能分发的信息，在解决信源与完整性认证以及传输安全的前提下，借助互联网广泛互联互通的信道，可以实现安全可控的信息传播。合理有效地使用互联网，可以大幅度减少专网建设，但是互联网的开放性不可避免地存在安全隐患。现有的互联网治理技术和规则不能有效地抑制网络犯罪、黄色信息传播、个人隐私泄漏和信息假冒等，此外借助互联网的监听、攻击和恐怖主义活动等也已成为全球公害。

正如技术都具有正反两面性，不能因为互联网的治理弱而限制互联网的应用，而应从全球规范治理的角度，与各国共同努力打造人类社会虚拟活动空间的公共传输、信息发布与共享平台。我国将实施“互联网+”行动计划作为国策，更需要充分利用我国市场和互联网用户群，主动地参与国际合作，掌握主动权和话语权。

2.1.2 移动互联网

移动互联网以互联网技术为基础，以智能终端为信息收发的端点设备，解决了互联网随机/随地接入的“最后一公里/一米”问题，并随着以智能手机为代表的智能移动终端价格低、功能全、服务广等特征而广泛普及，将移动通信技术与互联网技术充分融合，形成了移动社

交、移动支付、移动医疗等多种新的业务模式。在移动通信技术发展过程中,2G 技术实现了机卡分离和数字通信;3G 技术手机预装操作系统,可以实现个性化定制服务,移动互联网初步成型;4G 技术集 3G 技术与 WLAN 于一体,带宽大幅度提高,移动向互联网全面进军。移动互联网新服务模型和业务不断涌现,信息的获取和利用已经或者即将达到“信息随心行,交互在指间”的理想境界。

未来 5G (IMT-2020) 技术的发展将互联网、移动互联网、物联网、工控网等融合为泛在网络,国际电信联盟已制定到 2020 年全面部署的技术发展时间表^[1]。未来 5G 技术将以超过 10 Gbit/s 的网络传输速度为用户提供更加优质的服务,支持超高清视觉通信、多媒体交互、移动工业自动化、车辆互联等各种应用需求,已成为公认的解决移动网络支撑的最佳解决方案,同时也是全球移动通信领域的研究热点和技术竞争焦点。然而 D2D 等信息传播方式使得合法技侦、监测、管控等更加困难,同时在面临技术方案彻底革新的更新换代压力,以及用户的海量并发请求、高速流量和实时性等要求时,现有安全防护系统将因性能低而不可用,面临换代式的严峻挑战。

2.1.3 物联网

相对于互联网和移动互联网解决人和人之间信息交互和共享,物联网则旨在解决更大维度的人和物、物和物之间的信息交互和共享。物联网通过端节点实现信息感知以及安全控制,将大量传感器组成自治的网络,其自治网络可以也应该借助互联网架构以及云计算等信息服务基础设施达到广泛信息传播,从而实现对物理世界的动态协同感知。物联网将广泛应用于工业控制、智慧城市、医疗康复、老人看护、智障辅助等人类生活的各个方面,我国“十二五”曾大力推动物联网的相关技术及其产业培育,可预见十年之后,基于物联网技术的产品将铺天盖地,物联网相关技术及其产业也将成为我国新的经济增长点。为此,要在战略规划和技术研发方面未雨绸缪。

但是,无需将物联网看作新的网络,而应

将物联网及其安全技术聚焦于自治网络、端节点与互联网可控接入等方面。物联网按行业或者所有权等划分,物理或者逻辑边界易于集中。相比于物联网端节点数目,其组成的信息感知网络数目大幅减少。在集中的物理或者逻辑边界部署管控/代理设备,解决信息跨安全域传播管控、去隐私化处理,很易于平衡安全与利益冲突。

2.1.4 云计算

云计算以服务为基础,利用资源聚合和虚拟化、应用服务和专业化、按需供给和灵活使用的业务模式,并通过 IaaS、PaaS、SaaS 等服务模式完善泛在网络环境下的信息传播方式,使得“通过网络之网络访问系统之系统的信息化发展趋势”更容易实现。以云计算为代表的信息技术深刻地改变了人们的生产、工作、学习和生活方式,如电子政务、网上购物、社交网络等。

云平台的安全性问题愈来愈严峻,云服务日益成为网络攻击的重点目标;云平台的可信性一直是薄弱点,云平台数据安全的保护方面缺乏足够的重视;云服务商对用户信息的侵犯成为被忽略的角落;云平台的可控性往往是安全管理的死角,云平台的安全审核和管理机制不够健全。云计算技术的研究重点可聚焦于:资源虚拟化与认证授权;数据所有权与管理权分离;匿名、计费、作业的正确性,其实质是责/权/利的平衡;自身的安全与可靠性,第三方证明的可控性与可信性等。

2.1.5 大数据

大数据是互联网及其延伸所带来的无处不在的信息技术应用与信息技术的不断廉价化所产生的“自然现象”,通过对海量数据的“获取/存储/筛选/清洗/标记、集成/综合/描述、分析/建模、推荐”等环节,实现潜在价值的挖掘利用。大数据已成为继物质、能源之后的第三大国家战略资源,广泛应用于众多领域和行业,用于改善民生、促进产业转型、革新科学研究方法论、提高国家治理能力、推动服务模式创新和新型企业创立。信息技术创新、信息化模式变革与产业升级之间的关系如图 1 所示。

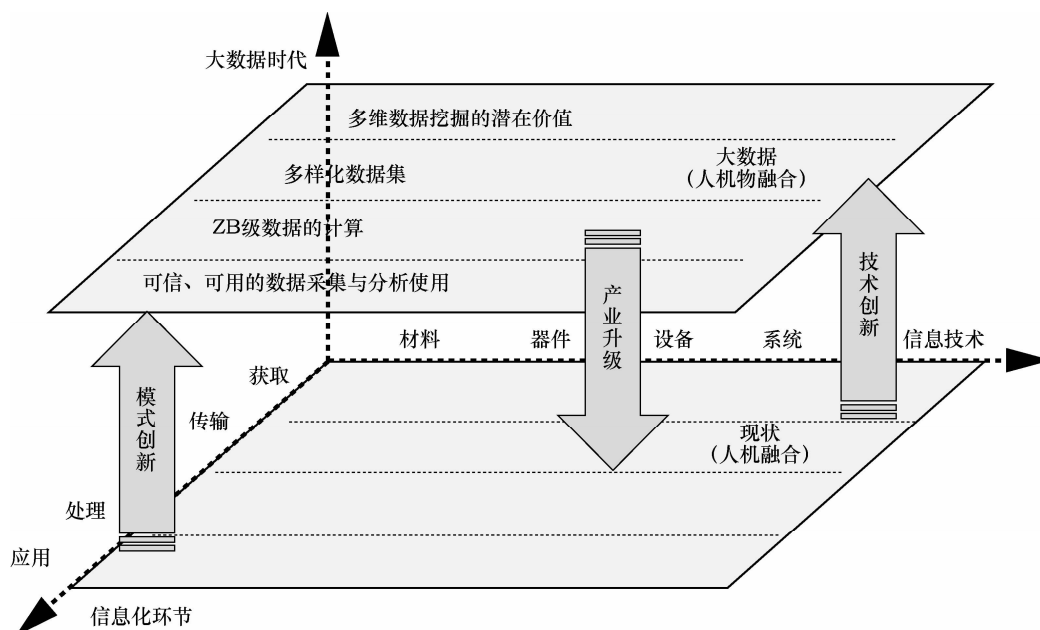


图1 大数据带来的模式创新

大数据具有海量性（volume）、多样性（varity）、时效性（velocity）、真实性（veracity）、潜在价值（value）等显著特征，被广泛应用于社交网络和民生服务中。据 Gartner 预测：2020 年，全球数据总量约为 40 ZB。然而，大数据的主要特征将带来规模、性能、安全和能耗等方面的挑战，其相互关系如图 2 所示。大数据面临大量冗余与局部缺失并存，决策更加困难；海量数据关联分析威胁用户隐私；大数据并发量大，海量用户随机交叉请求等问题。未来亟需在以下方面取得突破：数据来源多样，导致信任关系、数据认证以及数据机密程度复杂，对基于传统密码学的保护方案带来极大挑战；多样的数据来源和个性化的隐私保护需求使得单一隐私保护方案难以奏效，迫切需要多隐私方案融合的保护方法；面向计算设备能耗之外的信息系统和算法设计的能耗优化问题，研究新的系统设计理论和服务架构。

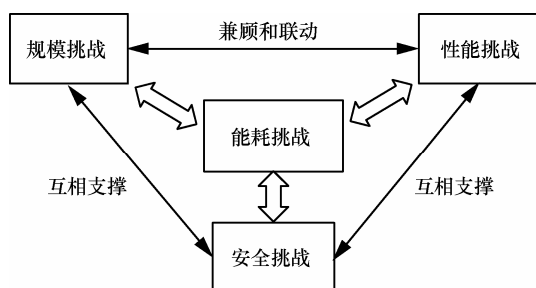


图2 大数据面临的挑战间的关系

2.2 信息传播方式与服务模式

2.2.1 信息传播方式的演化过程

信息传播方式的演进带动信息技术和服务模式的不断革新，如图 3 所示。以 Web 技术为例，Web 1.0 是以浏览器获取信息为特征的信息单向流动阶段；Web 2.0 是以社交网络消息推送为特征的信息双向互动阶段；Web 3.0 是以数据深度挖掘与融合应用为特征的信息深度整合阶段。

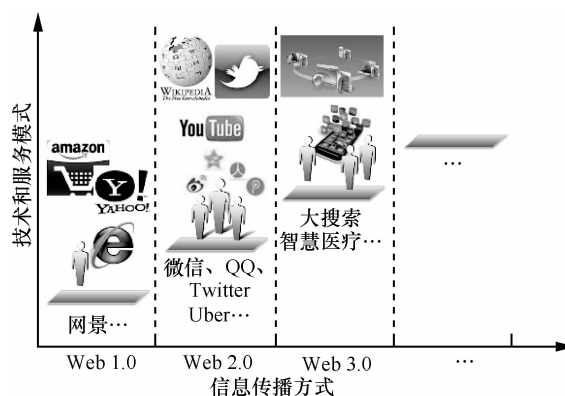


图3 信息传播方式演进带动技术和服务模式革新

回顾信息技术的发展过程，其技术呈现螺旋式上升的演进规律，以信息服务为例，其前后台服务架构可归为 3 个阶段：C/S 架构、B/S 架构和新一代的 C/S 架构，如图 4 所示。在初期的 C/S 架构中，客户端与后台服务器是一一对应关系，后台服务器只是被动地处理客户端的服务请求；

在 B/S 架构中, 客户端与后台服务器是一对多的对应关系, 其实质是基于 Http/Https 协议和 HTML 标识语言实现服务信息变更; 在新一代的 C/S 架构中, 客户端的 APP 与后台服务器虽然仍呈现出——对应关系, 但 APP 和后台应用系统是一个整体, 除了服务信息交换之外, 两者之间还需实现状态同步、信息融合等功能。

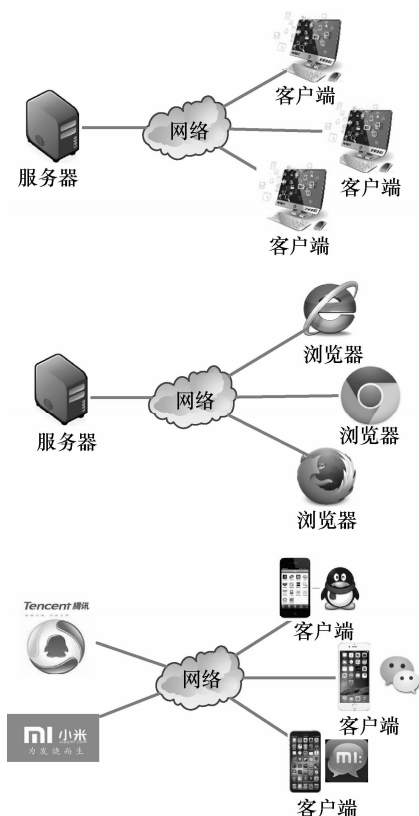


图 4 服务架构的演化规律

2.2.2 信息服务模式的演化趋势

大数据与云计算相互促进, 云计算是大数据的形成基础, 大数据也应以“云服务”方式提供服务。基于互联网技术构建的各种网络与信息系统, 其未来趋势是大规模互联互通, 其模型如图 5 所示。随着信息服务模式的演进, 实际上服务模式已经与骨干网、接入网无关, 信息服务更多地反映出不同部门之间跨行业的多信息系统联动。异构网络间互联互通及信息系统间业务协同促进信息服务模式演进为通过“网络之网络”访问“系统之系统”。在新的信息传播与服务模式下, 服务信息的来源和传输方式对用户透明, 但信息会到处留存, 存在安

全和隐私泄漏隐患。

2.2.3 新型访问控制技术

泛在网络具有异构性、分布式、开放性和移动接入等特征。在泛在网络环境下, 人们期待随时随地访问无处不在的信息资源, 即无论何时何地只要需要就可以通过某种设备访问到所需的信息, 并需要支持移动计算的远程访问、跨域协同远程访问和在线边交互边显现的局部访问。在访问信息资源时, 角色所经由的网络、所处的环境状态和时间状态, 以及欲访问的信息资源及其对象的安全属性等都将对访问权限产生重要影响。归纳起来, 新型访问控制技术需要从 8 个维度加以研究。

- 1) 谁: 泛指任何能够发起资源访问的实体, 可能是人, 也可能是设备, 或者是服务代理。
- 2) 何时: 指访问请求实体进行资源访问时所有与时态相关的信息。
- 3) 使用何设备: 指访问资源时所使用的设备, 例如电脑、智能手机、平板电脑等。
- 4) 从何处接入网络: 指资源访问请求实体在发起访问请求时首次接入网络系统中的空间位置和网络标识, 接入系统通过网络标识唯一区分不同访问。
- 5) 经由何网络: 指信息访问时信息传播的广义网络, 可以指任意相互连通的形成信息传播通道的网络集合, 还包括借助于传统媒介的传播方式, 例如光盘、U 盘、纸张等。
- 6) 访问何资源: 指访问的对象及其相关属性。
- 7) 做何处理: 指对所访问资源的操作, 例如只读、修改、删除、重组、分发等。
- 8) 数据保存多长时间: 指所访问资源在访问者所辖环境中留存的有效期。

当综合考虑上述维度时, 现有的访问控制技术显然难以应对, 亟需提出新的访问控制模型。

2.3 发展趋势

本文探讨的信息技术发展趋势并非针对某一单一技术而言, 对信息技术的总体发展趋势概括如下。

- 1) 万物互联。随着新一代移动通信技术、Web 3.0 等网络技术的发展, 以及移动互联网、物联网、云计算和大数据等应用的普及, 网络已进入“万物互联、智慧互通”的新时代, 同时也标

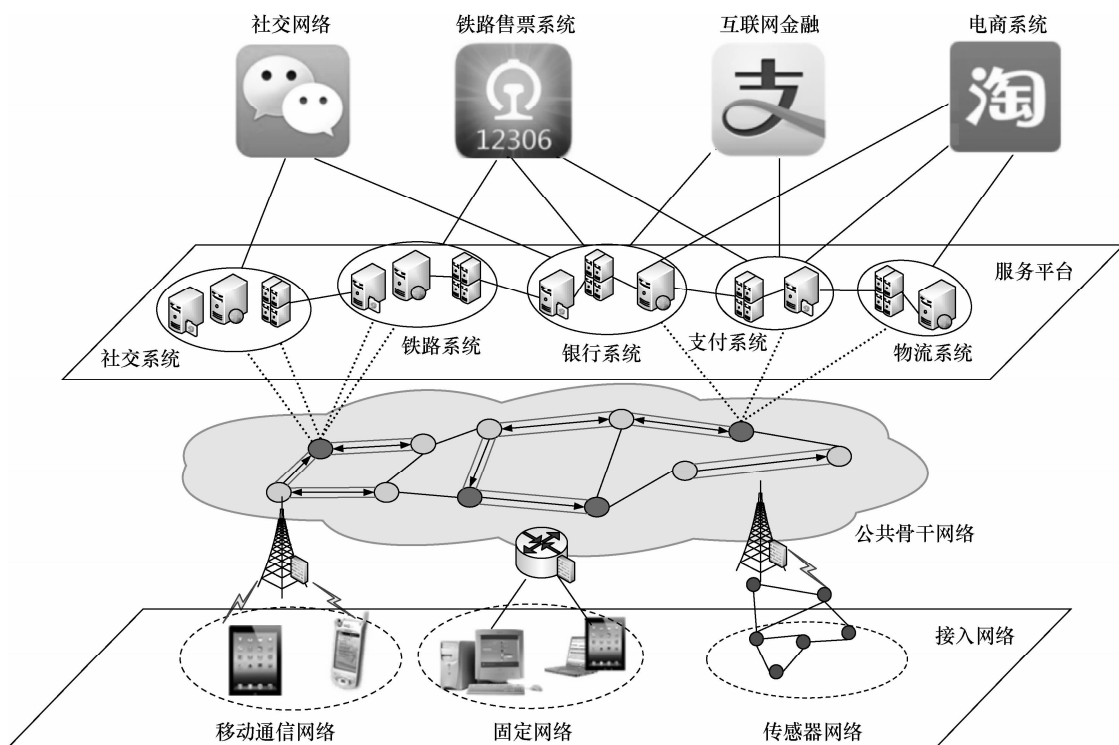


图5 不同信息系统广域互联模型

标志着信息化进入“以数据的深度挖掘与融合应用为特征的智慧化”新阶段，信息的获取和利用即将达到“信息随心行，交互在指间；搜索随意行，推荐在指间”的理想境界。

2) 后发式赶超。社交应用、网络金融、移动支付、移动健康等新服务模式不断涌现，催生了新媒体、微信支付、Uber等众多新业态，同时也推动传统产业的深刻变革。信息技术发展呈现螺旋式上升，某些技术或行业在网络时代被淘汰，而新技术借助互联网和大数据等技术实现跨越式发展，信息技术落后的国家或企业可以实现“后发式赶超”。

3) 利益平衡与绿色节能。不断演进的信息技术将推动网络边界扁平化、分散化、虚拟化、动态化、隐蔽化，网络的普及将加快信息传播与汇聚利用，已有信息技术和系统已远远不能满足信息获取、处理、应用的需求，未来信息技术发展应突出高带宽、低成本、易用性、兼容性、扩展性、安全性、参与方利益平衡，尤其更多关注绿色节能，并持续推动网络诚信服务和敏感数据保护，建立和平利用、服务大众的网络空间。

4) 大众创业、万众创新。信息技术发展源于

创新，其产业成长于符合时代特性动态变迁的用户需求与体验，壮大于不断推陈出新，其应用也昙花一现于新服务模式。信息技术及其应用发展需要并支撑着“大众创业、万众创新”，所有企业和个人均具有同等的起跑线，个人和小企业不一定落后于大公司，具有同等机会原始创新，比如，全球最早带摄像头的手机是夏普 J-SH04，带摄像头影响力最大的手机为诺基亚 7650，以手机摄像头、数字照相机为代表的数字摄影技术打垮了传统胶片的摄影技术及洗印产业，以柯达为代表的企业逐渐衰败，而以苹果为代表的企业重登巅峰。在信息领域，我国更需要像“苹果、微软、Intel、思科”能决定信息技术与产业发展方向的企业和优秀管理团队。

3 网络空间安全面临的挑战

3.1 业务网与工控网互联互通是未来发展趋势

未来各种业务网络互联互通是技术演化的必然结果，大多数场景下网络之间的物理隔离将不复存在，亟需研究高强度逻辑隔离技术才能应对未来广泛互联互通所带来的安全隐患。例如，过去的防护和管控往往分布在不同的设备上，未来

需要实现防护、管控、感知和处置的综合安全防护设备,其模型如图 6 所示。

3.2 工业 4.0 需要新的安全理论与技术保驾护航

工业 4.0 将传统制造业、物流等不同领域通过信息技术有机结合起来,形成“全链条式”的供产销新工业模式和体系,大幅提高生产效率和

降低成本,提升企业竞争力,同时为用户提供更加自主的个性化服务。可以将工业 4.0 的流程分为“需求、设计、原材料采购、加工生产、安装与调试、交付、订单与结算、物流”等环节,如图 7 所示。

在需求分析环节,利用全息投影、可视化等

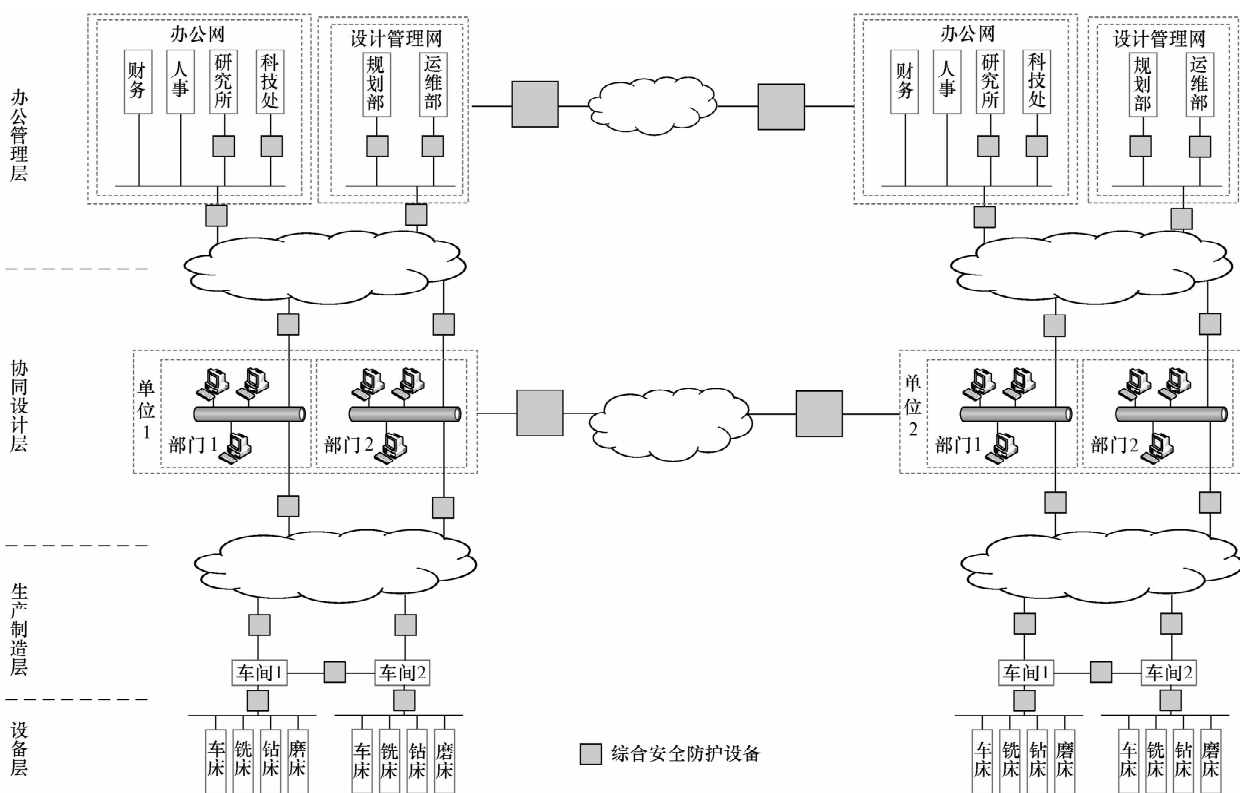


图 6 业务网与工控网互联互通模型

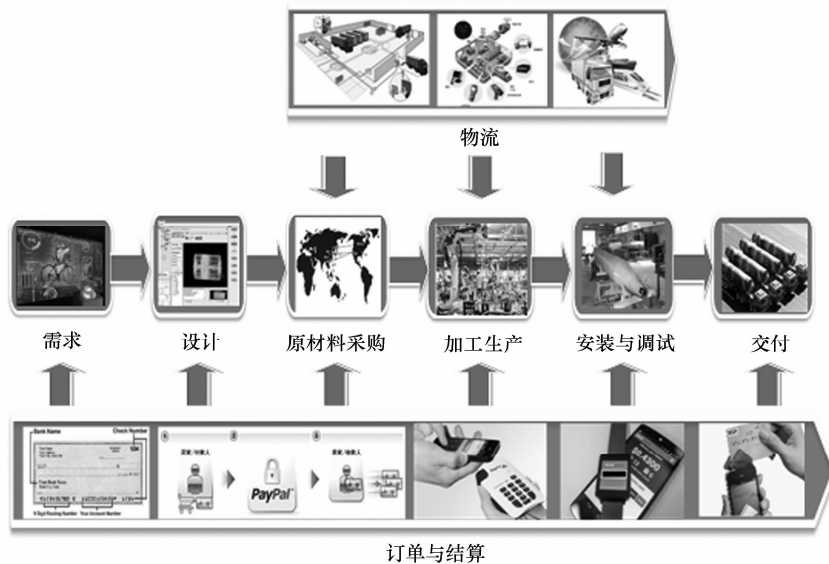


图 7 工业 4.0 贯穿工业生产各个环节

技术远程获取客户个性化需求；在设计环节，利用人机互动、3D 技术根据客户需求完成配件设计；在原材料采购环节，面临材料种类繁多、供应商数量庞大、信息管理系统复杂等问题；在加工生产环节，个性化、小批量生产带来诸多问题；在安装与调试环节，物流和客户时间如何相互配合，实时性和动态性问题更加突出；在交付环节，多参与方带来更多的信任管理问题；在订单与结算环节，需要安全的支付；在物流环节，需要达到高效、实时、全程跟踪的目的等。各环节均需重点关注所面临的商业秘密、知识产权、个人隐私、支付安全等问题，亟需解决面向“全链条式”供产销新工业模式的安全问题。

3.3 安全技术的研究应与信息技术的发展同步

Gartner 将信息技术的发展分为“创新的萌芽期 (technology trigger)、膨胀期望的高峰期 (peak of inflated expectations)、幻灭的低谷期 (trough of disillusionment)、光明的爬升期 (slope of enlightenment) 和生产率的稳定期 (plateau of productivity)” 5 个阶段^[2]。网络空间安全技术具有显著的伴随性，我国当前乃至更长时间内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可控，国家网络空间的安全威胁日趋凸显。

互联网、移动互联网、社交网络等网络信息传播形式多元化和密文化，网络边界扁平化、分散化、虚拟化、动态化、隐蔽化，导致对反恐和维稳支持能力不够并已成为瓶颈，网络边界保护与管理优势不断失去，网络攻击事件频繁发生，对移动通信基础设施的干扰和攻击危害不断加大，个人和企业的敏感数据保护不力，严重威胁了我国网络空间的安全。因此，要从根本上解决安全问题，唯有将安全技术与信息技术同步发展，即“光明的爬升期、生产率的稳定期”面临现在亟需解决的安全问题，“创新的萌芽期、膨胀期望的高峰期”面临未来将要解决的安全问题。例如，鉴于 5G 技术是未来泛在网络的核心支撑技术，其安全问题应同步加以研究，应充分认识对我国网络空间安全将带来的严重威胁与挑战。

3.4 挑战

网络空间逐渐被视为继陆、海、空、天之后

的“第五空间”，成为国际社会关注的焦点和热点。在我国，网络空间安全已成为维稳、反恐、社会服务与治理之基，面临着诸多安全风险与发展机遇，从“网络大国”向“网络强国”转变的道路异常艰巨。基于信息技术的演进，信息技术变革与服务模式创新将带来新的短期难以规避的高安全风险，概括如下。

1) 大数据带来的数据安全和隐私泄露风险。大数据的融合分析使得隐私更容易被挖掘出来；多源信息的获取与基于大数据的分析使得隐私化保护更加困难。

2) 云计算平台带来的窃取用户信息的风险。云服务已成为网络攻击的重点目标，其安全与隐私问题愈来愈严峻，可信性问题一直被诟病，云服务商对用户数据的侵犯易被忽略，并缺乏安全审核和管理机制。

3) 物联网给用户带来的攻击风险。终端安全已成为物联网安全的重点，基于 RFID 技术的产品容易泄露相关隐私信息，物联网控制终端会因传输通道或其本身被劫持而失控，物联网末端设施可能会因遭受物理攻击而失去控制。

4) 社交网络带来的煽动性社会安全风险。社交网络已成为“自媒体”的一种平台，使得任何人都能够发声，可能冲击主流媒体的影响力；社交网络已成为黑客攻击和网络犯罪的新途径。

5) 工业 4.0 或中国制造 2025 带来的多环节安全风险。工业 4.0 在“需求、设计、原材料采购、加工生产、安装与调试、交付、订单与结算、物流”等所有环节都面临安全与隐私保护问题。因此，现有的相互孤立的安全与隐私保护方案难以满足“全链条式”供产销新工业模式的需求，为此工业 4.0 的快速发展将带来巨大的安全风险。

6) 信息技术变革导致防护技术短期滞后的难以规避的高安全风险。信息技术变革将导致信息产品更新换代，虽然绝大多数应用软件能平台兼容、设备互通，但作为后安全加固而研发的安全防护软硬件严重依赖原信息产品的设计原理，信息产品更新换代必将导致防护技术短期滞后，从而造成防护能力下降甚至失效，产生难以规避的高安全风险。

7) “互联网+”促进不同信息系统快速运营，

其安全防护水平参差不齐,从而导致短期内个人隐私根本上不可保护。个人隐私会同时存在于不同信息系统中,客观上这些不同信息系统虽然可以通过“等级保护”来实现不同等级的安全保护,但某一信息系统的泄露将导致其他信息系统的隐私保护的失效,如何确保存有某人隐私信息的所有信息系统都安全,这是一个短时间内难以解决的问题。

4 发展机遇

4.1 机遇

网络空间安全涉及多学科交叉、知识结构和体系宽广,具有显著的伴随性。因此,最终决定网络空间安全的成败在于原始创新,“跟踪式”研究永远被动应付。目前,我国网络空间安全已经迎来5个主要机遇。

1) 工业革新。信息技术发展对世界各国、各行业发展带来了新机遇,在制造领域,德国提出了“工业4.0”,中国提出了“中国制造2025”,利用互联网技术形成“全链条式”供产销新工业模式,将促进信息技术及其安全技术的发展与演进。

2) 大数据促进新业态发展。大数据提供了人类认识自然和社会复杂系统的新思维和新手段,对国家治理、企业经营、个人生活都将产生巨大影响,是促进经济转型增长的新引擎、提升国家综合能力和保障国家安全的新利器。数据是大数据技术产生效益的前提,政府数据开放共享是起步,行业数据有序共享与交易是源泉。智慧城市、医疗康复、老人看护、智障辅助等应用为大数据、云计算和物联网等技术提供了广阔的市场。

3) 技术变革处于同等起跑线。信息技术及产品已处于更新换代的渐进演化进程中,在网络和计算等高端产品领域,我国应充分借助信息技术变革的同等起跑线机遇,加速体系化的原始创新,力争达到同步发展。在终端、低端产品领域及应用中应实现自主开发。

4) 技术变革与能耗。我国是人口大国,在注重经济发展、发展新业态的同时,节能降耗、可持续发展也成为重中之重。互联网和信息技术的应用有利于社会的精细管理和降低能耗。但是,信息产品的应用和信息服务的供给本身也带来了

能耗的增长,年电力增长的1/4左右被新增服务器等信息设备所消耗,在新一轮信息技术变革过程中,信息设备、信息交互及其在线高并发的软件开发平台和应用软件、各类算法并发融合等,都将严重影响能耗。这些理论和产品的创新需求也将带来同等机遇。

5) 安全与隐私保护亟需新理论和新技术保驾护航。互联网、大数据的安全与隐私保护问题是制约其潜在价值最大化的重大障碍,迫切需加大力度研究新一代安全与隐私保护技术,突破大数据的隐私感知、隐私形式化描述与规约机制、数据关联分析、多隐私方案融合、实时去隐私化等关键技术,建设平衡安全、隐私保护和服务质量的应用系统。这些新理论和新技术创新对全球各国都是同等机遇。

4.2 对策

为了更好地把握我国信息技术与网络空间安全发展过程中的机遇,重点从以下4个方面制定对策,为我国的网络空间安全和经济发展保驾护航。

1) 积极实施安全审查,弥补信息技术短板。我国各行业中普遍使用的计算机与互联网硬件设备、操作系统、编译环境和数据库等核心技术受制于人,产业供应链关键环节无法完全自主可控,加上漏洞、后门和恶意行为的检测能力不强,导致我国计算机和互联网系统长期面临被监听、被控制的风险。近年来,已发生了多起供应链关键环节被发现存在后门的事件。在不能自主可控产品方面,需要加强安全审查。重要信息系统所有部署的软硬件都要进行安全审查,其软硬件在运维过程中也应加强人员管理,升级变更需要审计,变更以后还应再次进行安全审查,并形成出现重大安全事件后的法律追责机制。自主可控是国家网络空间安全战略的核心对策,但是自主可控的顺利实施也是有代价的,在初期,自主可控的技术或设备的性能、可靠性与脆弱性等都难以保障,但不会有人为后门,并且经过若干年的持续技术更新和设备不断换代演化,上述问题都会逐步改善,最终逐步形成自主可控的技术和装备体系。

2) 安全标准与信息技术标准同步。过去,我

国重视“以市场换技术”，但网络空间安全领域具有特殊性，应转变为“以市场换国际主流标准”。历史证明，安全技术标准如不能与信息技术标准同步推出，对“信息技术消费大国”的我国将造成大量安全问题无法从根本上加以根除、安全加固成本难以承受、规避安全问题严重滞后等问题。因此，亟待积极参与到产业界真正认同的国际主流产品的标准起草和制定过程中，尤其要积极参与国际信息产品标准的起草、制定与执行，提升我国在国际互联网治理领域的话语权。

3) 加强创新能力建设，加快网络空间安全学科人才培养。加快建设以专业机构、骨干企业为主体的技术支撑体系，建立有效的政产学研用协同创新合作机制。继续完善国家实验室布局，增加数据安全、隐私保护等领域的国家实验室或工程中心建设。依托国家重点实验室、工程中心和企业技术中心，加强网络空间安全知识普及和专业培训，借助国家网络空间安全一级学科的设立，从理论研究和工程实践两方面制定具有不同层次的原始创新人才培养战略和具体实施方案，培育网络空间安全专业服务队伍，加大特殊网络空间安全人才选拔力度，为网络空间安全保障工作提供人才支撑。

5 结束语

纵观信息技术发展的历史，就是已有科幻不断成为现实的展现，未来的科幻将不断地涌现，也会持续不断地成为现实。期待信息技术以最小的自然资源消耗，使人类获得更加丰富多彩的生存空间和生活品质的提升，最终使全人类跨过国界共同繁荣进步。因此，应避免少数信息强国长久地领跑信息技术，而阻碍普惠全人类。

参考文献：

- [1] 万屹. 国际电信联盟确定 5G 正式名称、愿景和时间表等关键内容[EB/OL]. (2015-06-23). http://www.cena.com.cn/2015-06/23/content_281870.htm.
- [2] Gartner《2015 年度新兴技术成熟度曲线报告》指出各企业重点关注的计算创新[EB/OL]. <http://cio.zdnet.com.cn/cio/2015/0828/3060312.shtml>.

作者简介：



李风华（1966-），男，湖北浠水人，博士，中国科学院信息工程研究所副总工、研究员、博士生导师，主要研究方向为网络与系统安全、隐私计算、可信计算。