定义网络空间安全

方滨兴

摘　要：互联网的蓬勃发展给人类生产和生活方式带来了史无前例的变革，成为各国经济发展的新引擎。然而，互联网在带来社会发展新机遇的同时，其安全问题也面临巨大挑战。各国都在积极推进网络空间安全体系建设及关键技术研究，以期保障在这一新型空间中的可持续健康发展。因此，宏观论述了网络空间安全发展态势，并系统性分析了其核心要素及层次化模型。

关键词：网络空间；网络空间安全；互联网治理
中图分类号：TP391
文献标识码：A
doi: 10.11959/j.issn.2096-109x.2018002

Define cyberspace security

FANG Binxing

Abstract: The booming development of the Internet brought unparalleled revolution to production and social life style, and the Internet itself has become the new driving force of economy in almost every country. However, It is embraced that not only development opportunities, but also enormous security challenges in the cyberspace. So as to enhance the healthiness of cyberspace and social form, every state and nation is actively promoting the construction of cyberspace security system and in-depth research of key technologies. A comprehensive view of cyberspace security development status was provided in the globe and in major areas, with systematic analysis on its core elements as well as the hierarchical model.

Key words: cyberspace, network security, Internet governance

1　引言

随着计算机技术持续深入渗透到经济、文化、科研、教育和社会生活等各个领域，网络逐渐进入人们的日常生活和社会管理体系，极大地改变了人类生存和社会生产组织模式。

当前世界，全球网民覆盖率已达 50%，截至 2017 年 6 月，中国网民规模达到 7.51 亿，占全球网民总数的五分之一，互联网普及率为 54.3%，超过全球平均水平[1]。互联网的快速普及带来了巨大的资源膨胀，仅中国的云计算市场总额就会以 40%的年复合率增长，到 2020 年将会达到 200 亿美元[2]。这就对传统网络架构和应用模式的安全保障体系建设提出更大挑战。

随着网络技术的快速发展和网络覆盖的快速提高，软件漏洞、黑客入侵、病毒木马、恶意攻击等问题频频爆发，对全球经济发展和各国社会稳定带来极大冲击。卡巴斯基实验室发布《2016 年第三季度 DDoS 威胁报告》指出，在卡巴斯基监测到的所有 DDoS 攻击活动中，中国以 72.62%的占比位列首位最易受攻击的国家。

网络空间安全建设刻不容缓，本文从传统信

收稿日期：2017-11-21；**修回日期**：2017-12-27

息系统入手，分析了网络空间特征及其安全框架，旨在对网络空间安全体系建设以及关键技术研究提供一定参考。

2 网络空间安全定义

2.1 网络空间

何为网络空间？基于不同应用需求及研究领域，网络空间被赋予不同的内涵和外延。抽象地看，网络空间运行体系的组成要素可被分为4种类型：载体、资源、主体和操作。其中，网络空间载体是网络空间的软硬件设施，是提供信息通信的系统层面的集合；网络空间资源是在网络空间中流转的数据内容，包括人类用户及机器用户能够理解、识别和处理的信号状态；网络空间主体是互联网用户，包括传统互联网中的人类用户以及未来物联网中的机器和设备用户；网络空间的操作是对网络资源的创造、存储、改变、使用、传输、展示等活动。

综合以上要素，网络空间可被定义为“构建在信息通信技术基础设施之上的人造空间，用以支撑人们在该空间中开展各类与信息通信技术相关的活动。其中，信息通信技术基础设施包括互联网、各种通信系统与电信网、各种传播系统与广电网、各种计算机系统、各类关键工业设施中的嵌入式处理器和控制器。信息通信技术活动包括人们对信息的创造、保存、改变、传输、使用、展示等操作过程，及其所带来的对政治、经济、文化、社会、军事等方面的影响”。其中，“载体”和“信息”在技术层面反映出“Cyber”的属性，而“用户”和“操作”是在社会层面反映出“Space”的属性，从而形成网络空间——Cyberspace。

2.2 网络空间安全

广义地讲，传统的信息系统安全意味着通过实现一组准确“控制”所获得的特定能力。该“控制”可以是策略、惯例规程、组织结构和软件功能。建立这些控制以确保机构的特定安全目标得以满足。该特定目标表现在对信息系统、信息自身及信息利用中的机密性、可鉴别性、可控性、可用性4个核心安全属性的保护上，即确保信息与信息系统不被非授权所掌握、其信息与操作是可鉴别的信息与系统是可控的、能随时为授权者提供信息及系统服务，具体反映在信息系统的4个层面：物理安全、运行安全、数据安全、内容安全，也就是信息流转的各个协议层环节。

网络空间设备互联互通旨在交换、传输、存储和处理各类信息数据，是信息系统的超集。因此，除了共性的信息保密、网络基础设施等安全建设外，网络空间安全在各种部署模式中具有特定的安全需求，如移动互联网安全、电信网安全、可信计算、云计算安全、大数据安全、物联网安全、广电网安全等。同时也囊括在不同应用场景中衍生的特定安全保障，如在线社交网络、工业控制安全、支付安全等，以及作为全球性泛在系统而涉及的互联网治理问题，包括信息对抗、舆论安全和网络攻防体系建设等。

因此，基于传统信息系统的经典安全架构以及网络应用的多样性模式，从网络空间载体、资源、主体和操作出发，网络空间安全包括网络空间中电磁设备、信息通信系统、运行数据、系统应用中所存在的所有安全问题。既要保护包括互联网、各种电信网与通信系统、各种传播系统与广电网、各种计算机系统、各类关键工业设施中的嵌入式处理器和控制器等在内的信息通信技术系统及其所承载的数据免受攻击；也要防止、应对运用或滥用这些信息通信技术系统而波及政治安全、经济安全、文化安全、社会安全、国防安全等情况的发生。针对上述风险，需要采取法律、管理、技术、自律、教育等综合手段进行应对，确保信息通信技术系统及其所承载数据的机密性、可鉴别性（包括完整性、真实性、不可抵赖性）、可用性、可控性得到保障。

3 网络空间安全态势

近年来，全球网络安全形势愈来愈严峻，针对网络空间四要素（载体、资源、主体和操作）的各类安全事件频发，举例如下。

1) 基础设施频受攻击。网络空间基础设施遭受误操作配置或恶意攻击都可能致使局部甚至大面积网络不可用。早在2009年，美国国土安全部的报告便称，2005年就有4 095起针对美国政府和私营部门的网络攻击，但2008年这一数字已增

长至 72 000 起，这些攻击在近几年更是成倍增加，使关键基础设施和敏感信息保护面临严峻威胁，造成巨大损失。2016 年底，北美发生针对域名服务商 DYN 的 DDoS 攻击，造成包括 Aribnb、Amazon、BBC、CNN 等大量知名网站短时无法访问。2017 年 8 月，由于 Google 不慎操作造成 BGP 路由前缀劫持，导致日本大范围断网约 1 h。

2) 用户隐私保护亟待加强。网络空间存储、传输大量用户身份信息以及敏感数据，极易发生信息的泄露和滥用。据统计，2010 年美国有 810 万人遭受身份盗用或网络欺诈，造成 370 亿美元的损失。2011 年 12 月 21 日，中国最大开发者技术社区 CSDN 的 600 万用户数据被泄露，其中包含极为敏感的用户名和明文密码；2011 年 12 月 22 日，垂直游戏网站多玩网被传泄露 800 万用户数据；2011 年 12 月 25 日，号称“最有影响力华人论坛”的天涯社区 4 000 万用户数据分组被暴露传播；大量知名网站相继被卷入用户数据泄露风波，其中不乏主流大型互联网公司。据统计，2016 年我国网络空间通过不同渠道泄露的个人信息达 65 亿条次，即平均每个人的个人信息至少被泄露了 5 次。

3) 网络数据易遭窃取及篡改。互联网诞生于相对封闭可信的科研、军事应用，对于数据传输和管理并没有完整有效的安全保障，极易被监听、窃取和篡改。用户的通话数据、信息记录、邮件信息都可被监听和收集，且频繁发生于每个网络用户。2013 年斯诺登曝光美国棱镜计划的风波引发了全球性的数据安全恐慌，也将全球性的网络空间治理推到风口浪尖。

4) 应用可信亟待加强。网络应用是用户进入网络空间的入口，但当前层出不穷的网络应用安全保障体系参差不齐，有些应用漏洞极易遭受恶意入侵及伪造攻击。以网络钓鱼为例[3]，据 Trusteer 报告，美国金融机构每周会遭受 16 次网络钓鱼攻击，每年造成 240 万~940 万美元损失。中国反钓鱼网站联盟的报告也显示，当前网络钓鱼情况愈演愈烈，2016 年钓鱼总量高达 10 万例，且不断向移动互联网等新型网络环境蔓延，造成巨大损失。

网络空间安全形势严峻，引发全球重视。早在 2014 年，奥巴马就宣布启动美国《网络安全框架》，部署强化美国网络安全。截至目前，美国共颁布了网络安全相关文件达 40 多件。欧盟也通过了欧洲数据保护改革方案。作为中国亚洲邻国，日本和印度也一直在积极行动。日本 2013 年 6 月出台《网络安全战略》明确提出“网络安全立国”。印度 2013 年 5 月出台《国家网络安全策略（草案）》。我国于 2017 年 6 月 1 日正式颁布了《中华人民共和国网络安全法》，框架性地构建了许多法律制度和要求，重点包括网络信息内容管理制度、网络安全等级保护制度、关键信息基础设施安全保护制度、网络安全审查、个人信息和重要数据保护制度、数据出境安全评估、网络关键设备和网络安全专用产品安全管理制度、网络安全事件应对制度等。

总体来看，当前已有约 38%的国家发布了国家安全战略，43%的国家具有执法和司法系统的能力构建计划，网络空间安全已经成为一个国家安全稳定的重要部分[4]。正所谓“没有网络安全就没有国家安全”，网络安全是一个关系国家安全和主权、社会的稳定、民族文化的继承和发扬的重要问题。其重要性正随着全球信息化步伐的加快而变得越来越显著。

4　网络空间安全框架及关键领域

基于网络空间安全内涵，网络空间安全框架如图 1 所示。

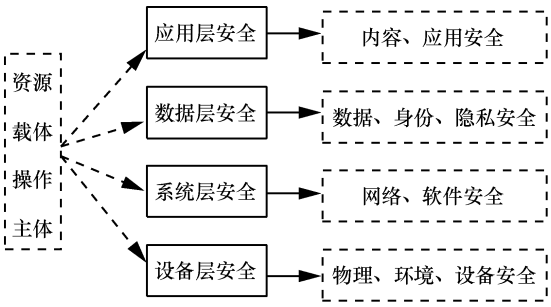

图 1　网络空间安全框架

1) 设备层的安全主要包括网络空间中信息系统设备所需要获得的物理安全、环境安全、设备安全等与物理设备相关的安全保障。

2) 系统层的安全主要包括网络空间中信息系统自身所需要获得的网络安全、计算机安全、

软件安全、操作系统安全、数据库安全等与系统运行相关的安全保障。

3) 数据层的安全主要包括网络空间中在数据处理的同时所涉及的数据安全、身份安全、隐私保护等与信息自身相关的安全保障。

4) 应用层的安全主要包括在信息应用过程中所涉及的内容安全、支付安全、控制安全、物联网安全等与信息系统应用相关联的安全保障。

网络空间的核心要素是数据与信息（即资源）。网络空间的四要素都是通过各类型的数据直接或间接发挥作用，因此，网络空间的四要素对于网络空间安全体系是网状映射，如资源的安全可能涉及设备层面的配置信息管理、系统层面的运行参数管理、数据层面的数据完整性验证以及应用层面的签名加密。操作安全也涉及各个层面的安全问题，包括对硬件设备的安全运行操作、对网络设施系统的安全配置管理、对数据资源的安全存储处理及对应用系统的安全开发维护。主体安全同样也涉及各个层面的安全问题，包括对硬件设备的使用权利、对信息系统的操作权利、对数据的共享权利、对应用的操控权利。

进一步，从网络空间的各应用领域及相关的各要素角度来考虑问题，其安全领域更加广泛，如在云计算环境中存在云环境的可控、安全、可信及可靠保障等问题；在社交网络中存在舆论安全、隐私保护以及平台安全保障等问题[5]。

以基础资源安全为例，传统互联网首先是服务于应用，在设计之初就以“好人假定”的模式将重点都放在应用之上，并假定人们都会遵守规则，没有人会试图破坏互联网，因此，传统互联网对安全可信的需求较弱，基础资源管理以及对应的基础协议也较少采用安全防护体系，从而使其成为当前网络安全的软肋。目前，互联网社群正在积极推进各协议的安全机制扩展及部署推广，从命名、寻址、路由3个层面可见一斑。

DNS是全球互联网的重要基础设施，用于实现域名到主机IP地址的映射解析。作为用户连接各种互联网应用的必经环节，对DNS的劫持相当于改变了互联网的运行规则。但是，DNS在创建之初并未考虑这类潜在的安全问题，如数据来源验证、数据完整性验证以及数据隐私保护[6]。为此，互联网工程任务组（IETF, Internet engineering task force）先后启动了DNS安全扩展协议（DNSSEC, DNS security extensions）[7]、DNS隐私保护协议（DPRIVE, DNS PRIVate exchange）等扩展协议来弥补传统DNS的安全缺陷[8]。

当前互联网所广泛使用的IPv4地址体系，由于缺失安全保障机制，使寻址过程面临严峻的安全风险，因此，在下一代IP地址——IPv6设计之初，就为其嵌入了IP安全（IPsec, Internet protocol security）体系[9]，旨在为IPv6环境下的网络层数据传输提供访问控制、数据源的身份验证、数据完整性检查、机密性保证及抗重播攻击等安全防护，以解决网络层端到端数据传输的安全问题。

BGP是互联网中唯一的域间路由协议，对全球互联网互联互通起着至关重要的作用。然而，BGP本身存在诸多安全问题，其中最为严重的便是路由劫持攻击，轻会导致互联网中流量的重定向，重则会导致整个互联网的瘫痪。面对近年来不断发生的路由劫持攻击及由其导致的网络故障，IETF启动了互联网码号资源公钥基础设施（RPKI, resource public key infrastructure）[10]和边界网关协议安全扩展（BGPsec, BGP security）[11]的相关协议制定。该协议体系通过构建一个公钥证书体系完成对互联网码号资源（包括IP地址前缀和自治域号码）所有权和使用权的验证，路由器以此检验BGP报文的真实性，从而实现BGP路由源认证和路径验证功能，以此防范其路由劫持风险。

由此可见，网络空间基础资源的安全保障体系建设已经成为网络空间安全防护的基石，以此保障互联网基础架构的安全稳定。

5 结束语

网络空间是所有电磁设施与信息系统的集合，是人类生存的泛在信息环境，用户在其中通过各类载体实现信息处理、交互、存储、传递和展示，构造出各种新型的社会形态。而网络空间对人类社会的影响又使其安全属性成为所有属性的核心。

为此，如何保障我国及全球网络空间安全成为进一步广泛普及互联网应用的一个首要前提。

网络空间安全需要从法律保障、行政监管、行业自律、技术支撑、舆论监督、人才培养、普适教育、国防守护、国际共治等维度多管齐下，才能保障我国网络空间健康有序发展，使我国从网络大国向网络强国迈进。

参考文献：

[1] 中国互联网络发展状况统计报告[EB/OL]. http://cnnic.cn/hlwfzyj/ hlwxzbg/hlwtjbg/201708/P020170807351923262153.pdf. Statistical report on the development of China's Internet Network[EB/OL].http://cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/201708/P020170807351923262153.pdf.

[2] BAIN B. Finding the silver lining in China's cloud market[EB/OL]. http://bain.com/publications/articles/finding-the-silver-lining-in-chinas-cloud-market.aspx.

[3] 张茜, 延志伟, 李洪涛, 等. 网络钓鱼欺诈检测技术研究[J]. 网络与信息安全学报, 2017, 3(7): 7-24.
ZHANG X, YAN Z W, LI H T, et al. Research of phishing detection technology[J]. Chinese Journal of Network and Information Security, 2017, 3(7): 7-24.

[4] 李欲晓, 谢永江. 世界各国网络安全战略分析与启示[J]. 网络与信息安全学报, 2016, 2(1): 1-5.
LI Y X, XIE Y J. Analysis and enlightenment on the cybersecurity strategy of various countries in the world[J]. Chinese Journal of Network and Information Security, 2016, 2(1): 1-5.

[5] SANTOS E E. Modeling insider threat types in cyber organizations[C]//IEEE International Symposium on Technologies for Homeland Security (HST). 2017.

[6] HUSTOON G, DAMA J. DNS privacy[J]. The Internet Protocol Journal, 2017, 1(20): 20-30.

[7] ARENDS R, AUSTEIN R, LARSON M, et al. DNS Security Introduction and Requirements[S]. IETF RFC 4033, 2005.

[8] BORTZMEYER S. DNS privacy considerations[S]. IETF RFC 7626, 2015.

[9] KENT S, SEO K. Security architecture for the Internet protocol[S]. IETF RFC 4301, 2005.

[10] LEPINSKI M, KENT S. An infrastructure to support secure Internet routing[S]. IETF RFC 6480, 2012.

[11] LEPINSKI M, SRIRAM K. BGPsec protocol specification[S]. draft-ietf-sidr-bgpsec-protocol-23. 2017.

[作者简介]

方滨兴（1960-），男，江西万年人，博士，中国工程院院士，主要研究方向为网络安全、信息安全、并行处理、互联网技术等。