第 1 章　网络空间安全概论

随着信息技术和网络技术的发展，网络空间（Cyberspace）安全的概念不断变化，其内涵不断深化、外延不断扩大。早期的网络空间安全仅包括物理安全、运行安全、数据安全等几个方面，可称为狭义的网络空间安全。当前，网络空间安全演变为更为广义的概念，其重点包括了信息内容安全、数据安全、技术安全、应用安全、资本安全、渠道安全等多个方面，其中涉及网络安全防护的目标对象，也反映维护网络安全的手段途径。网络空间安全的核心是信息安全。如今，信息技术以及其工业应用迎来了前所未有的繁荣，信息安全问题也变得越来越突出。此外，科学与技术的发展给信息安全带来了新的挑战，许多现存的公钥加密系统变得不再安全，网络空间安全问题越来越引起大众的关注。

1.1　网络空间发展历史

1.1.1　网络空间起源

人类社会在经历了机械化、电气化之后，进入了一个崭新的信息化时代。在信息时代，信息产业成为第一大产业。信息就像水、电、石油一样，与所有行业和所有人都相关，成为一种基础资源，并且正逐步成为信息时代人类社会发展的战略性基础资源，推动着生产和生活方式的深刻变革。信息和信息技术改变着人们的生活和工作方式。离开计算机、网络、电视和手机等电子信息设备，人们将无法正常工作和生活，在信息时代人们生存在物理世界、人类社会和信息空间组成的三维世界中。

网络空间（Cyberspace）一词来源于美国科幻作家 William Gibson 1984 年的短篇科幻小说《神经漫游者》（Neuromancer），指的是由计算机创建的虚拟信息空间。小说中描述了一种人们可以通过神经连接方式进入由计算机虚拟出的感官体验世界，作者将这个世界称为网络空间。不过现今我们所说的网络空间指的是由互相依存的信息基础设施、通信网络和计算机系统构成的全球性空间。在这个广阔的空间里，看不到物理世界，只有许多庞大的信息库和高速流动的各种信息，但人们照样可以在其中交换思想、分享信息、经营事业、指导行动、创办媒体、畅玩游戏、购买商品、提供社会支持、开展政治讨论、甚至发动战争，等等。实际上，互联网现在已经成为网络空间的主体。

2008 年，美国第 54 号总统令对 Cyberspace 进行了定义：Cyberspace 是信息环境中的一个整体域，它由独立且互相依存的信息基础设施和网络组成。包括互联网、电信网、计算机系统、嵌入式处理器和控制器系统。

从信息论角度来看，系统是载体，信息是内涵。网络空间是所有信息系统的集合，是人类生存的信息环境，人在其中与信息相互作用相互影响。因此，网络空间存在更加突出的信息安全问题。其核心内涵仍是信息安全。

当前，一方面是信息技术与产业的空前繁荣，另一方面是危害信息安全的事件不断发生。敌对势力的破坏、黑客攻击、恶意软件侵扰、利用计算机犯罪、隐私泄露等，对信息安全构成了极

大威胁。除此之外，科学技术的进步也对信息安全提出新的挑战。由于量子和 DNA 计算机具有并行性，从而使得许多现有公钥密码（RSA、ElGamal、ECC 等）在量子和 DNA 计算机环境下将不再安全。因此，网络空间安全的形势是严峻的。

对于我国来说，网络空间安全形势的严峻性不仅在于上面这些威胁，更在于我国在 CPU 芯片和操作系统等核心芯片和基础软件方面主要依赖国外产品。这就使我国的网络空间安全失去了自主可控的基础。

1.1.2 网络空间安全特征

网络空间是一个人造领域。这是网络空间与陆、海、空和太空等领域最为明显的区别。如果没有集成电路板、半导体、芯片、光纤及其他通信技术，网络空间就无法承载电磁频谱。即使人类不能将卫星发射到地球轨道，太空依然会存在；即使人类没有掌握浮力的复杂性，海洋依然会存在；同样，即使人类没有发现飞行的原理，天空依然会存在。而如果人类未能发明利用电磁频谱各种属性的技术，网络空间就不会存在。

网络空间可以被不断复制。作为物理域，天空、海洋、太空和陆地都是唯一的，但只有一部分天空、海洋或陆地是重要的，即存在着竞争的那一部分。美国的天空和阿富汗的天空几乎是一样的，唯一的区别是美国的天空不像阿富汗那样存在竞争（或者至少可以说美国天空上的竞争是理论上的而不是实际上的）。然而，在任意时刻都存在着多个网络空间，其中有些网络空间是存在竞争的，有些则不存在，在大多数情况下，网络空间里不存在任何最终结论。就空中力量而言，敌机被摧毁就意味着一切结束了。而在网络空间，判断一个“圣战”网站是否被关闭，要看“圣战”分子有没有在几个小时内更换服务器并且使用不同的域名建立一个新网站。由于成本相对低廉，硬件容易获得，网络可以迅速得到维修和重建。

网络空间由四个层面组成，控制了其中的一个层面并不意味着就控制了其他层面。网络空间包括基础层、物理层、语法层和语义层。基础层包括硬件、电缆、卫星、设备等。物理层包括各种电磁频谱特性（电子、光子、频率等），这些特性使得基础层富有生机和活力。语法层包括信息的格式以及指挥和控制信息系统的规则，这些信息系统构成了网络空间。语义层由用户可以理解的有用信息组成，在本质上语义层是连接网络与认知之间的桥梁。控制了基础层并不意味着就控制了物理层、语法层或语义层。同样，要控制语义层并不需要对基础层进行控制。在实践中，需要控制哪一层，取决于网络攻击的目的，如果想要摧毁或使一个网络瘫痪，那么只需攻击基础层就能产生很好的效果。但如果想要诱导敌方的指挥官做出特定的决策，那么控制基础层就无关紧要了，控制语义层才是至关重要的。

1.2 网络空间安全现状

随着信息技术的迅猛发展和互联网的普及，特别是以微信、Facebook 和微博为代表的新一代即时通信软件的推广和普及应用，使得信息传播的速度、广度和实时性都达到史无前例的地步。互联网应用正在深入到国家与社会的各个方面，同时也伴随着大量的不良信息以及恶意的网络行为，如计算机木马、拒绝服务攻击、垃圾邮件、恐怖主义视频以及泄露的机密信息等。网络不良信息和网络恶意行为不仅会造成重大的经济损失，而且会严重威胁国家的政治、经济、国防、文化等的正常秩序，干扰人民群众的正常生活，甚至会因为恶意散布的网络谣言引发国家与社会动荡。由此可见，网络空间安全在国家主权安全中的地位和作用越来越大。因此在下一代网络空间

中，针对海量数据基于数据挖掘算法和大数据处理技术以及云计算技术进行深度和及时的分析和处理，是任何国家政府和企事业单位必须解决的关键问题。对大数据的获取与智能处理是决定国家和社会发展的一个关键问题，是走出“有数据但无知识”困难局面的一个重要的突破口。网络空间安全面临的安全威胁包括：

（1）大规模分布式拒绝服务攻击

下一代网络 IPv6 只在网络层进行了深层次的改变，传输层和应用层没有改变。因此，基于传输层的分布式拒绝服务攻击还会存在。据相关机构报告：中国大型的电子商务网站和提供搜索引擎服务的网站屡次遭到大规模的拒绝服务攻击（DDOS），例如天猫和京东等网站都曾遭受过此类攻击，给网站的卖家带来巨大的经济损失；百度网站在过去几年也遭受过此类攻击，由此导致众多用户无法使用搜索服务。

（2）众多主机和服务器受控制

中国众多的政府机关、企事业单位以及个人的服务器和主机遭到境外机构的控制。据国家互联网应急中心发布的数据显示：2014 年中国有 650 多万台主机因感染了木马病毒而被境外服务器控制，2 万多个网站被篡改主页。这些被恶意控制的服务器和主机不仅泄露了国家机密和个人隐私，还成为境外机构发动分布式拒绝服务攻击的帮凶。从这些攻击的源头分析，我们发现大部分参与攻击的是这些被控主机，而实际上真正发起攻击的源头在其他国家。

（3）有害信息监控

中国非常重视互联网内容的监管工作，在国家多个关键的互联网接口处都有网络监控设施。但是，随着互联网翻墙软件的轻易获取，只要稍微懂得互联网技术的用户，就可以通过在计算机和手机上安装此类软件，突破网络监控，随意访问一些严禁访问的网站。另外，通过浏览器设置代理服务器的连接方式，能够完成网络攻击源 IP 地址的隐藏。因为在被攻击服务器的日志中总是留下代理服务器的 IP 地址作为网络攻击行为的源 IP 地址，除非各个国家政府之间进行互联网安全的协作，否则这种攻击行为难以完成源头的定位。

（4）骨干网的高速交换机和路由器受控制

在互联网技术方面，美国遥遥领先于其他国家，特别是在骨干网的基础通信设施方面。目前，中国骨干网的大部分通信设备主要由美国思科等公司提供。路由器配有独立的 IP 地址，人为设置的漏洞等会导致路由器控制者远程控制这些路由器。这些控制者也完全可以做到远程切断中国网络的通信服务等。

（5）网络空间海量数据处理面临挑战

网络空间中的大数据分结构化和非结构化两种类型。据互联网相关机构调查发现：在网络海量数据中，约 20%的数据是结构化的，约 80%的数据是非结构化或半结构化的，并且非结构化数据增长率是结构化数据增长率的两倍。对非结构化数据的处理需要大数据处理核心技术，而目前这些技术掌握在少数国家手中。海量数据用现在的检测过滤技术无法做到实时检测，因此很多入侵者可以利用这个漏洞进行浑水摸鱼式的系列攻击。

（6）基础设施面临瘫痪

随着社会重要基础设施的高度信息化，社会的“命脉”和核心控制系统有可能面临损坏和瘫痪。这主要有两点原因：

① 关乎国计民生的海量数据存储在非自主知识产权的数据库服务器中。数据库系统软件主要有微软的 SQL Server、甲骨文的 ORACLE 以及 IBM 的 DB2 以及 SYBACE。目前，中国的主要银行、铁路、民航、社保和其他关乎国计民生的行业都离不开上述数据库系统的支持。由于这些软件都不是开源的，因此我们对其存在的安全漏洞无从知悉。这些数据库系统软件公司可以配合

所在国政府轻易地删除或修改中国的核心数据，而这些数据的丢失则会引起社会的恐慌，从而达到“不战而屈人之兵”的效果。

② 涉及国计民生的大型服务器都是国外品牌。美国的IBM、惠普等公司占据中国大型服务器80%以上的市场，目前涉及的主要行业为金融、交通和电力等。这些服务器具有强大的计算能力，每天都在为政府机关和企事业单位以及个人提供各种各样的金融和电子商务等日常服务。如果这些服务器受到远程控制的话，可能随时被切断服务。这也将导致整个社会的混乱。

（7）根域名服务器受控制

根域名服务器主要用来管理互联网的主目录。所有的根域名服务器均由美国政府授权的互联网域名与号码分配机构——ICANN 统一管理。ICANN 还负责全球互联网根域名服务器、域名体系和 IP 地址等的管理。这些逻辑根服务器可以指挥 Internet Explorer 这样的 Web 浏览器和电子邮件程序控制互联网通信。自互联网被发明以来，世界对根域名服务器的依赖性非常大，美国通过控制根域名服务器而控制了整个互联网。从理论上说，任何形式的标准域名要想被解析，按照技术流程，都必须经过全球“层级式”域名解析体系，才能完成。层级式域名解析体系第 1 层就是根域名服务器，它负责管理世界各国的域名信息；在根域名服务器下面是顶级域名服务器，即相关国家域名管理机构的数据库，如中国的 CNNIC。美国可以通过其控制的根域名服务器，随时切断中国对外的互联网服务。

（8）计算机和智能手机的核心部件受控制

CPU 是计算机和智能手机的核心部件和主要计算单元。在 PC 端，CPU 主要有 Intel 和 AMD 两大品牌；智能手机所使用的 CPU 主要由高通公司提供。如果在这些 CPU 上植入木马，现存的任何检测软件都无法检测到此类硬件木马和病毒，并且它们可根据需要随时引发病毒，造成计算机系统停止工作。操作系统是软件之母，所有其他软件的运行必须建立在操作系统正常工作的基础上。在 PC 端，目前主要有 Windows 操作系统和 MAC 操作系统；手机操作系统主要是 IOS 和 Android。现有的信息安全软件无法检测到存在于 CPU 上的硬件木马，也无法检测到存在于操作系统核心模块的软件木马，但研发这些软硬件的公司可以轻易地远程控制这些木马。

1.3 网络空间安全发展趋势

针对上述网络空间安全的一系列挑战，总结出以下几点发展趋势。

（1）自主研发 CPU

到目前为止，世界上 90%以上的 CPU 芯片都由美国的 Intel、AMD 和高通公司控制。为了摆脱这方面的被动局面，中国现有的研发与生产 CPU 的公司需要进行整合，争取在未来 5 年内设计出 1～2 款具有国际竞争力的 CPU，特别要为军队和党政机关研发自主可控的 CPU。我国应该在未来十年，投入更多的资金加强这方面的研究和设计，以摆脱有机无芯的被动局面。

（2）自主研发操作系统

操作系统是计算机与智能手机的大脑，它能够指挥多个进程协同和并发工作。经过中国计算机科学家多年的努力，在基于开源操作系统 Linux 的基础上，先后研发出红旗、银河麒麟和中国操作系统（COS）等，但目前这些系统在应用的广度和深度方面还有很多欠缺。中国应该制订操作系统研发的中长期计划，加大在操作系统研发方面的投入，特别是在手机操作系统方面。

（3）自主研发可控的服务器和大型数据库系统软件

服务器与国民经济息息相关，关乎国计民生的数据都存放在大型数据库系统当中。因此，中国需要在未来十年，通过市场化等手段，加快国外知名品牌高速服务器的核心技术转让。另外，

还应该加强数据库等系统软件的研发和投入，组织 1～2 个核心科研团队，力争研发出具有市场竞争力的数据库系统。中国应该继续支持以山东浪潮为代表的生产大型服务器的高科技公司，在资金、市场等方面给予倾斜。

（4）使用国产品牌的路由器和交换机组织骨干网

目前，中国骨干网上的路由器和交换器主要由思科公司提供。但是，随着中国国内以中兴通讯、华为为代表的通信设备公司的崛起，中国应下定决心用国产的先进品牌逐渐替换非国产的品牌。为此，中国应该加大对这些产业的投入，在市场上加以引导，让大型国有通信企业在采购设备中加大国产品牌的比重。

（5）加强互联网内容的管理以及控制

目前，以百度、阿里和腾讯为代表的互联网公司在搜索引擎、电子商务和即时通信等新兴网络应用方面走在世界的前列。在带来可观的经济收入的同时也将大量的互联网数据留在了中国的服务器当中，减少了数据流量进入其他国家导致可能泄密的情况发生。因此，中国需要通过扶持互联网新型应用，争取出现更多的大型互联网公司。

（6）大力支持目前中国的网络安全公司

中国网民的技术涵养近几年得到了很大的提高，但是和西方发达国家相比，在网络安全意识方面还有一定的差距。另外，过去许多杀毒软件公司在升级病毒库时需要收取一定的服务费，导致许多用户不安装杀毒软件。上述这些因素都可能导致多达千万的中国主机被境外机构与组织控制。以 360 为代表的新型网络安全公司，提供了一种全新的、免费的网络安全服务，使得中国大部分主机都安装了杀毒和防护软件，这些安全软件能够为用户提供绝大部分的安全服务，避免了更多的主机成为肉鸡。因此，中国应该加大对以 360 为代表的网络安全公司的支持力度。

（7）在国际域名组织中部署和管理根域名服务器

除部分根域名服务器在欧洲与日本外，大部分根域名服务器主要受控于美国商务部。由于美国参众两院的阻拦，美国迟迟未将域名服务器转交给联合国等国际组织。随着信息技术实力的增强，广大发展中国家应该联合起来，要求美国交出根域名服务器的管理权限，将众多域名服务器部署在一些发展中国家。中国应该在此诉求中发挥主导作用。

（8）建立国家级网络空间攻防专业技术队伍

中央网络安全领导小组的成立为网络空间安全提供了组织上的保证，同时也还需要从技术上为网络空间安全提供保障。中国应该整合国内所有研究网络空间安全的企事业单位以及科研院所，从中抽调精英，组建具有中国特色的网络安全部队，加强互联网翻墙软件的破译工作，对其他国家的代理服务器进行有效拦截。

1.4　网络空间安全技术体系

传统的网络信息系统主要由基础硬件、系统软件、网络构件以及上层应用构成，因此一个传统的完整信息安全技术体系如图 1-1 所示。整个信息安全技术体系可以分为四个层次，物理安全技术、系统安全技术、网络安全技术和应用安全技术，基础安全技术和安全管理技术则贯穿这四个层次。

近几年来，随着智能移动终端的普及，人们的生活与网络的关系更为密切。因此，除了四个传统意义上的安全考虑之外，新形势下还有很多新的网络空间安全问题。这里所谓的新形势是指：在当代新技术不断涌现，各领域高度融合的前提下，网络空间安全所展现出来的新局面。主要包括以下几个方面：

图 1-1 信息安全技术体系

（1）智能移动终端安全

近年来，手机等智能移动终端迅速发展，很多安全问题也随之暴露出来，具体包括：

① 恶意软件。智能终端的恶意软件和 PC 端的恶意软件具有同样的危害。从所属层次上来说，终端恶意软件仍然属于应用层和系统层层面，但是由于移动终端的存储能力和计算能力有限，终端恶意软件多以后门、木马的形态存在。所以，终端恶意应用正逐渐向网络层过渡。

② 基于位置的服务。基于位置的服务是指通过运营商或外部设备获取移动终端设备位置信息的服务。如何保证一个位置服务提供商是可信的，不会将用户的位置信息暴露给第三方，是一个值得考虑的问题。基于位置的服务是网络层、应用层与物理设备层相互交叉的产物。

③ 数据销毁。当更换手机或硬盘时，人们会把旧的设备格式化，以清除数据，避免信息泄露。数据销毁则需要物理设备层、应用层与系统层协调工作。

（2）可穿戴设备安全

近几年还有一些其他类型嵌入式系统和可穿戴设备的安全性也引起了人们的重视。常见的可穿戴设备是指那些具有部分计算能力，与智能移动设备相辅使用的便携式设备。这些设备多以手表、鞋子、帽子等形式存在，边缘化的还有一些服装、书包、配饰等。然而，在 2015 年的 HackPWN 安全极客狂欢节上，有白帽子黑客向组委会递交了一个小米手环的漏洞，通过该漏洞，黑客可以完全接管小米手环的控制权。要想解决可穿戴设备的安全问题，应该从物理设备层与系统层进行考虑。

（3）云计算安全

云计算在近几年受到了学术界、产业界和政府等的共同关注。云计算的安全主要包括：

虚拟化安全。虚拟化技术在信息系统中发挥着极其重要的作用，它可以降低信息系统的操作代价、改进硬件资源的利用率和灵活性。但随着虚拟技术的广泛运用，其安全问题越来越受到人们的关注。

云存储安全。云存储可以为用户提供海量的存储能力，而且可以减少成本投入。然而，出于对数据安全性的担忧，仍然有很多用户不愿意使用云存储服务。如何保证用户所存储数据的私密性、完整性等都是云存储安全的范畴。

（4）物联网安全

物联网被视为继计算机、互联网和移动通信之后的第 3 次技术革命和信息产业浪潮，它广阔的行业前景和潜在的巨大市场规模受到了各国政府和研究者的极度重视。物联网涵盖了材料技术、生物技术、计算机技术、电子技术、通信技术，打破了行业之间的界限，实现了通信从人与人向人与物，甚至于物与物之间拓展。然而，也正因为如此，物联网的安全才更加具有挑战性。

（5）量子计算机与传统密码学算法

随着科学的进步与发展，诞生了很多新兴技术，如量子计算机技术。量子计算机的诞生，可能对传统意义上的密码学构成威胁，其特点是计算能力非比寻常，将在现有计算能力上实现指数

增长。目前来说，量子计算机还处于萌芽期，不具备可操作性，而且实验性量子计算机也不足以对传统加密算法发起攻击，但是随着政府资金的大量投入，理论和实践活动的开展，实用性量子计算机或许随时都会诞生。传统密码算法所依赖的大整数分解，椭圆曲线以及离散对数问题在大规模量子计算机面前，会变得轻而易举。

1.4.1　网络层防御技术

网络层防御是保证信息数据在网络传输过程中的坚固堡垒与屏障。防御模式不仅包括传统意义上的虚拟专用网络（VPN）、防火墙等。而且为了确保网络互连互通安全，需要加强对网络互连互通设备的安全设置，如中继器、网桥、路由器等。在新兴技术的支持下，网络层安全如虎添翼。服务器可以通过固化在用户终端的安全模块，对用户的网页浏览行为进行管控，确保用户所浏览的网页没有受到钓鱼网站的劫持冒用。同时，用户之间的会话在逻辑上是加密的，并且会话密钥的分享方式是安全可靠的。

1.4.2　系统层与应用层防御技术

系统层与应用层防御是针对软件而言的，在系统最先开始编译的时候，就可以将一些安防软件、病毒检测软件内嵌到系统中，尤其是在软件开源的大趋势下，我们完全有能力将安防体系作为系统模块的一部分，固化在操作系统结构中。面向的对象，包括一些底层是 Linux 嵌入式系统的可穿戴设备，以及拥有开源优势的安卓手机系统，都可以被这个防御思维有针对性地进行改造。在用户接入系统时，将通过系统对所有用户进行约束与管控：通过在终端上部署防病毒客户端，有效控制病毒的感染与传播，依托大数据云计算平台，进行终端和网络病毒查杀，以保证计算终端配置和软硬件信息不被恶意病毒修改。通过主机对终端硬件如磁盘、外接设备等的安全监控，可以实现移动存储介质的安全接入，控制终端用户对核心系统的读写等。

1.4.3　设备层防御技术

设备层防御体系是从硬件上构建的防御体系，从最底层打牢网络空间的基石。通过改良硬件的基础设施，在硬件最初被设计时就将其安全功能考虑进去，必要时可以在芯片中内嵌一些安全算法，布控一些安全防御设备，包括反窃听、反旁路攻击等。合理规划安排硬件安装过程中的每一个环节，对硬件的操作进行软件或物理上的监控。

1.4.4　人员防御技术

建设人员防御体系的核心是建设合理的人员管理体系。对人员的安防意识进行有针对性的强化，同时加强道德品质建设，对于具有专业能力的计算机从业人员进行正确引导，避免其误入歧途。加强法律的威慑力与约束能力，加强安防软硬件的基础设施建设，加快落实实名制，在实名制的基础上引入生物特征识别机制，提高网络犯罪的犯罪成本。人员的管理穿插在防御体系的每一个环节中，因此非常值得关注。

1.4.5　大数据与云安全

随着互联网、物联网、云计算等技术的快速发展，智能终端、网络社会、数字地球等信息体的普及和建设，全球数据量出现爆炸式增长，仅在 2011 年就达到 1.8 万亿 GB，IDC（Internet Data Center，互联网数据中心）预计，到 2020 年全球数据量将增加 50 倍，毋庸置疑，大数据时代已经到来。

大数据蕴含的巨大价值得到了产业界、学术界和政府部门的高度关注与重视，纷纷开展相关的研究来挖掘大数据的巨大价值。然而在使用大数据挖掘出各种各样的信息，享受大数据带来便利的同时，我们的隐私也不可避免地受到了严重威胁。

“大数据安全”是网络空间安全的难点和重点，也是未来的热点。从不同的角度看大数据面临的威胁与挑战，可分为大数据安全体系、Hadoop 安全架构、数据所有权确立、数据注册、防范 APT 攻击技术等几个方面，同时也包括了以数据为核心和面向数据的信息安全，即面向数据的安全体系结构（DOSA）。

习　　题

1．网络空间的起源？
2．网络空间的安全特性有哪些？
3．网络空间安全的现状？
4．网络空间安全发展的趋势是什么？
5．网络空间安全技术体系有哪些？网络层防御技术讲的主要是什么？

参 考 文 献

[1] Dong Yang,Wen-Feng Qi,Qun-Xiong Zheng. Further results on the distinctness of modulo 2 reductions of primitive sequences over \mathbf{Z}/(2^{32}-1)Z/(2 32-1)[J]. Designs, Codes and Cryptography . 2015 .

[2] 徐金伟. 我国网络空间安全建设历程的回顾与思考[J]. 网络空间安全. 2016(08).

[3] 王伟光. 网络空间安全视角下我国信息安全战略理论构建与实现路径分析[J]. 电子技术与软件工程. 2015(03).