第1章 网络安全问题研究

没有网络安全就没有国家安全，网络安全已经成为国家安全体系的重要组成部分。网络信息安全是一个关系到国家安全和主权、社会稳定、民族文化继承和发扬的重要问题。网络信息的发展改变了人类社会，促进了人类社会的进步，同时也给人们带来了很多的问题。本章针对网络安全的发展进行基础性的研究。

1.1 网络安全基本问题

随着信息科技的迅速发展以及计算机网络应用的普及，计算机网络被应用到国家的政府、军事、文教、金融、商业等诸多领域，可以说网络无处不在。然而随着计算机网络资源共享的进一步加强，信息安全问题也显得日益突出。

党的十八大以来，党中央十分重视信息化和网络安全等重大问题。社会的稳定发展需要网络安全保驾护航，没有网络安全就没有国家安全，就没有经济社会稳定发展，广大人民群众利益也难以得到保障。要树立正确的网络安全观，加强信息基础设施网络安全防护，加强网络安全信息统筹机制、手段、平台建设，加强网络安全事件应急指挥能力建设，积极发展网络安全产业，做到关口前移，防患于未然。

近年来网络安全问题时有发生，大量数据被窃取，并被不法分子利用，进行敲诈勒索，安全问题已经摆在了非常重要的位置上，如果不加以防范，会严重地影响到网络的正常应用。计算机网络安全主要涉及网络信息的安全和网络系统本身的安全。另外，计算机网络本身可能存在某些不完善之处，网络软件也有可能遭受恶意程序的攻击以致整个网络陷于瘫痪状态。同时网络实体还要经受诸如水灾、火灾、地震、电磁辐射等方面的考验。[①]

2011年12月，黑客利用存在的严重隐患以及漏洞问题，通过非法入侵获得用户数据库内的数据，在网上公开了当时最大的开发者技术社区CSDN网站600余万个注册用户的信息，其中包括注册邮箱以及明文密码。该事件导致CSDN网站被迫临时关闭用户登录功能，针对网络上泄露出来的账号数据库进行验证，对没有修改密码的用户密码进行重置；并通过群发邮件提醒用户修改密码，并提醒用户尽快修改其他网站的相同密码。天涯、人人网、当当网、新浪微博等多家网站的用户数据也被相继公开，并以压缩包的形式提

① 周良洪. 公共信息网络安全战略[M]. 武汉：湖北科学技术出版社，2000.

供下载,引起了互联网业界的极大恐慌,是中国互联网史上规模最大的一次用户资料泄露事件。工信部发出要求,各互联网站要高度重视用户信息安全工作,全面开展安全自查。该事件4人被拘留,8人被治安处罚。

从2014年开始,每年9月都开展国家网络安全宣传周活动,即“中国国家网络安全宣传周”,是为了“共建网络安全,共享网络文明”而开展的主题活动,围绕金融、电信、电子政务、电子商务等重点领域和行业网络安全问题,针对社会公众关注的热点问题,举办网络安全体验展等系列主题宣传活动,营造网络安全人人有责、人人参与的良好氛围。

2016年12月,国家互联网信息办公室发布了《国家网络空间安全战略》(以下简称《战略》),它是我国网络安全的战略框架,是建设网络强国的战略设计。在新的技术环境下,实现网络安全已成为国家安全的基本保障。

网络安全是网络时代的一种新的战略思维和部署。传统上国家安全主要指领土、政权、军事三大领域的安全,并不涉及网络安全。但随着网络技术在各行业的普及应用,网络安全领域的国家安全问题日益突出,而传统手段、措施又难以应对这些问题,正是在这样的背景下,网络安全就成为国家安全的重要组成部分。网络安全对国家安全牵一发而动全身,同许多其他方面的安全都有着密切关系。

1.1.1 网络安全定义

网络安全通常是指网络系统的硬件、软件和系统数据受到保护,不因偶然或恶意的原因而受到破坏、更改、泄露,使系统连接可靠正常地运行,网络服务不中断。也就是利用网络管理控制和技术措施,保证在一个网络环境里,数据的保密性、完整性及可使用性受到保护。①

网络安全包括物理安全和逻辑安全两个方面。物理安全指系统设备及相关设施受到物理保护,免于破坏、丢失等。逻辑安全包括信息的完整性、保密性和可用性。

网络安全,通常指计算机网络的安全,实际上也可以指计算机通信网络的安全。计算机通信网络是将若干台具有独立功能的计算机通过通信设备及传输媒体互连起来,在通信软件的支持下,实现计算机间的信息传输与交换的系统。而计算机网络是指以共享资源为目的,利用通信手段把地域上相对分散的若干独立的计算机系统、终端设备和数据设备连接起来,并在协议的控制下进行数据交换的系统。计算机网络的根本目的在于资源共享,通信网络是实现网络资源共享的途径,因此,计算机网络是安全的,相应的计算机通信网络也必须是安全的,应该能为网络用户实现信息交换与资源共享。安全的基本含义是客观上不存在威胁,主观上不存在恐惧,即客体不担心其正常状态受到影响。可以进一步把网络安全定义为,一个网络系统不受任何威胁与侵害,能正常地实现资源共享功能。要使网络能正常地实现资源共享功能,首先要保证网络的硬件、软件能正常运行,然后要保证数据信息交换的安全。从前面的介绍可以看到,由于资源共享的滥用,导致了网络的安全问题。因此网络安全的技术途径就是要实行有限制的共享。②

---

① 蔡立军. 计算机网络安全技术[M]. 2版. 北京 : 中国水利水电出版社,2007.

② 王国才,施荣华. 计算机通信网络安全[M]. 北京: 中国铁道出版社,2016.

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

1.1.2　网络安全基本要素

网络安全的基本要素包括保密性、完整性、可用性、可控性、可审查性5个方面。

1. 保密性

确保信息不泄露给非授权用户、实体或过程，或供其利用的特性，即保证信息不能被非授权访问。

保密性是指网络中的信息不被非授权实体(包括用户和进程等)获取与使用。这些信息不仅包括国家机密，也包括企业和社会团体的商业机密和工作机密，还包括个人信息。人们在应用网络时很自然地要求网络能提供保密性服务，而被保密的信息既包括在网络中传输的信息，也包括存储在计算机系统中的信息。就像电话可以被窃听一样，网络传输信息也可以被窃听，解决的办法就是对传输信息进行加密处理。存储信息的机密性主要通过访问控制来实现，不同用户对不同数据拥有不同的权限。

2. 完整性

所谓完整性是指数据未经授权不能进行改变的特性，即只有得到允许的用户才能修改实体或进程，并且能够判断实体或进程是否已被修改。

数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。数据的完整性是指保证计算机系统上的数据和信息处于一种完整和未受损害的状态，也就是说数据不会因为有意或无意的事件而被改变或丢失。除了数据本身不能被破坏外，数据的完整性还要求数据的来源具有正确性和可信性，也就是说需要首先验证数据是真实可信的，然后再验证数据是否被破坏。影响数据完整性的主要因素是人为的蓄意破坏，也包括设备的故障和自然灾害等因素对数据造成的破坏。

3. 可用性

可用性是指可被授权实体访问并按需求使用的特性，即授权用户根据需要，可随时访问所需信息，攻击者不能占用所有的资源而妨碍授权者的工作。使用访问控制机制阻止非授权用户进入网络，使静态信息可见，动态信息可操作。

可用性是指对信息或资源的期望使用能力，即可授权实体或用户访问并按要求使用信息的特性。简单地说，就是保证信息在需要时能为授权者所用，防止由于主客观因素造成的系统拒绝服务。例如，网络环境下的拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。Internet 蠕虫就是依靠在网络上大量复制并且传播，占用大量CPU处理时间，导致系统越来越慢，直到网络发生崩溃，用户的正常数据请求不能得到处理，这就是一个典型的“拒绝服务”攻击。当然，数据不可用也可能是由软件缺陷造成的，如微软的 Windows 总是有缺陷被发现。[①]

4. 可控性

可控性是指对信息的传播及内容具有控制能力，即对危害国家信息(包括利用加密的

① 黄国平. 计算机网络安全技术与防范措施探讨[J]. 中国管理信息化，2016，19(14)：139-140.

非法通信活动)的监视审计,控制授权范围内的信息的流向及行为方式。使用授权机制,控制信息传播的范围、内容,必要时能恢复密钥,实现对网络资源及信息的可控性。

5. 可审查性

可审查性是指对出现安全问题时提供调查依据和手段。建立有效的安全和责任机制,防止攻击者、破坏者、抵赖者否认其行为。

不可抵赖性也称不可否认性。在信息交换过程中,确信参与方的真实同一性,即所有参与者都不能否认和抵赖曾经完成的操作和承诺。简单地说,就是发送信息方不能否认发送过信息,信息的接收方不能否认接收过信息。利用信息源证据可以防止发信方否认已发送过信息,利用接收证据可以防止接收方事后否认已经接收到信息。数据签名技术是解决不可否认性的重要手段之一。

1.1.3 网络安全的重要性

网络安全和信息化事关经济社会发展大局,要深刻认识加强网络安全和信息化工作的极端重要性,切实增强使命感、责任感和紧迫感,努力走出一条信息化建设与网络安全同步谋划、同步推进、同步发展的新路子。要加快网络安全应急能力建设,加强网络安全技术平台建设,着力提高网络安全应急处置能力。要抓紧构建联防联控的网络安全大格局,严格落实基础运营商、增值服务商、重要信息系统部门的主体责任,加强对重点领域、重点环节的监管,促进我国网络信息产业持续健康发展。要不断创新网络信息安全体制机制,加快网络信息安全人才培养和队伍建设步伐,积极支持高校建立网络安全学科专业和培训机构,为加强网络安全管理提供坚实的人才保障和智力支持。要加强相关技术特别是关键核心技术的攻关力度,积极引进和推广新一代互联网安全技术,有效应对我国网络安全面临的各种挑战。[①]

1.2 国内网络安全研究

网络与我们的生活息息相关,网络安全也涉及国计民生的方方面面。网络信息具有共享性,人们在利用网络信息的同时,网络信息诈骗和各种网络信息安全问题也层出不穷,各种各样的网络犯罪活动也使人们的损失越来越大。

1.2.1 我国网络安全现状

1. 外部环境的影响

作为计算机网络信息系统的重要组成部分,各种硬件设备会受到外部环境变化的影响,自然因素也会对其造成一定的影响,例如温度和湿度的变化以及震动都会对其正常工作造成或多或少的影响。各种自然灾害对机房造成的影响比较难以进行事先防御,我国目前还没有一个有效的措施来应对自然灾害对机房的破坏。受到外部严重的噪声和电磁辐射的影响,会导致网络信息出现错误的情况,这也就导致了网络安全问题。

① 梁蕾. 试论网络信息安全管理[J]. 信息系统工程,2017(09):65.

2. 黑客的入侵

黑客的入侵也是对网络信息安全构成威胁的因素之一。黑客精通计算机及网络技术，他们通常被认为是网络的捣乱分子，他们通过对密码进行破译、发送病毒链接或者邮件、攻击程序漏洞等方式来对计算机网络系统种植木马病毒，从而来对机主进行信息盗取和破坏。黑客对计算机网络的攻击具有主动性，是有目标、有目的性地来对网络用户进行攻击，这在很大程度上会造成用户信息的泄露。所有的网络软件都是人为设计的，哪怕安全性再好，也会存在缺点与漏洞。正因如此，才给了网络黑客可乘之机。网络黑客往往是利用这些缺点和漏洞来侵入计算机网络系统，从而盗取网络信息，这种造成网络信息安全问题的现象就是因为不具备完善的安全措施而形成的。软件都是人为编辑代码而制作出来的，软件公司的工作人员为了操作方便往往留有该软件的管理员身份或者留有“后门”，这些一旦被别有用心者获得会对社会和个人造成难以想象的后果。

3. 网络信息安全管理制度不完善

完善网络信息安全管理制度也是实现维护数据信息安全的有效措施，在当今的信息时代和大数据时代背景下，网络信息安全管理制度存在着多方面的问题。第一，用户自身没有对网络信息重视起来，没有对网络信息系统进行日常的杀毒和维护，这就会导致网络信息系统运行时受到各种不良因素的侵害；第二，在政府、企业、医院和银行以及学校等机构中拥有大量的数据信息，往往会吸引犯罪分子进行网络攻击以及信息盗窃，如果没有一个严格的网络信息管理制度，这就会给这些机构带来巨大的损失和影响；第三，我国政府在治理网络信息安全的过程中，对网络信息技术的创新推动力度不大，在核心技术上没有太多的突破性进展。众所周知，科学技术改变了人们的社会和生活，科学技术的进步会促进全世界各国各项事业的发展，得到了各国政府的高度重视。我国网络信息安全技术近些年来虽然得到了较快的发展和进步，但是政府在对网络信息安全技术管理方面下的功夫还不够，我国应该多培养网络信息安全技术人才，应该加大对网络信息安全技术方面的投入。[①]

4. 计算机病毒的隐患系统

计算机病毒对计算机具有致命的影响，它可以破坏计算机的安全系统，从而使计算机中的信息遭到破坏、泄露。这就很容易给人们的隐私、财产造成严重的损失，甚至会对我国经济造成严重影响。所以对计算机病毒要引起高度重视，它给人们带来的损失有时难以想象。据国家计算机病毒应急处理中心副主任张健介绍，从国家计算机病毒应急处理中心日常监测结果来看，计算机病毒呈现出异常活跃的态势。据 2014 年调查，我国约 73％的计算机用户曾感染病毒，2015 年上半年升至 83％。其中，感染 3 次以上的用户高达 59％，而且病毒的破坏性较大。被病毒破坏全部数据的占 14％，破坏部分数据的占 57％，只要带病毒的计算机在运行过程中满足设计者所预定的条件，计算机病毒便会发作，轻者造成速度变慢、显示异常、丢失文件，重者损坏硬件以致造成系统瘫痪。随着科学技术的不断进步和发展，有更多的手机和平板电脑也接入了网络，因此计算机病毒不仅出现在计算机上，也会对手机或平板电脑进行入侵。现如今各种社交软件的大量出现和广

① 王杨. 试论新安全观下的网络信息安全管理[J]. 网络安全技术与应用，2018(08)：15-16.

泛应用，人们会留存同学、朋友、家人和同事的各种信息在手机里，并且在社交软件里面相互交流和钱财交易，因此就给了很多不法分子可乘之机，他们会对目前流行的微信、微博、QQ 等社交软件进行账号盗窃以及信息窃取从而进行诈骗活动。①

5. 信息污染的威胁

信息污染是指网络信息中夹杂着一些虚假的、不健康的信息，会对人们使用网络信息进行工作和学习时起到消极的影响。当前，我国对网络的治理缺乏一些有效的措施，网络中存在大量的垃圾信息不能够及时删除，造成了一定的信息污染。网络平台具有开放性和共享性，这就决定了人们很难对原创作品进行更好和更有效的保护，从而剽窃和抄袭已经成了普遍的现象，也在网络上形成了大量雷同的网络信息，这无疑给政府处理网络信息增加了难度。网络的发展使全世界的联系更加紧密起来，形成了一张世界网，人们可以在网上自由地发言和评论，可以转载、传播各种文字、图片以及视频等，操作简便、传播速度很快，这就给很多不法分子利用网络来传播淫秽色情和进行违法犯罪活动提供了便利。

6. 公民的网络信息安全意识较差

个人用户在使用网络的过程中，有的安全意识较差。由于人们的工作、生活以及学习都与网络息息相关，大部分人都在网上进行购物和钱物交易，只需简单操作就可以完成资金的流入和流出。但很多使用者并没有重视网络信息安全，他们对网络支付的了解也不多，很多较随意的操作行为就有可能造成信息安全问题。很多人正因为没有重视这些问题，随意地选择在网吧进行网上钱物交易，而大部分的网吧计算机中都有病毒，导致很多人在网吧上网之后出现账号被盗和支付宝钱财损失现象。也有很多的网络用户在上网的过程中被一些网站的各种虚假宣传广告诱惑从而进入其网站下载东西，这些都是非常危险的行为，这会对个人信息造成很大的威胁。

7. 法律保障体系不健全

一个国家如果拥有一套完善并且全面的法律体系，这个国家会有效并且稳定地运行。一个健全的网络信息安全法律保障体系为网络信息安全提供基本的法律保障，并将促进网络信息安全事业得到健康有序的发展。我国在刚进入 21 世纪时开始对网络信息安全进行系统的管理，属于起步较晚的国家，网络信息安全的管理经验尚浅，和西方发达国家相比在管理上还有一定的差距。就网络信息安全法律保障体系而言，我们现有的法律法规以及法律政策都不是很成熟，体系不健全，还存在很多问题。首先，没有形成统一性。在网络信息安全管理实践中，如果各部门不能够相互支持和配合或者遇到问题相互推诿，这样就会在很大的程度上降低了解决问题的效率。目前的网络信息安全的相关法律法规落后于现实的网络信息安全的发展。网络是一个虚拟的世界，现如今的网络环境非常复杂，对网络信息安全的管理有时要比对现实社会的管理有难度得多，也复杂得多。网络信息安全问题也比较复杂，往往会出现刚刚解决了旧的问题就会出现新的问题的现象，所以对网络信息安全进行法律法规建设也具有一定的难度和一定的挑战，很难及时地把网络信息安全问题归纳到法律范畴来加以管理。②

---

① 郭启全. 信息安全等级保护政策培训教程 2016 版[M]. 北京：电子工业出版社，2016.

② 夏冰. 网络安全法和网络安全等级保护 2.0[M]. 北京：电子工业出版社，2017.

1.2.2　我国网络安全对策与管理

网络信息安全是政府应该提供的公共产品，因此保障网络信息安全政府具有不可推卸的责任。进入网络信息时代以来，我国在治理网络信息安全方面取得了不错的成绩。通过有效的治理，我国网络信息安全事业得到了迅速的发展，也大力促进了我国政治、经济、文化和军事等领域的发展。网络信息产业也在当今的经济社会发展中处于重要的位置。但是随着网络信息安全技术的发展，也对如何更好地保障网络信息安全提出了更高的要求。

1. 我国网络信息安全管理发展现状

网络信息技术的发展大力促进了经济的发展，各种新兴产业在网络上诞生，例如淘宝、京东等电子商务产业，网络信息的安全也显得越来越重要。我国较早意识到网络信息安全的重要性，很早就开始了对网络信息安全的保护工作。我国在 20 世纪 80 年代就开始加强网络信息安全技术的研究，并不断地进行推广和应用，有些技术已经跟上了先进国家的发展水平。这些年来我国网络信息安全管理工作主要包括以下几方面，第一，对重要的网络信息的安全进行检查并且加大了检查的范围和力度，对医院、银行、学校等机构的网络信息安全工作也做了着重的检查和更加的关注，同时督促各单位以及各个团体、机构和个人加强对网络信息安全的重视和对网络信息安全问题的防范。第二，积极开展了网络信息安全的法律法规建设，保证网络信息安全能够得到法律的保障。同时，也加大力度对网络信息安全基础知识和基础技术进行普及和教育。经常组织各单位及社会各组织团体和个人进行网络信息安全法律法规的学习，也定期地组织广大人民群众学习网络信息安全基础知识和网络信息安全基础技术，不断地加强网络信息安全宣传力度和完善网络安全的各种管理制度，引起人们对网络信息安全的重视和防范，很大程度上降低了财产的损失和人身安全的损失，也给我国国家安全和公共安全带来了一定的积极作用。第三，重视网络信息技术的创新和发展，开展了网络信息技术体系建设。实施网络信息化建设，不断地加强网络信息技术的自主创新，网络信息安全保障工作得到了进一步落实，加快了我国信息现代化建设。第四，我国网络信息安全问题应急处置能力也在不断地进步，开展了网络信息安全问题应急处置工作，各单位都做出了应急预案，并且各单位进行协调作战，相互之间加强联系并积极配合，共同致力于网络信息安全事业发展，共同研究和制订网络信息安全问题的应急措施。第五，开展了信息安全风险评估工作。我国在信息安全风险评估方面也取得了很多的成就，有效地预防和遏制了很多的网络信息安全问题和突发事件，避免了由于网络信息安全问题造成的重大损失，对我国国家安全和公共安全以及信息化建设带来了很多积极的影响。

2. 我国网络信息安全管理所取得的成就

网络信息安全关系到国家安全和公共安全以及社会的和谐和稳定，缺乏安全的网络信息保障能力，也就无法保障经济的持续稳定发展。面对国内外复杂的网络环境，我们要重视网络信息安全观的树立。与此同时，我国的网络安全保障能力也在不断地进步和提

升。正是网络信息安全保障能力的不断提升，也给我国各项事业都带来了巨大的好处[①]。

近几年，我国的网络信息安全事业得到了显著的进步和提升，网络信息安全法律法规的建设也取得了较大进步，网络信息安全体系相较之前更加完善。我国网络信息安全保障能力在各方面都有了很大的提高，不仅培养了大量的网络信息安全技术人才，网络用户的权益也得到了保障，从而保障了社会的稳定，大力促进了我国网络信息产业的发展。以金融行业为例，网络信息安全屏障的增强也促进了金融行业的发展，人们对网上银行和网上支付安全更加有信心。这些年通过对网络信息安全意识的宣传和教育，网络信息安全得到了广泛的关注和重视，很大程度上增强了我国网络信息安全屏障，使我国迈向网络强国的步伐更进一步，彰显着我国综合国力和国际竞争力的提高，我国信息化、现代化建设得到了进一步发展。人才在网络安全领域扮演着重要的角色，技术人才越多，网络信息安全事业发展就会越快，网络信息安全屏障也就越牢固。

3. 中小型网络安全相关企业是专业领域技术创新的重要主体

要积极发挥多元化市场资本运作机制，引导天使基金、社会资本投资于网络与信息安全创新型企业，鼓励创新企业上市融资，配合财税、投融资、研发补贴等优惠政策，有力支持网络安全领域的大众创业和万众创新。

4. 以兼并收购、战略合作为途径打造龙头企业集群

兼并收购、战略合作是网络安全相关企业快速发展的重要途径，也是当前全球产业界实现资源和技术互补、打造综合竞争实力的普遍选择。阿里巴巴收购安全企业瀚海源，以及启明星辰与腾讯达成战略合作等行动拉开了网络安全领域转型洗牌的序幕，要进一步鼓励网络安全相关企业打破恶性竞争循环，寻求更广范围、更多形式的合作，形成技术优势突出、业务能力综合、能够支撑国家战略的龙头企业。

5. 以产业联盟、产业论坛为平台增进产业协作

全球性产业论坛和峰会对引导安全技术趋势、助力创新企业发展、扩大安全市场需求产生了巨大的影响力。例如，由美国 RSA 公司（被 EMC 兼并）组织的 RSA 大会，2015 年吸引了超过 500 家参展企业、超过 3 万与会人员，设立了 23 个专题论坛，发布上百个专题报告，引发全球热议。借鉴国外经验，鼓励科研机构、高校、网络安全相关企业及单位合作共建技术与产业联盟并组织产业论坛，同时充分发挥行业协会、认证测试和安全咨询机构的号召力和影响力，促进企业间开展技术授权和技术合作，加速形成产业链高度协同的产业生态。

6. 以优厚物质条件为基础吸引、留住、培育网络安全人才

大数据分析、云服务安全、APT 攻击防御等网络安全前沿技术领域创新突破的背后，是高精尖的安全人才和团队。当前，我国已将网络空间安全设置为一级学科，这将逐步改善安全人才总数少、结构失衡、培养机制落后等状况。但顶尖网络安全专家的极度匮乏依然是全球性的挑战，要打造我国的独特吸引力，招募国外权威网络安全专家，留住资深网络安全从业人员，并最终培育出网络安全新生力量，必须创造具有优势的资源、薪酬和福利条件，为网络安全从业者、创新者、建设者提供坚实的物质基础。

---

① 张显龙. 全球视野下的中国信息安全战略[M]. 北京：清华大学出版社，2013.

1.3　国外网络安全研究

信息安全建设需要基于国情出发进行战略统筹和顶层设计，通过规划牵引、政策扶持，将网络安全提升至战略高度，规定国家信息网络化以及维护网络安全等方面的责任，明确国家网络建设的战略目标、指导思想及其他相关原则，为国家网络安全建设构建整体蓝图。由于国情、国家网络发展状况以及国家制度的不同，各国的网络安全战略各有不同，但又有其共性。大多数国家都已经认识到网络安全对于国家安全的重要意义，将网络安全纳入国家安全的组成部分，在国家安全战略中提及或制定单独的专门关于网络安全的国家战略。[①]

1.3.1　国外网络安全现状

（1）西方发达国家高度重视安全产业，资金投入和引导政策持续加码。美国2016财年联邦政府预算中国家安全投入高达6120亿美元，其中以保持技术领先为目标的RDT&E（研究、开发、测试与评估）投入近700亿美元；同时，拟拨款140亿美元用于加强美国网络安全，相较2013年增长35.9%。2015年1月，英国宣布设立网络安全Pre-Accelerator项目，以支持初创型网络安全企业创新成长。2015年4月，美国国土安全部根据《培育有效技术支持反恐》法案，对FireEye公司的多方位虚拟引擎和动态威胁情报平台进行了认证，确立了FireEye在网络安全防御和应急领域的领先地位，有力推动了其产品的部署应用。

（2）威胁情报、大数据、可视化、物联网成为安全热点，网络攻防博弈呈现新格局。从2015年RSA大会话题热度看，Threat（威胁）、Breach（泄露）、Intelligence（情报）、Detection（检测）4个词成为出现频率最高的关键词，基于日志、流量等的大数据安全分析，基于威胁情报的实时监测，基于可视化、机器学习的安全威胁管理，物联网及工业控制系统安全防御成为企业创新的重点方向。同时，网络与信息安全领域的攻防博弈已经逐渐从边界防护的城防模式转变为塔防模式，未知威胁攻击监测与实时阻断、基于数据和情报的对抗、大规模即时服务和应急响应、安全专家资源的在线共享成为攻防博弈的新焦点。[②]

（3）国家战略与互联网发展状况相关。一方面，是否单独制定国家网络安全战略同互联网发展状况有很大联系。一方面，互联网发展越早、越成熟的国家，对于网络安全战略的治理越关注，更倾向于针对网络安全单独制定战略。例如，美国、日本的网络安全战略都是在互联网发展到一定基础上制定的。另一方面互联网发展起步较晚发展较慢的国家，在国家战略中更加侧重于推动互联网建设与发展、网络安全基础设施建设，针对网络安全问题多是出于防止国防信息泄露方面考量。另外，特殊的国家如朝鲜由于其国家政策原因，开放水平低，同其他领域一样，对网络实行严格管控。虽然目前朝鲜在平壤地区

① 赵爽，孟楠，廖璇. 国外网络与信息安全产业发展趋势及启示[J]. 电信网技术，2016(02)：42-44.

② 周丽娜，陈晴. 国外网络信息安全治理体系现状及启示[J]. 社会治理，2020(09)：71-78.

开始构建了新一代的通信网(NGN),并计划陆续推广到全国,但是朝鲜的用户仅可用移动终端设备接收电视信号或进行视频通话,访问光明网实时关注和浏览新闻。

(4) 各国的网络安全战略都体现出一定的政治或外交动机,甚至军事目的。法国在战略中力主向全球推广自己的互联网管理理念,期待带领欧盟摆脱对美国技术的依赖,打破美国互联网企业的垄断地位。法国虽明言发展重点是网络防御,但其信息技术的研发趋势势必是进攻型技术导向。韩国《2008 年国防白皮书》开始将网络安全作为国防战略的一个基本组成部分,《2010 年国防白皮书》将网络攻击作为非传统安全的主要威胁之一。韩国也在军方宪兵部门中建立了计算机应急响应机构,来监控国防信息系统。《俄罗斯联邦信息安全学说》要求向国内外舆论传递国家政策立场,通过信息技术保障国家文化安全。这些都反映出国家在制定网络安全战略中体现出的政治、外交以及军事考量。

1.3.2 国外网络安全对策与管理

(1) 以战略高度和力度布局网络与信息安全产业发展。纵观发达国家近些年颁布实施的网络安全战略、法律、政策及相关项目,国家级网络安全保障范围不断扩大,安全技术产品创新要求逐步落实,网络与信息安全专项资金规模持续高速增长,为网络与信息安全产业的技术创新、市场推广和人才培养等奠定了坚实基础。我国应从战略高度,尽快改变安全产业政策分散、支持力度不足的现状,统筹政策支持资源,明确重点引导方向,加大资金扶持力度,打造符合产业发展规律、发展特点和发展需求的政策环境。

(2) 以“互联网+”、两化融合为契机加快安全技术服务创新。从国际安全技术发展趋势看,由于工业控制系统、物联网等热点领域安全需求定制化,安全威胁监测、识别与应对等安全技术差异化,相应安全技术研发适用仍处于初级阶段。而我国《“互联网+”行动计划》《智能制造 2025》等战略规划已将加强网络与信息安全保障作为重要内容,明确提出要注重网络安全建设,加快体系化安全保障技术研发。因此,要把握发展机遇,加大新兴领域的安全技术服务创新投入,着力突破关键核心技术,力争在新兴领域实现网络与信息安全技术服务实力的弯道超车。[①]

1.4 网络安全对各国的影响

随着人工智能、大数据、5G 等新兴技术的发展,企业面临的威胁也日益增加。相关数据显示,在 2015 至 2025 这十年间,网络攻击导致的全球潜在经济损失可能高达 2940 亿美元。网络风险的升级,让政府、企业和个人都对该风险愈加关注。各国纷纷颁布数据保护方面的法律法规,我国自 2017 年 6 月开始实行《网络安全法》。2019 年 5 月,我国发布了等级保护 2.0 国家标准,增加了个人信息保护、云计算扩展等要求。

国家互联网应急中心发布的《2019 年上半年我国互联网网络安全态势》显示,2019 年上半年,我国互联网网络安全状况具有四大特点:个人信息和重要数据泄露风险严峻;多个高危漏洞曝出给我国网络安全造成严重安全隐患;针对我国重要网站的 DDoS 攻击事

① 陈文芳. 网络环境下计算机信息安全与合理维护方案研究[J]. 科技创新与应用,2016(32):108.