网络时代的美国国家信息安全

● 蔡翠红

20世纪60年代产生于美国的互联网将人类真正带入信息时代，“信息在我们的生活中非常重要而且很容易获得”①。约瑟夫·奈说，权力的性质已经由“高资本含量”变为“高信息含量”②。能够占据领导地位的国家并不是拥有最多资源的国家，而是那些可以控制政治环境并使别的国家“做其所想”的国家。1996年他在《外交》双月刊中更明白地指出，美国在信息方面的优势将使21世纪成为最辉煌的美国世纪：“实际

① Definitions of English Words “Information Age”, available at http://www.antimoon.com/words/information-age-n.htm.

② Joseph Nye, “Soft Power”, *Foreign Policy*, Fall, 1990, p.164

上，是21世纪，而不是20世纪，将会成为美国最辉煌的时期"。[①] 但与此同时，美国也意识到，美国的信息优势必须建立在信息安全的基础上，国家安全战略的主要内容之一就是维护信息安全。为此，从20世纪80年代至今，美国已建立起一整套信息安全防范体系框架。

一、信息安全的实质及威胁

信息化已成为世界主要国家当今及今后整体发展战略最优先的方面之一。一国各个关键性部门、产业和领域正在被网络连成一体，形成信息化国家"关键性基础设施"，它包括政府系统、电力、交通、能源、通讯、航空、金融、传媒和军事等运作、计划、清算、支付及交换的信息系统。这使信息安全从一个产业问题上升为一个事关国家政治、经济、社会、文化、军事等各方面的核心问题。信息技术发展水平的高低和信息安全保障能力的强弱，成为重新界定国家实力、国家安全、国家主权和国际地位的实质依据。

随着信息技术，尤其是因特网的发展，一国的军事、政治、经济和文化的信息很多都不再是秘密，因此，国家安全的脆弱性成为现代国家普遍感到头痛的问题。国家安全的概念不再只是维护国家主权与领土完整，它不仅存在于军事领域，还

① Joseph S. Nye, Jr., and William A. Owens :"America's Information Edge", *Foreign Affairs*, March/April 1996, p.21; p.35., 浮士德是欧洲中世纪传说中人物，为了获得知识和权力，向魔鬼出卖了自己的灵魂。

存在于经济、社会、科技等领域。无论在哪个领域，其安全的核心就是信息技术及其内容——信息。信息安全是信息时代国家安全中最突出、最核心的问题。对于信息安全的认识源自对波斯湾战争以来“信息战”（新的战争形态）[①] 的广泛思考，逐渐形成了关于信息安全的概念。广义的理解指综合性的信息安全，它包括经济、政治、科技、军事、思想文化、社会稳定、生态环境等各个领域。后者是人们通常讨论的信息安全问题的主要内容。[②] 也就是说，信息安全的主要内容包括政治信息安全及经济信息安全、科技信息安全、军事信息安全、文化信息安全、生态信息安全、民族宗教方面的安全。[③]

所谓国家信息安全是指维持国家政治、经济、科技、军事、文化和社会生活等系统不受内外环境威胁、干扰、破坏而正常运行的状态。[④] 冷战时代，由于苏美两大集团政治、军事的对抗，国家信息安全问题从属于政治与军事安全之中而不被特别注意，信息安全只被狭义地理解为各种与政治军事相关的

① 詹森认为，海湾战争主要是一场信息战，是软件和硬件的战争。这场战争是通过计算机技术和通读手段而取胜的，拥有最多的信息并能够得心应手地操纵信息的一方成为胜利者。今后战争争夺的是“非物质价值”——态度和感情。[丹麦] 罗尔夫·詹森：《梦想社会：第五种社会形态》，沈阳：东北财经大学出版社，1999，第44、214页。

② 张春江、倪健民主编：《国家信息安全报告》，人民出版社，2000年，第1－22页。

③ 金小川：“信息社会的重大课题：国家信息安全”，《国际展望》，1997年第17期。

④ 金小川：“信息社会的重大课题：国家信息安全”，《国际展望》，1997年第17期。

情报战与反情报战。冷战格局解体后，世界形势趋于缓和，政治对抗、军事对峙的局面不复存在，国家信息安全从政治安全、军事安全中凸现出来，成为和平时期国家安全内涵中特别重要的组成部分。

信息安全的实质就是要维护信息系统或信息网络中的信息资源免受各种类型的威胁、干扰和破坏，即保证信息的安全性。在美国国家信息基础设施（NII）的最新文献中，明确给出了信息安全的五个属性：可用性、可靠性、完整性、保密性和不可抵赖性。[①] 这五个属性适用于国家信息基础设施的教育、娱乐、医疗、运输、国家安全、电力供给及分配、通信等广泛领域。可用性（Availability）是指信息和通信服务在需要时允许授权人或实体使用。可靠性（Reliability）是指系统在规定条件下和规定时间内，完成规定功能的概率。完整性（Integrity）是指信息不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏的特性。保密性（Confidentiality）是指防止信息泄露给非授权个人或实体，信息只为授权用户使用。不可抵赖性（Non－Repudiation）也称不可否认性，即在一次通信中，参与者的真实同一性。

信息安全的以上属性包括两层含义：一是指运行系统的安全，即信息系统或信息网络的安全问题，这是信息安全的基础；二是指系统信息的安全，即信息系统内信息自身的安全，这是信息安全的落脚点和最终目标。

信息安全不仅是防范窃密活动，不仅是把保密性作为重点

① 张泽忠："因特网的安全问题及对策"，http：//www.1htelecom.com.cn/knowlodge/zyjs/wlaq/aqwt.htm

的安全观念，而是全面的信息安全观念，即是可靠性、可用性、完整性和不可抵赖性与保密性同等重要的安全观念。

信息安全面临的现实威胁主要来自四个方面：

一是内容的攻击，即信息时代的大量反动的、不健康的、无意义的信息对国家的冲击。尤其因特网是一个不需要特权的随意出版场所，为许多恶意的、非恶意的人士提供了这样一种畅所欲言的便利，同时也使信息的可用性受到影响。

二是泄密和内部人员犯罪。运用间谍软件进行网上窃密活动也是因特网面临的一个重要的安全问题。新一代的间谍软件通常隐藏在使用者下载的追踪股票及玩游戏的软件或者其他网络下载软件中，一旦装上这些软件，它会在上网时不被察觉的情况下启动，使用户的资料沿相同的电话线被传播出去。同时，由于大量的网络操作系统软件都在美国开发研制，这也给美国提供了极好的进行间谍活动的机会。

三是计算机病毒。计算机病毒实际上就是专门用来破坏计算机正常工作的特殊程序。它有繁殖力强、潜伏期长、破坏力大的特点。一旦染上病毒，传染极快。而且，许多计算机在不知不觉中就被染上病毒，而不能及时被发现，何时发作更难以知晓。一旦发作，就会使计算机网络系统出现大面积瘫痪，小则导致该机无法正常运转，大则造成严重的经济损失和作战能力的失效。

四是黑客和网络入侵。倚仗他们高超的电脑技术，黑客们可以非法访问对方的内部信息，以达到某种不可告人的目的。他们可以系统地查询某个企业的信息系统，寻找漏洞，然后利用这些漏洞非法谋利，甚至通过截获和篡改数据来非法获取巨额利润。他们在电脑系统中制造假记录或信息，对资料处理系

统下达假指令，让系统出错或死机。而且，他们并不满足于在经济领域内的商业间谍活动，也经常闯入军事信息系统内窃取情报、破坏数据、改变路径、修改指令，甚至以此来控制敌方的武器系统或部队。受威胁较大的领域主要集中于三个方面：一是国家的关键性基础设施，包括国防、执法部门等；二是政府上网工程启动后，开展信息化的有关政府部门；三是经济信息网络，包括银行、债券等。

此外，信息安全还面临着一些其他计算机犯罪的威胁，如预置陷阱、信息肢解、信息污染和信息侵犯等等。预置陷阱就是在信息系统中人为地预设一些“陷阱”，以干扰和破坏计算机系统的正常运行。在对信息安全的各种威胁中，预置陷阱是其中最可怕，也最难以防范的一种威胁。预置陷阱一般可分为硬件陷阱和软件陷阱两种。[①] 所谓信息肢解是指瞄准信息流程中载体与能量两个关键要素对其进行肢解、分割。如在 1991 年的海湾战争中，美军在其“沙漠风暴”行动的作战计划中，就将伊拉克的发电设施列为 12 个优先打击目标群的第二位，给予致命打击，造成伊军 C3I 信息系统（快速、灵敏、高效的指挥、控制、通信和情报系统）的能量来源断绝，使其指挥员对军队的指挥控制陷于一片混乱之中。信息污染是指针对信息的“质”而采取的一种措施。信息污染的程序是：信息截流—信息变质—信息输出，目的是使对方获得变质的信息，影响操作和决策。信息侵犯则是指蓄意对用户的程序和数据进行侵犯，其中对数据的侵犯还包括对联网或非联网的数据库的

① 李劲松：“信息时代如何保障国家安全：信息安全的主要威胁及其对策”，《国家安全通讯》，2001 年第 7 期。

滥用。

二、威胁美国国家信息安全的几个客观因素

1. 处处是前线的信息边疆：美国无法再享受到天然的“安全保障剩余”

守卫边疆一直是保卫国家安全、抵御外敌入侵的主要方式。随着生产力的发展，人类的活动范围不断扩大，国家的疆界也在不断地发生变化。

对陆地疆界和海上疆界的重视产生了两个经典的理论——海权论和地缘政治学，并决定了近两个世纪以来的国际关系。1983年，美国的里根政府提出了“高边疆政府”和星球大战计划，公开声明要取得“高边疆”的控制权，在空间技术上彻底击败苏联。

在信息时代，人们把一个国家或统治集团的信息影响力和传播力所能达到的无形空间称为“国家信息疆域”。它并非以传统的领土、领空、领海划分的，而是以带有某种政治影响力和传播力的信息圈或信息辐射空间划分的。

一般认为“信息边疆”是一种无形的代表国家或统治集团“信息疆域”的不规则界线。它以因特网为代表的形形色色的网络及其终端设备为基本表现形式和载体，人们可以将每一台上网电脑看作是信息边界上的一道关口。因此，从国家信息安全的客观角度上说，我们要把守的信息关口实在太多了，简直数不胜数，不免令人产生防不胜防、“处处是前线”的惊恐。

从信息疆域的概念出发，美国很显然在这块无形领土上捷足先登，在目前是拥有信息疆域最多的国家。信息疆域、网络边界的安全关系到一个民族、一个国家在信息时代的兴亡，世界各国纷纷拓展信息疆域，保卫无形的信息边疆，一场争夺网络信息领域的战争正在激烈地进行。

事实上，信息边疆是一个虚无缥缈的概念。信息网络的发展和信息战的出现正在模糊原有意义上的“界限”，如国内与国外、前方与后方、团体与个人、军人与平民、外交与内政、军事与非军事、局部与全局等，使得判断事件的性质、辨认发动攻击的来源、事先预警和防范变得更为困难。而且目前信息网络系统仍存在着诸多脆弱性，一旦遭受攻击易导致局部性甚至是全局性的系统瘫痪。因此，信息安全成为网络时代国家安全的重点。

按照国际政治周期性规律的创立者、美国著名学者莫德尔斯基的观点：一个国家要成为国际体系中的真正强国，一个不可或缺的条件是享有“安全保障剩余”（Security surplus），即居有岛国或半岛国的地缘位置，使自身享有一种进可攻、退可守的战略自主性。[①] 历史上，奉行“光辉孤立”政策时的英国和近代以前的日本都曾占尽这种优势，从而使国家首先获得了最基本的安全保障。而美国自建国以来依靠优越的地理位置、对技术和威慑政策的高度重视，其国家安全即使在冷战期间也未受到严峻的挑战。但在信息时代，信息攻击可从任何地方发起，可在瞬间穿过任何自然障碍，从而使地理作用降到有史以

① 陈效卫：“防不胜防：信息时代国家安全面临的挑战”，《国际展望》2001年第2期。

来的最低点，也使任何国家包括美国无法再享受到天然的“安全保障剩余”。

2. 信息安全威胁的潜在性、瞬间性和多样化：非国家力量成为美国国家信息安全威胁的主体之一

冷战时期，对国家安全构成的威胁有一个过程且较为透明，如敌对国家针对本国的军事力量部署的动向是可知的（除秘密战之外），可以有时间去寻求应对的办法。而冷战后全球信息网络迅速扩张、国际间相互影响和渗透不断增强，使构成对国家安全与稳定威胁的潜在性因素逐渐增多，且由于这些威胁的多样化、分散性以及有些威胁性因素如思想文化等具有“潜移默化”的特性，人们常常难以察觉或有所疏忽。因此，国家安全面临“瞬间威胁”的可能性大大增加了，并且破坏性后果范围更广、更严重。一旦网络化的“关键性基础设施”出现问题，不仅会造成经济损失，而且会给地区或国家安全带来巨大的、毁灭性的影响。

这一问题的严重性在于，国家所面对的是看不见的敌人。而且，由于网络自身所具有的“无政府主义色彩”使得以往以国家行为为主要特点的攻击、入侵活动，又增加了一种新形式——以个人行为为特点的攻击、入侵活动。他们仅仅依靠民间或个人所拥有技术、设备就能给企业乃至国家带来危害。信息网络技术是文明与知识的结晶，但它显示的“暴力”却使其破坏性大约不亚于“原子弹”。

网络攻击不像导弹袭击或飞机轰炸，可以用雷达和预警卫星等设备实现早期预警，从而能争取到一定的防备时间。网络攻击所需条件简单，具有很大的突然性，对这种攻击难以实现早期预警。匿名是信息技术的特点，在因特网上，不会有人来

验证用户的真实身份，用户在网络上的身份可以同实际身份毫无关联，个人、组织或国家在因特网上难以区别。这一特点给匿名攻击者带来了很大方便。网络的互联性则使攻击者可以无限制地、几乎不可能被追踪地进入计算机系统。这一特点同匿名性结合起来，给防范带来很大的困难。

冷战时期，国家安全面临的威胁比较单一和集中，威胁来源主要是“敌对国家”、核武器以及重大领土纠纷等问题。因此，国家安全问题的性质和特点主要表现为军事安全和政治安全问题。信息网络技术的普及，使战争的发动者不仅仅限于国家，而且企业、宗教团体、恐怖组织、贩毒集团和犯罪团伙均可能拥有发动各种形式战争的手段和能力，一个人只要有极少的金钱和足够的技术，就可以实施对国家的“战略进攻”。因此，战争更具有突发性和不可测性。特别是未来战争向政治、经济、科技、社会领域的扩展，将最终导致“战争”与“非战争”作战行动之间界限模糊不清。

传统的战争都是针对国家和社会发起的有组织的攻击，实施者一般为国家和跨国实体等。但在信息时代，非国家行为者针对个人、公司和国家发起攻击的数量激增。实施者有罪犯、蓄意破坏者以及在网络的青纱帐里隐藏着的不同身世背景、不同价值观念的各种黑客：网上淘金者、网络雇佣军、非法侵入者、好奇的中学生、心怀怨愤的公司雇员等。实施攻击的目的可以是收集情报或进行工业间谍活动；取得经济或技术上的优势；窃取金钱、产品或服务；采取防范行动，如发现可疑的或非法的活动，或进行计算机报复威胁；宣扬某一意识形态或政治观点；实施小恐怖行动；寻求个人刺激等等。专家认为，只要有一套程序、基本的训练和少量的设备，任何个人或小团体

都能发动信息攻击。这样，小莫里斯之辈在因特网上实施“游击战”的机会将大大增加，“电子珍珠港”事件也很有可能发生，被攻击一方将疲于奔命，防不胜防。

美国陆军在一份关于21世纪陆军战斗任务的报告书中，明确把“非国家力量”列为“未来的敌人”。[①] 在它的第二章第二节“未来敌人的特点”的B段“非国家力量”中写道：

“使用赋予它们类似于民族国家的适当能力的现代技术的非国家安全威胁，已经变得越来越明显，正在向传统的民族国家环境挑战。从范围看，这些非国家力量可以分为三类：

（1）次国家性的。次国家性威胁包括政治、种族、宗教、文化和民族冲突，这些冲突从内部对民族国家的规定性和权威提出挑战。

（2）无国家性的。无国家性威胁与他们所属的国家无关。这些实体不是民族国家的一部分，也不想建立这种地位。地区性的有组织犯罪、恐怖主义活动等构成了这类威胁。

（3）超国家性的。超国家性威胁超越了民族国家的边界，在地区间乃至全球范围内活动。它们包括宗教运动、国际犯罪组织，以及协助武器扩散的非正式经济组织。

美国陆军的这份报告已经清楚地说明了非国家力量所构成威胁的实在性及其大致的类别结构。从技术、资金、组织能力等方面看，这种现象几乎是信息社会的必然趋势。非国家力量对美国的信息安全将是巨大的威胁。

---

① Tradoc Pamphlet 525－5：Force XXI Operations，此为美国陆军编写的小册子，在网上公开，却未出版。网址为http：//11204.7.227.67：1100/force 21/tradoc 525－5 toc.html.

3. 网络化程度高的美国更易受到信息的攻击

网络能根据克劳塞维茨的“三维说”把纵横交错的不同层次的社会各部门联接起来，形成错综复杂的社会网络，这种关系越复杂，易遭到攻击的地方就越多。网络化程度高的国家在石油和天然气管道、水、电力、交通、银行、金融、商业和军事等等方面都依赖信息网络控制系统，因而容易遭受信息武器的攻击。如美国在1991年因计算机犯罪，各种公司损失达50余亿美元，到1995年每年被盗的数据价值上升到100亿美元。有鉴于此，美国已采取了许多措施。①

在冷战结束后十年来，美国在传统武器与核力量方面都处于世界领先地位，没有任何国家可以与之相匹敌，而且，其信息优势也是其他国家无法比拟的。然而，具有讽刺意味的是，正是这种绝对的优势同时使美国成为网络攻击中最易受害的国家。② 近年来美国国防部屡遭电脑“黑客”袭击的事实，至少给世人以一点启示，即利用信息技术手段可以使当今世界最强大的美国军事机器顷刻间陷入瘫痪状态。

美国一个战略家在谈到信息战的威胁时说，如果有人在不与美国军方发生对抗的情况下，利用计算机网络攻击美国的通讯、电力、金融和交通，他们将会轻易得手。在掌握了这些武器之后，“非国家实体，甚至个人，都能够挑战超级大国。”③

---

① 陈效卫：“防不胜防：信息时代国家安全面临的挑战”，《国际展望》，2001年第2期。

② James Adams, *Virtual* Defense, *Foreign Affairs*, May/June, 2001.

③ 袁鹏：“评美国未来的安全战略”，《现代国际关系》，1998年第10期，第6页。

大部分在信息革命中处于不利地位并与美为敌的国家，将可能采取“非对称”作战方式，[①] 攻击美国十分普及的经济和军事上日益依赖的节点和网络。此外，一些个人、非国家行为者，如国际犯罪集团、恐怖主义组织、分裂组织、邪教和黑客，都有可能获取信息战武器或雇用信息战专业人员，对美国的计算机网络目标进行攻击。再者，如果某个与美发生利益冲突的“民主国家”对美采取信息攻击，则由于其技术的先进而可能带来更大危害。美国前总统克林顿说过：“这个充满希望的时代也充斥着危险。所有受计算机系统驱动的系统都容易遭到入侵和破坏。重要经济部门或政府机构的计算机一旦受到合力攻击，就会产生灾难性的后果。”[②] 目前，美国的一切关键设施都是建立在计算机和信息基础之上的，一旦这方面遭受破坏，其影响将是大范围甚至是全局性的。“电子珍珠港”事件随时可能爆发。

军队是最早进入网络的部门，信息技术支持各种传感器、武器平台和指挥中心运行，美国以五角大楼为核心的信息基础设施，形成一个庞大而复杂的军事网络系统，其中包括 210 万台计算机、10000 个局域网和 100 个广城网、200 个指挥中心和 16 个大型计算机处理中心。从武器设计、跟踪敌方目标、动员后备力量到军饷发放、后勤供应管理，均依赖于这个信息网络系统。

① “非对称作战”是指对抗双方中实力或科技较落后的一方，避开对方的强点，以攻击敌人最软弱和最难以防备的方面为主要目标而采取的非常规和非传统斗争方法。

② “美国信息安全新动态”，eNet 网站，2001 年 3 月 9 日。

以最为敏感的美国军用计算机和通信系统为例，黑客在对ROME实验室、空军司令部和保密设施的攻击中，竟然控制了实验室的支持系统，与国外互联网接点建立联系，并窃取了战术研究和人工智能研究数据。

三、美国国家信息安全保障框架

随着信息技术的发展及对社会生活影响的日益深化，信息安全的内涵也在不断发展。对信息安全的认识经历了最初通信保密时代（强调信息保密），到20世纪90年代的信息安全时代（强调信息的完整性、可靠性、可用性），再到目前的信息安全保障时代（强调不能被动地保护，还要包括保护—检测—反应—恢复四个环节）。美国的信息安全框架主要包括以下三个层次：安全技术层、安全管理层和政策法规层。政策法规层保护安全管理层和安全技术层，安全管理层保护安全技术层。事实上，任何一个国家的信息安全都可以按照这样一种框架来分析。

1. 安全技术层

美国是网络的源起国，它的信息技术也是世界公认的处于领先水平。在使用技术发展的同时，美国一直致力于同时开发与完善信息安全技术。安全技术层主要包括物理安全、信息加密、数字签名、存取控制、认证鉴别、信息完整、业务填充、路由控制、压缩过滤、防火墙、公证审核、协议标准、电磁防护、媒体保护、故障处理、安全检测、安全评估、应急处理等。这些词语由于与技术相关，非常专业，相对较难理解。从

具体来讲，美国在以下两方面开发与完善信息安全技术：

（1）制定计算机安全评价标准，积极参与开发国际通用安全准则

早在20世纪80年代初，美国就开始着手制定“可信计算机安全评价标准”。1985年，国防部国家计算机安全中心代表国防部制定并出版了“可信计算机安全评价标准 TCSEC (Trusted Computer System Evaluation Criteria)”，又名《桔皮书》，(Orange Book)，它是国际公认的第一个计算机信息系统评估标准。最初，该标准只使用于美国政府和军方的计算机系统，但目前商业领域也开始使用，成为事实上公认的标准。各公司已经开始给它们的产品更新换代打上按《桔皮书》评定的安全级别的标记。TCSEC为计算机系统的安全定义了7个安全级别，最高为A级，最低为D，每一级内又包含一个或多个级别。安全级别按D、C1、C2、B1、B2、B3、A1渐次增强。任何不满足较高级别安全可信性条件的系统都划入D类。①

1987年，美国计算机安全中心（NCSC）为《桔皮书》提出了可依赖网络解释（TNI），通常被称为《红皮书》。1991年，美国国家计算机安全中心又为《桔皮书》提出了可依赖数据库管理系统解释（TDI）。由于20世纪90年代黑客活动开始日益猖獗，1992年12月，美国政府又公布了联邦评价准则(FC)，用以代替20世纪80年代颁布的《桔皮书》。

1993年，美国国防部国防信息系统局又提出在C4I系统

① 唐岚：“美国国家信息安全保障体系简介”，《国际资料信息》2002年第5期。

(Command, Control, Communication, Computer, and Intelligence system) 上采用多级安全 (MLS) 技术与概念。在上述标准的基础上，美国、加拿大和欧洲联合研制信息技术安全评测公共标准，并于 1994 年颁布了 0.9 版，于 1996 年颁布了 1.0 版。①

(2) 重视信息安全技术的发展和更新

保证信息的保密性、可用性和完整性的技术在体系上可分为密码技术、安全控制技术（如访问控制技术、口令控制技术）和安全保护技术（防火墙技术、计算机网络病毒防治技术、信息泄露防护技术）等。

以密码技术为例，由于密码技术是信息安全的基础和关键技术，美国历来十分重视对密码的管理。1996 年，美国总统颁布了关于密码出口条例的行政命令，允许支持密钥托管或密钥恢复、密钥长度大于 56 位的高强度密码出口。1998 年，美国政府宣布允许更高强度的密码出口到限定国家，但事实上却不允许密钥长度超过 56 位的密码出口，除非密码支持密钥托管与密钥恢复。2000 年 10 月，美商务部发布了新的密码出口条例，根据这个条例，任何密钥长度在密码产品或软件，经技术审查后无需许可证就可出口到除 7 个所谓的支持恐怖主义国家外的任何国家或非政府用户。②

再以防火墙技术为例。防火墙技术也是实现信息安全的一种重要手段，主要用来拒绝未经过授权的用户访问，阻止未经

① 网络信息安全状况，http://cn.tech.yahoo.com/020118/142/xi7q.html

② 唐岚："美国国家信息安全保障体系简介"，《国际资料信息》2002 年第 5 期。

授权的用户存取敏感数据，通常允许合法用户不受妨碍地访问网络信息资源。美国先后开放了多种防火墙技术，如 FTP 防火墙、Telnet 防火墙、Email 防火墙、病毒防火墙等各种专用防火墙技术，各种防火墙技术可以被一起用来弥补各自的缺陷，增加系统的安全标准。而且，为了解决各不同厂商的生产的防火墙兼容性，美国国家计算机安全保密协会 NCSA（National Computer Security Association）成立的防火墙开发商联盟 FWPD（Firewall Product Developer）制定了防火墙测试标准。

此外，在大量开发放火墙、安全路由器、安全服务器、用户认证产品等保护类技术和产品更新换代的同时，也加强了对预警、检测、追踪、响应和恢复等积极防范技术和产品更新换代的研制。

（3）重视发展信息战能力，开发反侦探技术，实行“积极防御”

密码技术不仅被美国用来保护自己的信息安全，还同时被作为一种反侦探的工具。目前，美国微软公司的 Windows 操作系统是全球市场利用率最高的软件。微软视窗系统的一个安全问题是视窗本身的保密功能不强，解决的办法是采用其他加密软件。视窗系统内设有一个用于加密和解密的应用编程接口函数集“CryptoAPI”，加密软件开发商可以通过 CryptoAPI 编制加密软件。当软件开发商得到微软的许可使用 CryptoAPI 时，他们实际上是得到了一个验证许可的密钥。[①] 1999 年 8 月加拿大 Cryotonym 公司首席科学家安德鲁·费尔南德斯惊人地

① 华涛：“网络信息安全与全球化时代信息安全国际体制的建立”，《世界经济与政治》2000 年第 3 期。

发现，视窗系统中存在第二把密钥，叫做 NSAKey，而 NSA 就是美国国家安全局（National Security Agency）的简称。也就是说，在风行全球的 Windows 系列操作系统中留有一个“后门”，从而使美国著名的情报机构国家安全局可以秘密地访问电脑用户的操作系统。[①] 费尔南德斯说，这一密码存在于目前常用的几乎所有 Windows 操作系统中，如 WIN95，WIN98，WIN2000 以及 Windows NT。也就是说，微软在每一份视窗系统中都安装了一个“后门”，专供 NSA 在需要时侵入全世界用户的电脑。这就是所谓的“NSA 密钥”事件[②]。经过密码技术处理后的信息，只有拥有密钥的相关人员才能得到相关算法，弄明白密文的意义。

国防系统信息安全是美政府保护的重点对象。因此，在遵循政府有关部门政策和法令的同时，国防部还制定了本部门专门的信息安全政策和措施，例如，国防关键基础设施保护方案、国防系统信息保护计划等，对国防信息保护行动进行协调、综合和监督。国防部门关键基础设施保护与政府其他部门和私营部门最显著的不同是，国防部在所有关键节点采用并不断完善入侵侦查系统（Intrusion detect systems，IDS），以及建立计算机网络保护联合特别小组来管理该项工作。目前，自动入侵侦察环境—先进技术示范（automated intrusion detection enrironment-advanced concept technology demonstration）计划开

① “中国工程院院士何德全谈信息安全”，《国家安全通讯》2001 年第 3 期。

② “恐怖的‘后门’：科学家发现 Windows 为 NSA 留有第二把密钥”，《计算机世界》，1999 年 9 月 13 日。

始启动，提供自动侦查和威胁预警及攻击评估。[①] 而且自 1992 年 12 月开始，美国防部就开始实施一项防御性信息战计划。1995 年 1 月，国防部组建了信息战争执行委员会。同年 12 月，国防部的防御性信息战管理计划提出了三项措施，用以防止、侦测和反击对国防部信息基础设施的威胁行为。到目前为止，美国陆海空三军相继成立了专门负责信息战争的信息战中心。

2. 安全管理层

安全管理层主要包括密钥管理、系统安全管理、安全服务器、安全机制管理、安全时间处理管理、安全审计管理、安全恢复管理、安全组织管理、安全制度管理、认识安全管理、安全意识教育、道德品质教育、安全规章制度、大众媒体宣传、表扬惩罚制度、安全知识普及等。此外，安全管理还应当包括人事管理。目前，因内外勾结对计算机系统实施攻击而造成的损失在成倍增长。因此，在“防外”的同时，也必须“安内”，即加强对内部涉密人员的管理。

在美国，信息和信息系统是由总统亲自领导的，投入力度也相当可观。以下是两个显著的例子。

（1）在联邦政府设立相关的委员会，为总统决策服务：2001 年 10 月，小布什政府颁布了《信息时代保护关键基础设施的行政命令》，组建了新的关键基础设施委员会，其成员包括国务卿、国防部长、司法部长、商务部长、行政管理与预算局局长、科学与技术政策办公室主任、国家经济委员会主席、

① “Defend American Cyberspace——National Plan for Information Systems Protection”（Version 1.0），January.2000

总统国家安全事务助理、总统国土安全助理等官员。根据该命令，委员会主席兼任总统有关网络安全的特别顾问，他有权了解各部、局内属于其管辖范围的所有情况，召集和主持委员会的各种会议，制定保护关键基础设施的政策和方案，并向总统国家安全事务助理和国土安全助理汇报。①

（2）建立各级信息安全主管机构。根据《联邦政府信息资源的管理通告》（A－130 通告）的规定，行政管理与预算局（OMB）负责制定和监督政府部门有关信息系统安全的政策、原则、标准和指导方针。在它统一领导下，美国的信息安全工作分别由商务部门下属的国家标准与技术局（NIST）和国防部下属的国家安全局（NSA）分工负责。NIST 主要负责非保密信息（即敏感信息）的安全工作，NSA 负责保密信息（即国家安全系统）的安全工作。所谓国家安全系统，是指有美国政府及其合同单位或代理机构管理的通信和信息系统，包括：存有保密信息、以及美国宪法 2315 款第 102 项规定的信息；涉及情报活动；涉及与国家安全有关的隐蔽活动；涉及军队的指挥与控制；涉及属于武器和武器系统的设备或对于完成军事或情报任务至关重要的设备。②

在明确主管机构的基础上，美国政府按照部门的重要程度进行划分，责成各部门内设相应机构，执行 OMB、NIST 和 NSA 的规定和计划，并根据各自具体情况，以国家有关部门

① Executive Order, Critical Infrastructure Protection in the Information Age, 16thOctober, 2001.

② 《信息战与信息安全战略》，国务院发展研究中心国际技术经济研究所，金城出版社，1995 年，第 74 页。

的信息安全法规政策为依据，制定类似“信息技术管理手册”的用户指示性文件，指导其下属部门的信息安全工作。各部是其下属基础设施部门安全的主管机构，由部门联络官员进行的信息的上传下达，同时必须任命一名首席关键基础设施保护官员（Chief Infrastructure Assurance Officer，CISO），主管本部门关键基础设施的保护工作。[①] 例如，国防信息系统局（NISA）是国防系统信息安全的主管部门。国防信息系统局下设信息系统安全中心和自动化系统安全事故支持小组（ASSIST）等部门，负责制定国防部信息安全标准，处理国防部所有的信息安全事故，分析薄弱环节并提出保护、侦测和应对措施。

隶属于联邦调查局的国家基础设施保护中心（National Infrastructure Protection Center，NIPC）成立于 1998 年 2 月，是美收集威胁关键基础设施有关部门信息的国家重要部门，在评估威胁、提供威胁预警等方面发挥越来越重要的作用。具体任务包括侦破、阻止、评估、预警调查涉及对计算机和信息技术构成的威胁，并对以美关键基础设施为目标的非法行动作出反应；主管计算机入侵事件的调整；实施与打击网络犯罪及入侵有关的法律，并执行反恐怖和涉外反间等任务；当违法行为超出一般刑事犯罪的范围并由外国发起旨在攻击美国利益时，对国家安全部门提供支持；与政府部门和私营机构联合培训网

① US President Decision Directives (PDD－63), Critical Infrastructure Protection, May 1998.

络调查员和基础设施保护人员等。[①]

3. 政策法规层

政策法规层主要包括制定各项安全政策和策略、制定安全法规和条例、打击国内外的犯罪分子，依法保障通信网和信息安全等。美国是信息安全的法律法规制定得最多、最完善的国家。目前，美国已确立的有关信息安全的法律无所不包，包括信息自由法、个人隐私法、反腐败行径法、伪造访问设备和计算机欺骗滥用法、计算机安全法、正当通讯法令、电讯法、儿童网上保护法、网络安全法、数字电话法案、电子签名法案及反黑客法案等。其中，1987 年经过修订的《计算机安全法》是美信息方面最主要的法律，[②] 在 80 年代末至 90 年代初被作为各州制定其他地方法规的依据。该法规定，联邦政府各机构必须确认存有敏感信息的信息系统，并制定保护这些信息的信息安全计划。

此外，自 1984 年以来，美国政府共颁布近 10 个涉及关键基础设施和信息安全的政策、通告、总统行政命令和国家计划，其中包括“关于通信和自动化信息系统安全的国家政策”（即 NSDD－145，1984 年 9 月 17 日）、《联邦政府信息资源的管理通告》（即 A－130 通告，1985 年 12 月）、关于反恐怖主义政策的总统令（1995 年 6 月）、第 13010 号（1996 年 7 月 15 日）及第 13025 号（1996 年 11 月）和 13064 号（1997 年

① http：//www. nipc. org. 以上内容同时摘自，唐岚：“美国国家信息安全保障体系简介”，《国际资料信息》2002 年第 5 期。

② 唐岚：“美国国家信息安全保障体系简介”，《国际资料信息》2002 年第 5 期。

10月）行政命令、第63号总统令（PDD—63，1998年5月）、《信息系统保护国家计划》（2000年1月）、《信息时代保护关键基础设施的行政命令》（2001年10月16日）等。[①] 这些通告、政策与命令各有侧重，是对前述法案的补充，保障了安全管理的顺利实施，并促进了安全技术的研究与开发。

信息安全涉及的安全技术、安全管理与政策法规三个层次是有机整体，任何环节的失误都有可能带来严重的后果。信息安全工作是一个全方位、综合性的工作，因此信息安全的措施也应该是全方位、综合性的，惟有如此，才能达到预期的效果。美国的信息安全从以上分析来看，已经走在世界的最前列。许多国家在纷纷效仿。但是，尽管美国政府花费了相当多的精力在安全技术、安全管理与政策法规层面齐头并进，以期提高美国的信息安全，信息安全对严重依赖于信息网络的美国来说，仍然是一个严峻的挑战。因为，信息安全不仅是政府的职责，它还必须由全社会参与。商业圈在国际交往中与它们的顾客、供货商、战略伙伴等共享信息的同时，也可能会无意将敏感商业信息透露给外国政府、竞争者、罪犯和战略竞争对手等。个人在免提、手提电话中交流的信息也会谈论到敏感信息，而这些都非常容易被监听。越来越多的商务及金融交易电子化……因此，信息安全是一个全社会的问题，是政府与民众必须共同承担的问题。

① 唐岚："美国国家信息安全保障体系简介"，《国际资料信息》2002年第5期。

金先宏　复旦大学美国研究中心

倪世雄　复旦大学美国研究中心

周　鹏　复旦大学世界经济系

徐以骅　复旦大学美国研究中心

夏立平　上海国际问题研究所

栾培强　中国太平洋保险公司

蔡翠红　复旦大学美国研究中心