doi :10.3969/j.issn.1671-1122.2010.01.024

美国国家信息安全战略的演变与评价

蔡翠红

（上海复旦大学美国研究中心，上海 200433）

摘　要：本文拟就美国的国家信息安全战略的演变与发展进行剖析，并对布什政府的《网络空间安全国家战略》进行评价与分析，以寻找今后的信息安全战略发展方向与目标。《网络空间安全国家战略》虽然经过了布什政府的多方酝酿，但仍然招致了褒贬不一的评价。然而，不管反应如何，在“9·11”后提出这样专门的国家战略，符合了美国国家安全的需求，是美国国家安全战略的重要组成部分。奥巴马政府将如何继续推进该战略的实施，我们将拭目以待。

关键词：《网络空间安全国家战略》；美国国家安全战略

中图分类号：TP393.08　**文献标识码：**A

1 起源与演变

作为互联网的源起国，美国对信息网络安全问题的关注由来已久。早在20世纪80年代初期，就已经着手解决并采取了一系列措施。美国的信息安全战略在发展演变过程中，经历了从信息发展优先到信息安全与信息发展并举、从适度信息安全到先发制人战略的转变。

1.1 从信息发展优先到信息安全与发展并举

美国的信息与信息安全政策是其基本价值观的反映，因为他们坚信，信息和美国大众文化的传播增进了美国观念及其价值观在全球的广泛认知和开放，传播美国价值观可以缓解和消除体系结构矛盾对美国安全的威胁。

因此，美国信息政策发端初期的报告和政策等大多以信息自由流动为主旨。可以说，美国从一开始就致力于成为世界信息化浪潮中的领导者。

1.2 从适度安全到先发制人

从20世纪90年代初至2001年“9·11”恐怖袭击事件发生之前，这一时期互联网经历了高速的发展阶段，出现了真正意义上的全球网络系统，国家对于信息系统的依赖程度也上升到了一个前所未有的阶段，同时各种对国家信息安全造成影响的事件也不断涌现，网络信息安全逐渐引起美国政府关注。虽然克林顿政府较布什政府更加注重信息高速公路、电子政府、全球信息基础设施等的建设，但是信息化过程中经常出现的信息安全问题、网络犯罪以及信息基础设施的脆弱性，也使克林顿政府采取了一系列适度信息安全措施。

为了打击计算机犯罪，保障信息安全，1994年美国议会通过了《计算机滥用法修正案》，扩大了计算机犯罪的责任范围。1997年1999年，总审计局（GAO）两度提出《计算机安全增强法》，用以更新1987年的《计算机安全法案》。1999年，美国通过了《政府信息安全法》，以保护政府的信息和信息系统安全等。而在基础设施保护方面，美国于1996年制订通过了《国家信息基础设施保护法》，对有关计算机系统联机犯罪、破坏信息网络基础设施等情况都作出了界定。1998年，克林顿总统签署了关于保护国家关键基础设施的第63号总统令（PDD-63），要求实施国家信息安全的保护计划，并围绕信息保障成立了多个组织和全国性机构。2000年，在美国政府的《国家安全报告》中首次把保卫能源、银行与财政、电信、交通、供水系统等重要的信息基础设施的安全，列为国家利益之首的关键利益。2000年1月，美国发布了《保卫美国的计算机空间——保护信息系统的国家计划》（Defending America's Cyberspace—National Plan for Information Systems Protection）[1]。该计划综合了其国内各界力量，涉及了信息安全各项内容，几乎涵盖国家和社会生活所有层面，是美国21世纪信息安全的首个战略性指导方针[2]。

“9·11”事件是“永远改变美国如何看待其全球角色和怎样思考安全问题方式的变革性事件”（布什总统国家安全助理赖斯语），“9·11”提升了信息安全在整个美国国家安全战略体系中优先性位置，改变了美国对国家信息安全的威胁认知，同时还使美国认识到其信息安全措施与效率的不足，认识到有必要调整政府机构内部涉及国家信息安全问题的不同机构之间的关系，以期提高处理相关信息的效率。从克林顿时期的“主张发展优先”逐渐变化为“主张安全优先”，从讲“适度安全”到“先发制人”，美国国家信息安全战略因为“9·11”事件的发生了重大变革。因此，“9·11”发生之后的几年几乎所有有关信息政策或战略的法案都与信息安全而非信息发展相关。

“9·11”之后，布什政府为了体现其对国家信息安全的重视，不仅宣布了新的《网络空间安全国家战略》，而且采取各种有效措施，全面加强网络与信息安全的防范工作，其中包括大规模增加反恐开支和用于信息安全的经费。“9·11”后，美

国赖以存在的国家信息基础设施成了信息安全的重点保护对象，打击互联网犯罪的重点也转向网络恐怖活动，以实现对国家基础设施的保护。经历了“9 · 11”的布什政府更采取了一些措施将之落到实处。“9 · 11”后，布什总统很快成立了总统关键基础设施保护委员会(President's Critical Infrastructure Protection Board，PCIPB)，其目的就是以期协调联邦各项基础设施保护措施。[3] 甚至刻意将总统关键基础设施保护委员会、国家基础设施保护中心（克林顿政府所设立的跨机构中心，National Infrastructure Protection Center, NIPC)、和关键基础设施保障办公室(Critical Infrastructure Assurance Office，CIAO)三个机构搬至同一幢办公楼，[4] 以促进相互之间的合作和共享。布什还大力鼓励企业间共享安全信息，并支持对信息自由法中的有关条款进行修改以扫除信息共享障碍 [5]。

布什政府还开始将网络安全教育科研与发展作为其预算中的优先项目。[6]“9 · 11”事件后，美国学者认为，目前仅有的“周边防线”的信息安全模型是脆弱的，需要从根本上解决问题，以一个新模型来替代原先的周边防卫模型；需要对信息安全进行新的定义；至此，可信计算技术得到了迅速的发展。这其实与美国“先发制人”战略即在威胁尚未成为现实之前就将它们消灭的主旨不谋而合。

2 战略构建与保障框架

2003 年 2 月，在美国联邦、州和地方政府、高等院校以及相关机构组织的共同努力下，以及向社会各界广泛征求意见的基础上，美国正式通过了《网络空间安全国家战略》(National Strategy to Secure Cyberspace)。[7] 由于到目前为止还没有类似战略文件出台，故而该战略目前仍然是美国的国家信息安全战略最主要的文件和战略参照。

2.1 战略构建

《网络空间安全国家战略》第一次针对性地系统确定了国家信息安全战略的三个基本要素，即美国国家信息安全的目标（利益）、面临的主要威胁以及保障国家信息安全的手段。这是美国历史上第一份专门针对国家信息安全而推出的国家安全战略文本，它的出现标志着国家信息安全的独立战略地位得到了最终的确认。

美国国家信息安全的目标与其信息战略目标相一致，即获取信息优势，降低国家信息系统脆弱性和以及对跨国信息流的管理和控制。具体而言，美国国家信息安全战略的目标包括如下三方面：[8] 第一个方面是国家基础信息设施保护方面提升网络威胁的可抗性。第二是在信息战方面进一步提高制信息权，从而获取信息优势。第三是信息战从军事领域向市民社会的拓展，即心理战与公共外交，从而通过对信息流的管理和控制达到一定的战略目的。

2.2 保障框架

无论是多么好的战略，都需要一定的实施与保障框架作为支撑。美国信息安全保障框架是由安全技术、安全管理与政策法规三个层次所组成，他们是一个有机整体，任何环节的失误都有可能带来严重的后果。信息安全是一个全方位、综合性的工作，因此信息安全的保障措施也应该是全方位、综合性的，唯有如此，才能达到预期的效果。

2.2.1 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。在开发密码认证、防火墙、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，美国也一直在探索预警、检测、追踪、响应和恢复等积极防范技术以及下一代互联网的研制。

美国还竭力制定计算机安全评价技术标准，积极参与开发国际通用安全准则。从 20 世纪 80 年代的“可信计算机安全评价标准 TCSEC”（又名“橘皮书”）和“可依赖网络解释 TNI”（又名“红皮书”）到 90 年代的“联邦评价准则”(FC)及目前的美、加、法、英、荷、德等六国提出并经国际标准组织认可成为国际标准的“信息技术安全评价公共准则“(CC，ISO/IEC 15408)，美国一直主宰着计算机安全评价标准。不仅如此，全球网络管理中所有的重大决定仍由美国主导作出。负责全球域名管理的 13 个根服务器有 10 个在美国，而且美国政府于 2005 年 7 月 1 日宣布，基于日益增长的互联网安全威胁和全球通信与商务对互联网的依赖，美国商务部将无限期保留对 13 台域名根服务器的监控权 [9]。

此外，为了实现其信息优势，美国还特别重视发展信息战能力，开发反侦探技术，实行“积极防御”。自 1992 年 12 月开始，美国国防部就开始实施防御性信息战计划，用以防止、侦测和反击对国防部信息基础设施的威胁行为，并在国防部所有关键节点采用并不断完善入侵侦查系统。在到目前为止，不仅美国陆海空三军都已相继成立了专门的信息战中心，而且美国国防部已经在积极筹备建立独立的网络安全指挥部。此外，借助美国主要的电子产品制造商的帮助，在出口的电子设备中留“暗门”、设“木马”，也是美国实施反侦探的手段之一。

2.2.2 安全管理层

信息安全管理可以分为多个层次，如国家的宏观管理、网络经营者的行业管理以及网络使用单位的具体管理等。美国对信息安全管理非常重视，这不仅体现在其设立的许多信息安全管理机构，同时也体现在总统对信息和信息系统安全的亲自领导。在执行《网络空间安全国家战略》的过程中，美国成立了整合有关 22 个联邦机构安全力量的国土安全部。国土安全部除了负责实施本部门所承担的计划项目外，还充当联

邦政府的主要联络点，为州和地方政府、私人机构以及美国公民就网络安全问题展开讨论提供沟通平台。此外，科学与技术政策办公室负责协调支持关键基础设施保护的技术研究与开发；管理与预算办公室负责监督联邦政府有关计算机安全计划的政策、规则、标准和方针的执行；国务院负责协调网络安全方面的国际事宜；中央情报局负责评估针对美国网络和信息系统的国外威胁；司法部与联邦调查局负责领导调查和打击网络犯罪。为了促进并加强合作，特别为每个容易受攻击的主要经济领域指定“领导部门”，如银行与金融领域的网络安全保护工作由财政部领导等。

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，执行联邦政府的规定和计划，并根据各自具体情况，以国家有关部门的信息安全法规政策为依据，制订类似“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。各部门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。

随着计算机网络的普及和计算机安全事故的频繁发生，美国国内一些重要部门，如国防部、能源部、美国宇航局、国家标准与技术局等也都设立了计算机应急处理小组，并由美国国防部高级研究计划局出资在美国匹兹堡卡内基一梅隆大学软件工作研究所内设立了计算机应急处理小组协调由心(CERT)。美国军方也有较为健全的信息安全管理机构，包括国防信息系统局、国防信息系统局信息系统安全中心、美国空军信息战中心、美国海军SPAWAR信息系统安全计划办公室、美国陆军信息系统安全办公室、美国宇航局自动化系统事故处理中心等等。

2.2.3 政策法规层

政策法规层，主要包括制订各项安全政策和策略、制订安全法规和条例，以打击国内外的犯罪分子，依法保障信息安全。美国是计算机网络发展最快、应用最普及的国家，同时也是计算机网络犯罪发生最早、数量最多以及信息安全相关政策法规最多的国家。目前，美国已确立的有关信息安全的法律无所不包，例如旨在加强信息网络基础设施保护、打击网络犯罪的《国家信息基础设施保护法》、《公共网络安全法》、《计算机安全法》、《加强计算机安全法》、《加强网络安全法》；旨在规范信息收集、利用、发布和隐私权保护的《信息自由法》、《隐私权法》、《电子通信隐私法》、《儿童在线隐私权保护法》、《通信净化法》、《数据保密法》、《网络安全信息法》、《网络电子安全法》；旨在确认电子签名及认证的《电子签名法》；关于其他安全问题的《国土安全法》、《政府信息安全改革法》、《网络安全研究与开发法》等等。

除了正式的法律，美国政府还先后颁布了许多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，例如《联邦政府信息资源的管理通告》、《关于反恐怖主义政策的总统令》、第13010号及第13025号和13064号行政命令、第63号总统令、《信息系统保护国家计划》、《信息时代保护关键基础设施的行政命令》等等。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。

对于各行各业的互联网，美国也力图采取不同的保护策略和管理制度，对不同级别的事件采取不同策略。对于国家机关、能源、金融、国防等部门的计算机信息系统采取重点保护的策略。不同领域有相应的不同法案，如针对商业秘密的《美国经济间谍法》、针对金融业的《金融服务现代化法案》、针对财务责任的Sarbanes-Oxley法案或公众公司会计改革和投资者保护法等等。在遵循政府有关部门政策和法令的同时，美国国防部还制订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。

3 评价与反思

《网络空间安全国家战略》出台后，各方意见褒贬不一。大部分人觉得该战略方向正确，但是力度不够，没有真正提出一些法规，有些问题讲述得不够。也有人觉得该文件根本方向性错误，文件中所针对的对美国国家信息基础设施的网络攻击或恐怖袭击根本不值得大惊小怪。当然，还有些人觉得该文件虽然有瑕疵，但总体合适，是政府对这一问题非常严肃思考的结果 （责编 程斌）

参考文献：

[1] http://clinton4.nara.gov/media/pdf/npisp-fullreport-000112.pdf .

[2] 吴汉平等译．信息战与信息安全[M]. 北京：电子工业出版社2004:76.

[3] Thomas R. Temin. Bush Establishes Cybersecurity Board. Government Computer News[R]. 2001 .

[4] See Diane Frank. Cybersecurity Center Takes Shape. Federal Computer Week[J], 2002.

[5] Michael Vatis.Cyber Attacks: Protecting America’s Security Against Digital Threats. ESDP-2002-04[J]. 2002.

[6] Carolyn Duffy Marsan. Security Chief Details U.S. Cybersecurity Plans. InfoWorld[J]. 2002.

[7] http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.

[8] 蔡翠红．美国国家信息安全战略[M]. 上海：学林出版社，2009.

[9] 邹学强，杨海波．从网络域名系统管理权看国家信息安全[J]. 信息网络安全，2005（9）.

作者简介：蔡翠红（1972-），女，副教授，主要研究方向：国际关系与政治。