# 国外信息安全战略与体系

## 第一节 美国

### 一 背景与目标

#### 1.经济背景：美国的“新经济”时代

新经济（The New Economy）是指在经济全球化背景下的信息技术革命以及由此带动的以高科技为龙头产业的经济发展形态，它成为美国20世纪90年代初期开始，由高新技术发展带来经济景气、经济扩张的代名词。

自1991年3月美国经济开始走出衰退，一直到2000年6月，美国经济的景气扩张已经连续达第111个月。统计数据显示，美国的财政预算从1992年的2900亿美元的赤字，到2000年时已经转为1600亿美元的盈余；美国纽约道琼斯工业指数于1992年仅约3000点，到2000年时则直线攀升至约12000点的高峰；失业率则由1992年6月的7.8%下降到2000年10月的3.9%，是1969年以来之最低点，而2000年的通货膨胀率亦控制在1.6%。短短几年内，美国经济仿佛在以一种惊人的态势疾速增长。但是，到底是什么因素导致了美国经济“收支盈余、高经济增长、低失业率、低通膨率”的繁荣景象呢？这个问题引起了世界范围内对美国经济的广泛关注和研究。1996年12月30日美国商业周刊发表的以新经济为专题的一系列文章指出，正是80年代以来高科技《产业的蓬勃》发展带动了美国20世纪90年代开始的经济景气扩张。此后，美国联邦储备委员会主席格林斯潘在发表讲话时多次引用“新经济”的概念，“新经济”的说法也传遍了世界。

事实上，信息技术是“新经济”的基石。

以信息技术为代表的高科技产业与“新经济”现象之间有着不容割裂的紧密关系，这种关系主要体现在：信息产业是最先体现“新经济”特征的产业，信息产业的特征就是“新经济”最典型的特征；没有信息技术的发展就没有“新经济”的发生，前者带动了后者的发展；信息技术是“新经济”最主要的组成部分，具有不可否认和不可替代的核心作用。自20世纪90年代初以来，美国对信息技术和信息产业的投资一直保持在很高的水平上，投资总额是其他产业投资的十几倍。相应的，自1993年以来，由信息所带动的美国工业增长的比例高达40%以上，信息产业已成为美国经济增长的主要动力。

信息技术对“新经济”

的贡献表现在对传统经济的信息化结构改造上。信息技术向整个经济领域的渗透，造就了一种与传统经济完全不同的经济形态，突出表现在工业、农业、商业、金融业和服务业等传统经济中的核心产业，在采用信息技术进行改造后，产销结构发生了重大变化，形成了新的模式。这种新模式通过信息技术实现了信息广泛、快捷的流动，更有效地实现了资源的优化配置，提高了企业的经济效益，进而提高了整个国民经济的健康发展。

信息产业具有创新能力强、技术更新快，以及对原材料和能源需求相对少，对经济运行中间环节的依赖程度较低，不易引发通货膨胀等优点。在信息技术和信息产业大发展的 20 世纪 90 年代，对美国经济起主导作用的是高技术信息产业，微软、英特尔等取代了汽车、石油和房地产等，在美国国内经济增长中居主导地位。美国信息产业的健康发展，培育出了一大批优质企业，它们对促进经济与就业的增长起了重要的作用。1993 年，年均增长不低于 20%的公司在美国有 23 万家，而到 1997 年则达到了 36 万家，这些企业为美国经济繁荣作出了显著的贡献。比如，1992 年，以计算机和网络为核心的 IT 产业对美国经济增长的贡献率已经达到 26%，1995 年更是高达 41%，信息产业已经成为美国经济增长的“催化剂”。20 世纪 90 年代中期以后，信息产业已经占到美国国内总收入（GDI）的 10%。尤其是进入 21 世纪以来，信息产业成为美国国家经济的支柱产业。

美国的信息产业具有非常雄厚的基础，全球知名的芯片公司、软硬件公司均成立于美国，而很多影响信息技术重大进步的发明和应用都源于美国。美国信息产业的“实力”领先是世界公认的事实。

**2.社会背景：2001 年 9·11 恐怖袭击**

美国政府认为其民主价值观念与美国国家安全之间存在一种内在的逻辑关联。美国学者托尼·史密斯指出：“在过去的一个世纪中，美国外交政策最宏伟的目标就是将在海外推广民主作为维护国家安全的重要途径。”美国民主文化的传播可以有效缓解和消除体系结构矛盾对美国安全的威胁。因此，美国信息政策初期大多以信息自由流动为主旨。美国一直致力于成为世界信息化浪潮中的领导者。

赖斯曾说过，“‘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”。9·11 恐怖袭击事件对美国社会产生了深远的影响，直接导致了美国公民安全观和国家安全政策的转变。

**（1）“9·11”恐怖袭击事件成为对美国国家信息安全悲观认知的重要根据**

自从冷战结束之后，由于美国在信息安全方面广泛遭到攻击，美国政府内部的部分决策者，

尤其是国防部认为，美国存在着严重的信息安全威胁，至今仍然处于非和平状态，他们对美国国家信息安全一直持悲观态度。但是对于大部分美国民众来说，在“9·11”恐怖袭击事件出现之前，他们对国家信息安全的问题的认知从未改变。有人研究表明，是1993年2月

26日第一次世界贸易中心的爆炸事件的成功处理掩盖了它对美国新威胁的特征和范围的需要，是美国民众低估了这种威胁，虽然这在一定程度上提高了对新的恐怖主义危险的认识。在传统观念上，人们大多数情况下并不认为“信息攻击”对国家安全构成了什么实质性的威胁，特别是针对政府机构信息系统的攻击行为，人们认为它损害了政府的威信、暴露了在日常维护中存在的漏洞。

所以，在“9·11”恐怖袭击事件发生之前，这些人始终无法提供信息基础设施是美国国家安全问题中百密一疏的相应证据，无论他们怎么强调都没用。但是“9·11”恐怖袭击事件发生之后，公民在信息安全观的认知上终于发生了改变，他们认为美国国家信息安全确实受到威胁，类似于恐怖分子的非国家行为体有能力、有意图借助非对称手段来对国家行为体发动恐怖袭击，他们也已经成功地通过互联网将这些行动策划变成了现实。“9·11”的拉登的恐怖分子只是手持裁纸刀就能劫持飞机撞向大厦，未来的恐怖分子就会通过敲打键盘、点击鼠标这些无法防范的方式来对美国具有漏洞的信息安全体系发起挑战，对美国进行新的恐怖袭击。尽管这种情况发生的概率微乎其微，但是不能完全排除其可能性，而且一旦发生了，造成的损失是无法估量的。

**（2）造成了美国国家安全战略决策过程中行政—立法关系的变化**

“二战”之后，制约行政权力扩张的最主要的外部环境是美国历史中广泛存在着的“滥用行政权力会对自由民权构成损害”这一认知，而且它是广泛存在的。但是随着“9·11”事件的冲击，人们的这一认知产生了淡化和转变，其结果就是在“9·11”恐怖袭击事件之后，行政机构再度占据了优势地位，彻底改变了立法机构通过越南战争在美国国家安全战略决策过程中占据优势的态势。

“9·11”事件过后，美国民众大力支持联邦政府运用包括窃听器在内的一些手段来搜集恐怖分子相关的信息，这与“9·11”事件之前国家使用行政权力（比如“监视嫌疑犯”）导致的侵害自由民权表示担忧和对政府的不信任形成了强烈的反差。这表明了美国民众仍然惧怕会再次遭到恐怖分子的袭击，“反恐”成为他们心中最为关注的问题。这种担忧和恐惧让他们认为希望政府采取更多的实际行动来保障国家和公民的安全，得到更高的安全保障水平，那么他们必须付出一定的代价，其中包括可能对自由权利的侵犯。为了达到更有效的行使权力和更快速地处理突发事件作出快速反应，行政权力从立法机关的手中接过了决策权力，重新获得了优势地位。

在这样的背景下，以国防部、中央情报部、国家安全局、国土安全部、联邦调查局、能源部等为代表的涉及国家信息安全的行政机构逐渐占据了优势地位，从此美国国家信息安全政策决策的权力结构发生了巨大的变化。上述这些机构的内部精英对信息安全的认识跨越了部门的范围，在整个国家信息安全政策的制定过程中发挥了重要的作用，他们的通力合作最后形成了国家信息安全政策的变化。

**（3）揭示了国家信息安全政策面临的新挑战**

“9·11”恐怖事件发生导致了美国国家信息安全面临的威胁形式发生了重大变化。在这之前，国家信息安全的主要威胁在于关键性设施受到的信息攻击，攻击者直接侵入或者摧毁至关重要的信息基础设施来损害国家的利益，因此防范的措施就是防止恐怖分子破坏关键性的信息基础设施。由于在“9·11”中，恐怖分子的攻击目标转换成了非信息基础设施，发达的通信网络只是他们组织和实施恐怖袭击的有效工具而并不是之前的目标了。而且通过这些信息通信手段，恐怖分子的攻击手段从单一向多样化转变，目标也就多样化。这对国家信息安全防范提出了新的难度和要求，乃至是全球的新的挑战。

**（4）要求保障国家信息安全的手段作出相应的变化**

国家信息安全政策和国家信息安全保障的要求随着国家信息安全的威胁形式的变化而变化。传统的防护措施是保护信息基础设施的安全，因为恐怖分子只是发动针对信息基础设施的直接攻击。然而现在所关注的重点发生了巨大的改变，因为信息基础设施成为了恐怖分子的工具也就是帮凶，那么对其就不能是保护而是控制，即控制其不会被恐怖分子利用。从之前的被动型防御转换成主动性的防御，意味着不仅仅要防护国家信息基础设施以及在其中存储、传递、交换和处理信息的安全，而且要更加积极加强对特定信息流动的监管，及时发现对国家安全构成威胁的信息。比如在反恐战争中，国家有责任有权力监控整个国内的信息传播和流动，必要的话，范围可以扩大至全球。在这些海量的信息流当中筛选和识别对国家安全造成威胁的信息并作出及时的反应。所以在开放的信息安全政策下有效地控制信息流动是国家信息安全政策的主导。

如何保证国家有足够的能力来控制国家信息基础设施传递的信息安全呢？可以从信息内容和信息流动的方向来控制。但是要达到这两者的目的需要先进的科学技术和完善的安全管理体制，而且要作出快速的反应。因为涉及的信息不仅包括公共的，而且还包括民众的隐私信息，所以在控制和监管的过程当中，民众的这些权利会受到损害，如何达到这两者的平衡也是国家信息安全保障的压力所在。能反应这个情况的一个例子就是 2002 年美国政府的保密文件数量的激增和解密文件数量的剧减。

在“9·11”

恐怖袭击事件刺激下，美国政府还开始了对于国家信息安全政策的调整。这种调整是通过一系列的政府文件表现出来的。其中具有代表性，并直接针对国家信息安全政策的有以下五个文件：2001 年 10 月颁布的第 13231 号总统行政命令，2002 年通过的信息安全管理法，2002 年发表的国家安全战略报告，2003 年 2 月 2 日发布的美国国家信息安全政策（草案），以及 2003 年第 13292 号总统行政命令。

**3.国家信息安全战略的目标**

美国信息安全战略的目标可以概括为三点：一是获取信息优势；二是降低国家信息系统脆弱性；三是对跨国信息流的管理和控制。

**（1）获取信息优势**

信息优势（Information Dominance）是源于美国军方的一个概念，指在信息的产生、处理及运用上取得足够优势，以使信息的拥有者能够保持军事上的优势。20 世纪 90 年代以来美国的权威性军事文件几乎都对信息优势进行了界定，例如 1998 年版《联合信息行动》条令、2001 年版美国陆军《作战纲要》和美国国防部的《2020 年联合构想》报告中均对信息优势进行了定义，并突出了其重要性。由此可见，美国信息安全战略中提到的信息优势，更多的是从军事和防务角度出发的。其目的是通过获取交互式作战空间态势的感知与共享能力，比敌方更全面地掌握战场空间情况、更快地收集和处理数据，拥有比敌方更强的信息进攻能力和信息安全防卫能力。

**（2）降低国家信息系统脆弱性**

降低国家信息系统的脆弱性，实际上就是降低国家关键基础设施尤其是信息基础设施的脆弱性。鉴于信息资源、信息技术在关键基础设施的核心地位，国家的经济、政治和军事的信息化水平越高，对关键基础设施的依赖性也就越大，从而产生了国家关键基础设施的脆弱性。保护关键基础设施的目标主要体现在两个方面：一方面要保护基础设施的物理实体，防止自然灾害、事故和人为破坏而造成基础设施各系统的运行中断；另一方面是保护基础设施的逻辑安全，即保障支持设施运行的信息资源、信息技术的保密性、完整性和可获性等几个方面。

**（3）对跨国信息流的管理和控制**

跨国或称越境信息流，是指经由各种信息通道（外交活动、媒体、伴随人员跨国流动、互联网络等）

在各国国际行为主体（主要是主权国家）之间流动的经济、政治、军事、社会、科技等方面的信息。越境信息流的长期过程是构成国际信息结构的基本途径。对越境信息流的控制和管理就成为国家信息安全战略和政策的主要内容。实际上，在具体的信息安全战略和政策中，每个国家都对越境信息流实行某种程度的控制，鼓励和支持有利于推行本国总体战略、树立国家正面形象和具体目标实现的越境信息流动，而从技术、政策和法律上对不利信息进行控制，防止有害信息自由越境传播。

## 二 体系

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。本章将信息安全战略体系主要分为三个子体系进行分析：管理体系、技术体系、评估体系。整个体系当中，信息安全技术的发展提供推动力，评估体系提供反馈结果，管理体系中的法律法规是保障、政策是手段。三者相辅相成、共同构成信息安全保障架构。

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。美国的信息安全战略是一个综合战略，是基于信息在国家安全中的重要作用，对信息资源在多个层次上进行控制和运用，来达到维护国家安全的目的。

### 1.管理体系

分为战略层、组织层、政策法规层。

#### （1）战略层

其管理体系总体战略可以分为外交、防务、技术三个方面：

维护国家信息安全的战略，其最高层面是理解并构造有益于本国安全的国际体系的信息结构，可以将其归纳为信息战略的外交层面，即通过各种外交途径和手段在国际上营造符合本国安全需要的国际信息空间。信息战略的外交层面就具体表现为对国际主导价值观念的影响和塑造、控制越境信息流在国际的流动、内政外交决策过程和结果的透明度等方面。外交包括政府外交和公共外交。从政府外交来看，主要通过国家元首的相互访问、外交发言人制度、政府间的国际组织国际会议，向国际社会传达有关本国对国际格局、国际安全、和平与发展的基本判断和对国际重大问题的态度的信息，并阐述本国外交政策和对外战略；从公共外交角度来看，则是通过鼓励或组织本国的经济、社会、文化等非政府组织参与国际社会的各种活动，以及通过各种媒体传达本国民众对国际事务的见解、支持或反对其他国家的政策

以及推进形成国际共同价值观念等活动。国家的信息战略主要体现在政府外交方面，反映了政府直接、主动地认识和影响国际体系的信息结构，而公共外交方面受到政府的引导和影响。

在信息战略的军事与防务层面，就是要立足于获取军事领域的信息优势，涉及军队的信息化改造、战场上对重要战役战术信息的感知和运用、军事冲突过程中信息心理的施加和克服，以及基于信息网络的新型战争比如网络战的应对等。历来各国军事力量的发展，总是先设定假想敌，根据假想敌的军事实力、指挥控制水平和后勤保障能力，来制定相对应的规划。发展军事实力的目标就是一旦发生冲突，迫使敌方按照所期望的方式行动，例如投降、犯错、失败、撤兵、停止敌对行为等。影响冲突各方的决定和应对措施的因素主要有三个，其一，可以量化的物理因素决定的行动能力，包括军队的物质实力和指挥能力；其二，心理层面的采取行动的意志，向对方作出人为决定的决心以及在多种可能行动中进行选择的倾向；其三，感知能力，通过观察形成对局势的判断和理解。第三点是一种抽象的信息因素，可以用准确度、全面性、可行度、不确定性或及时性来进行衡量。无论何种性质的冲突或军事行动，都可以归结为一方强制另一方采取有利于自身目标的行动的过程，在这个过程中，一方可以综合采取三个因素中的一个或多种方法对另一方的应对行动产生综合影响。比如直接对对方的行动能力发动进攻，可以影响对方的意志和改变对方对形势的判断；同样对对方的战场传感设施与通信设备进行攻击，也可以达到影响对方判断形势的能力，并进而影响对方的行动能力和意志的目的。整个过程包含了复杂的信息流动，并构成了冲突中的信息过程。基于国家安全的信息战略就是致力于对现有军事能力进行信息化改造，谋求在冲突中取得信息优势和主导权。

信息战略的技术与制度层面，包含了信息安全与信息保障、信息基础设施的可用性和稳定性、阻止危害本国安全的越境信息流动的技术手段等方面。鉴于信息技术和信息资源在国家的经济、政治和军事领域的重要地位，信息战略需制定保障以信息技术为核心的国家关键基础设施稳定运行的措施。关键基础设施包括“农业、食品、水资源、公共卫生、应急服务、政府、国防工业基地、信息与通信、能源、交通、银行和金融、化工和危险材料、邮政航运等部门的公共和私人机构”。

上述外交、防务和技术三者是一个有机的整体，共同构成了美国维护国家安全的管理体系的战略出发点。

**（2）组织机构层**

具体地讲，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，这不仅体现为其设立了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亲自领导。20 世纪 90 年代以来，美国相继成立、改组了一些有关信息保障、信息安全和信息作战的机构和部门。由于信

息战略的综合性特征，这些机构也跨越多个部门。

美国国家信息保障事务主要由美国国防部下属的国家安全局和全国计算机安全中心负责。美国国家安全局主要负责保密信息系统的信息安全工作。全国计算机安全中心具体落实国家安全局负责的信息安全工作。

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，还被赋予整合和协调美国联邦关键基础设施保护职责，统一负责协调计算机和物理基础设施保护的行为，并将保护信息基础设施放在首要位置，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。2002 年 9 月美国国土安全部宣布成立国家计算机安全局（NCSD），其任务是应急处理主要的计算机安全事件、帮助进行信息恢复、发出警告、指导当前计算机空间分析等，旨在抗击针对政府部门和互联网的攻击行为。国家计算机安全局的未来定位是“国家安全计算机空间战略”，它将更多地依靠非政府性业界合作，保护国家计算机资产，进而保护国家重要基础设施。

在国家安全信息的获取与流动控制方面，在国家安全委员会下成立了安全保密政策委员会和信息系统安全保密委员会，以及国家安全情报中心和国家情报评价小组，加强对有关国家安全的信息的获取和向外发布有关政策信息。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。

在保护国家关键基础设施方面，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，保护关键基础设施总统委员会的职责是研究国家重要支持系统的关键基础设施，发现它们的弱点、提出将来对其进行保护的办法，其成员包括来自联邦政府和企业的代表。此外，美国政府还成立了一些组织和机构来负责具体领域的信息基础设施的保障工作，例如 2000 年，美国国家安全委员会成立了第三支信息数字化部队，专门负责信息高速公路和数字化战场上秘密信息和敏感信息的安全保卫管理，该部队还被赋予保卫美国国家金融系统不受敌对国家信息攻击破坏的任务。

军队的信息化改造主要是在国防部及其下属机构中进行。美国军方设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。

此外，行政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；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由财政部领导等；国家标准与技术研究院（NIST）为商务部下属机构，在信息安全领域，该部门协助美国政府和产业界进行安全规划、风险管理、应急计划、加密、人员身份认证及智能卡应用等安全技术的开发、推广、计算机病毒检测与防治、安全教育培训等工作，同时负责制定安全技术和安全产品的国家、国际标准。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中心（CERT）。

奥巴马执政以来，也出台了一系列信息安全机构的调整政策，包括为了改善美国政府、民间力量和军方在应对网络突发事件时各自为政的局面，而增设白宫网络安全事务协调官和白宫网络安全办公室。后者负责统筹全国网络安全事务，高于军队和政府情报部门，直接对国家安全委员会和总统负责。体现了信息安全领导权的集中策略。为了提高网络攻防能力，2009年6月，美国国防部正式创建网络战司令部，有关其使命的许多方面是保密的。该司令部于2010年10月投入运行，隶属于美国战略司令部，是网络安全办公室的一个有益补充。外界将此变动看做是“从被动响应到积极防御的战略转变”，甚至有人认为美国此目的在于实施“先发制人”政策。

**（3）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，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。

2002年，美国就通过了《联邦信息安全管理法案》（FISMA）。FISMA是《2002年电子政务法案》的第三部分。2009年8月13日，美国政府又通过了《美国信息与通信增强法案》修订法案（U.S.ICE），将之作为FISMA所规定的IT安全规范指导的更新。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。

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。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。2008 年，美国政府还推出了“曼哈顿计划”，这一绝密计划表明美国对信息、网络安全方面的威胁的重视已经不亚于对核武器和生化武器威胁的重视程度。同年，美国总统还签署了第 54 号总统令，提出《全面国家网络安全计划》。

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。在遵循政府有关部门政策和法令的同时，美国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。

**2.技术体系**

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的。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。

（1）在密码认证、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。

（2）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 20 世纪 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。

（3）美国一向注重培养信息安全人才。近年来，为了研发信息技术和保障信息安全，美国政府通过一系列决议增强信息安全人才储备。比如《网络安全研究和发展法案》修正案旨在促进学校、大学和制造技术推广中心的合作；2010 年 6 月 29 日，通过了未来 5 年内推进全国高校网络安全课程的提案。

（4）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 台根服务器有 10 台在美国，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。

（5）为了实现信息优势，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。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，留“暗门”、设“木马”，也是美国实施反侦探的手段之一。

**3.评估体系**

信息安全风险评估是风险评估理论和方法在信息系统中的运用，是科学分析理解信息和信息系统在机密性、完整性、可用性等方面所面临的风险，并在风险的预防、风险的控制、风险的转移、风险的补偿、风险的分散等之间作出抉择的过程。所有信息安全建设都应该是基于信息安全的风险评估。只有在正确地、全面地理解风险后，才能在控制风险、减少风险之间作出正确的判断，决定调动多少资源，以什么样的代价，采取什么样的应对措施去化解、控制风险。

20 世纪 90 年代末至 21 世纪初，美国的安全风险评估体系处于以信息系统为对象的信息保障阶段，计算机网络系统成为关键基础设施的核心。2000 年前后，由于国际范围内出现了大规模黑客攻击，信息战的理论逐步走向成熟，且美国的军、政、经济和社会活动对信息基础设施的依赖程度空前，迫使美国又开始了对信息系统新一轮的评估和研究，产生了一些新的概念、法规和标准。

一直以来，美国高度重视网络与信息系统安全评估工作。在军方提出信息保障（IA）概念的基础上，《联邦信息安全管理法案》（FISMA）要求每个机构每年必须对其信息安全实践进行独立评价，以确认其有效性。评价的频率视风险情况而定，但不能少于每年一次。这种评价包括对管理、运行和技术三要素的控制和测试。在独立评价的基础上，联邦管理与预算局应向国会上报评价汇总结果，而联邦审计署则需要周期性地评价并向国会汇报各机构信息安全策略和实践的有效性以及相关要求的执行情况。2009 年通过的 U.S.ICE 授权国家标准和技术研究所（NIST）作为制定 IT 安全规范指导的重要机构。

美国对信息安全标准体系有着系统的规划。随着信息保障研究的深入，保障对象明确为信息和信息系统；保障能力明确来源于技术、管理和人员三个方面；认识到 CC 和 FI PS 140-2 等标准仅仅适合安全产品的测评认证，对于信息系统则需要确立新的包括非技术因素在内的全面评估后，逐步形成了风险评估、自评估、认证认可的工作思路，而风险评估工作贯穿于认证认可工作的各个阶段中，且实现了制度化。NIST 负责为实现美国联邦政府信息安全的目标制定安全标准，并专门启动了《信息系统安全认证认可计划》，该计划后来更名为《信息系统安全保护计划》。此计划分为两个阶段，在第一阶段制定如下的标准和指南：联邦信息和信息系统的安全分类标准；联邦信息系统推荐的安全控制指南；联邦信息系统安全控制的评估指南；在第二阶段，要求美国国内建立一个国家级的、由经过认可的机构组成的网络，使这些机构能基于相关的标准和指南为联邦政府提供经济、高效、高质量的信息安全评价服务。NIST 还颁布了 SP 800-37《联邦信息系统认证认可指南》，提出了美国联邦信息系统认证认可工作的角色和职责、工作任务和具体要求。

同时，美国非常重视信息安全测度指标体系的研究。2006 年 4 月美国发布的《联邦信息保障研究开发规划》，提出要用安全测度指标来衡量网络与信息系统安全措施的有效性，以改进安全审计、指导安全项目投资。2005 年 2 月，美国总统信息化顾问委员会于 2005 年 2 月向布什总统提交的《计算机安全：转折期的研发重点》（*Cyber Security：A Crisis of Prioritization*）报告中将建立信息安全测度标准列为十大优先研究领域之一。该报告认为：不少科学领域已经建立了通用的评价标准，信息安全的评价体系亟待开发。

## 三 评价

作为互联网的发源地，美国对信息安全问题的关注早在 20 世纪 80 年代就已经开始。而今，作为世界首屈一指的信息强国，美国的国家信息安全体系相较于其他国家来说是比较先进与完善的。管理体系、技术体系和评估体系之间的相互结合补充使得整个体系能够始终保持稳定性、安全性和高效性。

十几年来，美国政府一直努力构建一套全面并且严密有效的信息安全监管体系，尤其是“9·11”恐怖袭击事件的冲击使得美国对信息安全的必要性有了更进一步的认识，并且促使美国更加重视对制度体系的完善。美国的信息安全保障体系日益呈现出“规范化”、“法制化”的特点，监管措施也越来越周全、到位。为了巩固在信息领域的领先地位，并进一步扩大与其他国家的“信息鸿沟”，美国政府不满足于仅防护本国安全，还根据当前国际形势，制定了多项措施来推行“扩张性质”的信息安全政策。

通过近两年来美国信息安全的战略和政策变化等方面可以看出，奥巴马政府高度重视信息安

全在美国国家安全战略中的作用。奥巴马曾经宣布，要把保护美国计算机网络

的安全作为美国国家和经济安全的最优先项目。美国的国家信息安全战略已经进入了“网络威慑”期，经历了从“预防为主”到“先发制人”、从“控制”网络基础设施到“控制”信息流动的演化历程。而美国商务部将无限期保留对 13 台域名根服务器的监控权，和其中的 10 台设在美国这一现实，更是使全世界都认识到美国拥有着控制互联网“总闸”的特权，或许美国正朝着通过互联网来控制世界的终极目的迈进。2010 年，奥巴马政府颁布的《国家安全战略报告》改变了布什时期的单边主义做法，强调与外界合作对话，体现了奥巴马强调多边外交重于军事力量的想法，这一方案提出利用外交、经济革新、发展援助、军事力量以及教育，达到提升美国影响力的目的。

尽管美国政府对信息安全的保障措施越来越规范化、法制化，并且取得了一些效果，但其中也存在一些问题：

（1）“9·11”事件之后，美国行政部门相对于立法部门获得优势地位，但近几年的信息安全立法更像是信息安全主管权的争夺战。互联网本身过于活跃和不确定的属性导致网络监管体系越来越复杂，比如国防部、国家安全局、国土安全部之间存在着一定程度上的职能冲突，而一些新机构有严重的人员短缺现象。没有一个统一的部门可以负责制定相关安全政策，而信息安全各大相关部门都意图通过立法争夺信息安全主管权。不过奥巴马政府认识到这一点，并意图改善这一现象，这也是奥巴马设立白宫网络安全办公室的初衷。

（2）美国人一直最尊重民主和自由，强调个人隐私的保护，但在“9·11”事件之后当国家信息安全面临巨大威胁的时候，民众自主牺牲个人权利为国家利益让步。但是现在美国社会对行政权力日益膨胀的担心日趋严重，使得社会各界对于“开放”与“控制”的均衡和“控制”手段的争论一直十分激烈。

通过前文对美国国家信息安全体系的分析归纳，可以得出一些经验、教训以及启发：第一，管理体系作为国家信息安全体系的基础支撑，应当为技术体系提供更多的法律支持、政策支持，提供更多制度标准保证；第二，管理体系不能过于庞杂，甚至出现权力冲突，应当有统一的权力机构，将管理权力集中起来，下设其他组织，协调好权力划分问题，从而形成金字塔式的健康架构；第三，制定管理战略和政策法规的同时，要注意公众隐私和群众知情权，找到“管”和“放”的平衡点，在不影响公众情绪的同时，保障国家信息安全；第四，从奥巴马政府新发布的《国家安全战略报告》可以看出，美国开始通过谋求国际合作解决信息安全问题，事实上互联网的跨国特性和世界经济相互