美国国家网络安全战略

THE US NATIONAL CYBERSECURITY STRATEGY

沈 逸◎著

时 事 出 版 社

美国国家网络安全战略

THE US NATIONAL CYBERSECURITY STRATEGY

沈 逸◎著

时 事 出 版 社

图书在版编目（CIP）数据

美国国家网络安全战略/沈逸著. —北京：时事出版社，2013.11
ISBN 978-7-80232-653-8

Ⅰ.①美… Ⅱ.①沈… Ⅲ.①计算机网络—国家安全—国家战略—研究—美国 Ⅳ.①D771.235②TP393.08

中国版本图书馆 CIP 数据核字（2013）第 234375 号

出 版 发 行：时事出版社
地　　址：北京市海淀区巨山村 375 号
邮　　编：100093
发 行 热 线：（010）82546061　82546062
读者服务部：（010）61157595
传　　真：（010）82546050
电 子 邮 箱：shishichubanshe@sina.com
网　　址：www.shishishe.com
印　　刷：北京百善印刷厂

开本：787×1092　1/16　印张：21　　字数：250 千字
2013 年 11 月第 1 版　2013 年 11 月第 1 次印刷
定价：68.00 元
（如有印装质量问题，请与本社发行部联系调换）

序　一

世界已进入信息时代，网络安全是世界各国面临的新问题。进入21世纪之后，网络安全问题迅速凸显，无论是伊朗遭遇的“震网”病毒袭击、.cn域名遭遇的分布式拒绝服务攻击、名为“叙利亚自由军”黑客攻击美联社账号并引发股市动荡，还是美国国防部历次“网络风暴”演习中模拟的网络攻击场景，都确凿无疑地说明，网络安全确实已经成为了足以影响乃至挑战国家安全的重要问题。主权国家如何应对来自网络空间的安全挑战和威胁，成为国家安全战略制定者们必须面对和回答的问题。

作为互联网发源地和掌握了网络技术优势的美国，在网络安全战略实践上同样有着比较显著的先发优势。2011年美国制定并发布《网络空间国际战略》，2013年中央情报局前雇员斯诺登披露“棱镜”系统，证明美国国家安全局具有监控互联网信息流动的能力。由此提出的问题至少包括：如何认识美国的国家网络安全战略？这一战略的发展脉络、主要特点以及对中国的影响是什么？

在此背景下，复旦大学国际关系与公共事务学院沈逸博士撰写并出版了《美国国家网络安全战略》一书，对上述相关问题做出了比较系统、全面的回答，为所有关心网络安全问题的人及时提供了有益的参考。《美国国家网络安全战略》一书涵

盖了美国国家网络安全战略发展、演进的整个阶段，从网络诞生之前到2013年的“棱镜”事件，在比较充分地占有公开材料的基础上，沈逸博士运用其国际政治的视野，从国家安全战略的视角出发，对美国国家网络安全战略展开了细致、全面、深入的分析。这有助于人们更加全面地认识和理解美国国家网络安全战略的实质，也有助于推动建设和完善中国自身的国家网络安全战略。

相比其他网络安全的研究成果，《美国国家网络安全战略》一书的显著特点，是从国家安全战略的分析框架和视角出发，尝试整体性地把握美国国家网络安全战略的核心特征。沈逸博士在书中将美国国家网络安全战略的主要特点概括为防御、控制和塑造，并且指出，三者在不同时期会因为美国国内政治环境等非技术因素的变化而产生相应的变化。这一分析是比较准确的，也是比较重要的，因为它有助于人们从非技术的角度，把握美国国家网络安全战略的本质特征，进而比较均衡地认识和分析美国网络安全战略的实践。

从历史和实践的视角出发，结合一定的国际关系理论分析框架，对美国国家网络安全战略展开阶段性的深入分析，是此书第二个比较显著的特点。国家网络安全，是一个有着重大理论意义和实践意义的课题，对国家网络安全战略的研究，不仅要展开理论探讨，更要为实践服务。本书作者沈逸博士紧扣历史演进的脉络，以标志性的事实和代表性的政策文件为分析节点，将美国国家网络安全战略分为三个阶段进行分析，从而比较清晰地将美国国家安全战略的全貌呈现在读者面前。书中收录的代表性案例，有助于人们对美国网络安全战略的实践形成比较深刻的理解和认识，也显示了沈逸博士的研究能力。

从中国的国家利益需求出发研究美国的国家网络安全战

略，是本书第三个比较显著的特点。国际关系的研究、国家安全的研究，需要服从和服务于国家战略利益的诉求。沈逸博士研究美国国家网络安全战略的目标十分明确，就是为中国的国家利益服务，让中国在制定和确立国家网络安全战略的过程中有切实的经验和依据。由此使得本书的论述比较深刻，能够帮助对此问题有兴趣的读者明晰美国国家网络安全战略的本质。希望此书的出版能够让更多的研究者投身于相关问题的研究，推进研究深入的同时，也能够为推动中国网络安全战略建设贡献力量。

自2005年开始至今，沈逸博士长期跟踪研究美国国家网络安全战略的发展变化，搜集了大量的材料，包括文件、案例，并运用其国际关系和国际安全的研究背景，展开了比较有效的跨学科研究。2011年他在《文汇报》上发表《互联网绑上美国外交政策战车》一文，引起了比较广泛的关注，自那时开始，沈逸博士经常主动向我汇报其研究心得和主要成果，是一个专心致力于网络安全研究的青年学者。他所具有的国际关系学科背景，使得他能够顺利地开展跨学科研究，他对美国网络安全战略的研究，在国内具有一定的领先水平，体现了沈逸博士本人以及复旦大学国际关系与公共事务学院在相关研究领域所具有的学术底蕴。我很荣幸能够为此书作序，同时希望沈逸博士能够在今后的研究过程中，形成更多、更加精彩的研究成果，不断进步。

何德全

2013年10月于北京

序　二

在沈逸博士所著的《美国国家网络安全战略》即将付印之际，很高兴应作者和责任编辑之邀为此书写一序言。

信息安全，特别是网络安全，已经成为当代国家政治以及国际关系的一个重要问题。一方面，任何国家都必须充分利用网络技术最大限度地促进自身的利益，与此同时又必须防止其他国家通过网络技术损害自身的权利。另一方面，网络技术既为国家间的合作开辟了新的巨大空间，同时又会造就和加剧国家间的冲突。正因为如此，近年来，网络安全已经成为许多学者和专家所关注的一个重要课题。

网络安全问题可以从纯技术方面进行研究，但是却不能从纯政策方面进行研究。换言之，如果一个社会科学学者希望涉足这一领域，就必须在网络技术方面具备一定的基础。幸运的是，沈逸不仅掌握了国际关系研究所需的知识、理论和方法，而且对新兴的信息科学显示了特殊的兴趣和才能。

沈逸是一个典型的“复旦人”，先是在复旦大学国际关系和公共事务学院（原来的国际政治系）度过了十年求学生涯，完成了他的本科生和研究生阶段的学习，获得了博士学位。此后，沈逸就一直留在国际关系和公共事务学院任教。还在学生时代，他就对计算机显示了浓厚的兴趣，成了系里

的“电脑专家”。因此，在确定博士论文选题时，他就把对美国对外政策的关注与自己对网络技术的熟悉结合了起来，致力于研究美国信息安全政策问题。他的博士学位论文《开放、控制与合作：美国国家信息安全政策分析》集中显示了他在这两个方面的能力的成功结合。从当时来说，这篇论文具有明显的前沿性。

该论文较好地将理论工具用于现实问题的探讨，既研究了信息安全这一新的非传统安全问题，又从控制与合作这两个方面分析了美国的信息安全政策。具体地说，它从“认知”这一具有桥梁作用的概念出发，将基于杰维斯认知理论的决策者认知形成分析和基于温特建构主义途径的环境—行为体的互动联系起来，建立了分析国家信息安全政策的“认知—建构”的理论框架。以此框架为工具，论文进而通过文本和案例分析研究了美国国家信息安全政策的发展与演变过程。

沈逸在论文中具体提出：决策者的认知因素对美国国家信息安全政策的制定至关重要，关于国家信息安全认知的变化构成了推动美国国家信息安全政策变化的主要动力；美国国家信息安全政策制定过程的实质是决策者在“开放”与“控制”这两种手段中进行比较和选取的过程；总的来说，美国已经建立起了一套以“有限开放、积极管制和谨慎合作”为特点的国家信息安全政策；国际合作始终是美国国家信息安全政策的组成部分，但是，美国也指望通过国家间的合作在全球范围内实现对信息的严格控制。

该论文得到了参与评审和答辩的专家的普遍好评，当时本人就相信，如果这一论文能够在经过进一步修改以后得以出版，对于促进信息安全这一非传统安全问题的研究和我国的相应政策的制定都会具有相当的推动作用。所以，现在看到了沈

逸这本著作的出版，我是感到非常欣慰的。

《美国国家网络安全战略》一书无论是在基本观点和基本框架方面都是对原来的博士论文的继承。但是，它也有了重要的发展。与论文相比，该书的主要变化可以用“深化”和“扩大”两个词加以概括。所谓深化，一是将研究范围从国家信息安全浓缩于国家网络安全（这是两个相互关联但是其内涵和外延都并不相同的概念）；二是更加深入地探讨了网络技术与国家安全乃至国际安全的关系。所谓“扩大”，一是指延伸了考察美国信息安全战略的时间跨度，直至包括了作者完成书稿的2013年；二是增加了对美国网络安全战略所涉的文件和个案的分析。上述的这些变化就使本书具有更强的现实性和针对性，同时整个研究也能建立在更加扎实的理论和材料的基础上。

与此同时，《美国国家网络安全战略》一书也反映了近年来沈逸在网络安全以及美国的相关政策方面所作的新的研究和取得的新的成果：一方面，它们分析了网络技术的迅速发展和普遍应用对国际政治和国际关系造成的冲击。例如，从谷歌退出中国这一事例出发，《应对“明日帝国”的挑战：全球化时代的资本、信息与国家》一文（载于《国际社会科学》中文版，2010年3月）指出，国际体系正在经历着一种深刻变化：占有垄断技术优势的跨国公司与具有综合实力优势的国家正在形成一种“松散的联盟”，对于成为其目标的国家而言，它们所面临的是某种类似007系列电影《明日帝国》一片中所揭示的那种新型挑战，即具有垄断媒体与操控舆论能力的媒体大亨有可能同时在现实和虚拟世界中对主权国家提出尖锐而直接的挑战。《网络政治：特性、挑战及其限度》一文（与刘建军合著，载于《国际观察》，2012年第2

期）提出，2009 年至 2011 年发生在国际舞台上的诸多重大事件，背后都具有互联网发展、全球信息空间拓展、新媒体应用蔓延所带来的政治效应；网络政治带来的挑战在广度、深度、速度和力度方面都远远超过人们的想象。另一方面，沈逸最近发表的论文揭示了美国网络安全战略的新变化及其对中美关系带来的影响。譬如，《数字空间的认知、竞争与合作》一文（载于《外交评论》，2010 年第 2 期）认为，在奥巴马政府任期内，随着美国国家信息安全战略的调整，网络安全问题正在成为一个影响中美战略关系的重要变量，所谓“中国黑客威胁”问题对中美战略互信形成了一定程度的挑战。《应对进攻型互联网自由战略的挑战》一文（载于《世界经济与政治》，2012 年第 2 期）则着重讨论了中美在全球信息空间的竞争与合作。其中强调，自奥巴马入主白宫以来，美国的网络空间战略已经发生了重要而显著的变化，逐渐改变了其原有的以防御为主要特征的网络空间战略，转而发展并初步完善了一套以“互联网自由”为核心概念、以“控制－塑造”为基本特征的进攻型互联网自由战略，以期形成有利于美国的网络空间环境，争夺、树立并确保美国在网络空间的领导地位；这一战略的成型将对中美关系产生复杂的影响，两国将在全球信息空间展开复杂而微妙的博弈。显然，这些观点都在该书中得到了体现和发展。

总之，沈逸的《美国国家网络安全战略》一书给我们展示了国际关系/国际政治研究领域的一个新的分支，使我们从技术和政策结合的角度了解到什么是网络安全问题、这一问题对国家主权和国际政治造成的冲击、美国为了自己的利益制定的网络安全战略以及这一战略对中美关系造成的影响。它具有重要的政策意义和学术价值。沈逸能够写出这样一本书来是同他

在国际政治和信息技术方面具有的颇为扎实的基础分不开的，同时也是他多年辛苦耕耘的结果。

朱明权

2013年10月15日于上海

目　录

前　言

网络化时代的国家安全

2013 年 3 月，美国网络安全公司曼迪亚特发布报告，宣称“中国人民解放军网络战部队发动对美国公司的黑客攻击，窃取商业机密”。报告发布之后不到两天，奥巴马政府发布行政战略文件，以消除窃取美国商业机密所带来的威胁；奥巴马在致电新当选的中国国家主席习近平时，首先提到的是黑客威胁以及网络安全问题。[①] 同样在 2013 年 3 月 12 日，美国国家安全局局长、网络司令部司令亚历山大向国会坦诚美国正在建设网络战部队，其中包括 13 支进攻性网络战部队和 27 支防御性网络战部队。[②] 此番讲话后不久，首先是朝鲜宣布遭遇大规模分布式拒绝服务攻击，随后是韩国宣布部分媒体与银行的电脑网络遭遇分布式拒绝服务攻击；朝鲜认定袭击来自美国和韩国，韩国先是说“朝鲜嫌疑最大”，接着说攻击源头 ip 地址来自中国，紧接着又改口说这地址被韩国银行私设，来自韩国国内，最后判定攻击源头

---

① Reuters，“Obama，China's Xi Discuss Cyber Security Dispute in Phone Call”，http：//www. globalsecurity. org/military/library/news/2013/03/mil - 130314 - voa14. htm，March 14，2013，（上网时间：2013 年 6 月 19 日）

② John Reed，“Cyber Command fielding 13 ‘offensive’ cyber deterrence units”，http：//killerapps. foreignpolicy. com/posts/2013/03/12/us_ cyber_ command_ developing_ 13_ offensive_ cyber_ deterrence_ units，March 12，2013（上网时间：2013 年 6 月 19 日）

来自欧美。①

此后，2013 年 4 月，自称“叙利亚电子军”的黑客组织，借助植入了“木马”程序的“钓鱼邮件”，窃取美联社官方账号，发布消息称“白宫发生两次爆炸，奥巴马总统受伤”。消息发布 2 分钟内，计算机程序控制的交易系统大量抛售高风险资产，比如原油、美国十年期国债以及各种股票，道琼斯工业平均指数因此在 2 分 30 秒内下跌了 150 点。5 分钟后，美联社借助其他账号发布辟谣信息，道琼斯指数也收复失地，但黑客袭击行动凸显了网络时代国家安全面临的来自网络空间的特殊威胁。②

2013 年 6 月 15 日，由 29 岁的美国前国安局合同工斯诺登（Snowden）披露的“棱镜”（PRISM）项目，向全世界证实，美国政府可通过与掌握网络关键应用、技术和数据的跨国企业密切合作，具备对整个互联网进行实时监控的能力，而且这种能力事实上已经投入了使用之中，成为这种监控能力目标的，既包括中国这样的潜在竞争者，也包括德国这样美国公开的盟友。③

上述事例，凸显了网络时代的国家安全问题：发生在互联网空间的事件、行为，越来越紧密地与国家安全联系在一起。用美国总统奥巴马的话来说，来自网络空间的威胁挑战了美国的国家安全与经济安全，而美国总统国家安全事务顾问多尼隆则表示：

---

① Brian Donohue，“South Korea Blames North Korea for March Cyberattack”，http：//threatpost. com/south-korea-blames-north-korea-march-cyberattack-041013/，Apr. 10th，2013（上网时间：2013 年 6 月 19 日）

② David Jackson，“AP Twitter feed hacked；no attack at White House”，http：//www. usatoday. com/story/theoval/2013/04/23/obama-carney-associated-press-hack-white-house/2106757/，Arp. 23rd，2013（上网时间：2013 年 6 月 19 日）

③ Gellman，Barton；Poitras，Laura，“US Intelligence Mining Data from Nine U. S. Internet Companies in Broad Secret Program”，*The Washington Post*，June 6th，2013.

“国际社会不会容忍任何国家的此类行动（威胁网络安全的行动）。”①

因为上述美国对网络安全的关切，2013 年 6 月在美国举行的“习奥会”上，网络安全议题成为了中美两国领导人峰会的关键议题之一，其在国家安全议程中的重要性，变得显而易见。②

无论是曼迪亚特公司发布安全报告，美国政府发布应对威胁的策略，还是韩国与朝鲜面临来自网络空间的威胁，又或者是美联社“推特”账号遭遇袭击事件，以及美国的“棱镜门”，都是当今世界面临的全新挑战，即来自网络空间的网络安全挑战的具体表现。从最一般的意义上来说，应对网络安全的挑战，即来自信息技术发展以及在此基础上形成的全球网络空间③的安全挑战，正逐渐成为世界各国政府在信息时代的首要任务。在此过程中，最显著的表现以及在某种意义上最重要的分析对象，就是各国政府制订的网络安全战略。这些战略中所设定的目标、酝酿的规范以及偏好使用的实现战略目标的各种工具，必然对网络空间以及整个国际体系产生深刻而直接的影响。

---

① Reuters, “Obama, China's Xi Discuss Cyber Security Dispute in Phone Call”, http: //www. globalsecurity. org/military/library/news/2013/03/mil-130314-voa14. htm, March 14, 2013.

② Christi Parsons, “Obama presses cyber security issue in first talks with Xi”, http: //www. latimes. com/news/world/worldnow/la-fg-wn-obama-cyber-security-xi-20130607, 0, 2882418. story, June 7th, 2013（上网时间：2013 年 6 月 19 日）

③ 网络空间，对应英文为 Cyberspace，鉴于现有诸多文献中经常出现“信息空间”、“网络空间”、“赛博空间”等不同译法，本书统一使用“网络空间”这一概念，除非特别说明，本书中有关“信息空间”、“网络空间”、“赛博空间”这三个词在相同意义上使用，均指代由遍布全球的信息基础设施、在其中生产、存储、交换和流通的信息以及相关的用户所构成的复杂系统。而对本书的核心概念“网络安全”（Cyber Security）与“信息安全”（Information Security）、“互联网安全”（Internet Security）以及“网络安全”（Network Security）之间也存在重叠与差异之处，这些重叠与差异，将在本书第一章进行相关的辨析和界定。

从最宏观的层次上来说，网络安全问题的出现，以及各国对网络安全问题的关注，首先是由信息技术的发展以及全球网络空间的变迁所决定的。

一、信息革命挑战国家安全

广义上信息流动与国家安全之间的关联源远流长，北约研究网络战的文件明确指出，在主权国家诞生的1648年，对信息流动的控制已经成为国家主权最为重要的特征。当时的信息流动，是指宗教信息的流动；国家主权的特征，就是主权者有权控制国家地理边界范围内流动的与宗教信仰相关的信息。依据这一渊源，北约认为，从网络基础设施以及与此相关的活动来看，主权意味着国家有权控制处于其领土范围之内的网络基础设施以及发生在其领土范围之内的网络空间的活动。①

除了追溯到1648年的源起之外，网络安全比较近的渊源，则至少可以追溯到两次世界大战前后，特别是第二次世界大战结束之后，美国等国家政府的相关部门正式确立了主权国家对信息流动实施管理和控制的合法性原则：和平时期为了维护国家安全，政府有权合法地进行信号情报拦截行动，这种拦截行动，意味着通过各种手段监控跨越国境的信息流动。②

而导致全球网络空间产生、扩展和蓬勃发展的互联网革命，就是作为一个连续的历史进程的组成部分，发生在上述现实世界的结构之中的。这一互联网革命的本质，源自于信息处理和通讯

---

① Michael N. Schmitt ed., *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, "Section 1: Sovereignty, Jurisdiction, and Control", US Navy War Colleague, March. 2013, pp. 15 - 16.

② Legality of Signal Intelligence Activities, Memo for the Secretary of War, Aug. 16th, 1945.