CICIR 中国现代国际关系研究院中青年学者纵论

日本网络安全战略研究

韩　宁◎著

它是快速成长中的网络强国，它技术先进，野心勃勃，它将网络空间作为其重获大国地位的抓手，它就是日本！

时事出版社

日本网络安全战略研究

日本网络安全战略研究

韩　宁◎著

时事出版社
北京

图书在版编目（CIP）数据

日本网络安全战略研究/韩宁著. —北京：时事出版社，2018.2

ISBN 978-7-5195-0160-0

Ⅰ.①日… Ⅱ.①韩… Ⅲ.①计算机网络—国家安全—国家战略—研究—日本 Ⅳ.①D731.336②TP393.08

中国版本图书馆 CIP 数据核字（2017）第 314171 号

出 版 发 行：时事出版社
地　　址：北京市海淀区万寿寺甲 2 号
邮　　编：100081
发 行 热 线：（010）88547590　88547591
读者服务部：（010）88547595
传　　真：（010）88547592
电 子 邮 箱：shishichubanshe@sina.com
网　　址：www.shishishe.com
印　　刷：北京朝阳印刷厂有限责任公司

开本：787×1092　1/16　印张：19　字数：238 千字
2018 年 2 月第 1 版　2018 年 2 月第 1 次印刷
定价：102.00 元
（如有印装质量问题，请与本社发行部联系调换）

目　录

绪　论

第一节　选题立论依据

一、选题依据和背景

20世纪兴起的信息通信技术（Information and communication technology，ICT）是人类最重要的发明之一，给人类生活带来了巨大变化。从20世纪60年代至今，信息处理和通信技术的革命已经在全球创造了一个将不同类型行为体密切连接的网络空间。[①] 这个网络空间在造福人类的同时，引发了一系列问题，把这些问题归纳起来，就是我们所说的网络安全问题。美国国家情报委员会在2000年12月的一份研究报告中指出，“信息革命是18世纪工业革命以来最重大、最有意义的全球性变革。”[②] 习近平总书记于2016年4月19日在“网络安全和信息化工作座谈会”上指出，“从社会发展史看，人类经历了农业革命、工业革命，正在经历

① Yochai Benkler, “Form Consumers to Users: Shifting the Deeper Structures of Regulation Towards Sustainable Commons and User Access”, 52 Fed. Comm. L. J. 561, 2000.

② U. S. National Intellience Council, “Global Trends 2015: A Dialogue about the Future with Nongovernment Experts”, December 2000, https://www.cia.gov/library/readingroom/docs/DOC_0000516933.pdf（上网时间：2016年8月9日）。

信息革命。农业革命增强了人类生存能力，使人类从采食捕猎走向栽种蓄养，从野蛮时代走向文明社会。工业革命拓展了人类体力，以机器取代了人力，以大规模工厂化生产取代了个体工厂手工生产。而信息革命则增强了人类智力，带来生产力又一次质的飞跃，对国际政治、经济、文化、社会、生态、军事等领域发展产生了深刻影响。”①

当前，网络空间（cyber space）正在与现实空间快速融合，并随着物联网、云计算、移动互联、大数据、虚拟现实（VR）等众多计算机信息技术及概念的不断涌现和应用，与之快速地相互渗透，犹如整个社会的神经系统，已经无限地延伸到世界各国政治、经济、军事、文化等方方面面，人类社会的生活因此产生新的空间，人类社会的生产和生活方式因此发生重大变革，人类社会的思维和观念因此受到巨大冲击，人类认识世界、改变世界的能力也随之不断增强。

随着互联网的普及和信息技术的进步，网络安全风险日益加剧，网络空间的脆弱性不断显现，具体表现在：一是网络风险的“多米诺骨牌效应”不断增强。随着网络虚拟空间和人类现实空间的快速融合，网络风险从虚拟社会渗入现实社会，任何细微的风险都可能如多米诺骨牌一样，由一个很小的初始变量引发多领域的一系列连锁反应，形成难以想象的巨大风险，甚至带来难以估量的重大损失；二是网络难以实现绝对的安全。随着云计算、大数据、物联网技术的普及和发展，网络泛化已成为不可阻挡的趋势。在万物皆可互联的物联网时代，万物皆可成为网络攻击目标，万物也皆可成为网络攻击的借助对象，网络只有相对安全，而无绝对安全可言；三是网络威胁范围更广。网络在造福人类的

① 《习近平在网络安全和信息化工作座谈会上的讲话（2016年4月19日）》，《人民日报》2016年4月26日，第2版。

同时，也带来了更大范围的风险，从个人信息泄露，到财产和知识产权被窃取，再到恐怖袭击甚至国家间战争，可以说网络威胁已经无处不在；四是网络风险与人们现实生活日益接近。2017 年 5 月，不法黑客利用美国国家安全局网络武器库中泄露出的“武器级”黑客工具，制造出一种勒索软件“想哭”（Wanna Cry），短时间内该软件在全球肆虐，使医疗、电力、能源、银行、交通、教育等多个行业和机构受到严重影响，让人们深切感受到黑客就在身边、网络风险就在身边。

与此同时，各国网络安全也面临着三大挑战，分别是：（1）政府掌控的网络安全资源有限。现实空间的安全具有战略性、集中化、自上而下的特点，政府掌握着安全资源，提供相关公共产品，占据着主导和垄断地位。而网络安全则具有商业化、分散化、自下而上的特点，特别是西方发达资本主义国家 80% 的网络关键基础设施都掌握在私营部门手中，私营企业往往在网络安全中发挥着重要作用，政府难以全面掌握安全资源。网络安全已经上升为国家安全问题，政府如何与私营企业协调，全面掌握并支配网络安全资源，成为待解难题。（2）网络安全与隐私保护的矛盾突出。随着“维基解密”“斯诺登事件”的不断曝光，民众对各领域的网络管理产生信任危机，网络安全与隐私保护间的矛盾日益突出。加拿大国际治理创新中心（CIGI）2016 年的一份调查报告显示，仅有 37% 的网民相信他们的网络活动没有遭到监控，46% 的网民认为他们的网络活动并未受到任何审查，1/3 左右的网民相信他们的政府为保护其个人数据不受到私营企业侵害而做足了工作。[①] 这意味着 63% 的网民认为他们的网络活动遭到

① Centre for International Governance Innovation & IPSOS, “2016 CIGI-Ipsos Global Survey on Internet Security and Trust”, https://www.cigionline.org/internet-survey-2016（上网时间：2017 年 4 月 20 日）。

监控，54%的网民认为他们的网络活动受到审查，2/3左右的网民不相信他们的政府为保护其个人数据不受到私营企业侵害而做足了工作。民众对政府网络管理的信任度偏低，加大了政府网络安全建设的难度。（3）网络空间自由与规制的平衡问题。网络空间的发展离不开相对开放、自由的环境。政府介入网络安全是双刃剑，在保护网络安全的同时，也限制着网络发展，过度的网络监管必然会影响网络空间发展。规制网络，既不能管死，又不能放任，程度很难把握。

因此，世界各国都在不断完善本国网络安全战略，以适应网络安全现实需求。由于网络治理无先例可循，各国在应对日益复杂的网络安全挑战时，大多沿用各自治理现实空间的思路和做法，形成具有本国特色的网络安全战略。美国、俄罗斯、英国、德国、日本等世界主要大国都先后通过制定网络安全相关法律、发布网络安全战略、指定专门机构等手段来加强本国网络安全，力图在网络空间维护国家安全和国家利益，在国际政治、军事、经济等领域发挥更大作用。世界各国纷纷推出网络安全战略的目的主要有三个：一是加强顶层设计，宣示网络空间主权和利益。在发达国家中，美国连续推出网络安全新政，英国推出网络监管新法案，法国致力于自身网络系统保护，日本通过立法设置国家领导机构等。在发展中国家中，伊朗将网络战列为军队和国家情报机构的首要任务，泰国推出网络安全相关法案和国家领导机构等。目前，世界上已有超过50个国家将网络安全上升到国家战略层面进行规划，并作为总体安全战略的核心内容进行部署和推进落实。二是加强国际合作，提高国家安全保障能力。“斯诺登事件”显示，美国、英国、加拿大、澳大利亚、新西兰组建的“五眼联盟”已经形成有效网络安全合作，美英两国成立了“联合网络小组”并开展网络联合军演，日本与美国等多国开展“网络安全对话”，北约不断完善成员国间网络安全合作等。三是立足网

络权力争夺，参与国际网络空间竞争与合作。美国为首的西方国家利用先进网络技术和设备优势，谋求国际网络霸权，推出“网络威慑”理念，组建集体防御，积极拉拢发展中国家，敌视、打压俄罗斯和中国。这种冷战思维和行为方式严重激化了国际网络空间权力争夺。

在此背景下，日本大力加强和推进网络安全战略，其用心不止于网络安全，必定有着更深层次的战略考量和战术安排，对此，必须深刻剖析、全面认知。当前，中国正在实施网络强国战略，大数据战略和“互联网＋”行动计划已经被纳入“十三五”规划，《网络安全法》《网络空间国家战略》已经出台，国家网络空间治理体系和治理能力的现代化进程正在加速，需要凝聚更多的智慧力量，从国家层面统筹规划，形成结构科学、路线清晰的顶层架构。特别是2016年4月19日，习近平总书记在“网络安全和信息化工作座谈会”上提出了中国网络安全观，要求在网络安全方面，加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力。因此，研究剖析21世纪初以来的日本网络安全建设，了解掌握日本在网络空间的动态规划，对构筑中国特色网络安全保障体系、谋划中国网络安全战略、推进具有中国特色的网络安全建设具有重要现实意义。

二、研究目的

近年来，随着美国“亚太再平衡”战略的实施和日美同盟关系的重新定位，日本急剧“右倾化”，谋求成为“正常国家”的步伐加快，特别是在安倍晋三的直接鼓动和助推下，日本政府否定历史、突破和平宪法限制、梦想“夺回强大日本”，在错误的道路上渐行渐远。在此情况下，网络安全建设

已成为日本梦想实现所谓“正常国家”的一个重要抓手和意图率先突破的领域。因此，对日本网络安全建设进行全面研究，通过分析其特点、实质、趋势和影响，揭示日本21世纪以来网络安全建设的深层动因，透视日美网络安全战略的内在联系，把脉日本网络安全建设发展态势，具有十分重要的战略和现实意义，既可为中国正在进行的网络安全建设提供借鉴参考，也可站在维护并确保中国网络安全的角度，知彼知己，始终保持高度战略警惕。

三、理论和现实意义

在了解网络空间国际政治权力格局基本特征基础上，分析21世纪以来日本网络安全战略发展演变的内在动因，探讨日本在网络空间国际政治权力格局中的地位与处境，评估21世纪以来日本网络安全建设的成果，关乎国际网络空间政治格局的把握和中国多重安全与利益的保护，具有重要的理论与现实意义。

（一）理论意义

1. 廓清“信息安全”“网络安全”和“网络空间安全”的概念

目前，世界各国对上述三个概念仍没有达成一致意见，但是随着各国网络安全战略的不断发展演变，这三个概念逐渐清晰化。

关于“信息安全”的概念。1994年2月28日，美国联合安全委员会出台的《重新定义安全》报告对“信息安全”做出如下定义：“信息系统的安全是新领域，指的是保护在计算机和网络上创建、处理、存储和交换的涉密和非涉密信息的机密性、完整

性和可用性。”[①] 美国学者杜恩·帕克（Donn Parker）在其专著《反计算机犯罪——一种保护信息安全的框架》中，进一步将“信息安全”概念划分为六个层次。一是国家和国防信息基础设施的安全，这些基础设施包括国防信息系统、通信系统（如电台、电视台、电话系统）、电力分配系统、交通系统等。二是信息本身的安全。三是信息系统的安全，这些信息系统包括情报系统、信息传递和交换系统、计算机系统及指挥控制系统等。四是基于信息过程的安全，信息过程指的是信息获取、存贮、交换、传递和处理等各个环节。五是基于计算机网络的安全，主要是防止非法用户进入网络、过滤不良信息。六是信息设备的安全，主要是防止通过发射高能电磁脉冲、高功率微波、声波等使己方信息设备失灵的无线电干扰手段等。[②] 以上述定义为基础，日本确立了自己的信息安全概念，即：“信息安全是确保信息的机密性、完整性和可用性，其措施是保持互联网和计算机的安全使用，防止信息内容泄露和信息数据感染病毒等。”[③]

关于“网络安全”的概念。国际电信联盟（International Telecommunication Union）将“网络安全”定义为“工具、政策、安全概念、安全保障、指导方针、风险管理方法、行动、训练、最好的实践、保障措施以及技术的集合，这一集合能够被用于保障网络环境以及组织和用户的财产。组织和用户的财产包括相互连

① Joint Security Commission, “Chapter 8, Information systems Security”, in “Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence”, February 28, 1994, http://www.fas.org/sgp/library/jsc/chap8.html（上网时间：2016 年 11 月 3 日）。

② ［美］Donn B. Parker 著，刘希良等译：《反计算机犯罪——一种保护信息安全的框架》，北京：电子工业出版社，1999 年版，第 134 页。另可见于蔡翠红著：《美国国家信息安全战略》，北京：学林出版社，2009 年版，第 5 页。

③ 日本总务省网站保护国民信息安全主页，http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/intro/security/index.html（上网时间：2017 年 4 月 28 日）。

接的计算机设备、个人计算机、基础设施、应用、服务器、通信系统以及所有在网络环境里存储或传输的信息。网络安全旨在实现并维护组织和用户资产在网络空间的安全属性，反击网络环境中相关的安全风险。网络空间安全属性包括网络可用、可信度（包括真实性以及不可抵赖性）以及保密性。”① 日本在2014年11月出台的《网络安全基本法》（2014年法律第104号）中给出更加明确的概念，认为，“网络安全是指采取必要措施，防范以电子方式、磁方式及其他不能被人感知的方式（以下称为“电磁方式”）记录、发送、传输、接收到的信息发生泄露、丢失或损坏，对此类信息进行其他安全管理，确保信息系统及信息通信网络的安全性及可靠性（必要措施防范的对象，也包括经由信息通信网络或利用电磁方式制作的用于记录的记录介质（以下称“电磁记录介质”），对电子计算机实施非法活动所造成的危害）等，且该状态得到合理维护管理。”②

关于“网络空间安全”的概念。各国对“网络空间”的认知存在着差别。美国认为，“网络空间是涉及现代社会诸方面的全球范围内互联互通的数字信息及通信基础设施。”③ 英国认为，“网络空间是所有形式的网络数字活动形态，包含通过数字网络进行的操作和内容。”④ 加拿大认为，“网络空间是一个互连的信

① ITU，“Definition of Cybersecurity”，http：//www.itu.int/en/ITU-T/studygroups/com17/pages/cybersecurity.aspx（上网时间：2016年10月3日）。

② 衆議院：『サイバーセキュリティ基本法案』（第一八六回），平成26年11月6日，http：//www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g18601035.htm（上网时间：2015年10月25）。

③ White House，*Cyberspace Policy Review*：*Assuring a Trusted and Resilient Information and Communications Infrastructure*，Washington D.C.：US Government Printing Office，2009，p. iii.

④ Cabinet Office，*Cyber Security Strategy of the United Kingdom*：*Safety Security and Resilience in Cyber Space*，Norwich：The Stationary Office，2009，p. 7.

息技术网络和由该网络上的信息构成的电子世界。”① 日本则认为，“网络空间是以运用信息技术进行信息交换和互联网为基础的虚拟空间。”②

基于以上定义，本书认为：第一，网络空间安全应包含网络空间的诸物理要素、网络空间的诸信息要素以及与网络空间相关的现实空间诸要素（包括人在内）等三个维度的安全。第二，网络空间安全与信息安全、网络安全的主要联系与区别在于：“网络空间安全——网络空间中的国家安全问题，不能简单等同于信息安全、网络安全等狭义概念，而应根据高于技术、产业层次的定位，将其提上关乎国家安全的战略高度。”③

2. 透析以日美同盟为基础的日本网络安全建设，深化对“网络威慑理论”的认识和理解

“威慑理论”起源于核威慑理论。1946 年，耶鲁大学国际政治学教授伯纳德·布罗迪（Bernard Brodie）等人联合出版《绝对武器》一书，提出了威慑理论的基本思想。威慑理论的基本思想强调“威慑观”或“威慑逻辑”。其一般意义的定义是：威慑的成立，是处于对抗状态中的两方，一方以其实力（capability）及决心（resolve）说服另一方放弃攻击意图的过程与结果。换言之，只有当处于挑战地位的一方慑于对方的实力及实施这一实力的决心，认识到“如果其实施攻击，对方反击所造成的损失将大于其攻击所期待的政治所得”，并决定不再或放弃其攻击计划而安于

① Public Safety Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prospective Canada*, Ottawa: Government of Canada Publications, 2010, p. 2.

② NISC:『国民を守る情報セキュリティ戦略』, 2010 年 5 月 11 日, http://www.nisc.go.jp/active/kihon/pdf/senryaku.pdf（上网时间：2017 年 3 月 8 日）。

③ 陆忠伟：《网络空间安全：中美外交核心因素》，新华网，2016 年 11 月 18 日，http://news.xinhuanet.com/world/2016-11/18/c_129368714.htm（上网时间：2017 年 4 月 29 日）。