CIIS研究报告

网络战备、军控与美国

第 3 期

2014年6月

中国国际问题研究所

CHINA INSTITUTE OF INTERNATIONAL STUDIES

中国国际问题研究所简介

中国国际问题研究所系中华人民共和国外交部直属专业研究机构，主要对当前国际政治和世界经济等领域的重大问题进行中长期战略研究，对国际事务中重要的现实和热点问题做出及时分析，提出意见和建议，以供决策参考。

所前身为创设于 1956 年的中国科学院国际关系研究所。1958 年更名为国际关系研究所，1986 年起使用现名。1998 年，国务院下属的中国国际问题研究中心并入该所。

国研所现设 7 个研究部与 6 个研究中心。研究部分别为美国、亚太安全与合作、欧洲、发展中国家、欧亚、国际战略、世界经济与发展研究部；研究中心为中美关系、上合组织、军控与国际安全、能源战略、全球治理、海洋安全与合作研究中心。所里另设科研处、对外联络处等部门负责科研管理和对外交流。

国研所现有研究人员逾百人，其中约 40% 具有高级职称。从 1992 年起，国研所每年都有研究人员因贡献突出而享受国务院颁发的政府特殊津贴。迄今为止，共有 49 人享受过这一殊荣。

国研所图书馆是目前国内一流的国际问题研究专业图书馆，现有中、英、法、俄、德、日、西共 7 个语种约 30 万册图书。馆藏范围涵盖政治、经济、军事、外交、国际法等学科。

所内专设编辑部，负责编辑出版双月刊《国际问题研究》和 China International Studies。其中，《国际问题研究》杂志创刊于 1959 年，是国内创办时间最早的国际政治类学术期刊之一。China International Studies 创刊于 2005 年，是中国首个公开出版的外交与国际政治类英文学术期刊。

CIIS研究报告

网络战备、军控与美国

滕建群　徐龙第

第 3 期

2014年6月

中国国际问题研究所

作者简介

滕建群，研究员、博士。1979年高考进入军校学习，毕业后先后在海军南海舰队和北海舰队服役。1995年获军事科学院军事学硕士学位，留院任《外国军事学术》杂志编辑，后任总编。1999年获伦敦大学亚非学院南亚政治与经济硕士学位。2004年9月转业进中国国际问题研究所，2006年获北京大学博士学位。2013年起任该所美国研究部主任兼军控与国际安全研究中心主任，主持过两个国家社科基金项目，享受国务院政府特殊津贴。研究领域为中美关系、军控与裁军、国际安全理论等。

徐龙第，欧洲研究部副研究员，博士。2009年毕业于中国社会科学院研究生院，获国际关系专业博士学位，同年入所工作。主要研究领域为国际关系理论、国际安全、网络安全、欧盟政治与外交。

本报告为中国国际问题研究所军控与国际安全研究中心的研究成果。

引言 i

第一章 网络空间与战争 1

一、战争向网络空间延伸 1

二、“网络战”存在与否引发争议 4

第二章 网络空间与军备竞赛 7

一、“准网络战”频发 7

二、网络军备竞赛日趋激烈 12

三、美国对网络战的实践准备 15

（一）出台网络战政策文件 16

（二）创建机制和部门 17

（三）培育网络战能力 19

（四）提供资金保障 20

第三章 美国与网络军控 23

一、美国对网络军控的态度 23

（一）如何规范网络冲突与战争 24

（二）逐渐参与网络军控 25

二、网络军控的规则之争 29

（一）相互竞争的网络安全政策主张 30

（二）网络安全规则类型 31

三、网络战与网络军控规则 33

（一）网络战与国际条约 34
（二）网络战与武装冲突原则 36
（三）“先发制人”网络打击政策逆势而动 38

第四章 网络军控与中美网络关系 41
一、中国互联网发展与安全状况 41
二、中美网络关系视野下的网络军控 43
（一）区别网络军控的轻重缓急，以国家层面的网络行为规范为重点 44
（二）美国要主导网络军控，中国也应积极参与其中 44
（三）美国网络立法相对完善，中美可相互沟通借鉴 45
（四）中美应合作探讨可能的网络军控方案 46
（五）推动多边合作，促进全球互联网治理 48

结 语 49

引　言

人类以什么样的生产方式进行生产，什么样的作战方式就会出现。随着信息技术的发展，网络空间正成为继陆地、海洋、天空和外空之外的又一战场空间。当前，互联网已成为国家、社会及个人日常生活不可分割的重要组成部分，发展势头强劲。网络在给人们带来便利的同时，其蕴含的风险和挑战也在不断增加，如2011年网络攻击数量较2010年增加了36%，恶意软件数量增加了41%。2013年中国发表的国防白皮书指出，“机械化战争形态加速演变，主要国家大力发展军事高新技术，抢占太空、网络空间等国际竞争战略制高点”。和其他空间的战争行动一样，维护网络活动的规范性正在成为国际社会的共识。

美国学者认为，“21世纪掌握制网权与19世纪掌握制海权、20世纪掌握制空权具有一样的决定意义”。仅有50多年历史的互联网正以超乎寻常的速度在全球扩张，成为承载着政治、经济、军事、文化内容与意义的全新平台，成为影响社会稳定、国家安全、经济发展和文化传播的重要空间。从现实看，网络攻防既有国家层面的，如军队有组织的攻防行为，也有个人独立的行为；既可以是一次简单的黑客攻击，也可以是为达到战略目的而由国家发起的长时间、大规模针对基础设施的瘫痪国家运行的行动。

网络攻击尚没有明确的定义，一般是指计算机或网络的非授权渗透，主要表现在篡改、拒绝服务、数据窃取以及服务器渗透等。一些

非国家行为体网络团体的出现和发展，如政治色彩鲜明的“匿名者”以及其他网络犯罪组织，也增加了网络攻击的复杂性。据认为，世界前15名的军事预算国家均在发展网络攻防能力，2011年在联合国193个成员国中有68个国家有网络安全项目；到了2012年，有网络项目的国家达到114个之多，其中47个国家拥有军事网络项目，并在评估各自在军事网络方面的能力，发展相应的军事学说。在这样的大背景下，网络军控正在成为国际军控与裁军领域的一项重要内容，而目前涉及到该领域的军控措施几乎为零，这更增加了国际社会尽早谈判网络行为准则、达成网络条约以规范国际网络行为的重要性。

以美国为首的发达国家依靠其先进的信息技术和充足的经费保障，已制订出较为完整的网络战政策与战略，并加紧网络部队建设和网络战理论研究。作为二战结束后国际秩序的主要制定者，在国际军控与裁军领域，美国是其他国家不可替代的引领者，其在网络空间领域里的一举一动，也不可避免地牵扯到网络军控的发展方向。本报告围绕当前国际社会有关网络战的讨论、现有国际法对网络战的约束等问题，重点对美国等国家的网络战准备以及网络安全诉求等方面做出分析，提出要保证网络空间不被滥用和引发国际冲突，必须建立新的网络军控体制和规则，这其中美国有不可推卸的责任。

第一章 网络空间与战争

今天，互联网就像人的神经系统一样，已经延伸和渗透到世界各国的政治、经济、军事、文化、社会生活等各个领域。然而，互联网的不安全与它所带来的便利性相伴而生，形影相随，给人们的生活带来许多不便、甚至是麻烦。近年来，各种网络攻击更是频繁发生，对社会造成的巨大危害日益凸显，而有关战争向网络空间延伸的趋势也引起了人们的诸多讨论与担忧。

一、战争向网络空间延伸

网络空间理论最早是由美国科学家提出的，指的是网络电磁空间。它起始于计算机和网络技术的发展，是一场技术革命，也是人类生活方式的革命。20世纪60年代末互联网“传输控制/网际协议”（TCP/IP）彻底改变了传统通信传输方式，以有线传输为主的互联网迅速在全球推广开来。网络空间平台一经出现，便以惊人的速度发展，并朝着网络与电磁融合的方向发展，极大地拓展了人类活动的物理空间。经过半个多世纪的演变，战争也在逐渐向网络空间延伸。2006年美军出版的《联合信息作战条令》指出：“由于无线电网络化的不断扩展及计算机与射频通

信的整合，使计算机网络战与电子战行动能力之间已无明确的界限。”

战争向网络空间延伸也是社会信息化进程的发展结果。进入20世纪90年代，信息技术在社会生活中得以广泛地应用。1993年2月，刚上台不久的美国总统克林顿便在访问美国硅谷时明确表示要建立美国的“信息高速公路”。随后，日本、英国、加拿大、新加坡、印度、韩国、巴西、阿根廷等国也投入巨资，开始此项建设。信息化技术在民用领域里迅速普及的同时，也在向军事领域延伸。就在克林顿提出建立“信息高速公路”的同一年，美国兰德公司的约翰·阿奎拉（John Arquilla）和戴维·朗菲尔德（David Ronfeldt）宣称：“网络战来啦！”[1]其他国家在20世纪90年代也相继提出了信息作战等概念，指出信息作战通过综合各方面的信息，充分发挥其潜在能力以提高军事行动的效能。而信息优势达到一定程度后，它会使有优势的一方能够利用信息系统及能力，在冲突中夺取作战优势，或者在非战争军事行动中控制局势，同时阻止敌人获得这样的能力。

在当今之信息时代，互联网已成为军民兼用的一个重要平台和作战空间。早在1988年，美国便首次经历了计算机病毒入侵加州大学计算机系统的事件，该校计算机系统陷入瘫痪。美军也很快注意到，信息高速公路在带来巨大方便的同时，也带来巨大冲击，特别是在安全问题上，计算机、数据库、软件、操作者、路由以及数据传输过程等都存在严重漏洞。这些漏洞是由互联网本身的开放性以及信息技术的不成熟和迅速变化造成的。类似事件还包括：1992年，美国联邦航空公司管理局的光缆被挖断，致使所属4个空管中心系统被迫关闭35小时，上千架飞机延误

1 John Arquilla and David Ronfeldt, “Cyberwar is Coming!”, *Comparative Strategy*, Vol.12, No.2, Spring 1993, pp.141-165.

或取消；2009年1月，法国海军内部计算机系统的一台电脑受病毒入侵，迅速扩展到整个网络，致使海军全部战斗机“无法下载飞行指令”，被迫停飞两天。

进入21世纪，美国政府和军队把网络空间纳入新视野，认为网络空间是“人类信息环境中的一个全球域，由互联的信息技术基础设施网络构成，包括国际互联网、电信网、计算机系统以及嵌入式处理器和控制器等”。2009年5月，美国政府公布的《网络安全评估报告》也认为，来自网络空间的威胁成为美国面临的最严重经济和军事威胁之一。为此，美国不断加快网络战准备，大幅度提高对网络攻击武器的投入。

自2010年开始，美国政界、学界和媒体围绕网络战的辩论持续升温。理查德·克拉克（Richard Clarke）被称为美国的网络沙皇，曾任小布什政府的顾问。他在《网络战：国家安全的下一个威胁及应对》一书中指出，网络战已经开始，一些国家所遭受的攻击即是证明。网络战后果严重且快速波及全球，虽然信息技术的发展赋予一些组织和个人前所未有的能力，但真正有实力进行网络战的只有国家。[2] 美国国防部副部长威廉·林恩三世（William J. Lynn, III）在2010年发表于《外交》杂志的《保卫新领域：五角大楼的网络战略》一文中写道，国防部已开始建设保护国防部自身之安全网络的“强健防御系统”，计划把它的防御系统扩大到更为广泛的联邦政府系统，并最终扩大到私营领域。[3] 战争走向网络空间的步伐似乎在加快。

2 Richard Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, Ecco, 2012.

3 William J. Lynn, III, “Defending a New Domain: The Pentagon’s Cyberstrategy”, *Foreign Affairs*, Vol.89, No.5, September/October 2010, p.98.

二、“网络战”存在与否引发争议

网络战作为网络威胁和网络攻击的极端表现形式，正日益引起人们的广泛关注。其实自互联网诞生以来，国际上关于网络战的讨论和争议就不绝于耳，各国竞相争夺“制网权”。在1991年的海湾战争、1999年的科索沃战争、2003年的伊拉克战争中，网络工具都大显身手。许多国家近年来更是采取各种措施，纷纷出台网络政策，制定网络战略，建立网络司令部，加强网络建军，致使“网络战”似乎迫在眉睫，一触即发。然而，人们对战争的定义与理解不同，对网络战的认识也有差异。

事实上，网络活动种类繁多，其性质很难简单判定。目前，人们对网络威胁和网络安全的界定尚无统一意见。例如，英国皇家国际事务研究所（Chatham House）的保罗·科尼什（Paul Cornish）在于2009年2月提交给欧洲议会外交事务委员会的报告中认为，网络威胁可以分为网络侵入、有组织犯罪、意识形态和政治极端主义、国家发起的网络侵略等四个层次。[4] 亚历山大·科林伯格（Alexander Klimberg）等人则认为，网络攻击包括黑客行为、分布式拒绝服务（DDoS）、特洛伊木马等。[5] 斯科特·沙克尔福德（Scott J. Shackelford）却认为，网络攻击包括网络恐怖主义、网络战、网络犯罪、网络间谍等四种类型。其中，虽然恐怖主义组织在网上也有其存在形式，但真正的网络恐怖主义仍十分罕见，真正的网络战争也未发生过。相反，最紧迫的问题是网络犯罪和网络间谍。[6] 迈克尔·格伦农（Michael Glennon）认为，无论何种形式的网络攻击都是一

4 Paul Cornish, “Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks”, February 2009, pp.3-4.

5 Alexander Klimberg and Heli Tirmaa-Klaar, “Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU”, April 2011, pp.6-7.

6 Scott J. Shackelford, “In Search of Cyber Peace: A Response to the Cybersecurity Act of 2012”, *Stanford Law Review Online*, Volume 64: 106, pp.106-111.

种网络侵入，已经并将继续造成广泛危害，不应低估其危险。[7]

总体而言，目前对网络战的存在与否尚无共识，大体可以分为两种观点。一种观点认为存在网络战，已经发生；另一种观点则认为不存在网络战，尚未发生。

关于网络战的讨论和报道是如此之多，以至于它似乎已是既定事实。如前所述，甚至早在1993年，就有美国人宣称“网络战来啦”！威廉·林恩三世指出，“尽管网络空间是一个人造领域”，但对军事行动来说，它已变得“和陆地、海洋、天空、外空一样重要”。[8] 理查德·克拉克认为网络战使9.11事件都显得相形见绌，并敦促采取大量措施，“以便现在就开始防止网络战的灾难”。2011年2月，时任中情局局长的莱昂·帕内塔（Leon Panetta）更是发出警告，“下一个珍珠港很可能是一场网络攻击”。当然，有人认为这是一种“网络狂躁症”，是对网络攻击的过度反应。

与此“狂躁症”不同，伦敦国王学院的托马斯·里德（Thomas Rid）则认为，尽管有许多网络攻击发生，但网络战在历史上从未发生过，现在没有、将来也不可能发生。这是因为，一种进攻性行为必须满足某些条件才能构成战争行为。按照克劳塞维茨的定义，战争必须具备暴力性、工具性、政治性三个特点。或者说，任何战争行为都必须具有潜在的致命性、工具性和政治性。但是，在已经发生的网络攻击中，无论是较小或重大的网络攻击，尚无一起满足这些条件，也就不能构成战争行为。相反，所有过去和现在的政治性网络攻击都可以归为三种较为复杂的活动形式，即颠覆（subversion）、间谍（espionage）、破

7 Michael J. Glennon, “State-level Cybersecurity”, *Policy Review*, February & March 2012, pp.87-102.

8 William J. Lynn, III, “Defending a New Domain: The Pentagon’s Cyberstrategy”, *Foreign Affairs*, Vol.89, No.5, September/October 2010.

坏（sabotage），而它们与战争一样古老。[9] 同样来自伦敦国王学院的戴维·贝茨（David J. Betz）以及美国的科林·格雷（Colin S. Gray）等人也持有类似看法，认为关于“网络战”的许多说法都还只是比喻，在概念上并不准确，网络手段只是总体战争的一部分，“网络战并未到来”。[10]

在实践意义上，美军目前则把网络战分为三个等级：第一个等级是通过无线电干扰、破坏甚至控制敌方的军用电子系统；第二个等级是通过发动小规模的互联网攻击来策应、支援常规的战争行动或进行警告；第三个等级是全面的网络战争。与媒体报道和政府官员的说法不同，美军的这个分类方法仍算较为“务实”，最起码网络战是与“军事”联系在一起的。

由上可见，人们当前对网络战的存在与否仍有分歧，之所以如此，是因为对网络战的概念尚无共识，而短期内就网络战的概念达成一致也并非易事。但是，网络攻击的潜在破坏性巨大，这一点却是不争的事实；近年来发生的一系列网络攻击，更使网络空间“硝烟四起”。

9 Thomas Rid, *Cyber War Will Not Take Place*, Hurst & Company, London, 2013.

10 David J. Betz and Tim Stevens, *Cyberspace and the State*, Routledge, 2012, pp.75-97; Colin S. Gray, “Making Strategic Sense of Cyber Power: Why The Sky is not Falling”, Strategic Studies Institute and U.S. Army War College Press, April 2013.

第二章 网络空间与军备竞赛

信息与通信技术（ICT）的发展和应用都异常迅速，但人们对其在政治、经济、社会、军事上的影响的理解却明显滞后。例如，信息技术在军事领域的应用方面，各国的实践就走在了有关理论探讨和知识建构的前面。虽然在判断网络战出现与否时需要多一份谨慎，但频繁发生的网络事件，仍令各国对网络空间的军事维度极其敏感。因此，许多国家近年来都纷纷采取各种措施加强网络安全，致使网络空间军事化、武器化和“军备竞赛”的趋势明显。

一、“准网络战”频发

尽管网络战的存在与否仍有争议，短期内也难以对网络战的概念形成共识，但信息技术和互联网络用于军事领域的情况却早已不是什么新鲜事儿，许多国家还多次在现实战争中运用电子信息和互联网络手段。换言之，信息技术和互联网络已成为现代战争的手段和工具之一，甚至是整个战场的一部分，与以前人们常说的电子战、信息战、网络中心战等有相似之处。然而，互联网的广泛存在和普遍应用，使电子战、信息战等概念的内涵和外延都得以延伸。因此，即使不存在严格意义上的网

络“战争”行为，已经发生过的许多网络攻击行为或许也可以被视为“准网络战”或“类网络战”（quasi-Cyber War）。[11]

早在1991年的海湾战争中，美国就通过情报系统在伊拉克的防空系统中植入电脑病毒，在美军空袭前用遥控手段激活这些病毒，导致美国空军飞临巴格达上空时，伊拉克防空系统已经瘫痪。这次行动使人们开始重视网络战。在1999年的科索沃战争中，南联盟组织黑客，使用多种电脑病毒，使北约的军事指挥网络一度瘫痪。为了报复，美国便向南联盟军队网络指挥系统和民用系统中植入大量病毒和欺骗性信息，导致南联盟防空体系失效，大面积停电，通讯中断数小时。在2003年的伊拉克战争中，美军再次使用网络攻击手段。在2月底的短短几天内，数千名伊拉克人在他们的电子邮箱里看到一封劝降信：“放弃吧，起义并倒戈，到另一边来，否则美国就开战了。”在战争进行过程中，美国“网络特种部队”使用2000多种计算机病毒，对伊拉克的军事通信系统进行摧毁性攻击，致使伊拉克军队接受错误信息或得不到任何信息。这些事件都发生在传统意义上的战争期间，信息和网络手段显然是战争的手段之一，也被普遍视为较早的网络战案例。

与将其作为传统意义上的战争手段不同，近年来发生的网络攻击事件似乎更接近“准网络战”，也进一步为网络战的到来提供了佐证。例如，2007年和2008年爱沙尼亚和格鲁吉亚分别受到的网络攻击，以及2010年发现的“震网”蠕虫病毒，便被视为网络战的最新案例。

2007年4月，爱沙尼亚决定将位于首都塔林的苏军纪念铜像移到军人坟场，引起居住在爱沙尼亚的俄罗斯人大规模骚乱，并招致俄政府的强

11　鉴于目前国际上对网络战的认知存在分歧，已经发生的诸多网络攻击事件称为“准网络战”可能更为准确。

烈抗议，致使双方关系紧张。4月26日晚10时左右，爱沙尼亚政府网站突然被来自世界各地的电子信息淹没，包括政府、银行、新闻媒体在内的各大网站相继遭到攻击，陷入瘫痪。爱沙尼亚先后遭到三波大规模网络攻击，一直持续到5月18日才结束。爱沙尼亚还被迫关闭了与外界的链接，使其互联网成了“局域网”。尽管后来北约派遣专家出手相助，但仍无能为力。事后，爱沙尼亚国防部长在一次国际会议上说，这是“没有被注意到的第三次世界大战”。西方媒体普遍认为，此次网络攻击源自俄罗斯，西方网络战专家更称之为真正意义上的第一场网络战。

据媒体报道，在2008年8月的俄格冲突中，俄罗斯在开战之前就控制了格鲁吉亚的网络系统，冲突爆发后几乎所有的服务器均被冻结，使格鲁吉亚的交通、通讯和金融等互联网服务陷入瘫痪，格军更是得不到上级的指令，上级也无法获得战场的情况，从而为俄罗斯军事行动的顺利进行开辟了道路。

当然，由于进行网络溯源极为困难，并无确切证据证明这两起网络事件是俄罗斯所为。

以上两场网络攻击具有以下特点：一是攻击手段更加隐蔽。对爱沙尼亚的攻击数据来自包括美国在内的全球70多个国家的电脑，这些电脑很可能早就染上了“僵尸网络”病毒。由于攻击来源不同，遭受攻击的国家很难判断攻击的发动者到底是谁，也增加了发起攻击者的政治回旋余地。二是进攻的发起速度极为迅速。在网络事件爆发的第一天，爱沙尼亚就遭受了1000次攻击，第二天攻击次数猛增到了每小时2000次。2007年5月9日当天，攻击频率达到高峰，平均每秒钟遭受400万个数据

包的攻击。大量数据和高频率的攻击使服务器不堪重负，纷纷瘫痪，在政府和有关部门还没有反应过来时，网络防线已被攻破，达到了网络突袭的目的。三是攻击范围广泛，在这两场网络攻击中，两国的政府、军队、媒体、银行、学校等几乎所有重要部门的网络平台均遭到攻击。网络攻击在给军队机关造成指挥困难的同时，也给社会的正常运转带来极大混乱。

迄今，造成最严重物理或现实影响的当属“震网”蠕虫病毒。2010年11月，“震网”蠕虫病毒袭击了伊朗纳坦兹铀浓缩工厂等核设施，并导致俄罗斯援建的布什尔核电站发生放射性物质泄漏。专家在对“震网”病毒进行分析后发现，这是一种专门为袭击离心机而设计的病毒，但经过“适当调整后”可以转而攻击世界各地的工业控制系统。这种病毒结构异常复杂，隐蔽性很强，能突然更改离心机中的发动机转速，进而摧毁离心机运转能力且无法修复。“震网”病毒虽未能摧毁伊朗核设施，但致使伊朗约20%的离心机就此报废，从而大大延迟了伊朗核计划。普遍认为，这是美国和以色列所为，“震网”病毒的出现标志着又一种网络武器的诞生，网络战也进入了新阶段。美国《名利场》杂志的调查文章认为，“震网蠕虫病毒是网络战的广岛”。

按照前述克劳塞维茨的三个战争要素来分析，这起网络事件可能是最接近“网络战争”的网络攻击行为。首先，“震网”病毒背后的政治目的极其明显，显然具备政治性质。在伊核问题长期没有进展、伊朗不可能选择弃核、对伊朗进行公开军事打击成本极大而前景又极不确定的情况下，网络攻击手段就成为一种相对安全的政策选择，不仅可以延迟或破坏伊朗的核计划和核设施，而且政治成本相对低廉，避免了军事打

击可能造成的种种难以预料的后果。而且，研发“震网”这类复杂病毒的成本非常高昂，并非一般的黑客能力之所及，而是需要大量的投入，而这通常需要国家的大力支持。

其次，“震网”病毒的攻击性、针对性和目的性很强，工具性质也具备。该病毒在被发现之前就已经运行了长达七年的时间，从2005年11月至2012年6月。到2010年年底，该病毒已在多个国家感染了将近十万台主机，其中60%位于伊朗境内。不过，该病毒并未破坏所有被感染的主机，因为它对主机设置的选择非常严格，只针对西门子的两款型号分别为6ES7-315-2和6ES7-417的逻辑控制器。如果没有发现这两种类型的设置，“震网”病毒就不会发作，对主机也不会造成任何破坏。[12]

最后，存在疑问的是“震网”病毒的暴力性质。计算机病毒本身不具备暴力性质，没有通常的炸药所能产生的巨大当量。同时，就像有人所说的那样，虽然“震网”病毒使伊朗20%的离心机报废，但仍有80%的离心机未受影响，进而表明它的影响是有限的，伊朗也不会因此而丧失核子方面的科学知识和科研能力。更为重要、同时也是当前关于网络战的讨论中最难、最具争议的部分，是“震网”病毒并未造成人员伤亡，特别是大规模、大范围的人员伤亡。实际上，不仅“震网”病毒如此，迄今为止的其他网络攻击行为也都未造成人员伤亡的恶果。因此，这就使网络攻击的暴力性质大打折扣，并对受害方是否以及如何启动可能的应对措施（包括军事措施）造成困惑，甚至是困难。 因此，按照托马斯·里德的严格定义，即使是这起网络事件，也不能被定性为“战争”行为；但它却是最接近严格定义的网络战的“准网络战”。

无独有偶，2012年5月28日，俄罗斯网络安全软件生产商卡巴斯基

12 Thomas Rid, *Cyber War Will Not Take Place*, London: Hurst & Company, 2013, pp.43-44.

实验室发布报告称，他们发现一种比“震网”病毒更加复杂、更加先进的“火焰”病毒正在中东地区大范围传播。其中，伊朗受病毒影响最严重，以色列、叙利亚和其他中东国家也受到一定影响。该病毒能够对存储有特定信息，比如核工业相关信息的计算机，实施监控、截取信息乃至毁伤，是迄今为止发现的最大规模和最为复杂的网络攻击病毒。该实验室的技术人员以“网络重武器”定性“火焰”病毒，并推测这一病毒可能有政府背景。

虽然“震网”、“火焰”等没有引起人们通常所看到的激烈战争，但这些病毒背后所折射出来的政治、军事含义及其引发的国际影响却需要引起人们的注意。

二、网络军备竞赛日趋激烈

各种网络安全事件的频繁发生，增加了维护网络安全的紧迫性。为此，各国近年来纷纷采取各种应对措施，甚至大举进行“网络建军”，网络军备竞赛日趋激烈，进而使维护网络空间秩序、稳定的难度加大。

除美国外，俄罗斯对网络战的理论研究也很早就已起步。[13] 20世纪90年代初，俄就专门设立了“信息安全委员会”，并将信息网络安全与经济安全置于同等重要的位置。1995年，俄宪法将信息安全纳入国家安全管理范畴，颁布了《联邦信息、信息化和信息网络保护法》。2000年9月，时任俄罗斯总统的普京正式批准了《国家信息安全条令》，明确了俄罗斯在信息领域的国家政策。2002年，俄罗斯信息安全委员会通过了

13 美国的情况见下文。

《俄联邦信息安全学说》，将网络战称作未来的“第六代战争”[14]，提出了在信息网络安全领域实现国家利益的手段和相关措施，为俄军网络战的发展指明了方向。在思想上，俄军十分重视网络战，重视“先机制敌”，实施主动攻击，强调必须要夺取并掌握制信息权和制电磁权。为确保信息对抗中的主动地位，俄军建立了“特种信息部队”，专门负责信息战的防护与实施。

俄罗斯在发展网络技术和网络武器方面也处于领先地位。据报道，俄罗斯拥有无线数据通信干扰器、网络逻辑炸弹病毒和蠕虫病毒、网络数据收集计算机和网络侦察工具、嵌入式木马定时炸弹等先进网络武器，而且在实践中已有所运用，如爱沙尼亚和格鲁吉亚都曾谴责俄罗斯对其发动网络战。近年来，俄军又提出了新的要求：加强网络战的攻防实力，建设一支攻防兼备的网络作战力量；建构“网络威慑”力量，使自身的网络战实力在冲突爆发之前就起到强有力的威慑和吓阻作用；强化电子信息战，包括网络战在内的电子干扰、舆论信息战等，力求使网络战从理论到实践更加完善。同时，俄罗斯的黑客在世界上也具有极高的“声誉”。在专用网络和即时组网方面，俄罗斯技术专家正在研制各种计算机病毒武器，特别是“远距离无线注入病毒武器”，可对敌方指挥控制系统产生直接威胁。美国“防务科技”网曾估计俄罗斯有7300多人的网络战部队，长期经费达400亿美元。[15]

面对网络战的硝烟四起，其他国家也都积极应对。英国、韩国、日

---

14 “第六代战争”的理论最早由俄罗斯军事学者B. N. 斯里普琴科提出，是针对已有的前五代战争而言的。它们分别是步兵战与骑兵战、黑色火药与滑膛枪炮战、线膛轻武器与身管火炮战、重武器战争（导弹、飞机、军舰、坦克、装甲车等）、核战争。参见严涵：“第六代战争”，《航空世界》，2003年第2期；“各国摩拳擦掌周密部署网络战：未来第六代战争”，新华网，2012年1月9日，http://news.xinhua-net.com/mil/2012-01/09/c_122556679_3.htm?prolongation=1。

15 Ward Carroll, “Russia’s Cyber Force”, DT (DEFENSETECH), May 27, 2008, http://defensetech.org/2008/05/27/russias-cyber-forces/.

本、印度、以色列等国都在加强网络战的研究，相继成立网络战机构或部队，网络军备竞赛日益激烈。英国在2001年就秘密组建了一支隶属军情六处、由数百名计算机精英组成的“黑客”部队。英国还与美国、加拿大合作，建立网络作战单位，加强计算机病毒、“黑客”进攻等方面的研究。2009年6月，还出台了《英国网络安全战略》，计划征召包括黑客在内的网络精英以保护网络安全，并宣布成立网络安全办公室和网络安全行动中心，分别负责协调政府部门的网络安全以及政府与民间机构主要电脑系统安全的保护工作。

韩国在1999年就提出了未来信息建设的总体设想，2009 年又宣布将组建“网络司令部”，并于2010年正式启动。目前，韩国已经拥有约20万受过专业训练的人才队伍，每年国防经费的5%被用来研发和改进网络战技术。据报道，韩国国防部已组建了网络战特种部队——反黑客部队，吸纳了数万名信息战专业人员。韩国还计划大幅扩充网络战司令部兵力，达到1500人左右。[16]

日本试图通过掌握“制网权”达到瘫痪敌人作战系统的目的。日本在构建网络战系统时强调“攻守兼备”，拨付大笔经费投入网络硬件及“网战部队”建设，建立了“防卫信息通信平台”和“计算机系统通用平台”，实现了自卫队各机关、部队网络系统的相互交流和资源共享。日本防卫省已组建了一支约5000人的“网络空间防卫队”，专门从事网络系统的攻防，目前已具备较强的网络战实力。日本还注重与美国联合发展，在引进先进技术的基础上不断完善自身建设，提升“网络战”能力。[17]

16　安亮：“虚拟世界，战争动员已打响——从英政府关闭社交网站举措看外军信息网络动员”，《解放军报》，2011年8月18日第3版。

17　“网络军事化：各国手里都想握张牌”，新华网，2011年5月30日，http://news.xinhuanet.com/world/2011-05/30/c_121468822_4.htm。

近年来，印度在信息战硬件上加大投入，充分发挥自己软件开发水平高的优势，开发和引进先进服务器、防火墙以及超级计算机，积极准备网络战。目前，印军组建了陆、海、空三军联合计算机应急分队，并征召大批高水平“黑客”入伍，逐步完成未来网络战的人才储备。印度坚持自主研发、军民合作的原则，投入大量人力物力，力求在网络技术、密码技术、芯片技术以及操作系统方面自成体系。“闪光信使”高速宽带网络以及被称为“第三只眼”的海军保密数据信息传输网络的建成使用，将进一步增强印度军方应对未来网络战争的不对称优势。除完善防御体系外，印军还将网络进攻写入作战条例，明确提出要建立能够瘫痪敌方指挥与控制系统以及武器系统的网络体系，在陆军总部、各军区以及重要军事部门分别设立网络安全机构。[18]

三、美国对网络战的实践准备

美国军事预测专家詹姆斯·亚当曾预言：“在未来战争中，计算机就是武器，战线无处不在，夺取作战空间控制权的不是炮弹和子弹，而是网络里流动的比特和字节。”美国智库兰德公司也在其报告中指出，“工业时代的战略战是核战争，信息时代的战略战主要是网络战”。实际上，美国备战网络可谓由来已久。为应对网络空间可能发生的冲突和战争，美国近年来更是加大了网络建军的力度和速度，把技术、政策和机制管理上的优势发挥得淋漓尽致。

18　安亮：“虚拟世界，战争动员已打响——从英政府关闭社交网站举措看外军信息网络动员”，《解放军报》，2011年8月18日第3版。

（一）出台网络战政策文件

进入21世纪以来，美国先后出台一系列政策文件，为其备战网络空间提供指导和依据。2002年，美国总统布什签署了一项密令——“国家安全第16号总统令”，要求美国国防部牵头，制定一项计算机网络战战略，提升网络攻防能力。2003年，美国国防部长拉姆斯菲尔德批准了一份题为《信息战路线图》的国防部秘密报告，要求美国寻求对整个信息领域的最高控制权，美军应具备“摧毁全球电信系统、雷达以及所有基于电磁波的武器系统的能力”。2005年3月，五角大楼出台的《国防战略报告》明确将网络空间定义为与陆地、海洋、天空、太空同等重要，需要美国维持决定性优势的第五大空间。2007年，在美国空军制定的《国家网络战军事战略》中，首次将网络空间界定为可以采取军事行动的领域。2009年5月，美国完成了《网络空间政策评估报告》。2010年发表的美国《国家安全战略》重申了《网络空间政策评估报告》中提及的内容。2012年10月，美国总统奥巴马签署了关于网络空间军事行动的总统令，这是一项机密文件，具体内容不得而知。

2013年2月12日，奥巴马签署了《关于提高关键基础设施网络安全》的行政命令，要求加强对关键基础设施的保护力度，使其免遭网络攻击。命令要求联邦机构增强与运营商的信息共享，一些可能属于机密级的信息也将包括在内。新的行政命令还要求国土安全部部长统领的官员一年内制定出减少网络安全风险的标准。所谓关键基础设施部门，是指那些涉及国计民生的关键企业，其电脑系统或设施如遭受破坏，将影响到国家安全、经济安全或公众健康。由于美国大多数关键基础设施都由

民营部门经营，这项命令的最根本含义是政府介入商业运营。公权私用的目的是加强对网络的管制，但私营企业是否愿意配合政府不但是个安全问题，而且也涉及到美国多年来的商业运营模式问题。无论结果如何，政府强力介入私营部门的运行已成为美国确保网络安全的重要步骤。上述一系列政策文件的出台，为美国备战网络空间提供了战略指导和思想基础，使其实践活动有章可循，有据可依。可谓兵马未动，思想先行。

（二）创建机制和部门

美国还专门建立起负责网络战的“网络司令部”，在网络建制方面远远走在了其他国家的前头。2005年，美国组建了专门负责网络作战的“网络战联合功能构成司令部”，陆、海、空军和战略司令部也都设有“网军”。2009年6月23日，美国国防部长罗伯特·盖茨正式宣布成立“网络司令部”，隶属战略司令部，编制千人，把分散在美国各军种中的网络战指挥机构整合起来，强化各机构间的协同作战能力，争夺“网络战主导权”也成为美军的新使命。2010年10月，网络司令部开始全面运作，其分支机构包括陆军网络司令部、空军网络司令部和海军网络司令部。这不仅标志着美军网络战实现了统一指挥，也标志着美军有了在网络空间遂行作战任务方面的攻防能力，从而使网络战成为一种独立的作战样式。《华盛顿邮报》2013年1月报道称，美国国防部批准在未来几年把其网络司令部扩大五倍，从目前约900人增加到4900人，大幅增强保护关键计算机网络的能力。[19]

19 Ellen Nakashima, “Pentagon to Boost Cybersecurity Force”, *The Washington Post*, January 27, 2013, http://articles.washingtonpost.com/2013-01-27/world/36583575_1_cyber-protection-forces-cyber-command-cybersecurity.

2012年11月，美国国防高级研究计划局（DARPA）发表了名为“基础网络战（X计划）”文件，研究网络战的相关内容。文件称，“X计划将对网络战的本质开展创新性研究，制定主宰网络战场的基本战略，研究目的在于发现颠覆性技术，推动科技、设备或系统的革命性发展”。同年12月18日，美国国防部长帕内塔称，国防部已经制定了新的网络空间交战规则，即网络战部队作战条令，以规范美军在这方面的任务和能力，并使美军“能更快速地对网络威胁做出响应”。他还表示，国防部正在研究加强网络司令部的职责。根据奥巴马的指令，美军网络司令部的职责将从最初的负责处理军事网络基础设施所受的威胁，扩大到更为广泛的国家网络防御职能，包括实施进攻和防御行动。对美国来说，目前已基本完成了从理论到实战的全面网络战准备。

除“网络司令部”外，美国还设立了不少其他的网络安全机制，建立起较为完备的体系架构。目前，美国的网络安全事务主要由国土安全部、国家安全局、联邦调查局和国防部负责，国务院和商务部负责网络安全的磋商和标准的制定。国土安全部下辖网络安全分部，负责协调公共和私营部门以及国际机构，保护美国网络空间安全和网络安全利益。由13家联邦机构组成的“国家网络响应协调小组”负责对“国家级网络事件”做出反应。国土安全部还拓展了“国家网络安全和通信综合中心”的工作，提出加强网络态势感知和信息共享能力。2010年10月，国土安全部与国防部签署了合作协议，加强部门间的网络安全协调力度。2012年，美国政府两次向国会提出了关于授权国土安全部保护关键基础设施网络安全的决议，但均未能获得通过。此外，为加强对网络安全事务和政策的协调，白宫还于2009年12月任命了网络安全协调员，美国国务院也于2011年2月任命了网络问题协调员。

（三）培育网络战能力

美国非常重视发展网络战能力。1995年，美军16名“第一代网络战士”从美国国防大学信息资源管理学院诞生。此后，美国网络战部队逐渐发展壮大。美国前国防部长罗伯特·盖茨更是提出，五角大楼将把每年培训的网络安全专家数目提升四倍，每年为五角大楼培训250名网络安全专家。目前，美军共有3000至5000名信息战专家，五至七万名士兵涉足网络战。如果加上原有的电子战人员，美军网络战部队达8.87万人之多。美国还多次进行网络战演习，在2006年和2008年先后组织了“网络风暴I”和“网络风暴II”的网络战演习，18个联邦机构协同作战，更有思科和微软等40余家科技企业参与。奥巴马上台后，将网络战威胁等同于核武器和生物武器对美国的威胁，2010 年联合15国举行了规模空前的“网络风暴III”演习。

美国还积极开发网络战武器。据披露，在硬杀伤网络战武器方面，美国正在发展或已开发出电磁脉冲弹、次声波武器、激光反卫星武器、动能拦截弹和高功率微波武器，可对别国网络的物理载体进行攻击。在软杀伤网络战武器方面，美军已研制出2000多种计算机病毒武器，既可以利用网络战手段窃取情报，也可以利用特殊工具软件，在短时间内向目标集中发送大量垃圾信息，使对方出现超负荷、网络堵塞等状况，从而造成系统崩溃。2010年8月，《华盛顿邮报》报道说，美国国防部预算文件表明，国防部正在开发一系列网络能力，包括可对“敌方信息系统进行攻击和刺探”的工具，以及可以“欺骗、拒绝、阻断、羞辱和破坏”信息和信息系统的工具。[20] 该报2012年3月19日再次报道称，国防部

20 Ellen Nakashima, “Pentagon Considers Preemptive Strikes as Part of Cyber-defense Strategy”, *The Washington Post*, August 28, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/08/28/AR2010082803849_pf.html.

正在加快研发新一代网络武器，以帮助美军在敌方军事系统未接入国际互联网的情况下，也能对其施加干扰。这种“离线网络武器”将利用新兴技术，锁定“离线”军事系统，以施加干扰。美国不仅大力发展网络武器，还积极为使用网络武器的合法性而寻求和制造依据。2013年2月，据《纽约时报》报道，随着美国“网络武器的不断发展”，美对此进行了“秘密法律评估”，结论认为，若发现可靠证据，表明外国将对美发动“重大”数字攻击，那么总统将有权下令发动“先发制人”网络打击。[21]

（四）提供资金保障

在资金投入方面，美国毫不吝啬。2011年五角大楼决定在未来五年内拨款五亿美元给国防高级研究计划局，以加快网络武器及防御性网络技术的研发；2012年五角大楼在网络安全和网络技术方面的预算达34亿美元。美国防务与武器承包商洛克希德·马丁公司和波音公司都成立了网络安全部门。据它们评估，到2013 年，美国政府在网络安全方面的采购金额将达到107 亿美元。2008年，五角大楼还斥资300亿美元建造堪与“曼哈顿工程”媲美的“国家网络靶场”，意在保护美国网络安全，防止美国遭受敌对电子攻击，并对敌方展开在线攻击。为规范网络武器的使用，五角大楼制定了网络武器和网络工具清单，将武器的使用分为全球、区域和敌对地区三个等级，为美国开展网络战提供了依据。

美国应对网络攻击的努力没有白费，正在取得回报。例如，溯源问题一直是应对网络威胁的最大技术难题，美官员更是对其“网络战”能力讳莫如深。然而，2012年10月，帕内塔却对路透社表示，为解决溯

21 David E. Sanger and Thom Shanker, “Broad Powers Seen for Obama in Cyberstrikes”, *The New York Times*, February 3, 2013, http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html?_r=0.

源问题，美国在网络取证方面投入巨大，“正取得回报”。[22] 当月，帕内塔在他的首次网络政策演说中宣布，美军现在有能力追踪到计算机网络攻击的源头；他还承认美国拥有先进的网络进攻能力，若发现即将发生的攻击，有能力发起“先发制人”行动。他说，“潜在的攻击者应该知道，美国有能力定位他们，并让他们对其试图伤害美国的行动负责。国防部已发展出了对此采取有效行动的能力，制止对我们网络空间国家利益的威胁”。美国高级防务官员也表示，美国已把数千起小的网络攻击追踪到犯罪集团、外国和个人，尽管“目前人们普遍认为，不可能把攻击追踪到任何特定的个人或民族国家”，但“我们在国防部已投入很多，大力开发这种能力，并已取得巨大改进”。[23]

自2013年6月以来，美国国家安全局前雇员爱德华·斯诺登（Edward Snowden）曝光了美国对电话和互联网通信进行大规模监控的“棱镜”计划。如果说在此之前人们对帕内塔等人的表态或者对美国的网络溯源能力尚存疑虑的话，那么“棱镜”计划则不仅向人们展示了美国强大的网络能力，也在一定程度上表明帕内塔等人的话“此言不虚”。就像斯诺登曝光的“棱镜”等计划一样，美国的网络溯源能力或许也将大大超乎人们的想象。然而，美国对网络技术、绝对安全和网络空间霸权的追求并不利于网络空间秩序的建构，更不利于国家间信任的建立，并且加剧了网络空间的军备竞赛，对网络安全和战略稳定构成巨大挑战。

显然，美国在充分利用其在信息技术领域里的优势，以国家安全为由，滥用法律和技术手段，不但用于反恐怖行动中，而且对包括盟国和他国的政要以及重要的国际会议等都进行网络监控。这些领导人既不是

22 Nick Farrell, “US can Launch Preemptive Cyber Strikes: Military can Respond to Threats before They Happen”, 12 Oct 2012, http://news.techeye.net/security/us-can-launch-preemptive-cyber-strikes.

23 Chris Carroll, “US can Trace Cyberattacks, Mount Pre-emptive Strikes, Panetta Says”, October 11, 2012, http://www.stripes.com/news/us-can-trace-cyberattacks-mount-pre-emptive-strikes-panetta-says-1.192789.

恐怖分子，也不是普通百姓，美国着力对他们的网络监控主要是保证及时跟踪这些国家的政治、经济、军事领域里的情报，提前掌控主要国家的未来走向。从这方面看，国家安全对美国来说就不仅仅是反恐了，更多的是在国际上利用美国在信息技术领域里的优势地位，加强对有关国家的情况掌控，从而继续维系其世界霸权地位。大力推动网络空间的军事化和武器化已经偏离互联网发展的一般目标，而对互联网的大规模监控更是在滥用信息技术的道路上越走越远。

第三章 美国与网络军控

鉴于网络活动复杂多变，网络威胁广泛存在，可以说，制定应对网络威胁、维护网络安全的规则势在必行。然而，由于网络攻击等行为仍是一个法律和战略灰色区域，目前尚无普遍性的国际条约来规范网络行为，有关网络军控的国际条约也处于空白状态。最近针对该问题的政策辩论未能产生具体的国际协议，而美国在其中的态度和作用尤其引人注意。

一、美国对网络军控的态度

如前所述，当前人们对网络战的存在与否尚存争议。以美国为首的西方虽在探索网络战规则方面非常积极，但美国对网络军控的态度却经历了由反对到松动的转变过程。美国的态度之所以改变，有多方面的原因，包括网络溯源能力的提升、网络武器技术领先地位的确认（如“震网”蠕虫病毒对伊朗核设施的破坏）、对有关法律问题和国际法问题的认识加深、双边网络协议的达成（如2013年6月的美俄网络合作协定）、外交战略的考虑以及国际社会在网络问题上取得新进展（如联合国政府专家组2013年6月的共识文件）等。

（一）如何规范网络冲突与战争

对网络战进行规范，无外乎两种办法：一是制定新的国际法规则，签订新的国际条约，如中国和俄罗斯等国提出的《信息安全国际行为准则》（以下简称《行为准则》）；二是调整现有国际法规范，使之适用于网络空间和网络战，这得到了美国和北约等西方国家和国际组织的支持。2011年9月12日，中国、俄罗斯、塔吉克斯坦、乌兹别克斯坦共同致信联合国秘书长潘基文，请他把《行为准则》作为第66届联大的正式文件散发，呼吁各国在联合国框架内讨论该文件，以尽早就涉及信息和网络空间的国际准则达成共识，规范国家行为。这是国际社会首次较为全面、系统地提出有关信息和网络安全国际准则的文件。然而，“美国及其西方盟国在很大程度上”对该《行为准则》草案“置之不理”。最近，卡特政府时期的高级顾问阿米塔伊·艾次奥尼（Amitai Etzioni）表示：“如果不知道是哪些国家提交了该提案，那么就会很容易地认为，该提案95%的内容是由美国领导的西方国家起草的。”这充分说明了《行为准则》的普遍意义。

与此相反，美国、北约等西方国家和国际组织认为，现有国际法可以适用于网络空间，无需另立新法。2012年9月，美国国务院韩裔法律顾问高洪柱（Harold Hongju Koh）在美国网络司令部的部门间法律会议上正式表达了这种立场。[24] 同月，北约在历时三年的研究之后，也发布了《关于国际法适用于网络战的塔林手册》（已于2013年初由剑桥大学出版社出版，以下简称《塔林手册》）。[25]《塔林手册》提出了适用于网

24 Harold Hongju Koh, “International Law in Cyberspace”, September 18, 2012, http://www.state.gov/s/l/releases/remarks/197924.htm.

25 Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013.

络战的95条规则，涉及国家在网络空间的权利与责任、武力的使用等内容，并配有对每条规则的评论，反映了《塔林手册》制定过程中的有关讨论、共识及分歧。

当然，无论是制定关于网络战的新规则，还是把现有国际规范用于网络战，都不能忘记战争法的最初目的：一是保护那些没有或不再参加战斗的人（如平民、军队中的医务和宗教人员）以及那些已经停止参加战斗的人（如受伤、遇船难和生病的战斗员以及俘虏）；二是限制作战手段（特别是武器）和作战方法（如军事战术），进而减轻武装冲突的影响。推动网络军控和制定网络安全规则的意义也正在于此。

（二）逐渐参与网络军控

为防范网络领域的军备竞赛和网络战的发生，俄罗斯最早建议在网络空间领域采取军控措施，并希望与以美国为首的北约等军事组织通过谈判达成某种协议。1996 年，俄美两国军方首次就网络战问题在莫斯科举行秘密会谈。据当时参与对话的美方代表团团长阿奎拉表示，在这次初步接触后，美国军方对进一步磋商丧失兴趣，俄美关于网络安全的商谈也就此中断。[26]

1998年，俄罗斯向联合国大会第一委员会（裁军与国际安全委员会）提交了题为《从国际安全的角度来看信息和电信领域的发展》的决议（A/RES/53/70），未经表决便被通过。决议表示担忧信息技术和手段可能会被用于不符合维护国际稳定与安全的目的，对各国的安全产生不利影响；认为必须防止信息资源或技术受到滥用或利用以达到犯罪或恐

26 John Markoff and Andrew E. Kramer, “U.S. and Russia Differ on a Treaty for Cyberspace”, *The New York Times*, June 28, 2009, http://www.nytimes.com/2009/06/28/world/28cyber.html?pagewanted=all.

怖主义目的；吁请会员国推动在多边一级审议信息安全领域的现存威胁和潜在威胁。[27] 自此，“从国际安全的角度来看信息和电信领域发展”问题就被列入联合国议程。此后，俄罗斯每年都向联合国大会提交类似提案，秘书长也每年都向大会提交报告，联合国会员国在报告中表达各自对该问题的看法。[28] 然而，这些努力一再遭到美国的反对。

近年来发生的一些重大网络安全事件促使网络军控再度成为热点。虽然这些事件是否属于真正意义上的网络战尚有争议，但它们充分表明，网络攻击可以对国家的重要基础设施造成严重破坏，完全有可能被用于军事目的，凸显网络军控的现实性和紧迫性。因此，在时隔十多年后，俄罗斯重提网络军控问题。2009年3月，俄罗斯国家安全委员会副秘书弗拉迪米尔·索科洛夫再次表明了俄罗斯关于网络军控的基本立场，包括禁止国家秘密在计算机系统中嵌入可在日后危急时刻启动的恶意代码和芯片、禁止对非战斗人员和单位发起军事性网络攻击以及政府应当对互联网进行监管等。2011年9月，俄罗斯、中国等国共同提出了前述的《信息安全国际行为准则》，但美国对此并无兴趣，美国国务院的一名官员说，“他们（俄罗斯人）想限制攻击行为”，但“我们要有能力先给我们每天受到的五万次攻击定罪”。更有美国人对此持不同看法。例如，曾就职于国土安全部的斯图尔特·贝克认为，建立网络安全和网络隐私方面的全球规则可能是不现实的，因为“破坏那些规则能带来很多好处”。[29]

---

27 Developments in the Field of Information and Telecommunication in the Context of International Security, A/RES/53/70, 4 January 1999, http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=http://www.un.org/disarmament/topics/informationsecurity/&Lang=C.

28 “Developments in the Field of Information and Telecommunication in the Context of International Security”, http://www.un.org/disarmament/topics/informationsecurity/.

29 他还反对欧盟的“数据保护指令”，认为这是一种“新殖民主义”，企图把“隐私”的概念强加于世界。

2009年奥巴马政府任命了白宫网络安全协调员，负责协调联邦政府在信息安全方面的活动。有人认为，在拒绝俄罗斯提议多年之后，这代表着美国政策的重大转变，表明奥巴马政府准备认真对待对网络安全问题的承诺。2010年7月，美国、英国、中国和俄罗斯等15个国家同意进行合作，以减少网络攻击的威胁，“美国加入联合国网络军控合作”，支持以军备控制的方式应对网络战。这些国家建议联合国创立可以接受的网络空间行为规范，交换关于国家立法和网络安全战略的信息，加强最不发达国家保护其计算机系统的能力。

这些动向表明，美国正在重新考虑它对网络军控的反对立场。美国对外关系委员会（CFR）的网络战研究专家罗伯特·科纳克（Robert Knake）认为，美国的参与标志着其态度的重大变化，证明奥巴马政府的外交接触战略付诸实施。美国网络司令部司令兼国家安全局局长基斯·亚历山大（Keith Alexander）也支持这一方式，他认为“俄罗斯的建议可能是国际辩论的起点”，“这是我们应该而且可能将要仔细考虑的问题”。因此，有人认为，就俄罗斯政府提出的关于限制使用网络战的提议达成一致，也不是不可能的。

2013年6月，美俄在经过两年多的对话之后，签订了美俄信息与通信技术（ICT）安全合作协定。双方决定通过高层对话深化接触，在“双边总统委员会”的支持下设立新的工作组，致力于评估新兴的ICT威胁，并提出应对这些威胁的具体联合措施；建立ICT“信任建立措施”（CMBs），采取一系列步骤增加透明度，并加强两国计算机应急响应小组（CERT）之间的联系，共享网络威胁指标，以利于扩大技术性网络安全信息的数量，增强保护关键网络的能力；利用1987年建立的降低核风

险中心（NRRC）相互通报情况，交换信息，以减低误判和升级ICT安全事件的几率；建立白宫和克里姆林宫之间的直接沟通热线，授权美国网络安全协调员和俄罗斯安全委员会副秘书长，在需要直接处理因ICT安全事件而造成的危机形势时，进行直接、安全的语音通信。此前，双方还相互交换了网络安全方面的白皮书等政策文件，以及非保密的ICT战略和其他相关研究。[30] 这些措施有利于提高透明度，并逐渐建立起双方之间的信任感。

然而，鉴于当前网络安全的总体形势以及国际社会就网络安全问题达成国际协议的微妙前景，不少人认为，这些信任措施还只能算是在签订正式的网络安全（军控）条约之前的过渡性或中间性措施。无论如何，可以认为，美俄在加强网络空间的互信方面迈出了重要的一步。不过，非常不凑巧的是，“棱镜”计划曝光后，斯诺登逃到了俄罗斯，并在那里获得了为期一年的临时避难，给美俄关系造成不小的困难，对刚有起色的美俄网络关系，以及对更广范围的网络安全（军控）蒙上了一层阴影，带来了巨大的不确定性，而双方围绕斯诺登的去留问题进行的博弈还将会继续下去。

除美国自身的种种现实考虑外，从更大的范围来看，还有一些客观因素也在制约着网络军控的进展和前景。首先是战略上的冲突。各国在网络空间的战略意图不同，制约着网络军控的实现。美俄双方的博弈便是例子。其次是概念上的难题。目前，国际社会对“网络武器”、“网络攻击”、“网络战”等概念界定都存在很大分歧，很难进一步讨论对网络武器、网络军备的限制。再次是技术上的难题，特别是对网络攻击

30 The White House, “U.S.-Russian Cooperation on Information and Communications Technology Security”, http://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol.

进行溯源非常困难，增加了网络军控的难度。同时，由于溯源难题以及网络武器的虚拟性等因素，难以建立有效的网络军控核查机制，进而增加了网络军控的实施难度。最后是军事诱惑问题。信息和网络手段的潜力尚未被人们完全所知，其所能带来的政治和军事好处也有无限可能。在此情况下，讨论网络军控难言真心实意。除非网络攻击造成严重的人道主义灾难或对全球战略稳定和安全带来严重后果，网络军控或可获得发展动力，而这又只能是一种后见之明。[31]

由此可见，美国对网络军控的态度经历了一些变化，具有一定的矛盾心理，今后可能还会有新的变化。网络军控的目标是防止网络空间的全球军备竞赛，但要就网络武器和网络军控达成广泛一致，进而形成具有普遍约束力的网络军控国际条约，仍需许多细致的工作、深入的讨论，以及较长的时间。

二、网络军控的规则之争

网络军控之所以难以推进，一方面是因为网络空间是一个较新的领域，许多国际规则尚未建立；另一方面则是因为网络空间已成为世界各国竞争、冲突与合作的崭新领域，特别是主要大国进行博弈的重要平台。为维护网络安全，规范各种行为体的网络行为，许多人和国际组织都呼吁签订国际网络协定或条约。然而，作为网络安全（军控）博弈核心的规则之争，将会持续相当长的时间。

31　吴翔、翟玉成："网络空间：倡议、问题与前景"，《现代国际关系》，2011年第12期，第18-19页；程群："网络军备控制的困境与出路"，《现代国际关系》，2012年第2期，第18页。

（一）相互竞争的网络安全政策主张

就像在其他议题领域一样，由于在历史文化背景、经济发展水平等方面的差异，不同国家在互联网发展和网络安全问题上也有不同的政策立场和利益诉求。例如，英国外交大臣威廉·黑格2011年2月在“慕尼黑安全会议”上提出了规范网络空间行为的七条规则，包括：（1）各国政府需要根据国家法律和国际法在网络空间采取相称性行动；（2）个人要有能力访问网络空间，包括技能、技术、信心和机会；（3）网络空间用户要显示出对语言、文化和思想多样性的宽容和尊重；（4）确保网络空间不断创新，观念、信息和言论自由流动；（5）要尊重个人的隐私权，并为知识产权提供适当的保护；（6）所有人都要集体行动，应对网络犯罪分子的威胁；（7）促进竞争性的（网络）环境，确保在网络、服务和内容方面的投资得到公平的回报。[32] 在实践上，英国还大力推动“伦敦进程”，先后在伦敦、布达佩斯和首尔召开网络安全大会，力图影响甚至掌控网络安全规则制定的总体方向。

北约合作网络防御示范中心（CCD COE）的法律顾问英尼肯·蒂克（Eneken Tikk）提出了网络安全的10条规则，包括领土原则、责任原则、合作原则、自卫原则、数据保护原则、管理责任原则、预警原则、信息获取原则、有罪原则和授权原则。[33] 2011年10月20日，中国裁军大使王群在联合国大会第一委员会关于信息和网络空间安全问题的发言中，提出了“构建和平、安全、公正的信息和网络空间”应遵循的五条原则：（1）和平的原则；（2）主权的原则；（3）统筹协调信息自由流动

32 William Hague, “Security and Freedom in the Cyber Age —— Seeking the Rules of the Road”, 4 February 2011, http://www.fco.gov.uk/en/news/latest-news/?view=Speech&id=544853682.

33 Eneken Tikk, “Ten Rules for Cyber Security”, *Survival*, Vol.53, No.3, June-July 2011, pp.119-132.

与安全流动的原则；（4）合作的原则；（5）公平发展的原则。[34] 2010年在瑞士达沃斯举行的世界经济论坛，也讨论了签订网络战国际协定或条约的前景。国际电信联盟秘书长图雷在这次会议上呼吁签署一份网络战国际协定，“就像战争之前的和平条约”。他认为，两个国家之间发生网络冲突的可能性正逐年增加。[35]

上述网络安全政策主张不仅名称有所差异，在具体内容和重点上也不尽相同，实际上反映了不同国家在网络安全问题上的不同诉求。

（二）网络安全规则类型

总体而言，网络规则可以分为一般规则、网络犯罪规则、网络战规则以及信息技术规则四大类。其中，一般规则包括网络主权、网络自由和网络安全（管制）等。

网络主权是国家主权在网络空间的自然延伸，应受到尊重和维护。主权国家是维护网络空间秩序的主体；尊重网络空间国家主权，是维护网络空间安全的重要前提。各国为维护网络空间秩序和安全所实行的公共政策应当得到尊重。目前，联合国、北约[36]等国际组织以及美国[37]、中国等国家均承认网络主权原则，承认主权国家对网络事务的管辖权。这应成为今后全球互联网治理和网络安全的重要基础。

---

34 “构建和平、安全、公正的信息和网络空间——中国特命全权裁军大使王群在联大一委关于信息和网络空间安全问题的讲话”，2011年10月20日，纽约，http://www.fmprc.gov.cn/chn/pds/wjb/zzjg/jks/fywj/t869573.htm。

35 “Treaty could Help Prevent Cyber Wars”, *Red Orbit*, February 1，2010, http://www.redorbit.com/news/technology/1816280/treaty_could_help_prevent_cyber_wars/.

36 Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013.

37 Harold Hongju Koh, “International Law in Cyberspace”, September 18, 2012, http://www.state.gov/s/l/releases/remarks/197924.htm.

与网络主权规则不同，国际社会对网络自由的认知则存在一定差异，不少国家更是担心网络自由成为某些国家干涉他国内政、侵犯一国主权的幌子。总体而言，美、英等西方国家主张互联网信息自由流动，俄罗斯主张信息安全，中国支持信息自由、安全流动。美国前国务卿希拉里·克林顿积极开展网络外交，大力推动“网络自由”。2010年1月，她在美国新闻博物馆发表“互联网自由演说”，将“自由接入互联网，不受限制地接触各类信息”等概括为“互联网自由”，并与美国传统的四大自由概念并列。2011年2月，她在华盛顿大学再次发表演说，提出要鼓励、帮助和资助其他国家的民众借助新媒体接触信息，追求民主、自由、人权等“普世价值”。在实践上，美国重视利用各种信息平台，传递外交政策信息，社交网站就已成为美国“箭袋中的一支新箭”。然而，斯诺登事件却揭露了美国网络自由政策的两面性。

实际上，网络空间既没有绝对的自由，也没有绝对的安全。这些一般性网络规则既有普遍的适用性，也具有一定的相对性。各国在实践中都需要努力保持主权、自由与安全之间的适当平衡。

绝大多数网络攻击都属于网络犯罪，这也是网络安全当前面临的最大问题。为此，许多国家都出台了相关法律，联合国预防犯罪和刑事司法委员会也设立了打击网络犯罪问题政府间专家组。目前，各国在打击网络犯罪问题上已有不少合作，但尚无普遍性的网络犯罪国际条约或法律。其中，比较成型的是欧洲理事会2001年11月签署的《网络犯罪公约》（亦称《布达佩斯网络犯罪公约》）。[38] 不过，它也存在不少问题，如内容需要更新、代表性不足等。今后，开展国际合作，打击网络犯罪将是维护网络空间安全与秩序的重要组成部分。同时，制定普遍性

38 Council of Europe, *Convention on Cybercrime*, Budapest, 23 November 2001, Council of Europe Treaty Series No. 185, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

的网络犯罪法规也将是国际社会面临的重点和难点，既要考虑到法律条约的普遍适用性，也要考虑各个地区和国家的具体国情及历史文化背景。

信息与通信技术（ICT）规则与标准的制定是互联网治理的基础所在。由于世界各国ICT发展水平不一，在全球互联网的管理、基础信息资源的分享等方面也处于不同地位。围绕互联网的管理权、源代码的开放等技术和规则问题，国际社会一直进行着激烈的博弈。在ICT规则与标准的制定方面，国际电信联盟（ITU）的权威性应在今后得到充分发挥和尊重，互联网名称与数字地址分配机构（ICANN）等组织的民主性则应得到加强。

三、网络战与网络军控规则

前述《信息安全国际行为准则》、《布达佩斯网络犯罪公约》、《塔林手册》等有关网络安全的倡议，对未来的国际网络立法有一定借鉴意义。从国际法角度看，全面或专门涉及网络安全的普遍性国际条约和法律文件目前还是一个空白，国际社会更无直接适用于网络战和网络军控的国际准则。今后，国际社会可以通过不同层次、不同形式的国际规则，来规范不同类型的行为体在网络空间的行为，包括具有普遍约束力的国际条约、专门规范网络战行为及网络军备的国际协议等。然而，美国试图以“先发制人”网络打击政策为其网络攻击提供合法性，这不仅无益于网络军控及其规则制定，反而会引发系列难题。

（一）网络战与国际条约

与陆地、海洋、天空及外空等物理空间不同，网络空间有其独特性。为避免后见之明，虽然人们对网络战的存在与否尚存争议，虽然现有国际法在用于网络空间时会有许多问题，但这并不应阻止人们去探索国际法（包括战争法）在网络空间的适用性问题。在编撰《塔林手册》的过程中，北约汇集了成员国在国际法、国际关系、网络安全等领域的几十位专家，成员国政府也派代表作为观察员参与有关讨论。作为一部指导手册，内容非常全面。当然，北约表示《塔林手册》并不代表其官方观点，而是各位专家的个人观点。在人们对网络战的存在与否仍然存在分歧的情况下，该手册的出台表明西方国家在探索规范网络战方面走得可谓相当超前。

客观上，网络战对现行国际法构成不少挑战，包括：颠覆传统的领土及主权概念、较难追究国际损害行为的责任、合法自卫原则和宣战原则难以适用、挑战区分原则和军事必要原则、难以界定网络欺骗的合法性、无从保护中立国的利益等。[39] 因此，现有国际法难以简单直接地用于网络空间。例如，《联合国宪章》第二条第4款规定，全体成员国在国际关系中不得以武力威胁和使用武力来破坏其他国家的领土完整和政治统一，或采取违背联合国宗旨的行为。这一解释把通过网络进行的信息战也涵盖其中，确定了其非法性。但是，对手采取的网络战并不会轻易被发现，通常是在人们无法知道的前提下进入了交战状态，这实际上就要求对有关规则进行更为详细的解读，以适应网络空间的现实，切实达到维护国际安全与和平的目标。《外层空间条约》规定，各国必须把月球和其他天体绝对用于和平目的。但是，卫星却可以作为网络战的

39　田英：《浅议网络战中的国际法问题》，《法制与社会》，2007年第7期，第198-199页。

“中继平台”，该条约并没有禁止把卫星用于网络战的条款。《国际电信公约》则规定，无论出于何种目的，所有国家都必须确立并遵守如下立场，即不能对其他成员国的无线电广播或通信进行干扰。但是，正在研发中的网络战手段不仅会干扰成员国的无线电传播，还会改变信息的真假，这显然违背了该公约的宗旨。此外，经合组织1992年通过的《信息系统安全准则》也只论及了计算机犯罪，并没有涉及信息战方面的规定。前述《信息安全国际行为准则》内容广泛，寻求限制对互联网的非和平使用，并使互联网的治理国际化。然而，美国却认为现有的国际安排已经足够，因为它担心中国等国会使用一切可能的手段（包括国际民意和新的国际公约）来限制美国的军事选择。此外，美国坚持认为，溯源、核查等技术难题将严重影响国际网络军控条约的可信度和有效性，但实际上美国是要以此为借口，保持自己在网络空间领域的领先地位和技术优势。

如前所述，自1998年俄罗斯向联合国大会提交了有关信息安全的提案以后，信息安全便被列入联合国议程，并通过了一系列决议。此外，联合国还先后设立了三个政府专家组（GGE），考察网络领域的现有及潜在威胁，并提出应对这些威胁的可能合作措施。在2010年专家组报告（A/65/201）的基础上，第三个工作组于2013年6月提交了新的专家组报告（A/68/98）。与第一份报告相比，新报告取得不少进展。例如，“关于国家负责任行为的规范、规则和原则的建议”部分表示，专家组注意到了中俄等国提交的《信息安全国际行为准则》；国际法、特别是《联合国宪章》适用于各国使用信息与通信技术（ICT），对维持和平与稳定及促进创造开放、安全、和平和无障碍信息与通信技术环境至关重要；国家主权和源自主权的国际规范和原则，适用于国家进行的信息与

通信技术活动，以及国家在其领土内对信息与通信技术基础设施的管辖权。此外，新报告在建立信任措施、帮助发展中国家提高信息与通信技术能力建设等方面也取得重要共识。[40]

可以说，新报告既是各国相互谈判和妥协的结果，也是各国务实合作的结果，在一般性网络安全原则和具体问题上均取得进展，为探讨国际法在网络空间的适用性问题打开了一扇窗户，也为未来网络安全国际协议的达成提供了“最小公约数”。今后各国工作的方向应是在考虑网络空间特性的前提下，探讨如何把现有国际法的具体条款用于网络空间的新现实，同时也应根据网络空间的新现实而创设新的国际法律条款，进而增强其合法性、适用性和有效性。

（二）网络战与武装冲突原则

武装冲突法与网络战（军控）有着最直接的关联性。然而，在国际法的意义上，武装冲突法只适用于两国发生冲突的情形。根据《日内瓦公约》的定义，“交战”意味着身体上的对抗；“进入别国领土”意味着有形的越界行动。现有武装冲突法只涉及到“陆战”、“海战”和“空战”，而网络战根本无法用陆地、海洋、天空、外空来界定。网络战没有像爆炸一样的物理毁伤，也没有有形的军队攻城掠地。因此，武装冲突法在网络空间的适用性问题存在很大争议。目前，一般认为，只有在两种情况下，武装冲突法才适用于网络空间：一是国家间发生战争期间；二是网络攻击造成的损伤达到了现实战争的程度，特别是造成了直接的大规模人员伤亡。

40 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, 24 June 2013, http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=http://www.un.org/disarmament/topics/informationsecurity/&Lang=C.

武装冲突原则是参战方应遵守的行为准则，主要包括：（1）军事必要原则，强调参战各方只能使用战争法允许的正规力量，以最低的代价，部分或完全制服敌人。网络战所攻击的目标多是别国的关键基础设施，很容易使敌国整个社会都陷入瘫痪，这远远超出了“军事必要”的原则。（2）人道主义原则，强调参战各方的作战手段必须与达成战争的目的相符合。现有战争法对地雷、燃烧弹等都进行了限制，而某些信息网络武器，如“病毒”和“逻辑炸弹”的威力可能并不比常规武器差，但却不在现有战争法的范围内。（3）“骑士原则”，强调交战各方必须要有“完备的手续和礼节”。武装冲突法允许进行欺骗，但倘若交战一方以另一方最高指挥官的口吻向其部队发令放下武器，则会使对方军队遭受重创。这在伊拉克战争中已有所体现。如前所述，虽然当时这还只是劝降口号，属于心理战和宣传战的范畴，但互联网的威力却得以展示出来。如何使这种现象与战争法原则相契合，将是未来的讨论重点。

美国智库战略与国际研究中心（CSIS）的专家认为，现有的武装冲突法适用于网络空间，其中的比例原则、区分原则等已为保护民用目标提供了依据。在宽泛的意义上，这种看法并没有什么不妥。例如，尽管网络空间的民用和军用基础设施界限模糊，但《日内瓦公约》和《海牙公约》都有关于保护平民的规定，所有国家在网络空间都应同意遵守这些规定。然而，在实际运用区分原则时，可能遇到的首要难题便是如何区分民用与军用网络。与其他的物理设施不同，要把军用和民用网络区分开来可能是非常困难的。即使是采取了物理隔绝措施的民用或军事网络，所谓的离线炸弹、逻辑炸弹也可以渗入进去，实施破坏活动。此外，把网络活动定为网络攻击的门槛也应该很高，因为并非发生在网络

空间的每件坏事都是网络攻击或使用武力，其中的大多数恶意活动并非网络攻击或战争。否则，世界各国将陷入“所有人反对所有人”的霍布斯式战争状态。简言之，战争法的根本“精神”可能毫无疑问地可以适用于网络空间，但其具体的法律条文和原则，无疑需要根据网络空间的特性而进行某些调适。否则，只是抽象地谈论战争法在网络空间的适用性是没有意义的。

（三）“先发制人”网络打击政策逆势而动

无论是作为一种姿态，还是作为一种试探，或者是源于内心的自大，如前所述，美国的“秘密法律评估”认为，在有可靠证据表明外国将对美发动“重大”数字攻击时，总统将有权下令发动“先发制人”网络打击。事实上，在探索和制定网络规范时，美国一直努力掌控主导权。除大力支持网络自由外，美国更是试图以“先发制人”网络政策作为制定网络战规则的试金石，逆向推动战争法在网络空间的适用性。美国此举还旨在为其网络攻击行为提供合法性，尽管这种合法性并不具备国际法的合法基础，而是自我赋予的。此外，该政策还面临着内在的两难问题：遭“先发制人”网络打击的国家可以很容易辩称自己清白无辜，倘若美国难以提供有效证据，那么这将大大削弱其“先发制人”行为的合法性。美国高官也承认，“很难向世界提供证据，表明你打击的是某些有致命危险的计算机代码”。[41]

在制定新规则时，美国并非没有顾虑，甚至十分在意“先发制人”网络行动的影响。参与规则制定的官员表示，美国政府此项评估涉及

41 David E. Sanger and Thom Shanker, “Broad Powers Seen for Obama in Cyberstrikes”, *The New York Times*, February 3, 2013, http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html?_r=0.

的一个重大问题，就是界定在终止或报复网络攻击时，“什么才算是合理的、成比例的武力”。美国尤其担心“先发制人”政策成为他国对美发动攻击的理由，以至威胁自身安全。例如，在攻击伊朗核设施（美国从未承认）期间，奥巴马坚持认为应“精确定位”，不影响医院和电力供应，还屡次担忧美国使用网络武器一事可能被他人用作攻击美国的借口。美国国家科学院的网络专家赫伯特·林（Herbert S. Lin）也表示：“我们正在进行一场大辩论，即怎样才算得上在网络空间使用武力或武装攻击。在网络空间对他国采取进攻性行动时，我们需要知道界线在哪里，从而不至于越过这些界线。”[42]

实际上，“秘密法律评估”本来是要解决美国“先发制人”网络攻击所面临的上述法律难题。目前来看，该政策基本上为美国网络行动划定了“合法”界限，使其政策“清晰化”，并为今后的“先发制人”网络攻击扫平道路。然而，这里的问题在于，通过“先发制人”网络攻击政策，美国可能安全了，但其他国家却不安全了，徒增了其他国家的威胁感和恐惧感；而其他国家若要维护自身的网络安全，也可能不得不加强网络军备。这样，就引发了网络军备竞赛，对网络军控的推进、网络安全的维护和网络秩序的建构都极为不利。

42 Ellen Nakashima, “Pentagon Considers Preemptive Strikes as Part of Cyber-defense Strategy”, *The Washington Post*, August 28, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/08/28/AR2010082803849_pf.html.

第四章 网络军控与中美网络关系

美国是世界上最大的发达国家，在信息与通信技术方面也遥遥领先于其他国家。中国是世界上最大的发展中国家，也是世界上网民数量最多的国家。因此，网络空间不可避免地成为中美两国相互打交道和发展关系的新领域。近年来，网络关系实际上已成为中美关系的重要组成部分，甚至成为影响双方在其他领域关系的重要变量。

一、中国互联网发展与安全状况

中华人民共和国国务院新闻办公室2010年6月8日发布的《中国互联网状况》白皮书指出，“中国把发展互联网作为推进改革开放和现代化建设事业的重大机遇。中国政府先后制定一系列政策，规划互联网发展，明确互联网阶段性发展重点，推进社会信息化进程”。[43]2014年是中国全功能接入国际互联网20周年。20年来，中国互联网取得长足发展，已成为人们日常生活不可或缺的组成部分。根据中国互联网网络信息中心（CNNIC）2014年1月发布的第33次《中国互联网络发展状况统计报告》，截至2013年12月，中国网民规模达6.18亿，互联网普及率（Penetration Rate）为45.8%；手机网民规模达5亿；网民中农村人口占比

43 中华人民共和国国务院新闻办公室：《中国互联网状况》，2010年6月8日，http://www.scio.gov.cn/zfbps/ndhf/2010/Document/662572/662572.htm。

为28.6%，规模达1.77亿；中国域名总数为1844万个，其中.CN域名总数达到1083万，在中国域名总数中占比达58.7%；中国网站总数为320万。[44]由此可见，中国互联网发展迅速，应用广泛。

与此同时，中国也面临着不少网络威胁，网络安全挑战不容忽视。根据国家计算机网络应急技术处理协调中心（CNCERT/CC）2014年3月发布的《2013年我国互联网网络安全态势综述》，中国基础信息网络运行总体平稳，但域名系统依然是影响安全的薄弱环节；公共互联网治理初见成效，但打击黑客地下产业链仍任重道远；移动互联网环境有所恶化，生态污染问题亟待解决；经济信息安全威胁增加，信息消费面临跨平台风险。此外，值得注意的是，针对中国的国家级有组织网络攻击行为显著增多，给中国国家关键基础设施和重要信息系统带来严重威胁和挑战。其中，据CNCERT监测，中国面临大量来自境外地址的网络后门、网络钓鱼、木马和僵尸网络等不同类型的攻击行为。[45]

因此，除制定促进互联网发展和应用的系列政策外，中国还逐渐把网络安全提上国家政治日程，在网络立法、政策制定、机构设置等方面多管齐下，切实维护网络安全。2014年2月27日，中央网络安全和信息化领导小组第一次会议在北京举行。习近平主席在讲话中强调，网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国。习近平指出，网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统

44 中国互联网络信息中心：《中国互联网络发展状况统计报告》，2014年1月，http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201403/P020140305346585959798.pdf。

45 《2013年我国互联网网络安全态势综述——CNCERT观点》，2014年3月，http://www.cert.org.cn/publish/main/upload/File/2013%20Network%20Security%20Situation.pdf。

一实施。做好网络安全和信息化工作，要处理好安全和发展的关系，做到协调一致、齐头并进，以安全保发展、以发展促安全，努力建久安之势、成长治之业。总之，没有网络安全就没有国家安全，没有信息化就没有现代化。今后，中央网络安全和信息化领导小组将发挥集中统一领导作用，统筹协调各个领域的网络安全和信息化重大问题，制定实施国家网络安全和信息化发展战略、宏观规划和重大政策，不断增强安全保障能力。[46]

二、中美网络关系视野下的网络军控

如前所述，在各国加快网络建军的情况下，中国网络安全面临的压力事实上也大幅增加，网络问题对中国与其他国家之间关系的影响也越来越明显。例如，2013年1月至8月，中国境内被黑客篡改的网站达2万多个，被境外通过木马或僵尸网络控制的主机达800多万台。80%以上的中国网民受到过网络侵害，每年经济损失达数百亿美元。[47] 美国拥有对互联网域名根服务器的监控权，加之在计算机硬件和软件上的垄断地位，美国可以说牢牢掌握着国际互联网的控制权，但它对互联网的依赖程度很大，在网络空间同样也是脆弱的。[48] 面对共同的挑战和威胁，中国和美国在大力提升自身网络能力的同时，也要努力加强在网络军控领域的沟通和交流，带头确定网络军控的标准、原则和行动方法。

---

46 “习近平：把我国从网络大国建设成为网络强国”，新华网，2014年2月27日，http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm。

47 “全球网络空间合作峰会在美举行”，新华网，2013年11月6日，http://news.xinhuanet.com/world/2013-11/06/c_118032595.htm。

48 “美国政府网络面临极大挑战，封闭只会导致灾难”，中国计算机安全网，2012年10月8日，http://www.infosec.org.cn/news/news_view.php?newsid=16271。

（一）区别网络军控的轻重缓急，以国家层面的网络行为规范为重点

网络战通常分为两个层次：一是战略网络战，主要在国际互联网上展开，用于攻击对方的政治、经济和军事网络，从而使国家机器无法正常运转，导致社会动乱，迫使政府倒台。二是战场网络战，主要是指在战场上有线和无线网络的攻防行动，破坏敌人的指挥、控制、情报、侦察等系统。这是冷战结束以来世界主要国家军队建设的重要方向。

网络军控主要是指战略网络战，攻击目标是国家政治、经济、军事机构和设施以及整个社会系统得以运转的计算机系统，利用信息技术多渠道、多形式地瘫痪敌方军事、金融、电力、交通系统的网络。一旦这些系统受到攻击，停水、断电、交通瘫痪、战略武器失控便会接踵而至。美国正试图综合使用多种方法，保护国家关键基础设施免受网络攻击。方法之一就是通过多边协议来限制国家层面的攻击行为。因此，今后网络军控应着眼于国家层面的网络攻击行为。

（二）美国要主导网络军控，中国也应积极参与其中

2011年5月的《网络空间国际战略》报告，充分阐述了美国要在国际网络空间发挥的作用。英国《金融时报》评论称，这是美国第一次把其外交政策目标与互联网政策结合在一起，把外交、军事和网络安全议题结合在一起。美国国务卿希拉里·克林顿在报告发布会上声称，报告中提及的政策是美国互联网外交的要素，美国将会在这些政策领域发挥主导作用。

今后，美国仍会运用外交手段，辅助以其他手段，通过国与国之间、地区与地区之间以及国际组织等双边和多边方式宣传与推进美国的互联网战略，设置相关国际互联网发展、治理、自由与安全的全球议题，掌握全球互联网发展与安全标准及规则的主导权。在网络主权、自由、安全等问题上，中美双方都有不同观点，中国应更加积极，不仅要参与其中，更要主动把握创议权，争取更多话语权。

（三）美国网络立法相对完善，中美可相互沟通借鉴

美国凭借其信息网络的优势，还会促使发展中国家进一步开放信息网络技术、产品和服务市场。为通缉所谓的黑客和打击网络犯罪，美国还将谋求各国在网络执法与司法领域里的“协调一致”，这将给美国“越界执法”提供便利条件和行动自由。在这方面，美国现已建立起较为完善的国内立法，将对国际网络军控进程产生重要影响。

美国从20世纪50年代就开始制定信息政策，为世界上最早制定相关政策的国家，这些政策常常具有法律效力。从20世纪70年代开始，一批法律也随着计算机以及互联网络的普及而相继出台。[49] 这一时期的法律政策大都具有较强的专业和技术性质，涉及计算机通信安全与隐私保护等内容。20世纪90年代以来，美国出台的网络政策中包含了越来越多技术之外的因素，如1993年的《国家信息基础设施行动计划》（又称“信息高速公路战略”），标志着美国信息化建设工程的开始；1994年的

49　包括1977年《联邦计算机系统保护法案》、1984年《伪装进入设施和计算机欺诈及滥用法》、1986年《电子通信隐私法》和《计算机欺诈和滥用法》、1987年《计算机安全法》、1988年《计算机查找与隐私保护法》、1989年《计算机查找与隐私保护法修正案》、1990年《电子通信秘密法》和《中小企业计算机安全、教育及培训法》、1991年《高性能计算机及网络法案》和《统一电子交易法》、1994年《计算机滥用法修正案》、1995年《数字域名法》、1996年《全球电子商务框架》、1997年《域名注册规则》等。

《全球信息基础设施计划》致力于促进各国信息基础设施的发展和各国间的合作，鼓励政府和民间私人的合作，以促进全球信息发展。[50]

进入21世纪以来，美国进一步加快了网络立法的步伐，并且更多地考虑了国家安全和战略等因素，如2001年《爱国者法》；2010年《将网络空间视为国家资产保护法》、《国际网络空间与网络安全合作法》、《美国国土安全网络与物理基础设施保护法》、《促进全球响应网络攻击法》、《网络安全法》、《网络安全加强法》、《国际网络犯罪报告与合作法》；《2011年国防授权法》等。[51]

美国网络立法不仅起步较早，也较为全面，既涉及技术维度，也涉及法律、政治和国际等各个维度。中国在网络立法的过程中对美国经验有所借鉴，双方有所合作。然而，中国对美国网络立法的深入、系统研究尚有欠缺。今后，中国不仅要关注美国国内的网络立法，而且要加强与之沟通，表明中方立场，以有利于国际网络军控规则的形成。

（四）中美应合作探讨可能的网络军控方案

长期以来，美国一直抵制网络武器条约，唯恐全球对网络实行严格管理后，削弱其网络公司的主导地位，抑制其创新能力，并且限制其网络赖以生存的开放性。但是，由于过于依赖计算机及其网络，美国已成为最容易遭受网络攻击的国家。基斯·亚历山大曾表示，美国将响应俄

50　此外，还有1996年的“下一代网络计划”，旨在促进网络的更新换代，解决原有网络设施陈旧和不堪重负问题，以保持美国在信息通信技术上的绝对优势地位，确保其继续成为世界经济和政治的领导者；1997年的“二代互联网计划”保证大学和科研机构使用先进的网络，在全球范围内促进高层次教育和信息服务。

51　其他的还包括2002年《电子政务法》、《联邦信息安全管理法》、《信息网络安全研究与发展法》；2008年《身份盗用实施与赔偿法》；2009年《美国信息与通讯促进法》等。

罗斯长期以来关于制定一项网络条约的呼吁，并将其作为“国际社会辩论的起点”。但是，他认为这一条约不可能按照美俄《削减进攻性战略武器条约》的方式进行，因为核弹头可以清点计数、导弹的数量可以追踪记录，而网络武器却更像生物武器，可以随时应用。因此，对于美国对网络军控的关注点，中国应了然于胸。

总体而言，三大问题将决定美国是否愿意参加网络军控：一是美国的基础设施是否强大到足以应对国家级的网络攻击。二是美国是否具备可靠的网络战方法来攻击敌人的国家基础设施，并对其进行战略性打击。三是有规范价值的国际公约是否充其量只对美国有限制意义，其他国家能否确保它们对这种条约的承诺。鉴于网络战在军事上的重要性和威慑意义，美国不大可能认可任何可能阻碍其发展或弱化这方面能力的限制条件。美国还强调通过网络手段预先阻止网络攻击，作为其国家基础设施防御的一部分。

自20世纪90年代中期以来，美国政府就一直在努力改进关键基础设施的安全程度，包括升级系统的安全程序和技术，采用新的标准和规范，更重要的是向本国民众征求改进措施。克林顿、布什、奥巴马连续三任总统都宣布了美国在这方面的工作方案，政府部门和有影响的公司、行业协会和研究机构都参与其中。然而，唯一的结论是美国并没有在确保网络安全方面取得重大进展。没人能回答美国是否有足够的能力打击其他国家的关键基础设施，因此，美国将很难拒绝用国际公约来限制其他国家的网络战能力。

今后，中美应合作探讨可能的网络军控方案。

（五）推动多边合作，促进全球互联网治理

就像在国际关系的其他领域一样，中、俄两国与美国在网络空间领域的立场也有很大不同，并成为美国备战网络空间的借口。2009年，美国国家情报委员会指出，中国在全球范围内对美国构成了复杂的威胁，特别是中国可能在网络领域对美国发动攻击。

就网络军控而言，中国与俄罗斯和其他发展中国家在认识上更接近。除前述的《信息安全国际行为准则》外，上海合作组织2006年6月也通过了《上海合作组织成员国元首关于国际信息安全的声明》。此外，中、俄还在各自国内拥有自成体系的研究。中国和俄罗斯等国主要关注范畴更广泛的信息安全，而美国更关注的则是网络这一具体领域。在就网络安全和网络军控谈判的过程中，中国可以与俄罗斯等立场相近的国家加强沟通和协调。

美国在互联网领域的优势地位明显，但在网络规则和政策制定问题上，美国无法一手遮天，特别是国际电信联盟等联合国机构今后仍将是国际博弈的重要场所。今后，中美都应大力支持联合国及其机构，共同实现国际互联网基础资源管理的平等权利，建立多边、透明的国际互联网基础资源分配体系，促进全球互联网均衡发展，不仅维护自身网络安全，也为全球互联网安全与发展做贡献。

结　语

信息技术的飞速发展改变了人类社会的生活模式，改变了国家安全的内涵与外延，改变了现代战争的基本形态。过去只有动用实兵攻城掠地才能征服一个国家，而今网络攻击可以破坏一个国家的基础设施，影响人们的正常生活。网络正在演变成新的战争和犯罪的空间，国际社会，特别是中美两个大国必须要联手行动，建立起规范网络行为的准则和条约。脆弱性是共同的，挑战也是共同的，因此网络军控应成为中美建立新型大国关系的重要试验场。

从国际实践看，国际法规永远落后于国际技术的发展。面对快速发展的信息技术，如何规范和约束这种不带物理毁伤性的软杀伤能力，是国际社会需要认真对待和考虑的问题。如今的网络空间像上世纪初汽车行业刚刚兴起和高速公路得以兴建时期，掌握信息技术优势的国家可随心所欲地行驶，不需要交通规则。然而，随着这种技术的普及，越来越多的国家会掌握这种技能。同时，信息技术的特性也使普通百姓可以充当网络战士的角色，对国家造成灾难性的破坏。

美国是当今信息技术领域里的龙头老大，它并不愿意更多地谈论“网络主权”，也不愿意谈论战略性网络安全，而只愿意谈与美国利益密切相关的网络犯罪。和当年美国企图垄断正在发展中的核技术相比，信息技术具有更快的传播性和更强的普及性，美国无法抵挡。网络是连通的，也是脆弱的，需要国际社会联手维系其秩序，这就为网络军控提出了新的要求。

中美两国正致力于建设新型大国关系，网络安全是中国和美国极其关注的一项重要内容。首先，两国要明确这种关切的着力点有何不同，形成共识，才能有效地沟通。其次，中美的网络安全对话要把握住两国的共同需求，而不是以网络安全来向对方发难。最后，中美网络安全不单单是中美两国的问题，正像网络技术无法用传统边界来限定一样，需要联手国际社会所有成员国加以应对。这其中，中美两国都应该承担起负责任大国的责任，建章立制，规范网络空间的行为，从而保证人类文明在继陆地、海洋、天空和外空之后的第五空间有序地延续和发展。

已发布《CIIS研究报告》目录

第一期　2013年9月

中美新型大国关系：挑战与契机

作者：阮宗泽、刘飞涛、沈雅梅、崔　磊、杜　兰

第二期　2013年9月

追寻“世界梦”——中国推动建设和谐世界的进展评估与未来展望

作者：陈须隆

第三期　2014年6月

网络战备、军控与美国

作者：滕建群、徐龙第

《CIIS研究报告》简介

《CIIS研究报告》是中国国际问题研究所研究人员撰写的、不定期发布的专题研究报告。报告选题瞄准当前国际形势的热点和中国外交的重点，将形势研判、学理探讨和政策分析融为一炉，力求做到观点鲜明、语言精练、资料详实、立论有据、分析透彻。

《CIIS研究报告》同时发布中英文版，并在国研所网站提供全文下载。报告反映的是作者本人或相关课题组的观点，并不等同于国研所的立场。

内容提要

信息技术的迅速发展和广泛应用使网络电磁空间成为国家、社会及个人生活不可或缺的组成部分。在带来便利的同时，其蕴含的风险和挑战也在不断增加。有能力的国家纷纷采取措施，出台网络政策，制定网络战略，争夺“制网权”，网络电磁空间的战备进而成为多国军队建设的重要内容。“非国家行为体”也利用网络空间的脆弱性和连通性，给国家和社会带来巨大的创伤。

不论是爱沙尼亚、格鲁吉亚和伊朗受到的网络攻击，还是2013年曝光的美国监控事件，都表明维护网络电磁空间秩序和安全的难度在加大。然而，在网络空间的国家战备和个人入侵面前，国际社会至今还没有专门的国际法，特别是军控法律体系，来规范国家和个人的网络行为。部分国家凭借其在信息技术上的优势地位，也不愿谈论对网络空间相关行为的约束。在此背景下，制定应对网络威胁、维护网络秩序和安全、规范网络空间行为的国际准则以及健全法律体系已是势在必行，网络军控正成为国际军控与裁军领域的重要内容。

上世纪70年代开始，美国一直是信息技术的领军国家，依靠其先进的信息优势和充足的经费保障，制订出较为完整的网络政策与战略，并加紧网络部队建设和网络战理论研究。作为二战结束后国际秩序的主要制定者，在国际军控与裁军领域，美国扮演着其他国家不可替代的角色，其在网络电磁空间里的一举一动，不可避免地牵扯到未来国际网络军控的发展方向。

本报告首先分析了当前网络空间的形势，介绍了关于国际社会网络战的讨论、现有国际法对网络战的约束等问题，对美国等国家的网络战备以及网络安全诉求等做出分析，提出要保证网络空间不被滥用和引发国际冲突，必须建立新的网络军控体制和规则，这其中美国有不可推卸的责任。报告指出，中美正谋求建立新型大国关系，网络空间的合作应该成为这种关系建设的重要内容。

编辑：科研处
地址：北京市台基厂大街头条三号中国国际问题研究所　邮编：100005
电话：010-85119556　电子邮箱：keyan@ciis.org.cn　网址：www.ciis.org.cn