第六章
构建攻防兼备的网络部队

军事力量是维护国家安全最重要和最直接的手段，冷战后美国军力建设的核心是在军事领域维持绝对优势并形成威慑力和遏制力，胁迫对手放弃攻击企图或避免与美国直接对抗，必要时直接击败敌人。信息革命给美国军事带来了两个方面的变革：一方面是以信息技术手段改进军队的训练、管理和作战，即新军事革命；另一方面网络空间逐渐被纳入美军作战领域，进而构建攻防兼备的网络军队成为网络战略的核心内容。本章依次分析美国网络空间作战的战略构想、网络作战的管理和组织、网络攻防能力建设、网络作战的实践四方面内容。

第一节　战略构想：以信息优势制胜网络战争

根据美国国防部的定义，网络空间作战是“在网络空间或通过网络空间运用网络能力达成军事目的，包括运行和保护全球信息网格的计算机网络作战和行动”。[①] 这表明网络空间既是网络作

① U. S. Department of Defense Joint Chiefs of Staff, *Joint Publication 1 - 02: Dictionary of Military and Associated Terms*, Pentagon Publishing, 2015, p. 93.

战的平台，又是网络作战的路径，这种表述实际上是为了将传统的作战方式和武装力量和网络空间的攻防和网络部队统一起来，进而明确美国将网络空间军事化的战略意图。

一、网络空间的军事化

就概念而言，网络空间军事化意味着赋予网络空间军事属性、为网络空间配备武装力量和防御能力，或将网络空间用于军事用途。[①] 这意味着网络空间成为战场，成为发展和部署军事力量的场所，敌对各方运用特定软件工具和指令遂行阻塞、切断和破坏网络基础设施、应用系统和重要数据的攻防行动。网络空间军事化的程度取决于军事机构承担网络作战的目标定位、职责范围和手段运用，即判断网络空间军事化与否及程度可以从武装力量在网络防御上扮演的角色和在网络进攻方面拥有的自由度而定。

网络空间军事化问题一度成为美国决策层和学术界争议的焦点，媒体和社会公众也给予高度关注。对于一个在很大程度上取得国际共识的、以技术和商业活动为主要内容和可信、安全、互联互通为主要目的全球共享空间，是否允许军事力量的参与，是否适用于作战用途，国际社会倾向持反对意见，或至少需要建立一个各方共同遵守的原则，严格限定军事行动在网络空间的范围和手段。然而互联网的起源却赋予军事化论者另一种解释，互联网的前身是美国国防部为应对原苏联核威胁而研发的一个军事通信平台，原苏联发射第一颗人造地球卫星后，美国国防部针对如何维持遭到空基核武器攻击后的反击能力，要求国防部高级研究计划署

---

① 网络空间军事化（militarization of cyberspace）或军事化网络空间（militarizing cyberspace）的概念辨析参见 Sean Lawson，“Is the United States Militarizing Cyberspace?”，*Forbes News*，November 2，2012，http://www.forbes.com/sites/seanlawson/2012/11/02/is-the-united-states-militarizing-cyberspace/，最后浏览日期：2015 年 8 月 20 日。

(Advanced Research Projects Agency, ARPA)设计一个全国性通讯网络,该网络(即阿帕网)于 1969 年 10 月正式运行,成为连通加州大学洛杉矶分校和斯坦福大学间的通讯网络。所以从互联网的起源来看,它确实是一个军事项目,由军方和研究机构管理和运行,运用于构建国防军事和国家安全的信息基础设施,且一直是军事和战略通讯的核心部分,直到一个完全独立的商业平台开发出来并与军事部分分离。因而互联网的军事渊源成为美国国防部将网络空间军事化的特殊理由,如网络司令部首任军事法官格雷·布朗(Gary D. Brown)就声称是国防部"平民化军事网络"的努力促进了互联网的繁荣,这一逻辑成为支持在网络空间进行军事部署和攻防作战的理由。

对于是否将网络空间作为适用于全方位作战的领域,即是否推动网络空间全面军事化的问题上,主要还是取决于美国最高决策层的战略选择,即这样的选择对于美国总体的国家安全和长期的国家利益究竟有何利弊。网络军事化还要解决与现有法律规范对接以及获得公众认可和舆论支持的问题,由于网络空间攻防作战涉及域外军事行动,就必须获得相应的法定授权,由于在是否存在网络空间的主权及边界划分上没有得到国内和国际的共识,因而网络军事行动的授权主体及法律依据都存在模糊地带,至少在美国国内还不存在公开支持网络空间军事行动的法律和政策依据。2015 年国防部《网络战略》是一个重要的突破,按照该战略,既可以用传统的威慑和攻击手段来应对网络空间的威胁,也可以用网络威慑和攻击手段来应对传统威胁,该战略将网络空间和现实空间贯通,消除了军事行动界限的障碍。[①] 即便如此,授权问题依然存在,即网络作战行动是否需要得到国会授权及是否需要经过宣战的法定程序仍然存在争议。

---

① U. S. Department of Defense, "Cyber Strategy", April 2015.

当授权问题未解决之前，通过情报系统的秘密行动来实施网络攻击或者网络监控行为，还是能够从现存法律中寻找到一些依据，如《美国爱国者法案》允许情报机构采用包括侵入恐怖分子活动网络的方式以监控或破坏威胁美国国家安全的网络行动。而情报机构的秘密行动是无须获得国会预先授权的，这一方面是军事行动和情报行动日益密切交织无法清晰分辨，另一方面就是前面提到关于互联网本身就是一个军事通讯网络的逻辑，现在可利用该网络继续发挥军事支持作用和实施军事行动。从处理国家安全局和网络司令部的行政管辖和业务指导方面的关系时，也表明了将情报行动和军事行动结合起来可以获得对法律风险的规避和行政授权的便利。

对于是否确定将网络空间的军事化作为制定政策的基础，美国政府仍然持矛盾心态。一方面，出于保护本国经济社会运行所依赖的信息基础设施和网络应用系统，美国认识到维持网络空间非军事化的属性有利于其安全和发展利益，毕竟如果各国竞相发展网络攻击能力，则网络武器的扩散将会带来军备控制的新问题；另一方面，网络技术和网络应用提供了非常丰富的潜在军事可能性，又促使美国政府特别是军事部门力图充分运用和挖掘网络空间的军事潜力，以获取信息时代的战略优势。因而 2014 年 3 月美国时任国防部长查克·哈格尔在马里兰州米德堡网络司令部还明确表态美国不寻求将网络空间军事化，称国防部对在政府网络之外的网络行动保持克制，并敦促其他国家采取同样做法。

二、确保网络空间的战略优势

20 世纪 90 年代初，美国通过海湾战争验证了其强大的军事实力和新型军队的实战效果，之后，美国继续进行其军事力量的信息化改造，以继续保持军事能力上的绝对优势。这也构成了美国推动信息革命的一个重要动力，“一个国家如果能够最好地领导这

场信息革命，那么它将比其他国家更为强大，在可预见的将来，这个国家就是美国，美国有着显著的力量，在军事实力方面，它的更为精妙的比较优势在于它的收集、处理、运用和分发信息方面，一种几乎确定无疑地在下一个时代继续成长的优势”。①

从克林顿政府开始，《四年防务评估》《国防战略》和《国家军事战略》等政策文件显示美军已经着手筹划网络时代的作战能力。其重点逐渐从军队的信息化改造转向信息作战和网络作战，即要建立一支能运用“信息控制”和精确武器在各种不同作战环境中取得胜利的军事力量，这将是未来美国防务政策的基础。1997 年国防部《四年防务评估报告》将信息优势视为军事创新的支柱（backbone），认为“在先进的指挥、控制、通信、计算机、情报、监视及侦察（C^4ISR）能力的支持下，美国能迅速回应任何冲突，控制任何情况”，“精确、及时和安全的信息使得军人能够控制任何局势，日常训练得到优化”，“正如非军事世界已经通过互联网和通信网络变得日益相互连接，国防部也在致力于创造一个并行、安全和开放的 C^4ISR 网络架构。”该报告还披露国防部高级研究计划署正在研发一个“星光”项目和一个实时感知系统，星光项目可以根据战区指挥官的需要近乎实时地提供任何地方的雷达影像，而实时感知系统则可以让作战人员通过臂式终端随时连接互联网。”②参谋长联席会议《2010 年联合构想》提出了一个描述信息化战争的概念框架，这一框架的基础是在信息优势下不断提高的指挥、控制、通信及情报能力。③

随着军事和民用通信网络和互联网不断发展，越来越多的用

---

① Joseph S. Nye, Jr., William A. Owens, “American's Information Edge”, *Foreign Affairs*, March/April 1996, 75(2), p. 20

② U. S. Department of Defense, “Report of the Quadrennial Defense Review”, May 1997.

③ U. S. Department of Defense Joint Chiefs of Staff, *Joint Vision 2010: America's Military Preparing for Tomorrow*, Pentagon Publishing, 1996, p. 20.

户、设备和应用加入到一个相互连接的庞大网络中。美国国防部确定了一系列变革的方向，如基本力量结构和组织问题，加强前沿部署和侦察能力问题，超越跨境情报相关的限制问题等。国防部建立了信息联系系统，以确保来自卫星及其他国家级信息来源收集到的信息能及时支援军事行动。为了推动新军事革命，塑造信息化军队，美军在内部倡导树立“信息化军事思维”的观念，培养和重用创新型军事人才，根据《2010 年联合构想》《2020 年联合构想》等纲领性文件的指导，确立个军兵种信息化改造的优先重点，使各军种协调发展，用网络中心战理论带动军队信息化建设，信息化改造的目标是形成战争中的信息优势，同时阻止对手获得相对应的能力。在大量采用民用信息技术的同时，为避免信息基础设施的开放性和脆弱性可能带来的威胁，还要加大军事基础设施和军事技术科研的经费投入，在推进上述一系列构想的同时，注重在作战实验室和高技术局部战争中试验、验证与完善新式武器装备和战法。①

前美国国家安全事务助理理查德·克拉克（Richard Clarke）在《网络战》一书中披露，美国国防部很早就制定了一份秘密的网络空间军事战略，该战略确认了美军网络空间作战规划，并认为网络战是把握现代作战体系的核心，该战略宣称网络空间作战的目标是“确保美军具备网络空间的战略优势”，即确保美军在网络空间的行动自由，并剥夺敌方的行动能力，且必须获取并保持网络空间的进攻能力，这是取得优势的关键。② 秘密的网络空间军事战略将网络空间作战视为现代作战体系发展和美国军事变革至关

① 王保存：《对世界新军事变革本质特征的再认识》，《中国国防报》，2003 年 6 月 12 日，第 3 版。

② 该战略根据美国《信息自由法案》（Freedom of Information Act）而被部分公开，可供五角大楼内部讨论。参见［美］理查德·A·克拉克、罗伯特·K·科纳克：《网电空间战》，刘晓雪等译，国防工业出版社 2012 年版，第 45 页。

重要的方向，体现了美国军方对于网络空间作战的特殊重视。2015 年国防部《网络战略》首次明确当美国国家利益受到威胁时，美军可发动网络攻击，正式宣示将网络空间视为作战平台，软件工具成为攻击武器。具体而言，两种情况下美军将启动网络攻击，一是外来网络攻击达到可能产生严重后果时，二是运用网络攻击可阻止伤害美国利益的其他威胁时。而并未界定严重后果的条件及网络攻击的前提，这就为美军根据需要实施网络攻击开了绿灯。①

三、以能力原则应对非对称威胁

军队是军事力量的主体，制胜信息化战争的关键在于对现有的军队进行信息化改造，1991 年美军以绝对优势赢得海湾战争的全面胜利后，美国国防部提出要对军队进行一场信息化作战与指挥体系的全面再造，也就是“新军事革命”，其目标是进一步拉大与其他国家军队的时间差，维持美军的绝对优势。小布什政府的国防部部长唐纳德·拉姆斯菲尔德(Donald H. Rumsfeld)是新军事革命的积极倡导者，他特别强调美军应发展高技术武器，重视作战武器的技术性和灵活机动性，更加重视武器在战争中的作用。

过去美军建设的根据是基于威胁的原则，美军一度认为在海湾地区和东北亚地区存在着爆发大规模地区战争的可能性，因此，美军的建设主要是根据这两场战争的构想来进行的。而现在的所谓基于能力型，是指在未来数十年间，美国不可能有把握得知哪个国家、国家集团或非国家主体，将对美国及其盟友的关键利益构成挑战。但是，美国可以预测“敌人可能具备哪些能力来威胁邻国，或阻止美国采取保卫自己与盟友的行动，或对美国本土及其部署

① U. S. Department of Defense, “Cyber Strategy”, April 2015.

部队发动直接攻击”。也就是说，美国现在更加重视对手将如何作战，而不论战争将在何处发生。①

美国的战略研究者和政策制定者对冷战后的国际环境和国家安全威胁进行综合评估，非对称冲突的设想即是作为评估的一项结果被提出来。小肯尼斯·麦肯齐指出，美国在冷战后面临的主要安全威胁将是所谓非对称威胁，因此美国的国防规划要以应对非对称威胁为重点，美国应塑造一支新型军事力量，以应对各种形态的非对称冲突。“在新千年揭开序幕之际，美国无处不在，而无处不在带来脆弱性，敌对国家与敌对团体必然把这些脆弱性作为攻击目标，以削弱美国的力量。国防机构应对这些非对称威胁的利害关系之所在，就是承认这样一个永恒的真理：弱国或非国家弱势行为体将试图通过各种途径来削弱强者的领导。”②麦肯齐归纳了六类非对称的方式，包括核武器、生物武器、化学武器、信息战、另类战争观以及恐怖主义，其中信息战和另类战争观与网络作战和信息优势密切相关。克里斯汀·克里特(Kristin S. Kolet)认为，应对这类非对称威胁应充分认识并针对对手的逻辑：第一，当敌对双方存在利益不一致时，势力较弱的一方将积极寻求非对称方式；第二，所有非对称方案的攻击目标都是强敌的意志；第三，可以通过寻求战略层次上的心理影响达到非对称威胁的目标，是否卷入战争，是否出现战争升级与此没有直接关系。③ 为应对非对称威胁，美国应当提高自身能力，设法将脆弱性降至最低、突出特殊能力、防止不对称的后果，在这样三个不可或缺的基础上组织非

---

① U. S. Department of Defense, “Quadrennial Defense Review Report”, September 2001.

② Kenneth F. McKenzie, Jr., “The Rise of Asymmetric Threats: Priorities for Defense Planning”, in Michèle A. Flournoy ed, *QDR 2001 Strategy: Driven Choices for America's Security*, National Defense University Press, 2001, p. 82.

③ Kristin S. Kolet, “Asymmetric Threats to the United States”, *Comparative Strategy*, 2001, 20(3), p. 227.

对称的防御。①

为了在各种非对称冲突中获胜，美国确定了“基于能力型”军事力量发展目标，以获取绝对的国家安全保障。小布什政府提出要建立一支“世界上无可匹敌的军队”，将美军规划的重点由在东北亚和/或西南亚地区的冲突中保持优势，转变为建立一支“无论在功能上还是在地缘上都能在各方面满足部队使用要求的全能力量”。同时，小布什政府提出要将美军武器装备发展的重点放在信息武器和太空武器上，其目的就是使美军拥有多种关键性的军事能力，成为一支具有快速反应能力，高度机动，能够对付各种“非对称威胁”的军队。

四、进攻性与防御性网络空间作战

前美国国家安全事务助理理查德·克拉克认为，对于国家网络空间作战能力的评估，一般需要考虑三个因素：网络攻击能力、网络防御能力、国家对网络空间的依赖性。② 迄今为止美国的网络空间作战能力建设的重点还是在网络防御能力上，即在受保护网络外部，通过网络控制、切断信息流动路径、改变信息传播方向等方式，识别并制止恶意网络行为对受保护网络的进一步侵害。网络攻击能力则是以美国政府名义，侵入目标网络切断网络运行通道、或切断目标网络与互联网的联系，或破坏目标网络的系统、数据和信息。显然，美国联邦政府、军事部门、研究机构都非常依赖于互联网和网络空间，保护这种依赖性本身也是网络空间作战的主要目标。

---

① Kenneth F. McKenzie, Jr., “The Rise of Asymmetric Threats: Priorities for Defense Planning”, in Michèle A. Flournoy ed., *QDR 2001 Strategy: Driven Choices for America's Security*, National Defense University Press, 2001, p. 83.

② ［美］理查德·A·克拉克、罗伯特·K·科纳克：《网电空间战》，刘晓雪等译，国防工业出版社 2012 年版，第 254 页。

2012 年 12 月，奥巴马签署第 20 号总统政策指令即美国网络行动政策指令，明确提出防御性网络作战和进攻性网络作战，并详细规定了美国进行网络进攻和网络防御的原则、目标和方案。[①] 该指令界定了网络防御的概念，即“由计算机、网络、信息和通讯系统等设施的所有者或经其同意的使用者在这些设施上进行的计划和活动，主要目的是保护（1）计算机、网络和系统，（2）在计算机、网络和系统上储存、处理或传输的数据，（3）由计算机、网络和系统控制的现实和虚拟的基础设施。网络防御不得在未经所有者授权或超出授权范围的情况下，进行或要求访问和操作计算机、网络、信息和通讯系统。[②]

网络部队的功能定位经历了从注重防御到攻防并重的过程。2011 年国防部《网络空间行动战略》指出美军负有保护军事网络、国家信息基础设施和全球信息基础设施的职责，该战略将网络空间界定为作战领域，国防部将以此为基础进行组织、培训和装备，以应对网络空间的复杂挑战，并提出美军将变被动防御为主动防御，以更加有效地阻止、击败针对美军网络系统的入侵和其他敌对攻击行为。[③] 美国国防部负责国土防御和全球安全事务的助理国防部长埃里克·罗森巴赫（Eric Rosenbach）在参议院军事委员会听证会上称，美国将使用网络、外交和军事手段提升网络威慑能力，并且确保美国能在遭受网络攻击后迅速恢复。[④] 2015 年国防

① U. S. White House, “PPD－20: U. S. Cyber Operations Policy”, October 16, 2012.

② 两种网络作战形式分别为防御性网络作战（defensive cyber effects operations, DCEO）和进攻性网络作战（offensive cyber effects operations, OCEO），参见 U. S. White House, “PPD－20: U. S. Cyber Operations Policy”, October 16, 2012.

③ U. S. Department of Defense, “Strategy for Operating in Cyberspace”, July 14, 2011, p. 7.

④ 美国助理国防部长埃里克·罗森巴赫 2015 年 3 月 25 日在参议院军事委员会听证会上的证词发言，参见 http://docs. house. gov/meetings/AS/AS26/20150325/103241/HMTG－114－AS26－Wstate-RosenbachE－20150325. pdf，最后浏览日期：2015 年 8 月 20 日。

部《网络战略》进一步将美军在网络空间作战的职责确定为三项主要使命：第一，保障国防部自身网络安全；第二，反击重大网络攻击，保卫国家安全；第三，向总统提供跨部门、综合性的多种网络报复方案，遏阻重大的网络攻击行动。①

第二节　网络空间作战的指挥和控制

明确了网络空间军事化的方向和赋予了军队进行网络空间作战的职责，接下来就面临如何建立指挥和控制体系的问题，由于美国联邦政府有多个部门对网络空间行动有管辖权且希望获得更多授权，当网络事务是不多的可以在预算紧缩时期继续获得资金扩充的项目。因而建立网络军队并形成战斗力就要解决从军事、情报和国土安全部门那里获取必要的权限和确立自己的活动范围等问题。

一、网络空间作战主导地位的争夺

20 世纪 90 年代，美国军方重点是信息战和心理战，作战部队主要将网络用于扩展舆论传播途径，在战时通过密集的信息传播以分散敌方的注意力和瓦解敌方的意志从而影响战争结果。情报部门把互联网看作获取情报的新平台，从新闻媒体网站和各种论坛上寻找各国政治、经济和社会态势和变化的蛛丝马迹。

小布什政府时期，国防部逐渐意识到网络空间作战的重要性，并在全球反恐的总体战略下尝试通过网络途径反击恐怖主义的作战方式，陆军、海军和情报部门就开始为获得网络空间作战控制权而展开竞争。由于国家安全战略强调防范极端分子运

① U. S. Department of Defense, "Cyber Strategy", April 2015.

用网络等新的技术方法和路径对美国构成的威胁，新成立的国土安全部自然拥有在这一反恐新领域获得更大活动空间和发言权的理由。

到了奥巴马政府，形势已经发生很大的变化，网络环境蕴含的风险和网络活动带来的威胁已经上升为直接国家安全战略需要应对的重要领域。国土安全部认为国家网络基础设施的安全保障是其法定职责，因而要求其他机构不要介入政府和公共领域的网络安全，国防部的权限只能涉及针对其军事网络的网络防御，对于国会认为美国国土安全部的技术能力不能胜任处理网络安全威胁的任务，国土安全部认为正应当在预算和人事上给予国土安全部足够的支持，以保证它能够获得相应的网络防御能力。国防部希望网络司令部必须与国家安全局在同一位置，它们会为整个国家进行网络防御。社会舆论和公众则会要求国家安全局停止监控和搜索他们的电子邮件。

国务院则认为必须采取积极的政治和外交行动，建立网络空间的行为规范，对《联合国宪章》、武装冲突法及国际争端处理等方面的规范进行阐释，将网络空间纳入现有国际法有效管辖范畴，以应对来自中国、俄罗斯等国家的网络窃密威胁，虽然具体的网络威胁包括类似间谍活动这样的行为，而传统的间谍活动在国际法上并不违法。国会认为必须在网络安全议题上有所行动，但网络空间的军事行动涉及的法律问题争议非常广泛，故很多议案在国会无法达成共识，也无法通过成为有约束力的法案。

情报部门在侵入目标网络获取情报的同时，也获取了破坏和关闭网络的机会，这引起了情报部门和军事部门对于主导网络空间行动权的争夺。对于情报部门而言，如果将进入网络空间的授权和路径告知作战人员，就会失去网络空间的部分控制权；对于作战人员而言，网络空间提供了一种相对便利且有效降低人员伤亡就能给敌人造成巨大破坏的作战方式，这种新的战争能力无论如

何也是军方所追求的。①

上述各个部门都有出于部门利益的考虑，因而白宫权衡之下，国防部和情报部门都是强势部门，且具有相应的能力和权限，因而将这两家的诉求进行整合是最为简便的做法，且能很快形成战斗力。此间，还有一种设想是成立联合司令部，将各军兵种的网络作战部门整合为一个网络作战联合司令部，但基于太空司令部被并入战略司令部的经验，②建立一个联合作战司令部需要大幅增加预算投入，因而一直未能付诸实施，直到2002年战略司令部都承担着统一规划网络空间作战的职责，但空军拥有网络作战部队的实际控制权。2008年，国防部最终确定建立网络空间作战部队，将主导权从空军已交给到这个新成立的统筹指挥机构，平衡各方利益诉求的结果，是在战略司令部下设一个网络司令部，同时将以国家安全局为核心的情报系统已具有的网络攻防能力整合进来。

二、网络作战力量的构成

实际上，美军网络作战力量仍呈现为一种分布式结构，包括了由战略司令部下辖的网络司令部和各军种所属的网络部队以及归属于多个情报部门的网络情报力量。

空军网络司令部是美军首个在网络空间创建的作战机构。美军空军网络司令部即美国空军第24航空队，成立于2009年8月18日，编制为6 000—8 000名军职和文职网络作战成员，总部位于得克萨斯州的拉克兰德空军基地，负责空军信息和网络系统运行维护及网络空间作战。第24航空队的使命是“装备精良，训练

① ［美］理查德·Λ·克拉克，罗伯特·K·科纳克：《网电空间战》，刘晓雪等译，国防工业出版社2012年版，第37页。

② 1985年美军创建了独立的太空司令部，但受限于太空领域的高昂费用，太空司令部被并入战略司令部。

有素，具备与空天一体作战相适应的网络空间持续作战能力”，其专注于三种行动：第一是运作空军信息网络系统，确保军事网络的空军部分是可用和安全的，国防部和空军可以在该部分网络空间遂行指挥、控制和作战任务；第二是防御空军信息网络、关键任务系统和具体网络系统，包括空军核心网络、关键空军任务地形以及对于联合作战部队指挥官的重要任务和关键网络地形；第三是抗衡对手，需要空军能力与作战指挥的优先事项相一致，核心是空军部队面临的网络防御问题。第 24 航空队下辖第 67 网络战联队，即之前的空军信息作战中心，担负保护空军网络和攻击敌军网络的日常职责，专注于网络防御；第 688 信息战联队，作为空军网络空间作战的核心，承担未来发展的任务，即研发新的作战方法，为空军使用网络武器创造条件；第 689 通信战联队，负责通信领域的支持和作战。①

美国海军网络司令部即成立于 2009 年 6 月的海军第 10 舰队，总部位于马里兰州的米德堡。为了进行网络空间作战，海军重建了第 10 舰队，该舰队在第二次世界大战中是负责大西洋海域联合反潜的协调机构，1945 年对德战争胜利后第 10 舰队被解散。海军以第 10 舰队重建网络作战任务的目的是为了加强日益凸显重要的信息作战，作为提高海军信息作战能力，美国海军曾经于 2008 年 11 月在海军作战部设置专门负责信息网络作战以及情报工作的副部长，该部部长继而担任海军网络司令部司令。

美国陆军网络作战部队的成员大多属于陆军网络业务技术司令部，即位于亚利桑那州瓦丘卡堡的第九信号司令部，该司令部的成员被指派到世界各地的信号司令部。2008 年 7 月，陆军组建了第一个网络战营。隶属于陆军情报与安全司令部的网络作战单位

① 关于空军网络司令部的介绍可参见美国空军第 24 航空队网站，http://www.24af.af.mil/，最后浏览日期：2015 年 8 月 20 日。

也按照前沿部署的方式，与国家安全局等情报单位协同作战，陆军全球网络作战与安全中心管理国防部网络中位于陆地上的部分网络。

此外，海军陆战队和海岸警卫队也都成立了各自的网络司令部或网络作战部队。

2010 年 5 月 21 日，美军网络司令部在马里兰州米德堡基地正式宣告成立，网络司令部隶属于战略司令部，最初设定的任务是网络防御作战、打击敌对国家和黑客的网络攻击，并对美军在网络作战领域进行统一管理和协调各军兵种网络作战人员的行动。网络司令部的第一任司令是基思·亚历山大(Keith Alexander)。至 2010 年 10 月，网络司令部正式全面运行，初始规模约 900 人，2013 年 6 月，时任参谋长联席会议主席马丁·邓普西(Martin Dempsey)表示国防部决定将在未来四年将网络战司令部扩编至 4 900 人，以强化应对网络攻击的防御能力，为此将增加国防预算 230 亿美元。网络司令部的建立标志着美国将网络空间确定为与陆地、海洋、天空及太空同等重要的军事领域和作战平台，并以此为基础谋求建立网络空间作战的攻防优势。

美国网络部队由三个类别构成，包括保护重要基础设施的网络部队、协助作战部队策划并执行网络任务的进攻性网络部队及保护国防部内部网络的防御性网络部队(如表 6－1 所示)。2014 年 6 月，国防部《四年防务评估》提出未来将建立 133 个网络任务分队(mission teams)，总共 6 200 人。[①] 2015 年国防部《网络战略》进一步将 6 200 人的性质确定为网络部队(cyber force)，成员包括国防部和军事部门的军人、文职人员和合同员工。[②]

---

① U. S. Department of Defense, "Quadrennial Defense Review Report", March 2014.

② U. S. Department of Defense, "Cyber Strategy", April 2015.

表 6－1　美国网络部队的构成

任　务　分　队	数　量
国家任务分队(national mission teams)	13
国家支持分队(national support teams)	8
作战任务分队(combat mission teams)	27
作战支持分队(combat support teams)	17
国家网络保障分队(national cyber protection teams)	18
军队网络保障分队(service cyber protection teams)	24
作战司令部和国防部信息网络保障分队(combatant command and DOD information network cyber protection teams)	26

三、网络司令部的双重身份

国家安全局赢得了网络空间作战主导权，尽管这是一种阶段性的安排。国家安全局是情报机构，但在电子和信号情报领域居于绝对领先的地位。国家安全局对于互联网的介入源于其几十年来在窃听无线信号和通信内容的任务中积累起来的技术优势和人力优势。作为一种新型传播媒介，互联网的应用不断增长，情报价值也不断增长，国家安全局拥有大量数学、电子博士和密码专家，最有能力在这一新兴领域占据领先地位。尽管国家安全局没有获得破坏网络和修改数据的授权，但它已经完全渗透至全球网络基础设施，一旦需要，既可以完成情报侦察和监视任务，也可以胜任网络攻击和作战任务。网络司令部成立之时，时任国家情报总监约翰·麦康奈尔(John M. McConnell)和国家安全局局长基思·亚历山大都认为如果要成立网络空间司令部，国家安全局就应该是这个司令部。当然，军方也有不同的观点，认为国家安全局是一个政府部门和情报机构，不具有法定授权参与作战任务，这一观点

援引美国法典关于政府部门和情报机构的权力和限制，与支持者展开了第 50 章对第 10 章的争论，[①]因而将网络空间作战主导权的权力争夺演化为军方与法律专家间的辩论。

军方观点的支持者主张重建新的机构，复制国家安全局所拥有的网络攻击能力，时任国防部部长罗伯特·盖茨（Robert M. Gates）曾担任中央情报局局长，盖茨是一个实用主义者，他超越了部门利益之争，从国家利益和着眼长远的角度看待网络司令部的设置。最终的解决方案是：由国家安全局长兼任网络司令部司令，军衔升至四星上将，从而网络司令部司令具备双重权责，既作为战略司令部的下一级联合司令部以获取网络空间作战的权限，又与国家安全局分享人力和资源以获取执行网络攻防任务所必需的技术能力，这样既简化了机构组建的繁琐程序，也可以解决法律授权的争议，从而使网络司令部较快进入角色，但后来斯诺登揭秘事件的发生，网络司令部的双重身份引发了新的辩论。

网络司令部统领美军网络空间作战的职能规划、能力建设和任务协调，空军、海军和陆军仍然保持独立的网络空间作战任务编制，接受网络司令部统一指挥。从技术上来看，仍然是各军兵种的作战力量来执行网络空间的进攻和防御任务，而不是作为政府部门的情报机构参与了作战。根据美国法典第 10 章，国家安全局具备网络渗透和网络侵入的职能，但在搜集数据和信息方面受到限制，并不得参加作战任务。而根据法典第 50 章，为履行通过计算机摧毁敌方系统的职责，网络司令部将作为军方机构参与作战行动。

以“两块牌子、一套人马”模式处理网络司令部与国家安全局的关系体现了网络作战和网络情报的密切关系，是一种富有创意

① 美国联邦法典（U. S. Code）第 10 章是武装力量（Armed Forces）的相关法律，第 50 章是战争及国防（War and National Defense）的相关法律。

的制度安排，但这种权宜之计的弊端也很明显。约瑟夫·克拉克(Joseph Clark)认为，网络司令部应该与国家安全局拆分，这不是政治权力的争斗，而是着眼于长远的一种安排，需要独立和规范地发展军事和国家安全的网络功能，同时要避免对武装力量的使用造成束缚，以及避免对国家安全形成新的威胁。之所以国防部主张网络司令部应该与国家安全局拆分，或者在国防部从零开始建立网络司令部，是因为国防部需要独立的授权，调动网络作战力量，并将其纳入战略和作战条令，以确保在执行网络安全任务时不会受制于法律和机制的限制。

还有一些观点认为网络司令部不应隶属于战略司令部，而应建立一个联合网络作战司令部，发展特定的战术、技术和程序，以保证网络部队的人员和功能充分用于军事目的，从而在战略层面应对美国面对的网络作战的问题。这类观点认为建立联合作战司令部比起让现有的行政部门和军事机构履行职责是更好的解决方案。首先，尽快组建一支能够应对紧急形势的网络作战力量。如果让原有行政部门和军事机构履行新的职责，甚至建立新的军种，将引发组织机构之间的争执甚至对抗，可能减缓网络部队的建立和网络作战能力的形成。其次，就美国法典第 10 章和第 50 章而言，网络交战规则的模糊、对政治挫败的担忧，以及担心美国使用的网络武器可能被逆向工程(reverse engineering)[①]，并用来对付美国，所有这些问题都突出需要一个组织架构方面的解决方案以协同活动的重要性。总之，美国需要一个网络作战的联合司令部，一方面发展战术、战役和战略的网络功能，这是美国国家安全在未来几十年将需要的，另一方面监督这些网络战术、战役和战略能力

① 逆向工程，又称逆向技术，即对目标产品进行逆向分析及研究，推测和演绎出该产品的处理流程、组织结构、功能特性及技术规格等要素，从而制作出具有类似功能的产品。参见 Eilam, Eldad, *Reversing: Secrets of Reverse Engineering*, John Wiley & Sons Publishing, 2005。

的应用、整合和执行。

第三节　网络空间作战的能力建设

网络司令部和各军种网络部队构成美军网络部队的主体，在组织机构大体确定之后，美军开始全方位的网络攻防能力建设。就网络进攻能力而言，需要设定攻击目标，发现敌方系统的漏洞，选择和开发适用攻击工具和手段，并应对可能引发的反击；网络防御则更加复杂，因为需要防护的点太多，要完成对整个国家的网络基础设施、计算机系统和数据信息都纳入有效安全保障，对于现有规模的网络作战力量而言几乎是不可能完成的任务，所以美军网络防御的重点是军事部门的指挥和管理体系所依赖的基础设施和网络系统。

一、发现系统漏洞

网络防御作战的首要任务是熟悉计算机和网络系统的运行，寻找安全短板或漏洞并及时加固。网络部队的专家每个小时要对军事网络进行数千次探测以寻找漏洞，所以能否及时发现正在扫描防护目标的网站和系统的探测活动，所以在对手找到自身系统的漏洞并用以攻击之前，发现漏洞并尽快提出解决方法就是网络部队防御能力的重要内容。网络司令部司令迈克尔·罗杰斯(Michael Rogers)认可网络司令部的技术专家发现系统漏洞的能力，“在其他人发现心脏出血和破壳漏洞的同一时间，网络司令部和国家安全局也发现了这两个漏洞”。[①] 在发现系统漏洞之后，网

① 心脏出血(heartbleed)是2014年4月发现的开放安全套接层协议(OpenSSL)的设计缺陷，攻击者可利用该漏洞窃取信息，通常针对用来保护如网页、电子邮件和即时通讯等互联网应用的加密信息，攻击者可以窃听通信，直接从服务器和用户窃取数据，并模仿服务器和用户。而破壳漏洞(shellshock)让攻击者能够在系统上运行远程命令。

络司令部会及时通过网络司令部的网络通知各个部门的网络防护人员，并组织本机构人员或与其他部门合作开发软件补丁，以尽快提出应对方案，联邦政府的民事部门的也会迅速收到网络司令部关于漏洞存在和检测的信息。针对漏洞的检测方法和应对实践提出来后，技术专家也会进行评估确定最适合的方案，然后在整个国防部网络添加补丁并监督实施状况。发现系统漏洞并在对手发现之前实施行动，是一种最重要的网络攻防手段，由于国防部网络系统涉及的设备和软件供应商非常多，一些严重缺陷被潜藏在大量计算机和网络应用重，因而对系统、平台和应用进行全方位和不间断的探测，并在发现获知漏洞并试图侵入之前就采取措施，就成为网络司令部必须具备的防御能力。由于网络司令部与国家安全局的密切关系，当技术人员发现安全漏洞时，会对漏洞的情报价值进行评估，这样有时可能会延迟公布已经发现的漏洞，以取得相对于对手的领先优势。

二、保护国防部网络

网络司令部成立之初，即着眼于为国防部网络加强防御能力，并很快成立了专门保护国防部网络的网络分队，并帮助各作战司令部阻止对手获得网络空间中的机动自由。

网络司令部的防御范围涵盖了整个国防部网络，美军强大的作战和指挥能力很大程度上依赖于全球信息基础设施的稳定、连通和开放。美军在全球几十个国家运行着 1.5 万个网络和 700 万台计算机和终端设备，[①]2011 年国防部《网络空间行动战略》着重指出美军负有保护军事网络、国家信息基础设施和全球信息基础设施的职责，该战略将网络空间界定为作战领域，国防部以此为基

① U.S. Department of Defense, "Strategy for Operating in Cyberspace", July 14, 2011.

础进行组织、培训和装备，以应对网络空间的复杂挑战和巨大机遇。美军将变被动防御为主动防御，更加有效地阻止、击败针对美军网络系统的入侵和其他敌对行为。加强与其他政府部门及私人部门的合作，在保护军事网络安全的同时，加强国家重要基础设施的网络安全防护。同时还要加强与美国的盟友及伙伴在网络空间领域的国际合作。[①] 美国国防部常务副部长威廉·林恩(William J. Lynn III)称美军在网络空间的任务重在防御而非进攻，目的是打掉因攻击获得的利益，而前参谋长联席会议副主席詹姆斯·卡特赖特(James Cartwright)则认为该战略过于注重防御层面，过于可预知性。[②] 因而 2015 年国防部《网络战略》加强了主动防御的内容，其重点是指在促使对手认识到对美发动网络攻击可能面临的严重后果，从而放弃针对美军网络或国家关键基础设施的网络攻击行为。[③]

监测国防部网络的实时访问记录、识别网络攻击行为、从攻击灾难恢复，这些都是网络司令部应对网络攻击的内容。2011 年国防部《网络空间行动战略》将网络人员划分为三个类别：运行维护人员、信息保障人员和网络防御人员。网络防御人员的职责是侦测、识别、拦截和摧毁各种网络入侵或攻击活动。在国防部数万名网络人员中，明确承担网络防御任务的人员仅占 2%，但信息保障人员和网络防御人员之间的权责划分并不清晰，因而国防部可投入应对网络攻击的人员大约有数千人。

应对网络攻击需要加强国防部与联邦政府其他部门以及私营部门之间的合作。2015 年 3 月，网络司令部司令迈克尔·罗杰斯

---

① U. S. Department of Defense, "Strategy for Operating in Cyberspace", July 14, 2011, pp. 5 - 9.

② Ellen Nakashima, "U. S. Cyber Approach 'Too Predictable' for One Top General", *Washington Post*, July 15, 2011.

③ U. S. Department of Defense, "Cyber Strategy", April 2015.

在众议院军事委员会听证会上表示，美国网络司令部已经运作五年，一个很重要的认识是，来自网络空间的威胁已经模糊了政府机构之间、公共部门与私营部门、现实世界与虚拟世界之间的角色和关系。① 为了增强对网络攻击手段、路径和环境的感知，网络部队重视在联邦政府、各州和私营部门间共享网络威胁信息，2015 年奥巴马政府发布关于促进私营企业网络安全信息共享的行政命令，并指定国防部长在能源部长、国家情报总监及国土安全部长等协助和咨询下编制和维护《国家工业安全项目操作手册》，这实际上是赋予了国防部在整个联邦部门和私营部门应对网络攻击方面指导和教育职责。② 网络司令部很重视以“全政府”的理念来应对无所不在的网络攻击，“美国联邦政府、各州和私营部门不能仅靠自己对抗最强大的网络力量……必须做好准备，整个政府要采取一致行动处置网络攻击，而且利用美国独特的知识和所有的能力，与私营部门合作。”③

云计算提供了全局性、伸缩性和迁移性的数据存储、加工和传输的解决方案，由于云架构更有利于实施集中统一的安全保护，并有利于整个国防部网络中的数据共享，国防部正逐步将其系统转向云架构。云架构下的数据和信息管理“更能够对整个国防部系统范围内的风险实施管理，有利于保持企业化网络整体安全的前提下，平衡作战人员访问数据和能力的需要。”④2012 年国防部《云计算战略》提出将国防部网络转变为一个企业云环境，通过创建部

① Cheryl Pellerin, “Cybercom Chief: Cyber Threats Blur Roles, Relationships”, March 6, 2015, http://www.defense.gov/news/newsarticle.aspx?id=128305, 最后浏览日期：2015 年 8 月 20 日。

② U.S. White House, “Executive Order 13691: Promoting Private Sector Cybersecurity Information Sharing”, February 13, 2015.

③ Cheryl Pellerin, “Cybercom Chief: Cyber Threats Blur Roles, Relationships”, March 6, 2015, http://www.defense.gov/news/newsarticle.aspx?id=128305, 最后浏览日期：2015 年 8 月 20 日。

④ Ibid.

门数据中心和采购商业服务，使国防部网络从重复、繁琐、成本高昂的状态转变到一种更为灵活、安全和高效的服务环境，从而适应不断变化的任务需求。[①] 而对于云架构下的数据和信息，也会带来新的保障任务。2011 年国防部《网络空间行动战略》、2015 年国防部《网络战略》都将国防部数据保护作为网络部队的重要目标之一。

三、发展网络进攻能力

早在克林顿政府时期，隶属军方的情报机构就开始筹划网络攻击能力。[②] 小布什政府时期美军又将网络空间列为与陆、海、空、天同等重要的战略空间，[③]并在先发制人军事战略指导下，开发网络作战武器，加强网络攻击能力。奥巴马政府进一步将网络空间纳入作战领域，在此基础上加强军事的组织、训练和装备，以确保国防部充分运用网络空间的潜力，以及采取有效军事行动的能力。[④] 2014 年《四年防务评估》提出建设 133 支网络任务分队，2015 年国防部《网络战略》进一步明确网络攻击已经不限于网络空间的作战，也可以运用于常规作战的支持和替代选项，[⑤]网络司令部必须不断地学习和发展新的技能和技术，必须持续投入时间、精力和资源来建设网络攻击能力。

信息化进程的影响已经渗透到当今世界的每一个角落，国家

---

① U. S. Department of Defense, "The DoD Cloud Computing Strategy", July 2012.

② Jeffrey T. Richelson, Malcolm Byrne, "When America Became a Cyberwarrior: A Secret Document Shows the NSA Has Been Planning Attacks since the Clinton Years", *Foreign Policy*, April 26, 2013, http://www.foreignpolicy.com/articles/2013/04/26/when_america_became_a_cyberwarrior_nsa_declassified,最后浏览日期：2015 年 8 月 20 日。

③ U. S. Department of Defense, "The National Defense Strategy of the United States of America", March 2005.

④ U. S. Department of Defense, "Strategy for Operating in Cyberspace", July 2011.

⑤ U. S. Department of Defense, "Cyber Strategy", April 2015.

间冲突也不可避免与网络密切相关，美国网络司令部逐渐扩大网络作战行动范围，并且谋划执行多样化和更复杂网络作战任务的能力。“当今世界每一个冲突都有网络的维度”，迈克尔·罗杰斯从网络司令部的如何发展网络攻击能力的角度，指出网络时代国际冲突的四个新特点：一是一些国家将互联网带来的快速信息传播视为政治稳定的威胁来源；二是通过网络窃取商业机密和知识产权的行为不断发生；三是各种行为体通过拒绝服务攻击、网络流量操纵和破坏性恶意软件等各种方式制造网络中断事件；四是一些国家发展网络攻防能力，显示出加强网络威慑的意图，或作为未来网络破坏活动的主要方式。[①]。网络司令部需要发展应对来自上述四个方面的风险或威胁的能力，从而能够在冲突形成和演变的各个阶段，完成从预先阻塞对手的网络攻击路径、切断敌人军事活动的网络依赖以及在遭受网络攻击时发动反击等全方位的网络作战能力。

四、构建网络安全环境

美国国防部的现有架构形成于20世纪40年代，随后虽经历了一些调整和改组，总体上还是基于应对传统安全威胁和组织传统作战模式。通过冷战后的新军事革命和近年来网络作战的需要，已经逐步向一个更安全的、更精简的架构过渡，这个架构最终将成为联合信息环境的一部分。网络空间不仅仅是一个具有挑战性的环境，“现在它几乎成为美国军方作战空间的所有域和我们每一个行动线的一部分，现在对物理世界的事件与网络空间的事件进行区分几乎没有任何有意义，因为它们是如此紧密地联系在一起”，“虽然联合信息环境正在建设过程中，我们对原有架构的担忧

① Cheryl Pellerin, “Cybercom Chief: Cyber Threats Blur Roles, Relationships”, March 6, 2015, http://www.defense.gov/news/newsarticle.aspx?id=128305, 最后浏览日期：2015年8月20日。

促使我们组建了新的联合部队总部，以保护国防部的信息网络”。[①] 在网络司令部的指挥和控制下，国防信息系统局负责运作网络联合部队总部，监督整个国防部网络的日常运作，并为国防部网络提供主动防御的能力，保护它们的关键网络地形，并准备击退那些试图绕过国防部网络外围防线的任何对手。

对于美国国防部或是网络司令部而言，这都是一个更大目标，不仅意味着要构建一个安全坚固的国防部网络防御体系，而且需要将国防部网络改造为能够提供全方位作战需要的平台，包括形成对敌网络威慑的能力和破坏对手组织作战所依赖的网络平台的能力。就网络安全能力而言，美国国防部及网络司令部都具有绝对优势，特别是在发现、利用和控制硬件设备、网络协议和网络应用中的漏洞方面，即便如此，由于网络基础设施、网络系统和控制指挥所依赖的软硬件数量类型广泛、应用服务供应来源不一、攻击手段途径众多，因而构建安全、可信与可用的网络环境，仍然是一项异常艰巨的任务。

第四节　网络空间作战的实施和影响

美军的网络作战最早可追溯到第一次海湾战争，战前中央情报局设法将伊拉克防空系统使用的打印机芯片换上了带有计算机病毒的芯片，在空袭开始前激活病毒，造成伊拉克防空指挥中心主计算机程序错乱并导致伊防空系统失灵。[②] 从严格意义上而言，这次攻击并不能称作网络空间作战，因为攻击针对的是指挥系统所依赖的硬件设备，而不是关键信息基础设施或网络系统。尽管

---

① Cheryl Pellerin, “Cybercom Chief: Cyber Threats Blur Roles, Relationships”, March 6, 2015, http://www.defense.gov/news/newsarticle.aspx?id=128305, 最后浏览日期：2015 年 8 月 20 日。

② 张敏钰：《网络战与美国网络司令部》，《保密科学技术》2011 年第 1 期，第 71 页。

如此，第一次海湾战争的关注者都深刻感受到确保军事指挥系统的安全对于现代信息化条件下进行作战的重大意义，第一次海湾战争结束后不久，美国空军就建立了信息作战中心，即现在空军网络司令部下辖第 67 网络战联队的前身。

一、震网行动

震网行动是美国政府公开承认的首次经由网络空间遂行的作战任务，网络作战部门成功地将病毒植入伊朗核设施的计算机控制系统而致使离心机受到永久性破坏，从而大大延缓了伊朗的核计划进程。

伊朗长期以来寻求拥有核能力，2002 年媒体披露伊朗秘密研发核武器后，国际社会迅速要求伊朗停止铀浓缩、接受核查并提高核活动透明度，伊朗一定程度上接受了核查但未能满足国际原子能机构的全部要求。随后联合国安理会通过多个伊朗核问题决议，先后提出禁止伊朗武器出口、冻结参与核项目海外个人资产、国际金融机构停止贷款等制裁措施，欧盟和美国还追加对与伊朗有贸易往来的公司进行金融制裁。即便如此，伊朗政府仍坚持和平利用核能的权利和拒绝停止包括核燃料研究等在内的核活动。自 2004 年开始的伊核问题谈判先后经历欧盟与伊朗、俄罗斯与伊朗的双边谈判及六方会谈，一直到 2015 年之前，各方始终未能就停止核武计划和取消制裁达成一致。

这是震网行动展开的背景，伊朗很清楚，美国和以色列等国是一定会想方设法阻止其核活动的，故也同样想方设法加强防护措施。显然作为高度机密和最高安全等级的核活动，无论是和平利用核能的核电活动，还是具有核武器意义的铀浓缩活动，都在严密监视和严格保护之下，研发和生产控制的计算机系统也是独立运行，更不用说与互联网直接相连了。层层设防之下，网络攻击似乎不太可能发生。然而 2011 年 1 月 16 日《纽约时报》报道，美国和

以色列联合研制的震网病毒于2010年7月攻击了伊朗核设施，纳坦兹铀浓缩工厂(Natanz Plant)约1/5的离心机报废，从而大大延缓了伊朗的核计划。[①] 对此，伊朗原子能组织表示，伊朗的敌人希望借助于计算机病毒给纳坦兹铀浓缩工厂和布什尔核电站(Bushehr)制造麻烦，但伊朗计算机安全专家早就发现了这种病毒，病毒并没有能够触及目标。布什尔核电站也宣称只是一些工作人员的个人电脑受到感染，核电站主要系统没有受到病毒的影响，核电站运转正常，核燃料装载也没有受到影响。

而美国和以色列对伊朗核设施遭受震网病毒攻击后果的估计则要严重得多。2010年7月以前，美以曾声称伊朗只要一年时间就可以拥有制造核武器的能力，而7月以后美以两国对这一预估都进行了大幅修正，以色列战略事务部部长摩西·亚阿隆(Moshe Ya'alon)声称伊朗至少还需要三年时间才能制造出核武器，美国时任国务卿希拉里·克林顿也表示伊朗核计划因为技术问题已经被拖延。在当时看来，这些表态的变化怎么看都有偷袭得手意味。

伊朗核活动的事态变化一定程度上证实了媒体和西方国家的判断。2010年8月后布什尔核电站启用后就接二连三地发生故障，随后伊朗国家通讯社证实布什尔核电站遭到震网病毒攻击，继而伊朗总统内贾德也承认震网病毒给离心机带来了一些麻烦。2011年2月，伊朗宣布暂时卸载布什尔核电站的核燃料，而纳坦兹铀浓缩工厂也曾于2009年年底和2010年年初更换了大约1 000台离心机。2011年8月，一名伊朗议员称布什尔核电站因为不能按时提供足够的核燃料，无法按预期在8月底并网发电。9月4日，伊朗原子能组织宣布布什尔核电站并网发电，但联网功

① William J. Broad, John Markoff, David E. Sanger, "Stuxnet Worm Used Against Iran Was Tested in Israel", *New York Times*, January 16, 2011, p. A1.

率只有60兆瓦，大约是核电站设计总装机容量的6%，显示核电站建设遭受了重大挫折。

至此，震网行动的脉络大致得以呈现出来：这是一次目标明确、规划缜密和充满想象力的网络攻击行动，即设法在伊朗核设施的计算机控制系统里面植入病毒，使离心机异常运转并形成不可逆的物理损坏，同时传递正常运转数据以迷惑工作人员。至于病毒被植入计算机控制系统的过程则仍未得到美国和伊朗政府的证实，由于伊朗核设施的计算机控制系统是由德国西门子公司设计生产的，一种推测是在设备和软件运抵伊朗之前，美国及其盟国的情报部门设法在系统中安装了病毒，有报道称阿拉伯联合酋长国曾对一批用于计算机控制系统的西门子电脑经过霍尔木兹海峡运抵伊朗港口阿巴斯之前进行了检查。① 另一种推测是该病毒通过先感染伊朗核工作人员的个人电脑或移动存储，从而被带入了内部网络系统中。不论如何，震网病毒设计巧妙，包含许多专门针对西门子公司控制系统的代码和指令，绝非一般黑客所能完成，其背后必有网络攻击能力超强的组织甚至政府支持。俄罗斯安全公司卡巴斯基实验室也认为除非有国家和政府的支持和协助，否则很难发动如此规模的攻击。

2013年7月，美国前国家安全局合同工爱德华·斯诺登(Edward Snowden)证实，为了破坏伊朗的核项目，美国国家安全局和以色列合作研制了震网病毒，以入侵伊朗核设施网络，改变其数千台离心机的运行速度。斯诺登表示，美国国家安全局是通过外交事务理事会与以色列等国家进行安全事务合作的。根据《纽约时报》的报道，美国能源部下属的国家实验室和以色列迪莫纳核基地的技术人员用了两年时间研制出震网病毒，德国和英国也提

① William J. Broad, John Markoff, David E. Sanger, "Stuxnet Worm Used against Iran was Tested in Israel", *New York Times*, January 16, 2011, p. A1.

供了一些技术和情报上的帮助，以色列甚至在迪莫纳基地安装了与伊朗相同的离心机对病毒进行测试，以确保攻击能够达到预期效果。而后，美国国务院也间接证实了相关报告，参与震网行动的专家称奥巴马就任伊始，就决定加快小布什政府时期的“奥林匹克计划”——对伊朗核浓缩设施计算机系统发动攻击的计划，并最终得手。[①] 对于为何伊朗不愿承认核计划受病毒攻击而受挫，一方面是因为伊朗核活动有诸多不愿公开的内容，另一方面伊朗方面也很难拿出确凿证据证明震网行动确实是美国和以色列政府所为。

震网行动对各国的网络安全是一个警醒，因为病毒形成破坏的场所和对象是一般认为非常安全、在物理上与互联网隔离的内部局域网。卡巴斯基担忧电脑病毒的军事化运用将可能导致新型军备竞赛，“震网病毒是一种十分有效并且可怕的网络武器原型，这种网络武器将导致世界上新的军备研制热潮，一场网络军备竞赛时代的到来”。[②] 病毒武器的附带伤害也会带来很严重的问题，赛门铁克安全响应中心的调查显示伊朗境内大量个人电脑被感染，德国研究人员 2010 年 6 月已经发现这种蠕虫病毒，其恶意代码专门针对西门子公司的监控和数据采集系统。该病毒除了可以通过互联网传播外，还可经由移动存储感染未联网的计算机。印度、印度尼西亚、巴基斯坦等国不少计算机感染了这种病毒，但伊朗受害情况最为严重。据统计，震网病毒感染了超过十万台个人电脑和数万个工业控制系统，但迄今除了伊朗核设施的离心机外却未对其他电脑和工业设备造成任何物理损害。可见震网病毒被

---

① David E. Sanger, “Obama Order Sped up Wave of Cyberattacks against Iran”, *New York Times*, June 1, 2012, p. A1.

② Kaspersky Lab, “Stuxnet Manifests the Beginning of the New Age of Cyberwarfare”, September 24, 2010, http://www.kaspersky.com/news?id=207576183，最后浏览日期：2015 年 8 月 20 日。

设计为具有精确打击能力的网络武器，可谓网络精确制导武器。由此看来，震网行动战术上是成功的，也一定程度上避免了伤及无辜，但该行动多少还是给大量被感染了病毒的电脑、工控系统的使用者造成了不小麻烦，如何避免类似这种对无辜者的伤害也是探讨中的网络战争法的重要内容。

二、索尼事件

索尼事件的当事国是美国和朝鲜，导致矛盾冲突和激化升级的因素包含了捍卫国家尊严、维护创作自由、黑客侵入窃密、反击网络攻击等，其参与主体的主张诉求和攻防转换，预示了网络时代国家间冲突乃至战争的一种可能形态。

2014 年 6 月，一部由美国索尼影视娱乐公司出品的电影《采访》(*Interview*)的细节在互联网上被大量转载，影片以搞笑描述了一个美国脱口秀节目主持人和制片人采访并刺杀朝鲜领导人的故事，其中有大量取笑和丑化朝鲜领导人的情节。朝鲜方面对这部影片予以严厉谴责，外务省发言人将索尼影视娱乐公司及《采访》称作“最赤裸裸的恐怖主义”“对最高尊严的肆意亵渎”，宣称将采取“无情的反制措施”。此后索尼影视娱乐公司并未太重视朝鲜的警告，而朝鲜也并未采取什么实质性行动。一场可能的口水战由于黑客卷入而发生了出乎意料的变化，11 月 24 日，索尼影视娱乐公司的内部网络遭到严重的黑客攻击，大量内部资料被窃取，不久，公司多部未发行影片和剧本被放到网上，公司高官薪酬、财务信息和工作人员的内部往来邮件也被曝光。一个名为“和平卫士”的黑客组织宣称侵入了索尼影视娱乐公司的内部网络，并以公布更多信息来威胁公司不得公映该影片，一些公司员工及其家人也收到了黑客组织的警告邮件。重重压力之下，索尼影视娱乐公司一度宣布放弃圣诞期间的影片公映计划。

美国政府很快出来支持索尼影视娱乐公司，称绝不允许美国

的言论和创作自由受到恐怖威胁，并将矛头指向朝鲜，美国总统奥巴马和国务卿约翰·克里称调查结果证明朝鲜政府是针对索尼影视娱乐公司网络攻击的幕后操纵者，为此将采取回应措施，候任参议院军事委员会主席约翰·麦凯恩（John McCain）则断言这就是一场战争，众议院前议长纽特·金里奇（Newt Gingrich）直言不讳美国已输掉了一个回合。朝鲜方面则展示了维护国家尊严的坚定决心，外务省、国防委员会、中央通讯社连发声明抨击美国政府和索尼影视娱乐公司，并将黑客攻击称作“义举”和“正义的惩罚”，暗示是朝鲜的“支持者和同情者”发动的网络攻击行动。朝中社发表声明：“我们根本不知道索尼在美国的哪里，更不知道其为何遭到攻击，我们感觉也没必要知道。但从我们了解的情况来看，索尼正是拍摄电影、教唆恐怖分子伤害朝鲜最高领导人尊严的公司，它在利用美国政府针对朝鲜的敌意政策。”“美国国务卿只谈言论自由，试图将制作亵渎一个主权国家最高尊严的影片行为正当化。但必须明白，国际法也承认惩罚毁损名誉行为。”[①]双方冲突进一步上升到为外交口水仗。

在圣诞节即将来临之际，朝鲜境内互联网发生了大面积瘫痪，朝鲜包括政府和新闻机构在内的绝大部分网站从12月23日凌晨起一直处于不稳定及至完全无法稳定的状态，直到29日下午才恢复正常。27日，朝鲜公开指责美国是这次网络瘫痪事件的幕后黑手，并宣称受到了网络恐怖攻击。2015年1月7日，美国联邦调查局局长詹姆斯·科米（James B. Comey）在曼哈顿的一场网络安全大会上表示已掌握充分证据显示“朝鲜是对索尼公司实施网络攻击的幕后黑手”，美国国家情报总监詹姆斯·克拉珀（James R. Clapper）也认为“如果美国不进行反击，朝鲜就将继续攻击美国利

① 朝鲜中央通讯社：“朝鲜外务省发言人斥责美国就一制片公司遭网络攻击指责朝鲜”，2014年12月14日。

益”。2015 年 3 月 17 日，美国众议院国土安全委员会主席迈克·麦考尔(Michael McCaul)在华盛顿战略与国际研究中心的政策讨论会上表示，朝鲜网络瘫痪是美国政府采取的报复措施所致，这也是美国议员首次公开承认美国对朝鲜实行了网络攻击。[①] 显然，美国已将网络报复作为应对冲突的重要选项。

2015 年 1 月 3 日，美国总统奥巴马签署行政命令，授权财政部对朝鲜追加新的制裁，以回应索尼影视娱乐公司遭到的网络攻击，白宫发言人表示，新制裁针对三个机构和十个人，这只是寻求惩罚朝鲜的第一步，因为朝鲜多次挑衅，其中包括网络攻击。财政部声明称将加强针对朝鲜制裁的实施力度，包括不准一些指定的个人使用美国金融系统，以及禁止美国公民参与同朝鲜有关的事务。[②] 被列入制裁名单的三个机构包括一家情报机构——朝鲜侦查总局、一家国有军工企业——朝鲜矿业发展贸易公司以及一家科研机构——朝鲜檀君贸易公司，十名被制裁的个人都是同这三家机构或同朝鲜政府直接相关的个人。鉴于此前美国针对朝鲜的制裁已经非常广泛和严格，故此次制裁也是象征意义大于实质意义。

索尼影视娱乐公司是一家美国企业，对其进行网络攻击自然构成对美国国家利益的侵犯，奥巴马以维护宪法第一修正案赋予的创作自由为己任，并将对造成朝鲜网络长时间瘫痪的攻击视为反击恐怖主义威胁的正义之举。以“和平卫士”为代表的匿名网络黑客组织具备了与国家层级对手在网络空间对抗的实力，各方的支持者和反对者也在社交媒体上展开激辩，互联网提供的复杂技

① Center for Strategic and International Studies, “Cyber Leaders: A Conversation with Chairman Michael McCaul”, March 17, 2015, http://csis.org/event/cyber-leaders-0，最后浏览日期：2015 年 8 月 20 日。

② U. S. Department of Treasure, “Treasury Imposes Sanctions against the Government of the DPRK”, January 2, 2015.

术平台和广阔舆论场使得各方在此纷争中有了充分发挥的余地。索尼事件预示了未来国际冲突和战争的一种可能形态，即以互联网为主要平台的数字化对立和较量，参与者立场和诉求各异，方式和手段隐蔽，同时伴随着现实利益矛盾使得网络空间的多方博弈更加复杂。

三、网络作战的影响

震网行动和索尼事件都包含了美国对其他国家的网络基础设施或重要网络系统进行网络攻击的内容，但美国的网络作战部队直接参与了相关攻击尚未可知，所使用的攻击手段也尚未可知，中国外交部发言人曾表示“不支持在中国的任何一个地方从事网络违法犯罪活动”“反对任何国家或个人利用他国境内设施对第三国发动网络攻击”，[①]显示对索尼娱乐影视公司的黑客攻击和对朝鲜互联网的网络攻击都可能利用了中国的网络基础设施。而由于网络防御的复杂性和隐蔽性，很少有美国网络作战力量针对外来网络攻击的案例得到披露。尽管如此，两个案例已显示网络空间的作战远比传统作战方式复杂、手段更加隐蔽、冲突演变更加出人意料。

2015 年美国国防部《网络战略》称驱使国防部制定新网络战略的一个重要原因是美国政府和企业遭受网络攻击的紧迫性和复杂性都在不断增加，新战略将主要目标确定为国家层级的对手，表示美国将继续加大网络空间攻防能力的投入，以应对国家间的网络冲突乃至网络战争。[②] 美国也认为国家面临着一些尚未解决的问题，包括如何理解网络战争的要素，制定强有力的法律手段，倡导在冲突期间限制使用或者不使用网络武器库，了解网络空间中

---

① 中国外交部发言人 2015 年 12 月 18 日和 23 日、24 日针对索尼影视娱乐公司遭黑客攻击和朝鲜互联网中断事件回答记者提问的表态。

② U. S. Department of Defense, “Cyber Strategy”, April 2015.

自我防御的内容、定义责任和国家责任等。两大网络事件表明，人类历经战争毁坏的惨痛教训，已经缔结了《海牙公约》《日内瓦公约》等诸多界定战争参与方关系和作战行为规范的条约和协议，也赋予了联合国安全理事会维护国际和平与安全的首要职责。然而面对网络时代的相互言语攻讦和数据破坏，这些规则、共识和协调机构似乎全不适用，尤其应引起注意的是，在事件发展过程中，除了把自己塑造成为网络攻击和恐怖主义的受害者博得国际舆论支持外，还没有任何一方诉诸国际安全机制，显示了网络冲突国际协调机制的缺失。