美国网络空间政策国际法研究

朱路
(清华大学 国际关系学系, 北京 100084)

摘 要: 美国的网络空间政策主要体现在军方和政府的文件上,从最早的 1993 年白宫发布的关于发展信息基础设施的 12864 号行政命令至今,已有近 20 年的时间。政府文件主要来自白宫,自始至终强调对关键基础设施的发展与保护,基本不涉及国际法;军方文件来自国防部、陆军、海军、空军、军法官参考文献等,这些文件虽不同程度地提及国际法,但流于表面。美国的网络空间政策经历了一个长期演化的过程,采取了 4 种策略,呈现出 4 个特点。2011 年 5 月白宫发布的《网络空间国际战略》最终明确了美国将采取激进的网络空间政策,即网络空间的某些行为将导致美国在现实世界中使用武力,这对现有的国际法和国际法律秩序构成严重挑战,不仅会扩展领土和主权概念,延伸使用武力的含义,进一步滥用自卫权;而且使国际社会更难以接受侵略的定义,使国际法的中立制度形同虚设,挑战了国际法的责任制度,破坏了战争法的基石。

关键词: 美国网络空间政策; 自卫权; 国际法; 战争法
中图分类号: D923.4 文献标识码: A 文章编号: 1009-3370(2014)01-0097-13

2011 年 5 月 16 日,白宫发布《网络空间国际战略》(International Strategy for Cyberspace),2011 年 7 月 14 日, 美国国防部发布《网络空间行动战略》(Strategy for Operating in Cyberspace)。前者是美国政府关于网络空间的第一个全面战略性文件,后者是军方对前者的呼应,这两份文件较为清楚地反映了美国现阶段的网络空间政策。美国对于网络空间的认识和定性,经历了从模糊到清晰的长期演化过程,本文拟从国际法特别是战争法的角度,结合美国军方和政府的文件进行讨论。

一、术语选择:隐含的现实感

美国选择"cyberspace"而不使用其他类似术语如"network"或"internet"等,有一定语义方面的考虑。"cyberspace"是加拿大科幻小说家威廉·吉布森(William Gibson)生造的单词,在其 1984 年出版的小说《神经浪游者》(Neuromancer)中,吉布森用该词描述一个连接世界上所有人类、机器和信息的全球计算机网络, 该词强调人与机器和信息之间的连结与交互影响,是"计算机模拟的现实"[1]761。换言之,"cyberspace" 具有其他术语都不具有的现实感,或者说"cyberspace"与现实的联系更紧密、更明显, 这对于美国军方和政府将其视为物理意义的战场,有着一种预设的概念上的正当性。国内权威媒体机构如新华社将其译作"网络空间",更好地反映出事物的本质,本文沿用这种称呼。

研究美国的网络空间政策,必须充分和详细地考察美国关于网络空间的文件,这些文件主要来自军方和政府,下文将分别讨论。

二、政策演化:军方文件之考察

考察美国军方对于网络空间的态度和立场,最权威也是最快捷的方式是研究其战争法手册。这种手册无论名称为何,都会一方面列举战争时期国家的战争法义务和权利,另一方面陈述对有关法律问题的理解,作为在战争法方面教育、培训和决策的基础。出人意料的是,作为世界上的头号军事强国,美国迄今为止还没有一部统一的战争法手册,有关法律问题主要参考陆军发布的战地手册(Field Manuals)①,特别是 1954 年发布、1976 年修订的代号 FM 27-10 的关于陆战规则的手册。近 40 年过去了,FM 27-10 手册未作更新,但无论战争和武装

收稿日期: 2013-02-16
基金项目: 2013 年度国家社科基金重点资助项目"海外安全利益法律保护的中国模式研究"(13AFX028);教育部人文社科重点基地重大项目"全球安全基本法律问题研究"(12JJD820004);中国博士后科学基金第 53 批面上资助项目"当代战争私有化与国际法的未来发展"(2013M530586)
作者简介: 朱路(1982—),男,博士后,法学博士,E-mail:hank06@163.com
①这些战地手册涵盖范围广泛,数量庞大,常常被修改、取代或到期停止适用。根据美国陆军网站公布的信息,截至目前,共有 426 个正在使用的战地手册,参见 http://armypubs.army.mil/doctrine/active_fm.html。

冲突还是战争法，都在很多方面出现了新情况，遇到了新问题、新挑战。

鉴于此，美国国防部开始考虑制定适用所有军种的统一“权威”战争法手册，即将来陆、海、空三军的战地手册必须要遵守该手册中设定的标准[2]359。美国军方 1996 年初步同意制定战争法手册①，国防部 1998 年底正式启动“战争法项目”，本来预计在 2011 年发布战争法手册，但因故推迟，迄今尚未发布。因此，需要考察美国军方的其他相关文件。

(一)国防部文件

美国国防部有关网络空间的文件来自国防部本身及其下设的参谋长联席会议，主要有以下几个方面。

《国防部军事和相关术语词典》(以下简称《术语词典》) 提供了美军使用的网络空间和网络空间行动的标准定义。《术语词典》是美国国防部编纂、审核和认可的关于军事和相关术语的名称及含义的权威参考资料，每月更新，统一适用于国防部各机构部门和美军所有兵种，换言之，对术语的界定代表了美国军方的正式意见。根据最新版本的《术语词典》，网络空间是指“包括互联网、电信网络、计算机系统和嵌入式处理器和控制器等信息科技基础设施组成的相互依存的网络即信息环境之中的全球领域”，网络空间行动“主要目的是在网络空间或通过网络空间实现军事目标或效果而使用网络空间能力”的行为②。

代号 JP 1-04 的《军事行动的法律支持》(以下简称《法律支持》)由参谋长联席会议发布，旨在向美军提供进行各类军事行动时的法律指导与建议。《法律支持》本来从未涉及网络空间，但 2011 年白宫和国防部相继发布关于网络空间的战略文件后，参谋长联席会议紧接着于 2011 年 8 月 17 日发布了《法律支持》的最新版本③，这次更新有两个主要特点：一是首次列举在“所有武装冲突和其他军事行动中”需要遵守的战争法基本原则，即军事必要原则、不必要痛苦原则、区分原则和相称性原则。二是首次提及网络空间，规定美国战略司令部的军法参谋(USTRANSCOM SJA)提供的法律建议除了涉及在网络空间行动的自由，“特别关注网络空间等领域的国际法和行动法(operational law)。”《法律支持》虽然提到了网络空间，但是回避了网络空间与使用武力的问题。

《网络空间行动国家军事战略》(以下简称《军事战略》)可以说是国防部《网络空间行动战略》的前身。2006 年 12 月，参谋长联席会议发布了机密文件《军事战略》，原定于 2030 年 9 月 19 日解密，后提前公开部分内容④。《军事战略》声称美国在网络空间的军事战略必须要保持灵活，“确保美国在(网络空间)这个竞争激烈的领域有行动的自由，同时不准美国的敌人有同样的自由”⑤。尽管其他部门和机构也有责任保证网络空间的安全，但只有国防部有权为此采取军事行动。具体来说，国防部在网络空间的作用：一是保卫国家；二是国家事件回应(National Incident Response)；三是保护关键基础设施。“国防部将通过网络空间采取所有军事行动以击败、劝阻和威慑针对美国利益的威胁。”⑤《军事战略》特别强调国防部必须在科技方面持续投入以影响各式网络空间技术，特别是出现于商业领域的那些技术，因为获得在网络空间的主动权是在网络空间保持优势的前提。由于并非所有基础设施均在国防部控制下，国防部还必须加强与其他主体的伙伴关系以减少这些基础设施受攻击的风险，如国防承包商、联邦资助的研发中心、学术界、商业基础设施提供者和其他类似依靠网络空间的全球和地区盟友及伙伴⑤。在法律方面，《军事战略》仅提及国防部“必须在可适用的美国国内法和国际法以及美国政府和国防部的相关政策范围内”进行网络空间行动，但并未说明什么是“可适用的国际法”，而且从措辞上看，美国国内法优先于国际法，不仅如此，《军事战略》还声称“适用于网络空间行动的法律框架取决于将要进行的行动的性质”⑤。也就是说，是根据网络空间行动决定可适用的法律，而不是根据可适用的法律决定网络空间行动，这完全颠倒了逻辑。

国防部 2011 年 7 月 14 日发布的《网络空间行动战略》，宣布支持白宫《网络空间国际战略》和美

①参见美国国防部外交事务副法律总顾问黑斯·帕克斯在美国律师协会“法律和国家安全常务委员会”早餐会上的演讲，November 18，2010，http://apps.americanbar.org/natsecurity/hays_parks_speech11082010.pdf。

②Joint Chiefs of Staff. JP 1-02 Department of Defense Dictionary of Military and Associated Terms，8 November 2010 (As Amended Through 15 March 2012)：89。

③Legal Support to Military Operations，17 August 2011，www.dtic.mil/doctrine/new_pubs/jp1_04.pdf。

④The National Military Strategy for Cyberspace Operations，December 2006，http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf。

⑤Chairman of the Joint Chiefs of Staff. The National Military Strategy for Cyberspace Operations，December 2006。

国总统关于网络空间的基本自由、隐私和信息自由流动的承诺，并协助促进发展提倡“开放、互通(interoperable)、安全、可靠”的网络空间国际行为规范和原则，为此，国防部要占据 5 个方面的“战略主动权”：一是将网络空间视为“行动领域”以组织、训练和进行装备，使国防部能够充分利用网络空间的潜能。二是采用新的防御行动概念保护国防部的网络和系统。三是和其他美国政府部门和机构以及私营部门建立伙伴关系，使得政府整体网络空间安全战略成为可能。四是与美国的盟友和国际伙伴建立稳固的关系以加强集体网络空间安全。五是通过杰出的网络空间劳动力和快速的科技创新发挥美国的独创性[①]。《网络空间行动战略》绝大部分内容属于机密，公开的关键内容基本源自《军事战略》，但相比《军事战略》《网络空间行动战略》有 3 个值得注意的地方：一是首次明确提出“主动网络空间防御”，宣布国防部“已经”采用主动网络空间防御阻止侵入并击败有关国防部网络和系统的敌方(adversary)活动，但并未说明什么是“主动防御”，也没有说明什么情况下可以进行“主动防御”，“主动防御”又会采用哪些手段等。“主动防御”不禁让人联想到美国在伊拉克战争中进行的所谓“预先自卫/先发制人的自卫”(anticipatory /preemptive self-defense)，二者惊人的相似。二是为联结网络空间和现实世界留有余地，认为“发展国际共享的态势感知(situational awareness)和警告能力将使集体自卫和集体威慑成为可能”，但没有提及关键问题即这种集体自卫和集体威慑究竟是仅限于网络空间，还是超出网络空间延伸至现实世界中的武力行为。三是完全不提法律问题，无论是美国国内法还是国际法。相比国防部的其他文件，这个设定总体战略的纲领文件，虽然刻意保持隐晦，却真切地反映出美国军方对于网络空间态度的大倒退、大转向。

实际上，2011 年 11 月国防部向美国国会提交的《国防部网络空间政策报告》(以下简称《政策报告》)包含更实质、更直接的观点。报告的绝大部分内容都是网络空间的政策和法律问题，并坦承国防部和其他政府机构以及盟友和伙伴将通过在适用网络空间问题的规范上达成共识以进一步发展国际习惯法，认为尽管存在诸多困难，但“在网络空间进行的某些活动毫无疑问地构成使用武力并导致有关国家援引合法自卫的固有权利，在这种情况下，决定是否对即使是推定的非法行为采取防御回应，将由总司令决定”[②]。《政策报告》明确地宣称网络空间的某些行为将引发有关国家如美国行使自卫的“固有权利”，而且即使是“推定”发生了此类行为，也仍可能进行“自卫”。这是非常危险的做法，下文将详细讨论。

(二)陆军战地手册

陆军正在使用的战地手册中，涉及网络空间问题的主要有 2003 年 11 月 28 日发布的代号 FM 3-13 的《信息行动：原则、策略、技巧和程序》(以下简称《信息行动》)、2009 年 7 月 14 日发布的代号 FM 6-02.71 的《网络行动》以及 2011 年 2 月 22 日发布的代号 FM 3-0 的《行动》等，这些文件都已经过多次修改与更新[③]。

《信息行动》提供了目前美军通用的信息环境和信息行动的定义，前者是“搜集、处理或传播信息的个人、组织或系统的总和，包括信息本身”，具体由三个部分组成，即“世界范围内通讯网络的互联、友军、敌军(adversary forces)和其他组织的命令控制系统以及决策、处理信息的友方、敌方和其他人员”，并构成“战场的组成部分之一”[④]；后者是指通过“使用电子战、计算机网络行动、心理行动、军事欺骗和安全行动的核心能力，和特定支援与相关能力一起影响或防御信息和信息系统并影响决策”[⑤]。《信息行动》有 2 个方面值得注意：一是详细阐述了来自信息环境的威胁及应对措施并宣称信息环境是战场的组成部分，但并未直接涉及网络空间与使用武力的问题。二是将基于信息环境的威胁能力分为 4 个等级[⑥]，但这种分类完全依靠一个预设的大前提，即能够清楚无误地识别和确定造成威胁的主

①Department of Defense Strategy for Operating in Cyberspace, July 2011, http://www.defense.gov/news/d20110714cyber.pdf。

②Department of Defense. Department of Defense Cyber Policy Report Pursuant to Section 934 of the NDAA of FY 2011[R]:9。

③由于部分最新文件尚未公布，本文参考的是公布的最新版本，如《网络行动》是 2008 年 11 月 19 日的版本。

④Headquarters. Department of the Army. FM 3-13 Information Operations: Doctrine, Tactics, Techniques, and Procedures [M]. Chapter 1 Design of Army Information Operations: 1-2。

⑤Headquarters. Department of the Army. FM 3-13 Information Operations: Doctrine, Tactics, Techniques, and Procedures[M]. Preface: iii。

⑥第一等级来自没有重大支持、简单地使用一般黑客工具和技术的单独或小范围的业余爱好者；第二等级来自复杂地使用黑客工具、受商业实体、犯罪组织或其他跨国组织支持的个人或小组；第三等级来自使用复杂工具、由国家支持的机构(军方或民间)和大量资源支持的个人或小组；第四等级来自国家支持的、进攻性的信息行动，特别是使用最先进的工具和掩护技术、协同军事行动进行的计算机网络攻击。参见《信息行动》，第 1-4 页。

体,而在现阶段,发展并实现这种技术能力远非易事。

《网络行动》详尽说明了网络行动的各个方面,如原则、组成部分、作用与责任等,是陆军关于网络行动最细致的战地手册。网络行动是"为操作和防御全球信息栅格 (Global Information Grid,GIG)而进行的(联合)行动"①,全球信息栅格②则是"全球互联的、终端到终端的成套信息能力,以及根据战士、决策者和支援人员的要求搜集、处理、存储、传播和管理信息的相关过程,包括一切自有的和租用的通讯和电脑系统和服务、软件及其应用、数据、安全服务、其他相关服务和国家安全系统"③。《网络行动》的显著特点是将所有问题置于网络空间这个大环境下讨论,也就是说,用网络手段在网络空间回应网络威胁,强调预防网络威胁,一旦发生网络威胁则应尽快清除并降低损失, 同时迅速将其定级,完全不涉及网络空间与使用武力的问题,也几乎不涉及国际法。例如,根据《网络行动》,有多个机构负有应对和处理来自信息环境威胁的职责④,但它们都只通过信息保护手段如信息保证(Information Assurance)、计算机网络防御和电子保护能力(Electronic Protect Capabilities)来"保护和防御友方信息和信息系统……同时拒绝敌方出于自己的目的刺探(exploit)友方信息和信息系统"⑤。而计算机网络防御的回应包括防御和恢复:一是增强己方防御能力; 二是停止攻击或将攻击的影响或损害最小化;三是迅速和彻底地对攻击或刺探定性⑤。

《行动》是陆军两个最基本的文件之一⑥,供陆军中高级领导层、指挥大型行动和战役的少校和以上军衔军官及其参谋人员使用,对开展行动提供原则指引和方向,反映了陆军对于如何进行迅速和持久的陆地行动的看法,并构成制定其他基本原则和关于战术、技术和程序的下级战地手册的基础。《行动》宣称"陆军将在复杂地形和网络空间作战(fight)和行动"⑦,提出"网络战"(Cyber Warfare)的概念⑧,认为网络战"将战斗力量扩展至全球信息栅格的防御性界限之外, 以探测、拒绝、退化(degrade)、干扰、破坏和刺探敌人",断言网络战需要完成五项任务, 即"研究并定性网络空间威胁""识别、定性和刺探敌人""增进网络空间情景意识""进行网络空间刺探、攻击和防御"以及"协助调查攻击以决定归属"⑨。因此,综合来看,《行动》中所称的在网络空间的"作战",应该不能理解为物理意义上的、在现实世界中的作战行为,而是发生于网络空间的行为,即《行动》并不涉及网络空间与使用武力的问题。

(三)海军文件

代号 NDP 1 的《海军原则出版物 1:海战》(以下简称《海战》)是海军关于海战及其职责的纲领文件, 最近的一次更新是在 2010 年 3 月。《海战》认为,未来美国军事行动成功与否日渐依靠空气空间和网络空间,对于全球公有领域(global commons)即不属于任何国家的海洋、空气空间、太空和网络空间部分,"提供适当的提升(lift)和保持足够的控制将是极为迫切的事项"⑩,而"控制海洋要求在海洋领域、太空和网络空间的所有方面都具备能力"⑩。《海战》虽然反复强调网络空间的重要性,但没有进一步就网络空间展开叙述,而且,有 2 个问题需要特别注意:一是术语选择问题,《海战》没有选择使用与"全球公有领域"意思相近而且更通用、更常见的术语 "人类共同继承遗产"(Common Heritage of

①Joint Chiefs of Staff. JP 6-0 Joint Communications System (10 June 2010):IV-1。

②需要说明的是,《术语词典》中的定义来自代号 JP 6-0 的《联合通讯系统》文件,已公开的最新版本即 2010 年 6 月 10 日《联合通讯系统》中全球信息栅格的定义大部分与《术语词典》中一致,但没有包括国家安全系统,而且用"为获得信息优势而必需的"来修饰组成部分。参见 Joint Chiefs of Staff,JP 6-0,Joint Communications System (10 June 2010),II-1. 可见,虽尚未公开,但《联合通讯系统》在 2010 年 6 月至今的某个时候,已经进行了部分修改,删除"为获得信息优势而必需的"也许是为了增加概念的中立或客观色彩。

③Joint Chiefs of Staff. JP 1-02 Department of Defense Dictionary of Military and Associated Terms,8 November 2010 (As Amended Through 15 March 2012):138。

④如国防部计算机应急反应小组(DoD-CERT)、陆军全球网络行动和安全中心(A-GNOSC)和陆军计算机应急反应小组战术行动中心(ACERT)等。

⑤Headquarters. Department of the Army. FM 6-02.71 Network Operations,19 November 2008。

⑥另一个是代号 FM 1 的《陆军》。

⑦Headquarters. Department of the Army. FM 3-0 Operations,22 February 2011.P

⑧需要说明的是最新版的国防部《术语词典》并未收录该词,因此该词主要是在陆军内部使用。

⑨Headquarters. Department of the Army. FM 3-0 Operations,22 February 2011. Chapter 6 The Science of Control:6-21。

⑩NDP 1 Naval Doctrine Publication 1 Naval Warfare,March 2010:19,28。

Mankind)[①]，似乎仍是出于语义方面的考虑。从字面意思上看，“全球公有领域”暗示着使用的自由，而“人类共同继承遗产”暗示着使用的责任与道义。二是不进行任何法律分析，直接扩大全球公有领域的覆盖范围，将网络空间也包括进去。即使不考虑网络空间为何是全球公有领域这个先决问题，那么网络空间究竟全部是全球公有领域，还是某些部分是？判断的标准和依据又是什么？《海战》完全回避了这些问题。

(四)空军文件

空军是唯一在使命中明确提及网络空间的美军军种：“在天空、太空和网络空间飞行、战斗并获胜”[②]。在 2006 年公布的一份概要中，空军就已经明确将网络空间视为“战斗领域”(warfighting domain)和“战场”(battlespace)[③]。空军有关网络空间的文件主要是 2010 年 7 月 15 日发布、2011 年 11 月 30 日更新的代号 AFDD 3-12 的原则文件《网络空间行动》(以下简称《网络空间行动》)。《网络空间行动》的观点较为明确，具体来说，一是明确承认网络空间的匿名性固有特征使得行为归属成为“最有挑战”的事情，即以“足有把握和经得起检验”的方式将网络空间中的主体或行为联系到实际的、现实世界中的主体(无论是个人还是国家)，并告知决策者和政策制定者。二是明确承认“法律考量和国际法律义务适用网络空间能力的使用，国际法、国内法和政策决定、武装冲突法以及交战规则构成评估作战行动的法律框架”，认为“贯穿计划和执行网络空间行动的合理法律建议对于成功完成任务极其重要”。至于如何才能合法地进行网络空间行动，《网络空间行动》指出应参考参谋长联席会议发布的《法律支持》。但如上所述，《法律支持》回避了网络空间与使用武力的问题，因此，《网络空间行动》也同样回避了这个问题。

(五)军法官参考文件

除了上述国防部和陆海空三军关于网络空间的文件，美国军方还有一种关于网络空间的文件，相比之下，实用性似乎更大，这就是以《行动法手册》为代表的军法官(Judge Advocates)参考文件。

美国军方确实发布过名为《战争法手册》的出版物，国内有人误以为这本《战争法手册》就是那部统一适用整个美军的战争法手册，实则不然。军法署国际法和行动法法务部(International and Operational Law Department，The Judge Advocate General's Legal Center & School)主编了一套 3 卷的参考文件供军法官使用，《战争法手册》是其中之一，另外 2 卷是《行动法手册》和《战争法文献补充》。2005 年最新版的《战争法手册》几乎不涉及网络空间或相关概念，但在第 3 章《联合国和使用武力的法律基础》中提出“什么构成使用武力”“经济压力、计算机网络攻击是否构成使用武力”这种开放性问题，并用括号注明“在决定是否构成使用武力问题上，西方观点倾向于考察该行动的动能(kinetic)效果或影响，然而这种观点容易引起大量争议”[④]。军法署国际法和行动法法务部 2010 年还主编了一本供“入门及中级”军法官使用的《战争法案头参考书》，2011 年又进行更新，但均未提及网络空间或相关概念。

实际上，这些参考文件中只有《行动法手册》涉及网络空间问题，但也经历了从无到有的过程。《行动法手册》主要有关军法官遇到的实践问题，每年更新，以最新版本为准。下文将考察不同版本的《行动法手册》以分析该手册对网络空间认识的沿革。

《行动法手册》可能至迟在 2001 年才提及网络空间相关问题[①]，根据《信息行动》一章，信息行动

①实际上很难说这二者存在实质区别。一般来说，人类共同继承遗产除了是法律概念，更多的是一种法律原则，而全球公有领域主要是法律概念。人类共同继承遗产往往比全球公有领域涵盖范围更广，除了都包括海洋和空气空间的一部分和太空，人类共同继承遗产还常涉及南极、海床、海底文化遗产等。参见 Bradley Larschan & Bonnie C. Brennan. Common Heritage of Mankind Principle in International Law Columbia Journal of Transnational Law，1983 (2)：305-338; Rudolph Preston Arnold. The Common Heritage of Mankind as a Legal Concept International Lawyer，1975 (1)：153-158; Jeffery Loan. The Common Heritage of Mankind in Antarctica：An Analysis in Light of the Threats Posed by Climate Change New Zealand Yearbook of International Law，2004(1)：149-190; Ellen S. Tenenbaum. A World Park in Antarctica：The Common Heritage of Mankind Virginia Environmental Law Journal，1990 (1)：109-136; Edward Guntrip. The Common Heritage of Mankind：An Adequate Regime for Managing the Deep Seabed Melbourne Journal of International Law，2003 (2)：376-405; Steven Kotz. The Common Heritage of Mankind：Resource Management of the International Seabed Ecology Law Quarterly，1976 (1)：65-108; Anastasia Strati. Deep Seabed Cultural Property and the Common Heritage of Mankind International and Comparative Law Quarterly，1991 (4)：859-894; Tara Murphy. Security Challenges in the 21st Century Global Commons Yale Journal of International Affairs，2010(2)：28-43; Stuart Kaye. Threats from the Global Commons：Problems of Jurisdiction and Enforcement Melbourne Journal of International Law，2007(1)：185-197。

②参见美国空军网站主页，http://www.af.mil/main/welcome.asp。

③Headquarters U.S. Air Force. Cyberspace：A Warfighting Domain，26 Sep 2006。

④International and Operational Law Department. The Judge Advocate General's Legal Center and School. Law of War Handbook 2005：

“由影响敌方信息和信息系统同时防御我们自己的信息的行为构成”，贯穿所有层次的战争和军事行动的全部范围，但此时军方仍在争论“信息行动是否给作战能力增加了新的维度或是否是重塑军队达成战略目标方式的革命”，而且认为实践中信息行动会带来很多无法精确归纳以便列在情况说明清单中的实际问题和法律问题，“正在形成中的信息行动的原则包括关于情报搜集和监管的法律和政策、空间法、计算机安全、心理行动、任务计划、武装冲突法目标限制、信息安全和刺探以及搜索和捕获指导”②。《信息行动》一章虽然只有 9 页，却用近一面篇幅说明了信息行动与战争法的关系问题，认为数字时代的互联本质导致任何信息行动都涉及与中立法有关的问题，使用中立国电线或网线进行信息行动将危及中立国的中立地位，如果中立国不能或不愿保持中立，交战国“可以采取必要措施使敌人的努力无效”，同时，在策划计算机网络攻击时，策划者“应该考虑区分军事目标与民用物体的问题”②，并必须谨记战争法的四个基本原则，即区分原则、不必要痛苦原则、预防原则和比例原则②。总的来说，2001 年版《行动法手册》对于网络空间有关问题的叙述，整体上是积极而且正确的。

2002 年版《行动法手册》的《信息行动》一章基本照搬自 2001 年版，但 2003 年版则有如下 5 个方面有显著改动：

第一，首次提出并增加了信息战(Information Warfare)概念，认为信息战是信息行动的子概念，是在危机或冲突中针对特定的一个或数个敌人以完成或推进特定目标所采取的信息行动；是无论何种手段，针对信息系统的任何攻击，如轰炸电话转接设施和破坏转接软件均属于信息战；是无论何种手段，保护“我们自己的”信息和信息系统的任何行为；是达到特定目标的一种战争手段。

第二，首次提及“防御美国关键基础设施和信息系统”，但仅仅简略介绍了数个官方文件，并未说明军方在此方面有何具体计划或行动。

第三，首次讨论了计算机网络攻击与使用武力的关系，认为虽然远不清楚国际社会多大程度上能接受将计算机网络攻击视为武装攻击或使用武力以及将自卫原则适用于计算机网络攻击，但极可能接受受到国家支持的计算机网络攻击的国家可以合法地以同样方式回应，在某些情况下使用自卫的传统军事手段也是合理的。除非国际社会就计算机网络攻击问题的国际条约开始谈判，否则该领域的有关国际法将会通过国家行为和公开立场而发展。

第四，首次提出未经授权的电子入侵可被视为侵犯有关国家主权，甚至“等同于物理意义上非法侵入该国领土”，但承认这有待国际社会进一步讨论，不过认为受害国如果能够“可靠地”将有关行为定性为故意并归于另一国机构，则至少有抗议的权利。

第五，首次从国际电信法(International Communications Law)角度讨论信息行动问题，认为 1982 年《国际电信公约》允许国家在某些情况下干涉国际通讯，但其条款主要适用于和平时期，并未清楚说明是否在武装冲突中适用②。

2004 年版《行动法手册》的《信息行动》一章没有显著改动，2006 年版则删去了信息战概念，并首次从“诉诸战争的权利”(Jus ad Bellum)和“战时法”(Jus in Bello)的角度论述信息行动与国际法的关系，但内容与观点并无实质改动②。2007 年版《行动法手册》的《信息行动》一章首次引用国际法学者关于信息行动是否构成联合国宪章下的使用武力的看法，列举战争法的四个基本原则并首次认为应适用于信息行动，这些基本原则是军事必要原则、区分原则、比例原则和不必要痛苦原则②，不同于 2001 年版所列举的 4 个基本原则。2008—2012 年《行动法手册》的 5 个版本与 2007 年版基本相同，而实质观点均沿袭 2003 年版，即目前使用的最新版 2012 年版《行动法手册》中，有关网络空间、信息行动的实质观点与 2003 年版一致。

三、政策演化：政府文件之考察

美国军方强调网络空间的“防御”，而美国政府强调对关键基础设施的保护。此外，与军方文件来自多个主体不同的是，政府关于网络空间的文件主要来自白宫。下文将分 3 个时期进行讨论。

(一)克林顿政府时期

美国的网络空间政策始于克林顿政府时期，这个时期关于网络空间的政府文件为后来美国网络空间政策的许多重要方面定下了基调。

1993 年 9 月 15 日，克林顿签发 12864 号行政命令，建立美国国家信息基础设施顾问委员会以发展国家信息基础设施[3]，这是美国政府关于网络空

①目前公布的《行动法律手册》中，1997 年版没有涉及网络空间相关问题，1998 至 2000 年以及 2005 年的四个版本无法获得。

②International and Operational Law Department. The Judge Advocate General's Legal Center and School. Operational Law Handbook 2001.

间的第一份文件。1996 年 7 月 15 日，克林顿签发 13010 号行政命令，成立保护关键基础设施总统委员会，并列举了八类对美国的国防和经济安全“至关重要”的国家基础设施，即通信、电力系统、石油和天然气的存储和运输、银行和金融业、运输、供水系统、应急服务和政府的持续（continuity）[4]。1998 年 5 月 22 日，克林顿签发两个总统决定指令。62 号文件《打击恐怖主义》关注了所有针对美国的非常规攻击，如恐怖行为、使用大规模杀伤性武器、攻击关键基础设施和网络攻击、网络战等[5]，这是第一个提及网络攻击和网络战的政府文件，而且将其定性为非常规攻击。63 号文件《保护关键基础设施》要求采取所有必要措施以迅速消除美国关键基础设施易受物理或信息攻击之重大弱点，并反复强调政府机构与私营部门建立伙伴关系以减少脆弱性[6]，该政策沿用至今。1999 年 12 月，白宫发布的《新世纪国家安全战略》中声称美国比任何其他国家都依靠网络空间，多次提及网络攻击（cyber-attack）、网络威胁（cyber-threats）、信息行动、信息攻击，并将信息攻击定性为与大规模杀伤性武器并列的“非常规工具”①。

（二）小布什政府时期

小布什政府时期，政府的网络空间政策在克林顿政府工作的基础上进行了扩充，并有了一些推进，但整体上缺少引人注目之处。

2001 年 10 月 22 日，小布什签发 13231 号行政命令《信息时代关键基础设施保护》，成立总统关键基础设施保护委员会取代克林顿政府时期的保护关键基础设施总统委员会[7]。2003 年 2 月 14 日，小布什签发《保障网络空间安全国家战略》和《关键基础设施和重要资产物理保护国家战略》。《保障网络空间安全国家战略》设定了三项战略目标和 5 个优先事项，前者是指：一是防止针对美国关键基础设施的网络攻击；二是降低国家对网络攻击的脆弱性；三是发生网络攻击时将损害和恢复时间最小化。后者包括：一是国家网络空间安全响应系统；二是减少国家网络空间安全威胁和脆弱性计划；三是国家网络空间安全意识和培训计划；四是政府网络空间安全；五是国家安全和国际网络空间安全合作。《保障网络空间安全国家战略》指定国土安全部为保护网络空间安全的主要机构[8]。《关键基础设施和重要资产物理保护国家战略》界定和列举了关键基础设施和重要资产，前者扩大了上述 1996 年 13010 号行政命令所列举的八类国家基础设施，认为关键基础设施分布于农业和食物、水、公共健康、应急服务、国防工业基地、通信、能源、运输、银行和金融业、化学工业和危险材料、邮政和船运等领域，后者包括国家纪念物和象征、核电站、水坝、政府设施、关键商业资产等[9]。

2003 年 12 月 7 日，小布什签发 7 号国土安全总统指令《关键基础设施识别、优先和保护》，国土安全部随后建立国家基础设施保护计划，该计划授予国防部迅速查明制造网络攻击之主体的职责。2004 年 12 月，国土安全部执行根据 5 号国土安全总统指令制定的国家回应计划（National Response Plan），对各部门在出现危及国家安全事件时进行分工。根据该计划，国防部在军事行动中可以使用计算机安全和计算机网络防御活动保卫国家，在网络攻击对国家安全构成“即将发生的威胁”时可以根据“可适用的法律和政策授权”，采取行动进行“威慑或防御”[10]，但国家响应计划回避了界定所有关键概念，并未说明什么是“即将发生的威胁”，“可适用的法律”具体包括哪些，进行“威慑或防御”会采用何种形式。

2008 年 1 月，小布什总统签发机密文件国家安全总统指令 54 号/国土安全总统指令 23 号文件，建立“国家网络安全全面计划”（Comprehensive National Cybersecurity Initiative），该计划为高度机密，根据公开的信息，计划包括 12 项互相增强的核心内容，以实现三个目的：一是保证美国在网络空间具有防御当今即刻威胁的前沿阵地，二是防御网络空间所有类型的威胁，三是加强未来的网络安全环境[11]。

（三）奥巴马政府时期

奥巴马政府时期，政府的网络空间政策采取了咄咄逼人的态势，在一些长期保持模糊态度的重大问题上进行了明确的突破。

2009 年 2 月 9 日，奥巴马要求其国家安全和国土安全的顾问在 60 天内对美国的网络安全政策作出全面评估②，110 天后，即 2009 年 5 月 29 日，白宫发布《网络空间政策回顾：保障可信任和有弹性的信息和通信基础设施》，强调美国 21 世纪的经济繁荣将依赖于网络空间安全，将网络空间安全风险定性为美国面临的“经济和国家安全方面最严重的

①A National Security Strategy for a New Century，December 1999，http://www.fas.org/man/docs/nssr-1299.pdf。

②President Obama Directs the National Security and Homeland Security Advisors to Conduct Immediate Cyber Security Review/Melissa Hathaway Selected to Lead the Review，February 9，2009，http://www.whitehouse.gov/the_press_office/advisorstoconductimmediatecybersecurityreview。

挑战”，并将网络安全定性为“国家优先事项”①。2011 年 4 月，白宫发布《网络空间政策回顾：网络空间可信任身份国家战略》，意在建立一个以用户为中心的“身份生态系统”(Identity Ecosystem)，该系统中的个人、组织与设备由于获取和验证了数字身份而可以彼此信任，以此提高网络环境和在线交易的安全程度[12]。

2011 年 5 月白宫发布《网络空间国际战略》，宣布美国的目标是促进网络空间的“开放、互通、安全、可靠”，强调网络空间的稳定需要“通过规范”，这种规范将由美国和具有类似想法的国家一起确立，“构成外交和防务的基础，并指引国际伙伴关系”。《网络空间国际战略》列举并阐述了 7 个政策优先事项：经济方面推动国际标准和创新的、开放的市场；“保护我们的网络”方面提高安全性、可靠性和弹性；执法方面扩展合作和法治；军事方面准备应对 21 世纪的安全挑战；互联网治理方面推动有效的和包容的结构；国际发展方面构建能力、安全和繁荣；互联网自由方面支持基本自由和隐私。相比之前所有关于网络空间的政府文件，《网络空间国际战略》相当激进，具体表现为：一是宣称自卫权构成网络空间规范的基础之一，网络空间中的“某些侵略(aggressive)行为”将引发有关国家援引固有的自卫权，为此，美国保留所有“和可适用的国际法一致的、合适的”必要手段，无论是外交、信息还是军事、经济。二是宣布美国的网络威慑战略，确保攻击或刺探美国网络的行为所产生的风险大大超过其可能带来的好处，为此，需要使用所有符合“可适用的国际法”的必要手段。三是宣布和盟友及伙伴的军方和民间机构一起发展“在网络空间”集体自卫的方法与手段②。

《网络空间国际战略》的观点似是而非，解释余地很大。例如，为什么是网络空间中的“某些侵略(aggressive)行为”而不是所有侵略行为会使美国行使自卫权？这些侵略行为具体包括什么？判断的标准是什么？再如，对网络空间中的“某些侵略行为”进行自卫是仅限于网络空间（如上段第三点所述）还是主要是现实世界中的武力行为？需要认识到，在网络空间进行自卫的方法与手段的确需要进一步研究和发展，而在现实世界中进行自卫即使用武力则不必如此。从这个角度看，《网络空间国际战略》回避了明确网络空间与使用武力的关系问题，但实际上将网络空间与使用武力联系起来，而且，又特意强调和盟友及伙伴一起发展“在网络空间”集体自卫的方法与手段以增加迷惑性。

《网络空间国际战略》虽然不经任何法律分析便抛出上述观点，但也确实提及国际法，声称“发展国家在网络空间的行为规范并不要求重塑(reinvent)国际习惯法，也不使得现存的国际规范过时，长期以来指引和平和冲突时期国家行为的国际规范也适用于网络空间。然而，网络科技的独特属性需要进一步工作以澄清这些规范如何适用以及存在哪些对于补充这些规范可能是必须的附加理解”②。这个观点乍看之下可能是正确的，但关键在于事情的先后顺序，即应该首先通过国际社会的共同努力澄清哪些现存的国际规范适用于网络空间，以及如何进行必要的补充和调整，而不是首先抛出单方面制定的规则如网络空间中的某些行为将导致有关国家行使自卫权，将其贴上“必须的附加理解“标签，试图以此为基础发展国际习惯法。

四、政策演化：策略及特点

美国网络空间政策在演化的过程中，主要采取了 4 种策略：

第一，权宜对待法律，伺时予以突破。国际法只是美国在制定和发展网络空间政策时的权宜之计。从政府文件看，几乎从未提及国际法，近年来偶尔提之也只是点缀，并且只提对自己有利的部分。从军方文件看，尽管大部分文件确实不同程度地提及战争法，但流于表面。而且，美国一直在试图突破相关的国际法，只是以往动作较小，而近年幅度加大。

第二，精心选择词句，转移关键问题。如在遣词上，使用“网络空间”预设现实感，选择“全球公有领域”强调使用的自由，使用“主动防御”代称先发制人③，全部使用通俗概念而非法律概念称呼有关主体以掩盖问题，即“敌军”和“友军”“敌方”“友方”和“其他人员”(下文将详述)。在酌句中，暗示美国国内法优先于国际法④，暗中将网络空间与使用武力

① Cyber Policy Review Assuring a Trusted and Resilient Information and Communications Infrastructure, May 29, 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf。

②The White House. International Strategy for Cyberspace – Prosperity, Security, and Openness in a Networked World, May 2011. (2011-05)[2012-04-20]. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf。

③实际上，美国国防部长已经明确宣称美国对网络攻击要采用先发制人的战略。参见 US prepares first-strike cyber-forces, 12 October 2012, http://www.bbc.co.uk/news/technology-19922421。

④如《军事战略》。

联系起来，但特意明确提及发展“在网络空间”集体自卫的方法与手段[①]。

第三，暗中颠倒逻辑，增加辨识难度。如声称根据网络空间行动决定可适用的法律，而不是根据可适用的法律决定网络空间行动，以及在尚未明确规范的领域首先抛出单方面制定的规则试图以此为基础发展国际习惯法，而不是首先与国际社会寻求共识。

第四，着重进行微调，扩大解释余地。如提及国际法时，声称必须是“可适用的”国际法[②]，在列举战争法的基本原则时，用军事必要原则代替预防原则[③]，这些都是为了扩大自由裁量的空间。

美国网络空间政策演化的主要特点，可以归纳为以下四方面：

第一，始终的领先性。这可以用“一早三多”来概括，即起步早、主体多、文件多、概念多。美国几乎在网络空间的每一个具体问题上都抢占了先机，试图主导话语权，如 1993 年提出发展信息基础设施，正式宣告网络空间政策的开始，1998 年提出网络战并将其定性为非常规攻击，2001 年认为网络空间属于战场的组成部分或本身就是战场，2003 年将网络空间与使用武力联系起来，2011 年白宫和国防部相继出台各自的网络空间战略等。在近 20 年的发展历程中，除了白宫、国土安全部、国家安全委员会等政府部门和机构，网络空间政策的参与主体更多地来自军方，特别是国防部和陆海空三军，并产生了大量相关正式文件与概念[④]。

第二，相对的稳定性。在网络空间的某些具体问题上，美国一旦形成结论，便会长期坚持，少有实质更改。例如，自 1998 年将网络攻击和网络战定性为非常规攻击并和恐怖行为、使用大规模杀伤性武器等发生于现实世界中的行为并列至今，美国一直坚持网络攻击和网络战与这些行为并无区别。再如，自 1998 年宣布采取所有必要措施保护关键基础设施、强调政府机构与私营部门建立伙伴关系至今，美国一直沿用该政策。

第三，持续的挑战性。美国的网络空间政策构成对国际法的持续挑战，而且程度在不断增加。美国是世界上第一个提出网络战的国家，但当时并未实质涉及国际法，如网络战是否构成国际法上的攻击，美国的回应是否构成自卫等。从 2001 年开始，军方认为网络空间属于战场的组成部分或本身就是战场，但通常将网络空间的“战斗”限于网络空间，区别于现实世界中的使用武力[⑤]。2003 年，军方将网络空间与使用武力联系起来[⑥]，但承认国际社会多大程度上能够接受这种观点远不明确。2011 年，白宫和国防部陆续明确宣布网络空间中的某些行为将使得美国使用武力以自卫。

第四，明显的跳跃性。在一些重大问题上，美国的网络空间政策呈现出突进式的发展。1998 年白宫提出网络战后，军方和政府部门与机构并未实质跟进。2001 年军方还在争论信息行动是否构成新的作战能力，但 2003 年就已经正式提出信息战概念并将网络空间和自卫、主权挂钩。同样是关于网络空间的战略文件，2006 年军方还在规定网络空间行动必须符合国际法，2011 年就已经基本不提法律问题。2003 年军方将网络空间与使用武力联系起来后，一直没有明确态度，直到 2011 年，白宫宣布自卫权构成网络空间规范的基础之一，美国将针对网络空间中的某些行为行使自卫，同年底，国防部宣称网络空间中的某些行为构成使用武力并将导致美国行使自卫权，即便是推定而非确定存在此种行为时也如此。

五、国际法分析：渐行渐远还是越来越近

美国目前的网络空间政策，至少将在以下 7 个方面对国际法有关概念、原则、规则和制度造成严重影响、构成严峻挑战：

第一，扩展了主权和领土的概念。美国认为，网络空间中的某些行为可视为侵犯美国主权、非法侵

①如《网络空间国际战略》。

②如《军事战略》《关键基础设施识别、优先和保护》《网络空间国际战略》。

③战争法的基本原则并无定说，但一般认为包括区分原则、军事必要原则、不必要痛苦原则、比例原则、预防原则的全部或大部。军事必要原则包含允许和禁止两方面，一方面允许使用任何“根据现代战争法和战争惯例合法的且对于确保战争目标不可缺少的”手段，一方面禁止使用任何不是“不可缺少的”且不是为了确保战争目标的手段。军事必要原则也要求不应在军事行动中使用超出所需的武力或暴力，即不致引起过分伤害或不必要痛苦。预防原则是指在攻击时应采取预防措施以及尽一切可能减少攻击对平民及民用物体的影响，计划或决定攻击的人如果没有采取预防措施，无论实际效果如何，都违反了有关规定。预防原则的法律义务显然比军事必要原则重。参见黄德明，朱路. 贫铀武器合法性的国际法考量《广西大学学报》(哲学社会科学版)，2011(2)：77-83。

④如网络空间、网络空间行动、信息环境、信息行动、全球信息栅格、信息保证、计算机网络攻击、计算机网络防御、计算机网络刺探、电子战、电子攻击、电子保护能力、身份生态系统等。

⑤如 2001 年版《行动法手册》《行动》《网络行动》。

⑥2003 年版《行动法手册》。

入美国领土的行为。主权是一个国家独立自主地处理对内对外事务的最高权力，是国家的固有属性[13]91。领土是国家赖以存在的物质基础，也是国家主权活动和行使排他性权力的空间，传统国际法理论认为，领土包括领陆、领海和领空。主权原则是国际法的根本原则，也是国际法的基础，因此，对主权概念及原则所做的任何调整或改变，都必须异常谨慎。同“主权虚无论”、“有限主权论”等试图否定或缩小主权的观点相反的是，美国将主权的范围扩展至网络空间，然而，网络空间的主权是否存在，还未形成共识①。相比对主权问题的突破，美国将网络空间等同于领土(至少在部分情况下)的突破更大、更激进，也更缺乏法理基础。学界虽然早就开始讨论网络空间与管辖权、主权，但从未将网络空间与领土联系起来。网络空间和主权都是抽象的事物，有兼容的可能性，而领土是具体的事物，即便国际社会将来能就网络空间存在主权形成共识，也不大可能认为网络空间构成领土的组成部分。美国认为网络空间存在主权并构成领土，无非是为行使所谓自卫权创造先决条件。

第二，延伸了使用武力(force)的含义。禁止以武力相威胁或使用武力是国际法的基本原则之一，是具有强行法性质的规范，《联合国宪章》是第一个对此做出明文规定的国际公约，第 2 条第 4 款规定，“各会员国在其国际关系上不得使用威胁或武力，或以与联合国宗旨不符之任何其他方法，侵害任何会员国或国家之领土完整或政治独立。”但是，宪章并未说明什么叫做使用武力或提供判断标准。美国及其主要盟友长期以来认为“武力”是指军事攻击或武装暴力，而其他理解如“强制”(coercion)或“干涉”从未获得国际社会的广泛支持[14]427-430。关于网络空间与使用武力的关系问题，学界一般持谨慎观点，认为网络攻击还没达到使用武力或武装攻击的层次[15]39 或无法直接适用《联合国宪章》第 2 条第 4 款[16]92，这与美国政府和国防部断言网络空间中的某些行为构成使用武力形成鲜明对比。实际上，正如美国学者所坦承，“对《联合国宪章》和使用武力规范划清法律界限会产生地缘政治的赢家和输家，因此，关于宪章解释的争论一直反映出权力和脆弱性的分布”[14]458，在网络攻击和使用武力问题上，美国和其他主要国家对于战略风险和机遇有不同的理解，因此很可能在法律问题上存在不同的观点，因此很难就《联合国宪章》第 2 条第 4 款的解释形成共识，而且，“网络攻击的某些特性，如攻击和反措施的低能见度、对关键事实的可能争议、确立归属和因果关系的难度，将使就美国的立场形成法律共识格外困难。在可预见的将来，美国将不得不在不确定和不稳定的国际法律领域执行其进攻和防御战略。”[14]459 同样，美国关于某些网络空间行为构成使用武力的立场，也无非是为行使所谓自卫权创造先决条件。

第三，继续滥用了自卫权。自卫权是国家主权的重要体现，是指在国家遭遇外来武装攻击时可以采取相应的武力措施进行反击的权利[17]121，《联合国宪章》第 51 条明确规定联合国任何会员国在遭受武力攻击时有自卫的“自然权利”。然而，关键在于是否首先存在武力攻击，如上所述，美国已经认定某些网络空间行为构成使用武力并以此作为行使自卫权的根据，但这缺乏足够的法理基础。如果说美国所谓的“预先自卫/先发制人的自卫”是在时间范围上对自卫权的滥用，那么声称对网络空间中的某些行为进行自卫是在回应对象上对自卫权的滥用，而对网络攻击采用先发制人的战略则将自卫权滥用到了极致。而且，即使将来国际社会能就某些网络空间行为构成使用武力形成共识，也不能对其进行“预先自卫/先发制人的自卫”，因为这种自卫不是针对特定的和迫在眉睫的威胁，而是为了防止更一般性的威胁实际产生，与其说是“先发制人的自卫”，不如说是“预防自卫”，“先发制人的自卫”就已经因为主观性和潜在危险性而争议颇多，“预防自卫”由于概念难以捉摸，将进一步加剧争议[18]599。

第四，使国际社会更难以接受侵略的定义。美国声称某些网络空间行为是“侵略”，美国因此可以行使自卫权，但这首先需要确定这些行为是否可被

①西方学者很早就已经开始讨论网络空间与主权的关系问题，但对于是否存在网络空间主权或避而不谈，或言辞模糊，如 Timothy S. Wu. Cyberspace Sovereignty—The Internet and the International System Harvard Journal of Law & Technology，1997 (3)：647-666; James Boyle. Foucault in Cyberspace：Surveillance，Sovereignty，and Hardwired Censors University of Cincinnati Law Review，1997 (1)：177-206; Joel P. Trachtman. Cyberspace，Sovereignty，Jurisdiction，and Modernism Indiana Journal of Global Legal Studies，1998 (2)：561-582; James A. Lewis. Sovereignty and the Role of Government in Cyberspace Brown Journal of World Affairs，2010(2)：55-66. 近年来有学者认为，网络主权和网络空间管辖的国际机制存在的最大障碍是国家认为这恰恰不利于实现其最佳利益，美国是否主张发展网络空间主权，将有单边、多边和国际三种途径，或者继续沿用特别回应措施，以期保持优势，并使得其他国家或非国家主体无法通过网络空间成功攻击美国或重创美国。参见 Patrick W. Franzese. Sovereignty in Cyberspace：Can It Exist Air Force Law Review，2009(1)：1-42。美国目前的做法是单方面发展网络主权和特别回应措施的混合。

视为使用武力，其次需要解决什么叫做侵略，因为国际法中尚不存在确定的关于侵略的定义。联合国大会 1974 年 12 月 14 日曾通过《关于侵略罪定义的决议》，根据该决议，“侵略是指一个国家动用武力侵犯另一个国家的主权、领土完整或政治独立，或以本《定义》所宣示的与联合国宪章不符的任何其他方式使用武力。”但是，该决议与其他国际法律文件的联系并不紧密且缺乏法律实用性，也没有依附于《联合国宪章》的解释[19]41，因此未被广泛接受。2010 年 6 月，《国际刑事法院规约》审查会议通过了侵略罪定义及对其行使其管辖权的条件，但侵略（行为）仍然沿用了 1974 年《关于侵略罪定义的决议》中的定义。侵略罪定义“将对国际政治法律秩序带来挑战，主要是安理会与国际刑事法院均有权认定侵略行为可能导致结论的不一致和有关行动的不协调，不利于国际社会秩序的稳定”[20]106。在这种背景下，将某些网络空间行为与“侵略”等同，只能使侵略的定义更难以为国际社会所接受，同时也给侵略罪的前景带来了更多的不确定性。

第五，使国际法的中立制度形同虚设。中立是传统战争法的概念，是指两个或几个国家之间发生战争时，非交战国所选择的不加入战争和不支持任何一方的法律地位[13]513。中立国有自我约束的义务、防止的义务和容忍的义务[17]651。美国认为，如果中立国不能或不愿阻止交战国使用其信息系统，那么中立国就失去了中立地位，其他交战国因此取得针对中立国的有限的自卫权以采取必要和相称的措施阻止敌国的行为①。这种观点存在两处重大疏漏，一是根据现有的互联网结构，中立国无法阻止网络攻击“离开其管辖范围，除非它在其他国家提供电脑系统的所有连接，但对任何武装冲突中的中立国施加这种义务都是非理性的，因为这很可能导致互联网停转。”[21]210 二是网络空间中大量防护薄弱的系统极有可能被攻破、操纵为“僵尸网络”或“肉鸡”而毫不自知，发起攻击的系统经过层层隐藏和代理可能根本无法察觉，而“无辜”的系统则代人受过。简单地说，中立国的信息系统完全可能被交战国利用而无法察觉，或者即使察觉却无法确定来源，如果因此攻击中立国，不仅难以在国际法上找到合适的理由，而且将使得国际法的中立制度完全失去存在的价值，因为根本不存在中立国。

第六，挑战了国际法的责任制度。国际法律责任是指国际法主体对其国际不当行为或损害行为所应承担的法律责任，国际不当行为在如下几种情况中可归因于国家而成为该国的国家行为，如国家机关的行为、经授权行使政府权力的其他实体的行为、实际上代表国家行事的人的行为等[13]127-32。美国将网络空间的威胁根据来源是个人、组织还是国家分为四个等级，但问题在于将行为归于特定个人、组织或国家甚至一个具体地理位置都很困难，有时甚至不可能[15]39。在缺乏具有操作性、可靠性的行为归属、身份确认的技术能力的背景下，无法区分网络攻击等行为是独立的黑客行为还是由国家机关发起，而且很多网络攻击的效果并不是立即发生，而是长期潜伏，在合适的时机才被激活以产生作用，如病毒、木马、间谍软件、后门软件等，这种情况下能否察觉“威胁”都是一个问题。美国乌托邦式的网络空间威胁分级，形式意义超过实质意义，虽然于法理上瑕疵不多，但在行为归属的操作层面问题太大，将给国际法的责任制度带来实践上的随意和混乱。

第七，破坏了战争法的基石即区分原则。区分原则是在战争和武装冲突中始终对战斗人员和平民、军事目标和民用物体加以区别，是战争法的逻辑基础和核心原则。美国网络空间政策对区分原则的破坏分为两个层次，一是人的层次，二是物的层次。从人的角度来说，网络攻击的发起者可能是普通黑客，也可能是军队中网络部门的士兵，还可能是任何人，考虑到美国近年来严重依赖私营军事安保公司支持战场行动，而且在各类文件中反复强调要加强与公司、团体合作以提高网络空间安全程度，有理由相信美国的网络防御和攻击能力至少有一部分来自平民。根据战争法，平民一旦在武装冲突中“直接参加敌对行动”，就将失去战争法赋予的免受直接攻击之一般保护。但问题在于，没有任何国际条约对直接参加敌对行动进行定义，或提供如何判断某种行为是否构成直接参加敌对行动的标准。实际上，直接参加敌对行动是战争法中“最为困难且至今未获解决的问题”，为此，红十字国际委员会召集了数 10 名来自学界、军队、政府和非政府组织的专家，通过 5 次会议，历经 6 年的讨论和研究，于 2009 年 5 月发布《国际人道法中直接参加敌对行动定义的解释性指南》（以下简称《解释性指南》），试图解决这个问题。《解释性指南》认为，在武装冲突中对敌方造成军事损害的计算机网络攻击明确构成敌对行动的一部分[22]46。简单地说，除却其

①International and Operational Law Department. The Judge Advocate General's Legal Center and School. Operational Law Handbook 2012：133.

他更加复杂的因素,平民进行网络攻击可能构成直接参加敌对行动而丧失保护①。从物的角度来说,如何保证网络攻击只限于军事目标而避开民用物体或尽量减少间接伤害,在实践上非常困难,特别是考虑到互联网相互依存的特性。例如,如果网络攻击使用病毒,病毒自我复制和传染的特性很可能导致扩散范围无法控制,这种攻击一旦造成平民生命财产的损失,就构成了具有国际习惯法效力的《日内瓦公约第一附加议定书》第 41 条第 4 款禁止的不分皂白的攻击(indiscriminate attack),进而违反了区分原则,并可能违反比例原则和军事必要原则。正是由于对区分原则的实质影响,美国网络空间政策的有关文件全部回避了使用战争法中的术语称呼有关主体,代之以通俗概念。概而言之,美国的网络空间政策模糊了战斗员与平民的界限,而且很难区分军事目标与民用物体,这从根本上导致区分原则失效。

六、关于中国:启示与对策

从国际法的角度来看,美国的网络空间政策对于中国的启示和中国的对策主要包括以下四点:

第一,推进整体战略建构。美国的网络空间政策起步早,参与主体多,形成了从战略到细节相对完整的体系。《国家信息化领导小组关于加强信息安全保障工作的意见(2003 年 8 月 26 日)》和《2006—2020 年信息化发展战略(2006)》作为目前我国网络空间安全方面的纲领文件,将我国网络空间安全保障工作的指导思想定为"坚持积极防御、综合防范的方针","全面加强国家信息安全保障体系建设","大力增强国家信息安全保障能力"。但是,尚缺乏一个兼具系统性和前瞻性的网络空间发展战略以及对具体问题的细化和跟进,这落后于时代的要求,需要进一步推进。

第二,重视国际法律评估。网络空间的防御涉及众多国际法,特别是战争法问题,如网络空间主权理论体系如何构建;某些网络空间行为是否构成使用武力;网络空间行为与使用武力互连的法律评价与应对;中立制度、区分原则受到的影响与应对;责任制度遇到的挑战和适用的困难等。目前我国对于有关问题的研究刚刚起步,非常零散,需要进一步加强。

第三,加快网络能力建设。美国已经在网络空间具有无可比拟的技术优势,无论政府还是军方,仍都反复强调要加大资金投入,加快科技创新,保持技术优势。一方面,我国应加大对网络空间新技术、新应用以及安全防御技术的研发力度,加强对国外先进技术和应用的跟踪研究,提高我国网络空间的防御能力。另一方面,应加快网络空间技术、应用、安全防御技术的国产化进程,掌控核心技术,避免依赖他人,提高我国网络空间的创新能力。

第四,积极参与国际进程。确如美国所言,关于战争与和平的国际法适用网络空间,只是需要就网络空间的特性做出相应调整。如今,关于网络空间的国际法存在较多"灰色地带",一些概念、原则、规则和制度亟待厘清,在涵盖范围较为全面、接受程度较为普遍的关于网络空间的国际条约出现之前,发展相关国际习惯法可能是网络空间规范化的必由之路。美国清楚地认识到这一点,并且在网络空间的每一个重要法律问题上都抛出单方面的规则,试图争夺话语权与主动权,发展美国主导的国际习惯法。这需要我国以完备的战略设计、充分的法律评估和足够的网络能力为基础,从维护我国国家利益的角度出发,积极参与关于网络空间规范的讨论、调整与发展的国际进程,坚决反对任何不符合国际法的主张与立场。

七、结语:危险的优势

"一条条光线在思想、数据簇和数据群的非空间中延伸,像城市的灯光那样渐渐模糊……,"[23]51 威廉·吉布森近 20 年前曾如此设想网络空间,遗憾的是,这种宁静的画面可能很快就会被数字的枪林弹雨取代,美国将网络空间视为物理意义的战场并将其与使用武力连接起来,其影响已经远远超过"引发网络军备竞赛"之类的担忧。

美国在网络空间具有世界各国都没有的优势,如占有、控制、生产绝大部分互联网的根服务器、交换机、Windows 操作系统、CPU 等,但这种优势同时也是潜在的巨大危险,如今任何人只要能够上网(无线网络时代甚至抛弃了网线)并有足够的技术能力,就能在任何地方、任何时间对任何他想要攻击的系统进行攻击。正因如此,美国承认"网络空间的安全威胁是美国在国家安全、公共安全和经济方面遭遇的最严峻的挑战之一"[24],同样,这也是为什么美国经过 10 余年的徘徊,终于采取了明确的、激进的网络空间政策,力图保持在网络空间的优势,保证"自己有行动的自由,同时不准敌人有同样的自由"。遗憾的是,美国的政策几乎都缺乏坚实的国际法理论依据,但美国也有一定的优势,即由于关

①不过《解释性指南》仅仅是反映红十字国际委员会自己观点的文件,不具有法律效力,因此只能起到参考作用。

于网络空间的国际法规范需要厘清和发展，美国和盟友可能以实践抢占先机，发展美国主导的关于网络空间的国际习惯法。从美国的角度来说，这合情合理，甚至是必然选择，然而，这种做法在大多数国家看来，只能是滥用实力的表现，不仅冲击和影响现有的国际法和国际法律秩序，而且也不利于关于网络空间的国际法的发展。

参考文献：

[1] Encyclopedia Britannica. Britannica concise encyclopedia[M]. Chicago：Encyclopedia Britannica，Inc.，2006：761.

[2] Stephanie Carvin.The US department of defense law of war manual：an update[C]//Schmitt M N. Yearbook of International Humanitarian Law 2010. The Hague：T.M.C. Asser Press，2011：359.

[3] Executive Order 12864 of September 15，1993. United States advisory council on the national information infrastructure[EB/OL].(1993-09-15)[2012-04-10]. http://www.archives.gov/federal-register/executive-orders/pdf/12864.pdf.

[4] Executive Order 13010 of July 15，1996. Critical infrastructure protection [EB/OL].(1996-07-15)[2012-04-10]. http://www.fas.org/irp/offdocs/eo13010.htm.

[5] Presidential Decision Directive （PDD） 62. Combating terrorism [EB/OL].(1998-05-22)[2012-04-12]. http://www.fas.org/irp/offdocs/pdd-62.htm.

[6] Presidential Decision Directive（PDD） 63. Critical infrastructure protection[EB/OL].(1998-05-22)[2012-04-12]. http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

[7] Executive Order 13231 of October 16，2001. Critical infrastructure protection in the information Age [EB/OL].(2001-10-16)[2012-04-12]. http://www.fas.org/irp/offdocs/eo/eo-13231.htm.

[8] The White House. The national strategy to secure cyberspace，February 2003 [EB/OL].(2003-02)[2012-04-15]. http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf.

[9] The White House. National strategy for the physical protection of critical infrastructures and key assets，February 2003[EB/OL].(2003-02)[2012-04-15]. http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf.

[10] The White House. National response framework：cyber incident annex，1 December 2004 [EB/OL].(2004-12-01)[2012-04-15]. http://www.learningservices.us/pdf/emergency/nrf/nrp_cyberincidentannex.pdf.

[11] The White House. The comprehensive national cybersecurity initiative [EB/OL].[2012 -04 -20].http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

[12] The White House. National strategy for trusted identities in cyberspace—enhancing online choice，efficiency，security and privacy，april 2011[EB/OL].(2011-04-15)[2012-04-20]. http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

[13] **梁西. 国际法（修订第 2 版）**[M]. **武汉：武汉大学出版社**，2000.

[14] Matthew C Waxmant. Cyber-attacks and the use of force：back to the future of article 2 （4）[J]. Yale Journal of International Law，2011（2）：427-430.

[15] Todd C Huntley. Controlling the use of force in cyber space：the application of the law of armed conflict during a time of fundamental change in the nature of warfare[J]. Naval Law Review，2010（1）：39.

[16] Daniel B Silver. Computer network attack as a use of force under article 2（4） of the United Nations charter[J]. International Law Studies Series，US Naval War College，2002（76）：92.

[17] **王铁崖. 国际法（第 1 版）**[M]. **北京：法律出版社**，2002：121.

[18] Miriam Sapiro. Iraq：the shifting sands of preemptive self-defense[J]. American Journal of International Law，2003（3）：599-606.

[19] **王秀梅. 论侵略罪**[J]. **法学家**，2002（2）：39-44.

[20] **王秀梅. 侵略罪定义及侵略罪管辖的先决条件问题**[J]. **西安政治学院学报**，2012（3）：102-112.

[21] Davis Brown. A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict[J]. Harvard International Law Journal，2006（1）：179-221.

[22] **红十字国际委员会. 国际人道法中直接参加敌对行动定义的解释性指南 （中文版）**[M/EB].(2009-11-06)[2013-01-21]. htttp://www.icrc.org/chi/resources/documents/publication/p0990.htm.

[23] William Gibson. Neuromancer[M]. New York：Ace Books，2000：51.

[24] The White House. National Security Strategy，May 2010 [EB/OL].(2010-05)[2012-04-20]. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

（下转第 125 页）

The Outline of the Chinese Traditional Folk Law

—Based on the Perspective of Legal Characteristics, Cultural Quality and Functions

YU Yuhe

(Law School, Nankai University, Tianjin 300071, China)

Abstract: The origination history of the legal characteristics of folk law comprises the process of the development of legal thoughts from simplicity to pluralism.Involving the epitome and summary of life experience and with its multiple effective paths, Chinese traditional folk law has the special cultural quality that the state law does not possess. In the construction of the order of modern society, traditional folk law has three actual functions: first, in the generation of order, the folk law is the rule itself; second, in the aspect of maintaining order, the folk law affects the behavior of the people; third, in the aspect of protecting the order, the folk law inherits and develops traditional ethics as its historical mission. The construction of modern legal order needs to take into account Chinese traditional folk law.

Key words: legal culture; folk law; legal character; culture character; rational order

[责任编辑：孟青]

(上接第 109 页)

The United States' Cyberspace Policy under International Law

ZHU Lu

(Department of International Relations, Tsinghua University, Beijing 100084, China)

Abstract: The United States' cyberspace policy is mainly reflected in the documents from the government and the military. It has been almost 20 years since Executive Order 12864 of 1993 related to the development of the National Information Infrastructure was promulgated. Most government documents on cyberspace were issued by the White House, which barely touched upon international law. Their military counterparts range from documents from Department of Defense, the Army, the Navy and the Air Force to judge advocates' references. Although these military documents did mention about international law, in-depth analysis were scarce. The United States' cyberspace policy has experienced a long-term evolving process during which four tactics were employed and four characteristics were formed. International Strategy for Cyberspace, issued by the White House in May 2012, finally made it clear that the United States would adopt a radical cyberspace policy via connecting certain acts in cyberspace with using force in the real world. It will pose grave challenges to international law and international legal order for not only would the traditional concepts of territory and sovereignty be overthrew and the meaning of using force be expanded, but also the right to self-defense would be further abused and the international society be more reluctant to accept the definition of aggression. Moreover, the neutral institution in international law would be nullified, the responsibility settings in international law would be challenged, and the foundation of law of war would be destroyed.

Key words: the United States' cyberspace policy; rights to self-defense; international law; law of war

[责任编辑：孟青]