美国网络威慑理论之争

何奇松

内容提要 美国理论界对网络威慑是否有效存在争议,主要原因在于归因问题无法有效解决。虽然美国可以利用核威慑信息传递方式,向潜在对手发出网络威慑信号,但也存在困难,毕竟网络武器一旦展示,对手就有了破解美国网络武器威胁的机会。鉴于网络报复打击危害的严重性,理论界赞同以拒止威慑手段为主,尽管这种方式还不能彻底打消攻击者实施网络攻击的念头。网络威慑也需要解决如何控制网络冲突、战争升级的问题,为实现网络威慑战略,理论界开出了诸多药方。

关键词 地区与国别政治 美国 网络威慑 理论讨论

美国军方在冷战时期创立的网络空间被广泛地运用到政治、经济、军事、金融、电力等社会各领域,成为继海、陆、空、天之后的第五维空间。因此,制权理论随之扩大到网络空间,制网权理论由此形成,各大国在网络空间的控制与反控制的博弈也随之展开。高度依赖互联网的美国宣布网络空间是国家战略性资产。但是,随着网络技术的发展,网络安全风险也不断增加,依赖网络的程度越高,其风险程度也就越高。因此,美国政府和军方高度重视网络安全,表示保护网络空间免受攻击的力度,要与其依赖网络空间的程度相一致,①唯有如此,才能确保其在网络空间的安全与利益。鉴于此,美国理论界开始进行网络威慑理论研究。

---

* 何奇松:上海政法学院国际事务与公共管理系教授。(邮编:201701)

** 本文得到上海政法学院政治学重点学科建设项目资助。作者在此要非常感谢《国际政治研究》匿名评审专家和编辑部的建设性修改意见。本文一切缺陷与不足,概由作者本人承担。

① General Norty Schwartz, "Space, Cyberspace, and National Security," 18 February 2010, p. 2. http://www. af. mil/shared/media/document/AFD-100219-034. pdf, 2012-08-15.

美国网络威慑理论研究来源于目前所进行的第四波威慑理论研究。[①] 1995 年,美军战略司令部制定了一份秘密文件《后冷战时代的威慑实质》(Essentials of Post-Cold War Deterrence)。[②]该文件建议扩大威慑的使用范围,不仅仅限于与俄罗斯的双边关系框架,尤其是要使用诸多威慑战略,威慑多种来自外部的威胁。这个文件为学术界正在进行的新一轮威慑理论研究注入了"养料"。根据要求,政府和军方大力支持理论界对威慑理论的研究。在吸收了理论界成果之后,2006 年,美国国防部签发《威慑行动联合作战概念》(Deterrence Operations Joint Operating Concept)。该文件认为冷战时代的威慑理论可适用于后冷战时代的各种威胁。[③]很显然,美军所说的威胁自然包括了恐怖主义、网络攻击等威胁。该文件为大力倡导威慑理论研究进一步提供了强有力支持。

因此,自从国际关系理论家詹姆斯·德·德里安(James Der Derian)在 1994 年首次提出"网络威慑"概念、[④]哈克尼特(Richard J. Harknett)在 1996 年的一篇文章集中论述之后,[⑤]借着军方大张旗鼓重新研究威慑理论的东风,美国理论界、军界、政界等大兴网络威慑研究之风。2007 年和 2008 年,爱沙尼亚政府网站和格鲁吉亚政府等网站受到攻击,为美国网络威慑理论研究提供了鲜活的案例。2009 年和 2012 年先后肆虐于中东(尤其是伊朗)的"震网"病毒(Stuxnet)与"火焰"病毒(Flame),再一次为其网络威慑理论的研究提供了丰富素材。借助冷战时期的核威慑理论基础,以及丰富的个案,美国理论界对网络威慑理论研究方兴未艾,成为美国第四波威慑理论研究的重点之一。其中著名智库如战略与国际研究中心(CSIS)、兰德公司、东西方中心(East-West Center)、史汀生中心(Henry L. Stimson Center)、布鲁金斯学会(Brookings Institution)等发挥了主导作用。这些机构组织辩论会,出版论文集及专题研究报告,探讨网络威慑理论与实践。军方杂志如《战略研究季刊》(*Strategic Studies Quarterly*, SSQ)在 2010 年和 2011 年连续两年为网络威慑研究开辟专栏,集中刊载军界内外专家学者对网络威慑理论的观点。2012 年,该刊秋季号再次以整期刊载网络领域的论文,其余三期也刊载相关论文。军方的其他杂志如《联合军力季刊》(*Joint Force Quarterly*, JFQ)等,也不定期刊载该领

---

① Jeffrey W. Knopf, "The Fourth Wave in Deterrence Research", *Contemporary Security Policy*, Vol. 31, No. 1, April 2010, pp. 1-33.

② US Strategic Command, "Essentials of Post-Cold War Deterrence 1995"。目前,这个文件已经解秘,可以从多个网站下载看到原文,例如,http://oldsite. nautilus. org/archives/nukestrat/USA/Advisory/essentials95. PDF, 2012-08-15。

③ US Department of Defense, "Deterrence Operations Joint Operating Concept," http://www. dtic. mil/futurejointwarfare/concepts/do_joc_v20. doc, 2012-05-10。

④ James Der Derian, "Cyber-Deterrence," *Wired*, Vol. 2, No. 9, September 1994, pp. 116-122.

⑤ Richard J. Harknett, "Information Warfare and Deterrence," *Parameters*, Vol. 26, No. 4, Autumn 1996, pp. 93-107.

域的最新理论研究成果。当然也有专业学术期刊登载,诸如网络攻击与国际武装冲突法之间关系等具体问题的学术文章,从侧面讨论网络威慑理论。①

2008—2011 年四年间,美国进行了大量网络威慑研讨,尽管对许多问题并没有达成一致意见,但还是就一些问题取得了共识。在此基础上,美国国务院与五角大楼吸取了理论界的成果,先后于 2011 年 5 月和 7 月颁布了《网络空间国际战略:互联网世界的繁荣、安全和开放》②和《网络空间行动战略》,③明确宣布美国实施网络威慑战略:美国采取各种手段慑止对手对美国发起网络攻击;保留诉诸武力的权利回应敌对网络行动。美国不仅仅采取这种宣示性政策,而且还高调宣布研发、部署攻击性网络武器,采取先发制人的打击手段应对网络攻击。④即使在美国宣布实施网络威慑战略之后,美国国内并没有就此放弃对网络威慑理论的研究,而是继续进行探讨,其目的都是为了完善网络威慑理论。

从总体上看,美国网络威慑理论争论焦点集中于几个方面:第一,把威慑理论尤其是冷战时期的核威慑理论移植到网络空间是否可行?为此,就要解决归因(attribution)问题,即能否明确哪个行为体即将或者已经发起了网络攻击?在网络危机之时,如何向对手传递网络威慑信息?冷战时代核威慑信息传递的方式能否移植到网络空间?第二,如何进行网络威慑。经典威慑理论包括两种威慑手段或者方式,即拒止威慑(deterrence by denial)和惩罚威慑(deterrence by punishment)。在网络空间,采用拒止威慑手段,确实可以抵消潜在对手发起攻击的收益,但是是否鼓励潜在对手进一步发起网络攻击?惩罚性威慑是否可适用于网络威慑?要解决这个问题,就需要明确网络攻击是否等于武装攻击。进行报复惩罚,怎样符合相称原则?⑤ 这就需要解决如何看待网络攻击的影响程度。还有诸如如何处理网络

---

① Matthew C. Waxmant, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *The Yale Journal of International Law*, Vol. 36, No. 2, 2011, pp. 421-459; Oona A. Hathaway, et. al., "The Law of Cyber-Attack," *California Law Review*, Vol. 100, 2012, pp. 817-885; Col. Gary Brown, USAF, "The Customary International Law of Cyberspace," *Strategic Studies Quarterly*, Vol. 6, No. 3, Fall 2012, pp. 126-145.

② The White House, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, 2012-05-10.

③ Department of Defense, "Strategy for Operating in Cyberspace," July 2011, http://timemilitary.files.wordpress.com/2011/07/d20110714cyber.pdf, 2012-05-10.

④ 例如,美国网络司令部正在与六个地区司令部紧密合作,在地区司令部中建立网络支持分队(Cyber Support Elements, CSEs),可以由地区司令部直接指挥作战。参见 Zachary Fryer-Biggs, "U.S. Military Goes on Cyber Offensive," March 24, 2012,参见美国防务新闻网 http://www.defensenews.com/article/20120324/DEFREG02/303240001/U-S-Military-Goes-Cyber-Offensive,2013-01-02。

⑤ "相称原则"英文原文为"Principle of Proportionality"。本意要求交战者所使用的作战手段和方法应与预期的、具体的和直接的军事利益相称,不得进行过分的或不成比例的武力攻击,以免造成不必要的伤害。《日内瓦公约》第一议定书第 57 条对此做了详细规定。参见《1949 年 8 月 12 日日内瓦第四公约关于保护国际性武装冲突受难者的附加议定书(第一议定书)》。http://www.icrc.org/chi/resources/documents/misc/additional_protocol_1.htm,2013-06-06。

冲突升级问题、网络报复是否需要立即实施,等等。第三,如何构建完善的网络威慑体制。这更多是一个技术问题,争论不是很激烈,前面几个问题是综合性的,不仅涉及技术,还涉及政治、伦理等方面问题,因而争论很激烈。下面主要围绕这几个方面进行分析。

一、网络威慑是否可行?

冷战时期的核威慑理论到底能否适用于网络领域?除了下述归因问题限制了威慑理论运用于网络领域外,是否还存在其他一些制约因素呢?美国战略与国际研究中心(CSIS)的研究员刘易斯(James Lewis)认为,把核威慑理论运用到网络领域存在一些困难,其效度是有限的。首先,美国有世界上最先进的网络军力,但并没有慑止潜在对手对美国进行有害的网络行动。其次,行为体有着非对称性的风险承受力。不像冷战时代的威慑,在网络空间实施威慑,美国把非国家行为体作为"人质"存在困难,因为这些行为体几乎没有多少基础设施,也没有多少人口需要保护。因此,难以向这些非国家行为体施加适当、可靠的威胁。因而也就侵蚀了网络威慑效果。再次,相称原则问题使得核威慑模型运用到网络领域存在困难。网络犯罪与网络间谍不能证明美国使用武力是合法的,如同冷战时期的核威慑不能慑止间谍、代理人战争与低烈度冲突一样。正因为这些原因,他认为,较之核威慑理论和太空威慑理论,网络威慑理论更具有限制性。其结论是,美国不应该在网络空间寻求慑止对美国发起网络间谍、攻击等活动的努力,而是应该获取并维持打仗并能够赢得胜利的能力,维持行动的持续能力与交战能力。[①]此外,根据核威慑理论,要想发挥威慑作用,还要指望行为体是理性的,即能够理性思考、理性行动。所有向美国发起网络攻击的行为体都是理性的吗?美国空军太空司令部司令希尔顿(William Shelton)就有这样的疑问。[②]不能保证这一点,将威慑理论运用到网络空间其成功率就打折扣。

尽管上述这些研究者和指挥官认为把核威慑理论运用到网络领域有些削履适足,但是,有相当多的理论家认为核威慑理论还是可以运用到网络领域的。当然要想实施威慑,先要确定网络攻击的来源(包括哪个行为体在何时何地发起了网络攻击),也就是归因问题。因此,麻省理工学院计算机科学与人工智能实验室资深

① "Jim Lewis of CSIS Speaks at Stimson on Cyber Deterrence," November 15, 2012. http://www.stimson.org/about/news/jim-lewis-of-csis-speaks-at-stimson-on-cyber-deterrence/, 2013-01-02.

② Zachary Fryer-Biggs, "U.S. Military Goes on Cyber Offensive," March 24, 2012.

科学家大卫·克拉克(David D. Clark)明确表示"归因是威慑的核心"。[①]系统规划与分析公司(System Planning and Analysis)的系统与技术分析员乔纳森·所罗门(Jonathan Solomon)明确谈到,要想让惩罚威慑起作用,威慑方必须能够高度自信地确认攻击方。[②]理论界对能否解决归因问题存在分歧,这是确定网络威慑是否具有可行的关键因素。

在可视的物理空间,从陆、海、空、天发起攻击,或者对陆、海、空、天发起攻击,利用各国各种技术手段,一国很快就能确定哪个行为体对打击目标实施了攻击。目前,虚拟的网络空间处于"霍布斯"状态下,各种各样的行为体在网络空间匿名地从事各种活动;拥有先进网络技术的行为体可以从第三方(实时或离线)攻击另外一个行为体的网络,甚至完全可以从隐藏的 IP 地址发起攻击。因此,明确确定哪个行为体在何处、何时发起了网络攻击,是有一定难度的。即使确切知道来自某国的一台计算机发起了对一个国家机构的网络攻击,但是不能随便断定这个国家是其"幕后黑手"。例如,2007 年、2008 年爱沙尼亚、格鲁吉亚政府网站分别遭受了猛烈的网络攻击,但是西方一直无法确认是否为俄罗斯政府所为。同样,国际社会也无法确认伊朗核设施所遭受"震网"、"火焰"的网络攻击为美国、以色列所为。一家云安全公司负责安全研究的迈克尔·萨顿(Michael Sutton)甚至认为,一些国家可能把网络攻击外包给黑客。[③]这就使归因问题变得更加复杂。

就技术而言,美国国家科学院全国研究委员会(National Research Council of National Academies)的赫伯特·林(Herbert Lin)归纳了归因技术存在 5 个方面困难:攻击者使用了先前未曾见过的技术;没有技术失误,入侵者没有留下庭审线索;入侵者保持着完美的行动安全,没有留下其他情报线索;入侵行动的动机不明,或者攻击行动并不是发生在冲突或敌对关系的政治气氛之时;因需要对入侵进行快速回应,阻碍了对入侵行动进行彻底调查。[④]

因此,总的来说,以目前的技术还不能完全确定网络攻击的来源。乔纳森·所罗门认为,任何单一技术不能为解决归因问题提供万灵药方,"归因技术并不能为防御者提供'免费午餐'"。[⑤] 但是,大卫·克拉克则认为,目前"最大的归因障碍"

---

① David D. Clark & Susan Landau, "Untangling Attribution," in Committee on Deterring Cyberattacks & National Research Council, eds., *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U. S. Policy*, Washington D. C.: National Academies Press, 2010, p. 25.

② Jonathan Solomon, "Cyberdeterrence between Nation-States: Plausible Strategy or a Pipe Dream?" *Strategic Studies Quarterly*, Vol. 5, No. 1, Spring 2011, p. 5.

③ David Goldman, "Nations Prepare for Cyber War," January 7, 2013. http://money.cnn.com/2013/01/07/technology/security/cyber-war/index.html, 2013-01-09.

④ Herbert Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly*, Vol. 6, No. 3, Fall 2012, pp. 49-50.

⑤ Jonathan Solomon, "Cyberdeterrence between Nation-States: Plausible Strategy or a Pipe Dream?" *Strategic Studies Quarterly*, Spring 2011, p. 6

来自于跨越司法管辖权的攻击问题。[①]毕竟,一国到被怀疑的一方(包括发起网络攻击的国家和第三国)调查取证网络攻击,涉及到国家主权问题。美国战略通讯与信息战略问题专家詹姆斯·法韦尔(James P. Farwell)说,如果改变归因的标准,《国际武装冲突法》等国际法也将随之发生改变。[②]

因为技术、司法问题,理论界对归因问题的解决表示悲观。奥巴马政府的国土安全部顾问委员会高级网络专家小组通过调查得出结论说,试图归因网络攻击是"徒劳"的。[③]这一观点代表了许多学者的看法。美国外交关系协会(Council on Foreign Relations)的高级研究员史国力(Adam Segal)认为,找不到哪个行为体发起了网络攻击,美国就没有惩罚对象;不能惩罚攻击者,威慑失效。[④]因此,归因问题一时难以解决,那么实施网络威慑就存在困难,或者至少其效果是有限的。同时,因为错误的归因,不仅弱化了威慑的效力,而且还会产生新的敌人,同时也会给新棋手网络恐怖主义以机会,他们乘机浑水摸鱼,从事以前只有民族国家所进行的战争。

可是,一些理论家则认为,网络威慑在实践上比理论上更加容易证明,因为网络攻击总是发生特定时空背景下,从攻击的时间可以确定攻击源头。[⑤]他们认为,对美国经济基础设施、政治、社会领域发起网络攻击的国家,一般来说具有政治目标。在战争开启之前的冲突期间,其政治目标包括逼迫美国作出让步;通过削弱美国的经济与工业基础设施,降低美国进行战争的能力,迫使美国就范。在这个过程中,一国会向美国发出威胁,提出要求让美国妥协。当然,这个国家也会向美国提供其他一些信息,例如,如果美国能够满足其要求,就会停止网络攻击。这些信息可以消除归因问题。在交战的情况下,如果对美国发起网络攻击,与美国正在交战的国家可以被确定为嫌疑国。因此,在特定的国际关系背景下,美国确认攻击者的概率,足以慑止对手对美国发起网络攻击。相反,如果不能慑止攻击者发起攻击,只能说明美国对对手的报复规模小,而不是来自归因的失败。当然,他们也承认,

---

① David D. Clark & Susan Landau, "Untangling Attribution," p. 40.

② James P. Farwell & Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival*, Vol. 53, No. 1, 2011, pp. 30-31.

③ Richard A. Clarke & Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, New York: Harper Collins, 2010, p. 132.

④ Adam Segal, "Can U. S. Deter Cyber War?" January 12, 2012. http://thediplomat.com/flashpoints-blog/2012/01/12/can-u-s-deter-cyber-war/, 2012-06-20.

⑤ 持这种观点的学者包括美国参议员帕特里克·莱希(Patrick Leahy)的防务顾问古德曼(Will Goodman),参见 Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly*, Fall 2010, pp. 102-135;迈克菲公司(McAfee)公司的副总裁迪米特里·阿佩罗维奇(Dmitri Alperovitch)也持有这种观点,参见 The Brookings Institution, *Deterrence in Cyberspace: Debating the Right Strategy with Ralph Langner and Dmitri Alperovitch*, Washington, D. C. Tuesday, September 20, 2011, p. 12, http://www.brookings.edu/~/media/events/2011/9/20%20cyberspace%20deterrence/20110920_cyber_defense.pdf。另可参见何奇松:《近年美国网络威慑理论研究探析》,《现代国际关系》2012 年第 10 期,第 8 页。

美国很难确认那些没有政治目标向美国发起网络攻击的行为体。恐怖分子与黑客属于此类行为体。另外,也可能存在错误归因情况。例如,在美国与一国进行交战之际,第三方(他国、黑客、恐怖分子)借机向美国发起网络攻击,美国有可能错误地把一国当作网络攻击者。此外,他们认为还可以从谁获利中分析网络攻击的来源。①当然,美国可以通过一些高质量的情报信息来辨析对手。②

国际合作的方式也可以为解决归因问题提供帮助。威尔·古德曼认为,如果美国认为一国通过第三国向其发起了网络攻击,美国可以要求该第三方国家进行合作,确定嫌疑犯国家。如果该第三国不支持、配合美国的调查,美国可以根据双方的法律援助协议,或者固有的自卫权利,把攻击的责任转移到这个不进行合作的第三国。在这种情况下,责任转移排除了进一步调查的需要。③因此,克拉克很赞同这种做法,他认为以这种方式通过国家的政府工具而不是工程设计可以取得威慑效果。④当然,这是一种国际合作解决归因问题的方式,还存在另外一种方式,那就是网络领域的"道路规则",即网络空间的行为规范与准则。没有国际网络行为准则与规范,无法确认哪些是违法的,毕竟没有规范就没有违规者。同时,国际网络行为准则为美国确立网络红线提供了依据。⑤

二、如何传递威慑信息

根据威慑理论,要想实施威慑,就必须通过可视的威胁、报复让对手放弃改变现状的决策。因此,美国的威慑行动必须让对手确信,如果他们对美国发起网络攻击,美国将否决其收益,无法让其实现预期收益,而且还会向他们施加其不可接受的成本。根据基辛格对威慑的界定,即威慑是实力、使用实力的意志,以及潜在进攻者对这两方面因素的评估,而且威慑是这些所有因素的乘积,而不是它们总

---

① 在这一点上学者之间存在分歧。例如,网络安全咨询公司兰纳通讯(Langner Communications)的创始人和总裁、网络安全专家拉尔夫·兰纳(Ralph Langner)认为这是有问题的。他举例说,在"震网"行动中,美国与以色列绝对从中获利,难道德国、英国、法国、沙特和埃及就没有从中获利?参见 The Brookings Institution, "Deterrence in Cyberspace: Debating the Right Strategy with Ralph Langner and Dmitri Alperovitch," p. 15。这里需要说明的是,兰纳是德国人,这是他在受美国布鲁金斯学会邀请出席网络威慑研讨会时谈到的。

② Mason Rice, Jonathan Butts & Sujeet Shenoi, "A Signaling Framework to Deter Aggression in Cyberspace," *International Journal of Critical Infrastructure Protection*, Vol. 4, No. 2, 2011. p. 62; Herbert Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly*, Vol. 6, No. 3, Fall 2012, pp. 50-51.

③ Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?" pp. 108-109.

④ David D. Clark & Susan Landau, "Untangling Attribution," p. 40.

⑤ 例如,美国陆军上校罗斯玛丽·卡特(Rosemary C. Carter)等人就是这样认为的:美国确立网络战的规范标准,可以避免一些国家通过网络活动确立先例,有别于美国的道德规范。参见 Rosemary C. Carter, et. al, "Offensive Cyber for the Joint Force Commander: It's Not That Different," *Joint Force Quarterly*, Vol. 66, No. 3, July 2012, p. 23。

和,[①]那么一旦缺乏威胁,也就是对手感觉不到来自美国即将施加的威胁,威慑的可靠性就会动摇。因此,美国众议院的武装力量与科学委员会、国防部长办公室的高级官员埃里克·斯特纳(Eric Sterner)就认为,要明确让对手感到美国有报复的决心,并向其发出实实在在的威胁。为此,美国要采取一系列可视的报复行为——政治的、经济的、军事的、网络的——以产生合理的期望,即让潜在攻击者感知来自美国进行报复的风险预期。[②]因此,美国贝尔维尤大学(Bellevue University)政治学教授、国际安全与情报研究项目主任马修·克罗斯顿(Matthew D. Crosston)主张把冷战时期的"相互确保摧毁"(MAD)核威慑理论运用到网络领域,形成网络MAD,也就是一旦一国对美国发起毁灭性的网络攻击,那么美国就向其发起报复性攻击,以确保相互摧毁。[③]所有这些主张就是让对手感知美国有决心和意志对对手发起的网络攻击进行报复。至于如何向对手传递美国决心与意志呢?理论家提出了以下几种方式:[④](1) 发展与展示美国对网络威胁的探知能力。尽管不能做到十全十美,但可以威慑攻击者;(2) 发展与展示美国对网络威胁的反击能力。如果不展示攻击能力,对手就不知道其存在,也就不能产生威慑效果。(3) 美国应该明确宣示性政策,阐明美国网络威慑姿态。例如,美国战略与国际研究中心成员、退役的参联会副主席卡特莱特(James Cartwright)赞同确立威慑姿态,认为这有助于消除来自海外无尽网络攻击的浪潮。[⑤] 而且宣示性政策要画一条清晰的"红线"。斯特纳认为画红线,可以阻止小的摩擦,就能产生累积效果,威慑坏行为体升级到更为严重的行为。[⑥]在这里,学者们没有提及哪些活动是"红线"。

有些理论家对此并没有提出相左观点,但发出了其疑问。[⑦] 所谓的发展探知能力,也就是发展归因能力。这个问题目前在技术上存在很大困难。一旦展示反击能力,对手可能知晓其漏洞,就有机会应对这些威胁。例如,佐治亚技术研究所(Georgia Institute of Technology)的杰夫·莫尔顿(Jeff Moulton)就明确说,一旦展示,网络武器就现原形了,因为网络攻击与网络利用都是一次性资产,一旦你使用

---

① Henry Kissinger, *The Necessity for Choice*, *Prospects of American Policies*, New York, 1961, p. 12.

② Eric Sterner, "Retaliatory Deterrence in Cyberspace," *Strategic Studies Quarterly*, Spring 2011, pp. 62-80.

③ Matthew D. Crosston, "World Gone Cyber MAD: How 'Mutually Assured Debilitation' Is the Best Hope for Cyber Deterrence," *Strategic Studies Quarterly*, Vol. 5, No. 1, Spring 2011, pp. 100-116.

④ 有关这方面内容参见何奇松:《近年美国网络威慑理论研究探析》,《现代国际关系》2012 年第 10 期,第 8 -9 页。

⑤ Andrea Shalal-Esa, "Ex-U. S. General Urges Frank Talk on Cyber Weapons," November 6, 2011. http://uk. reuters. com/article/2011/11/06/oukin-uk-cyber-cartwright-idUKTRE7A514R20111106. 2012-06-15.

⑥ Eric Sterner, "Retaliatory Deterrence in Cyberspace," p. 75,作者借用了阿尔莫格的"累积威慑"(cumulative deterrence)概念,参见 Doron Almog, "Cumulative Deterrence and the War on Terrorism," *Parameters*, Vol. 34, No. 4, Winter 2004/2005, p. 8。

⑦ 何奇松:《近年美国网络威慑理论研究探析》,《现代国际关系》2012 年第 10 期。

了,人们很快就计算出来了,抵御美国的网络攻击。[①]这一点完全有别于核威慑。在核威慑中,美国追求的是最可靠、最可信的核力量,让其他国家准确知道美国的核生存与报复能力有多大。展示美国的第二次核打击能力,告知对方美国拥有相互确保摧毁的能力,因此就没有一个国家可以通过发起核攻击获取收益。此外,展示网络反击能力,不可避免引发网络军备竞赛,让美国陷于自我竞赛之中。莫尔顿还认为,网络军备竞赛让美国财政吃不消。他说尽管存在这样的观点,即美国迫使苏联与其进行军备竞赛,使苏联筋疲力尽,最后导致对手破产,但是网络世界却不同。因为世界上有很多无赖的行为体可以进行网络军备研发,他怀疑美国是否有足够的财源,更不用说是技术,能适应网络军备竞赛的升级。[②]

更严重的是,防止网络武器比预防导弹、核武器更困难。拉尔夫·兰纳认为,反(防)网络武器的扩散是不可能的:在核领域的反(防)扩散主要集中于防止裂变材料的扩散,而不是防止如何制造核武器知识;而网络领域的"裂变材料"是字节,世人是不能控制字节的生产与传播的。[③]事实已经证明,个人完全可以把网络病毒编程出来,不像制造核武器那样需要集体攻关;研发经费也远小于核武器;只需要一台计算机就可以了,不需要庞大的工业基础设施。

另外,宣示性网络威慑政策是否奏效呢?首先,确定红线,等于邀请对手进行红线以下的活动。[④]加州大学欧文分校的资深教授摩根(Patrick M. Morgan)认为,从理论上讲,宣示性政策强调进行报复,同时也会对对手进行安抚,即对手采取克制行动,美国取消报复惩罚,还会给予一定"奖励"。尽管有研究表明,恩威并用的手段增加了威慑成功的机会,但也有相反情况,即对手把"奖励"看成是威慑者虚张声势的证据。[⑤]

在学者讨论如何进行传递威慑信息之际,2013 年 1 月,美国国防部防务科学委员会(Defense Science Board, DSB)借用了核威慑的措辞,企图用强硬语言向对手传递美国网络威慑的信息。这些信息出现在该委员会解密报告《弹性军事系统与先进网络威胁》中。该报告说,国防部应该从军力中分割部分军力,确保在灾难

---

① Zachary Fryer-Biggs, "U. S. Military Goes on Cyber Offensive," March 24, 2012. http://www.defensenews.com/article/20120324/DEFREG02/303240001/U-S-Military-Goes-Cyber-Offensive, 2013-01-07.

② 迈克菲公司(McAfee)进行的一项全球调查表明,57% 的专家认为网络军备竞赛正在上演。参见 Brandon Valeriano, "Mind the Cyber Gap? Deterrence in Cyberspace," July 11, 2012 http://www.acus.org/new_atlanticist/mind-cyber-gap-deterrence-cyberspace, 2013-01-08。

③ The Brookings Institution, "Deterrence in Cyberspace: Debating the Right Strategy with Ralph Langner and Dmitri Alperovitch," pp. 18-19.

④ 此外,所罗门认为,确立明确的网络威慑门槛是困难的,参见 Jonathan Solomon, "Cyberdeterrence between Nation-States: Plausible Strategy or a Pipe Dream?", *Strategic Studies Quarterly*, Spring 2011, p. 8。

⑤ Patrick M. Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," in Committee on Deterring Cyberattacks & National Research Council, eds. *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U. S. Policy*, p. 64.

性网络攻击事件中执行肩负的使命,包括发射核武器,同时该部分军力拥有包括核动力潜艇——装备巡航导弹、常规弹道导弹——能力。①

三、如何进行网络威慑

威慑有两个手段即惩罚威慑与拒止威慑,斯奈德(Glenn Snyder)认为,惩罚威慑立足于报复能力,给对手严厉惩罚,使其认识到得不偿失;拒止威慑则立足于防御能力,让对手无法实现预期收益目的而放弃攻击。② 美国理论界对这两种威慑手段是否可行,以及如何运用于网络空间进行了讨论。③

拒止威慑,就是增加网络安全的弹性,加固网络基础设施的防御,不让对手从攻击中获取收益。国防部网络问题协调员办公室的高级政策顾问迈克尔·马尔科夫(Michael Markoff) 认为,增加网络空间设施的弹性与冗余,在慑止对手对美国基础设施发起网络攻击中是有效的,辅之以可信的非军事回应,如执法、外交与经济制裁。④ 摩根教授认为,提高网络防御能力,不仅可以提高威慑效果,而且还间接地为解决归因问题作出贡献。美国的防御越有效,就越能发现网络攻击的特征,也就能发现是"谁干的",并为报复提供依据。⑤ 佐治亚技术研究所的斯蒂芬·卢卡西克(Stephen J. Lukasik)甚至认为,防御在网络威慑中比在核威慑中发挥的作用要大。因为在核威慑中,防御被视为破坏了核均势。⑥ 同时,有人提倡把公共卫生领域的风险与后果管理模式运用到网络领域,改善美国的防御姿态。联邦政府应该支持公私联合,发出新威胁的早期预警,快速反应并遏制有害影响的传播,长期致力于消除在网络空间蔓延的有害活动。⑦

针对以上情况,有些人认为纯粹的网络防御可能存在一些弱点。他们认为,采

---

① Defense Science Board task force report, "Resilient Military Systems and the Advanced Cyber Threat," January 2013, pp. 40-45, http://www. acq. osd. mil/dsb/reports/ResilientMilitarySystems. CyberThreat. pdf, 2013-03-08.

② Glenn Snyder, *Deterrence and Defense: Toward a Theory of National Security*, Princeton University Press, 1961, pp. 3-16.

③ 有关此部分讨论可参见何奇松:《近年美国网络威慑理论研究探析》,《现代国际关系》2012 年第 10 期,第 9 - 10 页。

④ "Overlapping Defense Essential to Deter Cyberattacks: Panel Members," November 8, 2011. http://defensesystems. com/articles/2011/11/08/agg-cyber-defense-panel. aspx, 2012-06-10.

⑤ Patrick M. Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," p. 59.

⑥ Stephen J. Lukasik, "A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains," in Committee on Deterring Cyberattacks & National Research Council, eds. *op. cit.*, p. 102.

⑦ Greg Rattray, Chris Evans, and Jason Healey, "American Security in the Cyber Commons," in Abraham Denmark and James Mulvenon, eds., *Contested Commons: The Future of American Power in a Multipolar World*, Washington: Center for a New American Security, 2010, pp. 137-176.

用冗余的方式,对慑止对手发起网络攻击可能会起作用,但是纯粹的拒止威慑手段是有局限性的。因为在常规军事战略中强调拒止威慑,对手认为发起攻击的成本局限于士兵与军事物资的潜在损失,但是网络攻击几乎没有成本。良好的防御可能会抵御攻击,但同时削弱了威慑效果,毕竟防御能力不可视。①摩根认为,目前这个事实似乎加剧了拒止威慑的难度,即现在有关美国网络攻击能力和用于报复的生存能力,是一个相当的秘密。世人普遍认为美国拥有最好的网络能力,但不知道这些能力在遭受重大攻击之后到底有多强大。② 此外,斯特纳认为,公共卫生领域的风险管理经验不能很好地为网络领域的拒止威慑服务。因为风险管理集中于最高风险挑战,不注意较低层次的威胁,诸如网络刑事犯罪活动。网络空间的隐蔽性,为隐藏攻击者身份和攻击的动机提供了方便,可以为声东击西的网络攻击提供便利。例如,一国可以使用僵尸对另一国的某些网络发起分布式拒止服务攻击,作为吸引力,在别处发起重要的网络攻击。黑客也可以获得政府足够的资金,租借、购买网络武器,向一国发起破坏性的攻击。换句话说,“意图与能力变化快速”,“昨天的犯罪威胁可能是今天的战略攻击”。③ 因此,防御者要特别关注这样的袭击事件,以免遭受突然性攻击,造成措手不及。此外,过分强调风险管理方法等于拱手把网络安全的主动权交给了攻击者。因为风险管理集中于减少网络的脆弱性,并把其后果最小化,只是对特定网络攻击与行动进行回应,不给攻击者施加战略的、战役的或战术的反击后果,那么防御方完全被动挨打。④

赫伯特·林并没有否定防御的作用,但是主张采取积极防御的方式,也就是采取进攻方式。他认为,要想防御成功,就需要所有的防御措施必须每次都能够抵挡住进攻。但是进攻行动则不一样,只需要一次成功就行了,因失败的进攻行动而没受到惩罚的对手会继续发起后续进攻,直到成功或者选择停下来。这样就给只采取被动防御一方造成沉重的与非对称的负担。要想加强美国的防御能力,一种可能性就是消除或破坏对手成功进行网络攻击的能力,就是在对手发起网络进攻之前或进行之中,美国可以让进攻者的行动无效。第二个可能性就是给对手施加其他成本,这个战略建立在两个前提上:一是施加这些成本降低了对手进行发起攻击行动的意志与能力;二是传递这样的信息,即采取进攻行动对于对手来说成本巨大,威慑其他对手试图进行此类型行动。当然,传递这种可能性的信息或许也可以慑止最初的对手首先发起网络进攻。这种战略方式包括诸如经济制裁的经济惩

① Stephen J. Lukasik, “A Framework for Thinking about Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains,” p. 108.

② Patrick M. Morgan, “Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm,” p. 62.

③ Eric Sterner, *op. cit.*, p. 68.

④ Eric Sterner, *op. cit.*, p. 69.

罚、断交的外交惩罚,甚至诸如巡航导弹打击的动能军事打击,网络反击也是一种选择。①

威慑的另外一个手段即惩罚威慑可否适用于网络空间?冷战时期之所以没有发生核战,就在于美苏拥有强大的第二次核打击能力,也就是强大的核报复能力。理论界对惩罚威慑可否用于网络空间也有不同的声音。

斯特纳主张,美国必须对有害的网络行为进行报复,但是并没有界定何谓"有害"。他认为,美国想通过执行国内法律来惩罚网络入侵者是必要的,但是此类工具是完全不够的,应该利用政治、经济、军事手段作为报复选项。尽管这些手段通常是在国与国关系之间考虑的,但也可以用来打击非国家行为体对美国实施的网络攻击,而且主张在进行政治与经济报复时,所要求的门槛必须很低,只要满足了一些条件,就立即实施。②

拉尔夫·兰纳认为,一个国家不应也不可能对所有网络攻击进行报复。他认为,除了利用网络打击作为一种心理手段外,还存在三种网络攻击:③(1) 秘密攻击。国家资助的隐秘攻击,也就是网络间谍活动,对美国及其盟国产生了重要威胁。就网络经济间谍而言,无法使用武装冲突法或国际规则进行报复,要找到替代办法也是困难的。唯一能使用的手段就是通过制裁、贸易手段和外交压力,给对手产生经济成本,来影响他们对行动的成本—收益分析。而对于涉及国家政治、安全的间谍活动而言,则是不能进行报复威慑的,这是一个可接受的国际规范,如同前述,美国战略与国际研究中心的刘易斯也持这样的观点。网络犯罪则不会构成战略性的网络威胁。(2) 完整攻击(integrity attack)。对数据的完整攻击,则比间谍攻击要阴险得多,目的在于获取战术、战略优势,破坏美国重要的军事、民用信息系统。此类网络攻击很危险,当发起大规模攻击时,则对国家经济、安全产生灾难性影响。这是进行报复性威慑所要重点考虑的事情。但如果是小规模的,则可以忍受,不必进行报复。(3) 截取信息或信息系统。这种攻击就是进行离线攻击,切断或破坏重要的物理或虚拟空间,或者阻止获取信息。当然,规模与影响是考虑进行报复的绝对关键性因素。对手发起网站拒绝服务的攻击是大量存在的,但不会对国家造成战略性威胁,不需要进行报复。但是那些尽管是短时但却造成巨大破坏的网络攻击,应被视为战略性攻击,必须进行报复。例如,对情报收集和分析能力

---

① Herbert Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly*, Vol. 6, No. 3, Fall 2012, p. 50.

② Eric Sterner, "Retaliatory Deterrence in Cyberspace," pp. 71-72.

③ The Brookings Institution, "Deterrence in Cyberspace: Debating the Right Strategy with Ralph Langner and Dmitri Alperovitch," p. 6。也有人把网络网络攻击分为两类,即网络攻击(Cyberattacks)和网络侦探(cyberexploitations),参见 William A. Owens, Kenneth W. Dam, and Herbert S. Lin, *Technology, Policy, Law, and Ethics Regarding U. S. Acquisition and Use of Cyberattack Capabilities*, Washington D. C.: National Academies Press, 2009, p. 81。

发起网络攻击,破坏美国获取主要态势感知和情报收集能力。①

实际上,是否需要报复,在很大程度上取决于网络攻击是否等同于武装攻击或使用了军力。乔纳森·所罗门认为,因为国际社会对何谓网络攻击没有国际共识,很难确认哪些、何种网络攻击等同于军力使用、武装攻击。如果一国使用网络攻击造成了损失,如同武装攻击造成的一样,这就等同于武装攻击。尽管销毁数据、窃取数据、收集情报的网络攻击达不到武装攻击的标准,但是一些网络攻击造成人员伤亡、造成国土安全部所界定的重要关键基础设施的破坏,则应该视为武装攻击。对商业、非防务系统发起拒绝服务攻击不应视为武装攻击,对军事行动的指挥、控制网络发起类似攻击,是否视为武装攻击,则取决于攻击的影响。对战略指挥、控制、早期预警资产与网络进行的网络,则被视为特殊的武装攻击。② 詹姆斯·法韦尔等人则认为,无论从规模还是影响上来看,网络攻击是否等于武力攻击是很难界定,毕竟相关国际法并没有对此进行界定,因此需要从政治、外交、战略考虑来寻求答案。③

四、对网络攻击采取报复行动相关的几个问题

如何对网络攻击采取报复行动呢?核威慑理论的一个关键因素就是进行报复,在实施报复中,防御者给对手施加的成本至少与对手所获取的利益相等,实现相互确保摧毁。从理论上讲,以其人之道还治其人之身地进行网络报复是合情合理的。针对伊拉克叛乱分子使用网络、手机遥控路边炸弹的情况,遵照小布什总统的命令,美国国家安全局对其所使用的移动手机和网络进行了攻击。许多军事分析家认为,对叛乱分子的网络报复打击产生了巨大影响,扭转了局势。因此,对对手的网络攻击实施网络报复是有效的,可以瘫痪对手的网络攻击能力,实现威慑目标。但是,乔治·华盛顿大学埃利奥特国际事务学院(Elliott School of International Affairs)的教授查尔斯·格拉泽(Charles L. Glaser)认为,如果实施网络军事报复打击,有可能导致威慑失败,导致网络冲突升级为战争。过分注重网络攻击报复,有可能增加对手对美国常规能力估计不足,从而使威慑失败。因为有关战争结果的不确定是双方进行讨价还价的基础,也是威慑失败之源。有关战争结果的不确定

① The Brookings Institution, "Deterrence in Cyberspace: Debating the Right Strategy with Ralph Langner and Dmitri Alperovitch," pp. 7-9.

② Jonathan Solomon, "Cyberdeterrence between Nation-States: Plausible Strategy or a Pipe Dream?" *Strategic Studies Quarterly*, Spring 2011, pp. 12-13.

③ James P. Farwell & Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival*, Vol. 53. No. 1, 2011, pp. 34,30.

性,阻碍了国家达成政治协定,使得他们愿意进行战争。[①]因为网络攻击也存在附带损失,尤其是给无辜国家的系统造成损失,引起不必要的政治风险,因此还是采用被动防御方式比较可行。被动防御方式就是建立多层次的防御,包括深度防御、增加弹性、系统硬化和入侵探测等。[②]

当然,包括美国海军战争学院(US Naval War College)国际法系主任迈克尔·施密特(Michael N. Schmitt)等人认为,对对手的网络攻击进行惩罚报复,则不应该被限制在网络领域。[③] 尤其对于那些很少依赖网络但发起的网络攻击给美国造成巨大破坏的国家,军事打击似乎是必然的选择,例如,朝鲜就是这样的国家。美国使用网络报复,形成不了威慑效果,因为网络报复攻击所产生的威胁达不到朝鲜给美国造成的威胁。所以,朝鲜用网络攻击开启了美国的水坝,美国可用巡航导弹打击对手的水利设施。[④]甚至格拉泽主张,如果一个国家发起高度破坏性的网络攻击,美国可以威胁侵略这个国家,或者进行政权更迭。[⑤]也有学者认为,对于对手有意使用致命、进行物理破坏的网络攻击,采取非动能报复威慑的作用极为有限。因为非动能报复的影响要么不可预测,要么不如动能报复打击所产生的效果那样直观。对于此类网络攻击,应该采取包括常规军事回应。美国的报复惩罚应该直接针对对手的常规军力部队、其珍视的机构与设施。有学者甚至认为,在极端情况下,美国可以用核升级的方式威胁潜在对手,慑止其对美国关键基础设施进行灾难性的网络攻击,所罗门就是其中的一位。他含蓄表达美国应该用核报复回应对手对美国"关键基础设施"实施的网络攻击。[⑥]如同前述的国防部防务科学委员会就建议,在美国遭受灾难性网络攻击之时,美国应该使用核武器进行惩罚。

进行报复如何处理相称原则问题?对手对美国网络进行攻击而不产生附带伤

---

① Charles L. Glaser, "Deterrence of Cyber Attacks and U. S. National Security," p. 6. http://www.cspri.seas.gwu.edu/Seminar%20Abstracts%20and%20Papers/2011-5%20Cyber%20Deterrence%20and%20Security%20Glaser.pdf, 2012-06-16.

② Kevin L. McLaughlin, "CyberAttack! Is a Counter Attack Warranted?" *Information Security Journal*, Vol. 20, No. 1, 2011, pp. 62-63。网络攻击对无辜系统产生破坏是有先例的,例如,"震网"病毒给印度卫星造成了破坏。"如果攻击方得到确认,这就造成了潜在的严重政治反弹的风险"。参见 James P. Farwell & Rafal Rohozinski, "Stuxnet and the Future of Cyber War," Survival, Vol. 53, No. 1, 2011, p. 34。

③ Michael N. Schmitt, *Cyber Operations and the Jus Ad Bellum Revisited*, 2011, http://www.usnwc.edu/getattachment/f1236094-416b-4e5b-bf58-32e677aed04a/villanova_cyber_ad_bellum; Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, *Yale Journal of International Law*, Vol. 36, 2011, pp. 421-459.

④ The Brookings Institution, "Deterrence in Cyberspace: Debating the Right Strategy with Ralph Langner and Dmitri Alperovitch," p. 10.

⑤ Charles L. Glaser, "Deterrence of Cyber Attacks and U. S. National Security," p. 4.

⑥ 参见 Jonathan Solomon, "Cyberdeterrence between Nation-States: Plausible Strategy or a Pipe Dream?", *Strategic Studies Quarterly*, Spring 2011, pp. 13-14。目前,奥巴马政府官员和议员越来越频繁地提及敌国和恐怖组织可能利用网络战打击美国重要基础设施。参见 David Goldman, "Nations Prepare for Cyber War," January 7, 2013. http://newsle.com/article/0/54050639/。

亡,美国使用报复手段打击对手是否恰当?许多人认为,使用军事手段或者网络手段打击对手,做到相称报复都很困难。有人认为,美国用网络或军事打击关闭了对手的电厂或水处理设施,就会产生附带损失,[①]而避免附带损失是美军所力图避免的。另外,美国打击其他目标,如金融系统也是愚蠢的。小布什政府的反恐专家顾问理查德·克拉克(Richard Clarke)说,小布什政府一直考虑打击本拉登的银行账户,但是政府最终并没有实施,因为担心由此导致市场对金融系统失去信心,引发国际金融危机。[②]

在理论上,美国确实珍视生命要胜于字节,因此,美国用各种报复手段(尤其是军事手段)反击网络攻击,一旦产生附带伤亡,此类报复威胁就不可信。但有人认为,不能简单地看待相称原则问题。即使对手的网络攻击没有直接损害建筑物,也没有直接杀死一个人,但因为摧毁了信息,却造成了可见的人员、机构损失与社会成本。[③] 因此,不能因相称原则问题来说明美国报复过度。斯特纳就认为,相称原则不是简单的"生命换字节"问题。相称概念来源于战争或法律体系中的正义理论:对罪犯必须进行惩罚;大规模回应军事挑衅是不适当的。网络冲突介入两者之间,因此没有必要把网络冲突上升到战争水平。但是,目前国际法还不足以作为国际关系中的战略手段处理网络冲突。另外,攻击意图与后果并不总是一致。因此,相称原则应根据具体情况来考虑。决策者在个案的基础上,考虑攻击者意图、攻击后果、对确认发起者的信心水平、战略局势及可使用的报复手段选项,最终决定对攻击者实施怎样的报复打击。[④]

对于报复是否需要立即进行?这个问题也存在争论。经典威慑理论要求报复是肯定要实施的,而且要立即、严厉。因此,有人主张美国应该对网络攻击进行报复,而且立刻进行且严厉。但是,也有学者认为,网络威慑强调报复的确定性,要远超报复的严厉性与即刻性。因为涉及到的直接后果,核威慑要求相互实施威慑的国家能够快速进行压倒性的反击;但是,网络攻击一般不会造成诸如核打击那样的直接严重后果,而且因为归因问题还不能立即确认攻击者。因此,就较少严重后果

---

① 《纽约时报》的记者大卫·桑格(David E. Sanger)通过调查发现,攻击伊朗核设施的"震网"(Stuxnet)已经产生了很多附带伤亡,如脱缰野马逃进了"狂野之地"。参见 Steven Cherry, "Stuxnet: Leaks or Lies," September 4, 2012, http://spectrum.ieee.org/podcast/computing/embedded-systems/stuxnet-leaks-or-lies, 2013-01-19。美国国会并没有把这个被命名为"奥林匹克运动"工程的"震网",看成是一个成功的战略来进行赞美,相反却要威胁调查政府在实施过程中的漏洞。当然,有些理论家认为,正由于这些网络武器有着巨大的附带伤亡,也为网络威慑提供了基础。参见 Brandon Valeriano, "Mind the Cyber Gap? Deterrence in Cyberspace," July 11, 2012, http://www.acus.org/new_atlanticist/mind-cyber-gap-deterrence-cyberspace, 2013-02-20。

② The Brookings Institution, "Deterrence in Cyberspace: Debating the Right Strategy with Ralph Langner and Dmitri Alperovitch," pp. 17-18.

③ 但有人预测2013年的网络攻击将导致真实的、直接的人员伤亡。参见 David Goldman, "Nations Prepare for Cyber War." http://newsle.com/article/0/54050639/, 2013-01-09。

④ Eric Sterner, "Retaliatory Deterrence in Cyberspace," p. 73.

而言,反制措施不需要压倒性的严厉报复;反制也不需要立即进行,因为不像突然性的首次核打击一样,很少有网络攻击能彻底瘫痪一个国家的反应能力。因为这些原因,网络威慑惩罚措施不需要即刻、严厉,只需要确信实施报复即可。①

而兰德公司的马丁·里比克基(Martin Libicki)则详细地探讨了报复的限制性。尽管他认为网络报复所产生的影响不如军事报复那么直观、强烈,损失也可能较小,但对对手的网络攻击行为进行报复存在几个问题:(1) 报复是否足够,也就是报复是否给攻击者造成足够的困难,施加足够的成本,迫使他们重新思考网络战的逻辑。他认为,一般来说,报复要设立一个较低的门槛。(2) 报复传递了报复者姿态与意图的何种信息?这种姿态与意图是强化报复(例如,报复者公布其宣示性政策,增强报复的可信度),还是弱化报复?(例如,攻击是危机的一部分,威胁使冲突失控而升级)(3) 报复与被承认的冲突规范相互符合吗?如前述,因为国际法滞后于现实,他的主张是应该采取司法途径而不是报复手段。(4) 在一些情况下,报复指导出现错误。这主要来源于错误的情报、夸大对手给己方造成的威胁,等等,这些情况影响了报复者的报复决策,这无疑导致错误的报复。美国在没有确切证据表明伊拉克拥有大规模杀伤性武器(WMD)情况下,对萨达姆政权发起了攻击,就是典型例子。(5) 报复可能导致局势失控而升级冲突或战争。这里存在几种情况,例如,报复者无论如何都需要对对手进行报复;出于各种目的,需要对攻击者进行报复,以现实自己的目标;报复者的报复打击引起攻击者的反报复行为。②

使用军事手段报复对手的网络攻击,会不会导致网络冲突升级为战争?格拉泽认为,使用动能军事手段进行报复,可能被视为常规战争的一部分,能否慑止对手的网络攻击,这就要看美国的相对网络能力,以及美国和对手的常规作战能力。美国拥有赢得常规冲突能力,即使对手拥有网络优势,对手可能被慑止发起常规进攻。但是,即便美国拥有的常规能力优势很明显,但是对手在网络攻击能力上拥有净优势,对手是不能被慑止的。③

赫伯特·林比较详细分析了网络行动是否会升级的问题。他把网络冲突升级分为四种情况:(1) 故意升级。或为获取优势,或先发制人,或避免失败,或向对手发出其自身意图与动机的信息,或惩罚对手先前的行动,一方故意升级冲突。进攻性网络行动特别是网络攻击,就是故意升级的一种。(2) 无心之故的升级。一方有意采取它不相信会升级的行动,但是被冲突的另一方解释为是升级的行动。这

① Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?" p. 107.

② Martin Libicki, "Pulling Punches in Cyberspace", in Committee on Deterring Cyberattacks & National Research Council, ed., *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U. S. Policy*, pp. 130-136.

③ Charles L. Glaser, "Deterrence of Cyber Attacks and U. S. National Security," pp. 5-6.

是因信息不对称、缺乏共享的关系框架,一方不清楚其他方的门槛而造成误解形成的升级。向对手传递有关网络空间活动的门槛信息,尤其存在问题,即使是在正常和平环境之下。(3) 意外升级。就是一些行动产生了不是领导者所要的影响。比方,武器打偏击中错误目标、部队进行了未经授权的行动。当使用某些网络攻击行动时,由于缺乏对多个目标的足够情报,其结果就具有更大的不确定性。(4) 催化升级。就是第三方成功地挑拨离间让双方发生冲突。网络行动的固有匿名性使得"嫁祸"(False-flag)行动在网络空间更容易进行。

在哪些情况下,冲突会升级呢?在动能武器上,通过危机稳定(crisis stability,即不刺激双方首先发起攻击)相对好处理冲突或战争的升级。防御方只要存在第二次核打击能力,攻击国不可避免受到报复打击。尽管不能想象一国可以消除或明显降低另一国的网络攻击能力,但是,第二次网络攻击能力是否是保证网络空间危机稳定的条件,这是不清楚的。这是网络冲突是否会升级的一方面。在传统威慑理论中,信息传递在危机管理中很重要,但是在较之其他领域的冲突,在网络领域信息传递更为困难。一国如何理解冲突一国向其传递的信息,存在不确定性。由于缺乏历史先例,使得理解对手希望通过发起网络攻击获取怎样的收益更加复杂化。当网络攻击已经发生,希望通过有限的、受控的军事行动向对手发出信息更成问题。另外,一国对网络攻击的反应程度也是冲突是否升级的因素。不像核武与常规打击,首次网络攻击的影响范围是不确定的,使决策者陷于两难境地:即政策需要迅速回应,但需要时间收集足够的信息,明了受到攻击的影响和受损程度。决策者感到有压力需要在危机之时立即有所作为,但是在缺乏足够的信息的情况下,认为最坏的情况已经发生,作出错误的回应。这有可能导致升级。还有一种情况,就是当两个国家之间陷于网络冲突之际,双方的爱国黑客组织起来向冲突一国发起网络攻击,使得局势复杂起来,升级管控复杂化。在最坏的场景下,即使他们没有得到政府同意,或者也不是在政府指导之下,爱国黑客的行为被视为得到政府批准的网络打击。另外,爱国黑客的行动得到政府指导、鼓励或者容忍,但是看不到政府之手,也会导致冲突升级。①

五、如何构建网络威慑体制

那么,如何构建网络威慑体制呢?美国国内呼吁国家建立一套完整的网络威慑战略。首先,宣布网络政策,作出网络威慑姿态。美国国际与战略研究中心在2008 年的一份报告中,建议总统发表一份网络空间政策声明,应明确指出网络空

① Herbert Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly*, Vol. 6, No. 3, Fall 2012, pp. 52-61.

间是重要的国家资产,一旦受到威胁,美国将调用一切可用的国家力量和手段予以保护,[①]但并没有提及美国对哪些网络威胁进行回应。曾任助理国土安全部长帮办的保罗·罗森茨魏希(Paul Rosenzweig)建议,政府应该把对手探测发电厂、水厂之类的关键基础设施的行动视作"为战场做准备",他说,借用中国人的话来说就是"不要派第七舰队来拯救台湾,否则我们将切断洛杉矶的电力供应"。[②]所罗门称美国应该公开警告对手在紧张时期网络攻击战场、战区、战略的防御系统与网络的危险性,这样的网络攻击应被视为动能打击的前奏。[③] 一个明确的网络政策对于发展全面、有效的网络安全体系是必要的,政策包括如何对网络攻击进行立刻回应;发展给人印象深刻的防御;建立合适的报复能力;让网络空间资源有更大的冗余;积极支持网络空间的集体军控与相关管理。当然,其中发展网络条令是必要的。条令是战略与国家安全部门之间的联系,是一个军事概念,确立军事行动的指导原则。国家网络条令是一个工具,界定美国政府各部门的作用,以应对网络攻击。[④]

其次,通过国际合作,形成建立国际网络规范共识。智库第三条道路(The Third Way)的国家安全项目主任安迪·约翰逊(Andy Johnson) 呼吁美国应该带头召开网络安全峰会,制定网络规则,也就是网络空间行为规范,划定哪些是可以接受的网络行为,哪些是合法的防御与进攻措施;形成一个可验证的机制,确定攻击源头,并且让攻击的源头方承担责任。[⑤] 再如,有人倡导提升全球协议,诸如《日内瓦公约》,以反映现今的网络现实。[⑥]

---

① Center for Strategic and International Studies, "*Securing Cyberspace for the 44th Presidency*," Washington, D. C, December 2008, http://csis. org/files/media/csis/pubs/081208_securingcyberspace_44. pdf, 2012-06-10.

② Nick Hopkins, "Militarisation of Cyberspace: How the Global Power Struggle Moved Online," *The Guardian*, 16 April, 2012. http://www. guardian. co. uk/technology/2012/apr/16/militarisation-of-cyberspace-power-struggle, 2012-06-18.

③ Jonathan Solomon, "Cyberdeterrence between Nation-States: Plausible Strategy or a Pipe Dream?" *Strategic Studies Quarterly*, Spring 2011, p. 18.

④ Mark D. Young, "National Cyber Doctrine: The Missing Link in the Application of American Cyber Power," *Journal of National Security Law and Policy*, Vol. 4, No. 1, 2010, p. 174.

⑤ Andy Johnson and Kyle Spector, "Deterring Cyber War: A U. S. -Led Cybersecurity Summit," October 2010, pp. 3-4. http://211. 154. 83. 46:82/1Q2W3E4R5T6Y7U8I9O0P1Z2X3C4V5B/content. thirdway. org/publications/343/Third_Way_Idea_Brief_-_Deterring_Cyber_War-A_US-Led_Cybersecurity_Summit. pdf, 2012-06-20.

⑥ Mike Cronin, "U. S. Cyber Strategy: The Perils of Deterrence," *World Politics Review*, 10 Jun 2011。英国人斯蒂芬斯(Tim Stevens)较系统了提出了网络国际规范。参见 Tim Stevens, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace," *Contemporary Security Policy*, Volume 33, Issue 1, April 2012, pp. 148-170。麻省工学院的计算机科学与人工智能实验室的科学家罗格·赫维茨(Roger Hurwitz)在 2012 年《战略研究季刊》秋季号载文,表示支持网络空间身份管理,该项目得到美国海军研究局的资助。他利用诺贝尔经济学奖获得者埃莉诺·奥斯特罗姆的公共事务治理理论,认为要加强网络"空间道路规则",从容易的事情做起,通过国际合作,进行信任建设,避免网络空间沦为"公地悲剧"。参见 Roger Hurwitz, "Depleted Trust in the Cyber Commons," *Strategic Studies Quarterly*, Vol. 6, No. 3, Fall 2012, pp. 20-45.

再次,与其他国家结成伙伴关系,形成相互依赖。这是许多战略专家开出的一剂药方,其好处有二:一方面,美国可以利用他国网络系统进行自卫与反击;另一方面,攻击者冒着遭受多国打击的风险。这一点要求美国与盟国在网络(技术)上相互联系与相互依赖,甚至与对手相互依赖。"我们是如此地相互联系,因此,如果你要伤害我,你也会伤害你自己"。① 同时,美国与他国结成伙伴关系,广泛地执行兼容(interoperable)的归因技术与方法,有助于解决归因问题的解决。②

最后,建立"网络三位一体"(Cyber Triad)威慑能力。美国空军退役中将小哈里·拉多哥(Harry D. Raduege, Jr.)明确提出,在网络空间中,美国面临新的大规模杀伤性武器,如果不做好准备,终有一天面临网络攻击,政府、经济与社会将瘫痪。冷战时期美国建立了海陆空三位一体的战略核力量,对威慑一国对美国使用大规模杀伤性武器发起攻击发挥了重要作用。在网络数字时代,美国也应该建立网络三位一体,威慑一国使用网络大规模杀伤性武器对美国网络空间发起攻击。③ 具体做法包括:

其一,增加网络空间的弹性与冗余,否决对手网络攻击收益。在冷战时代,由于美国拥有三位一体的战略核力量,即使对手摧毁了美国的陆基战略力量,但美国还有海基、空基战略核力量进行报复。因此,美国在网络空间也应该建立弹性与冗余,使对手知道其网络攻击并不能完全摧毁美国的经济、政治与军事。具体措施包括:增加关键节点的冗余;增加网络通讯能力;保护与确保敏感信息安全的能力;也要对关键基础设施实施级别更高的保护。实际上,就是增加美国拒止威慑的能力,也就是美国采取加固、增加网络空间的弹性与冗余,让对手确信,发起网络攻击的成功概率很低,减少其预期收益,从而实现成功威慑。完美的威慑让攻击者感知成功的机会近乎为零。在此过程中,重要的国家安全网络必须有别于一般的公共网络,例如,退役的空军将军、小布什政府的中央情报局局长海登(Michael Hayden)提出了".secure"概念,重要网络应该使用".secure",而非".com"和".net"",而且用户需要放弃在".com"领域的许多隐私权利。④

其二,实施报复威慑。为了增加惩罚威慑的可信度,美国应该提高攻击对手网

---

① 有学者构想了美国与盟国在网络上形成相互依赖的技术框架,参见 Jonathan Solomon, "Cyberdeterrence between Nation-States: Plausible Strategy or a Pipe Dream?" *Strategic Studies Quarterly*, Spring 2011, p. 21.

② Jonathan Solomon, "Cyberdeterrence between Nation-States: Plausible Strategy or a Pipe Dream?" *Strategic Studies Quarterly*, Spring 2011, p. 7.

③ Harry D. Raduege, Jr., "Fighting Weapons of Mass Disruption: Why America Needs a 'Cyber Triad'," in *Andrew Nagorski*, ed., "Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway," April 2010, pp. 3-5. www.ewi.info/system/files/CyberDeterrenceWeb.pdf, 2012-5-30.

④ Molly Bernhart Walker, "Hayden: Policymakers Should Consider a Hardened, Secure Domain for Critical Services," July 11, 2011, http://www.fiercegovernmentit.com/story/hayden-policymakers-should-consider-hardened-secure-domain-critical-serices/2011-07-11, 2012-07-30.

络的能力。美国应该研发先进的网络攻击武器,让对手知道美国拥有平衡的系列网络进攻武器和防御武器,如同在常规与核领域的武器一样。因此,发展“反制网络空间”(Countercyberspace)能力至关重要。反制网络空间被界定为是一种功能,通过摧毁、降级或者破坏敌人使用网络的能力,获取和维持期望的网络优势的行动,也就是希望在假定的时间与地点进行网络反制行动,而不受对手的限制性干扰。①为此,国防部防务科学委员会建议,美国应该发展世界一流网络进攻能力,并提出了具体措施。② 在实施报复过程中,要奉行这样的信条,即攻击优于防御,在预见到敌人要发起网络进攻之际,可以使用网络武器、空中力量、海上力量先发制人地进行打击敌人的网络节点或所珍视的目标。③

其三,改进网络态势感知能力。不管是使用拒止威慑,还是使用惩罚威慑,要想使网络威慑取得成功,其中一个重要因素就是明了攻击的源头。限于技术原因,以及其他一些因素,归因问题一时还无法解决,威慑的可信度降低,限制了美国有针对性采取措施进行防御或报复。因此,提高网络态势感知能力显得迫切。与金融信息等暂时的损失比较起来,投资于网络态势感知技术的开支成本很少;而且网络冲突造成了包括人员、信息、物资、资金在内的各种成本,而改善了网络态势感知能力从而使网络冲突避免,因而也就免除了这些成本。这是一笔划算的买卖。发展网络归因技术,不应该偏废传统的人力情报,以及早期雷达预警系统、卫星侦察和海底监听技术的发展。拥有了强大的网络态势感知能力,可以即时进行分析、发布网络安全预警通知,公私做好预防准备,必要时对对手实施报复。网络预警系统,不管是战略的还是战术的,对于网络威慑至关重要。④

其四,需要企业、公众广泛参与,并于国外结成伙伴关系。军事威慑尤其是核战略威慑,基本上是政府与军队的事情,但网络威慑则不一样,需要民众的参与。对手会攻击那些没有安装防火墙的公众、企业的网络,并通过互联网进行传播,给美国政府、军方造成破坏。美国政府和军方需要向企业、民众发起公开教育,宣称网络安全意识,鼓励他们给计算机安装必要的防护软件与设备。还要创造公—私伙伴关系,形成联邦政府—企业—个人三位一体的“网络防御伙伴关系”。⑤这是

---

① Eric D. Trias and Bryan M. Bell, “Cyber This, Cyber That... So What?” *Air and Space Power Journal*, Vol. 24, No. 1, Spring 2010, pp. 90-100.

② Defense Science Board task force report, “Resilient Military Systems and the Advanced Cyber Threat,” January 2013, pp. 49-54.

③ Matthew D. Crosston, “World Gone Cyber MAD: How ‘Mutually Assured Debilitation’ Is the Best Hope for Cyber Deterrence,” p. 103.

④ Stephen J. Lukasik, “A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains,” p. 102.

⑤ Department of Homeland Security, *Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action*, March 23, 2011. http://www.dhs.gov/xlibrary/assets/nppd-cyberecosystem-white-paper-03-23-2011.pdf, 2012-05-10.

包括国土安全部在内许多政府机构和安全专家的建议。

结　论

发明互联网的美国,几乎各行各业与计算机网络密不可分。正如美国空军退役中将、洛克西德马丁公司信息系统与全球服务部门负责网络安全的副总裁查尔斯·克鲁姆(Charles E. Croom)所说,"世界上还没有哪个国家像美国这样如此依赖网络",但是"没有任何事物像网络那样与生俱来就那么脆弱",[①]因而美国把网络空间视为国家战略资产,从国家战略层面上重视网络安全。为确保这一国家战略资产,美国希望借助冷战时期的核威慑理论,把威慑理论的运用扩大到网络领域。对此,美国理论界进行了热烈讨论,尽管在一些方面存在分歧甚至对立,但还是在一些领域取得了一些共识。

从理论上讲,网络威慑理论研究,与美国目前正在着手进行的太空威慑理论、对恐怖分子进行威慑等理论研究,形成了美国的第四波威慑理论研究的重点,扩大了传统威慑理论研究的范围。从研讨的行为体上讲,目前的网络威慑理论集中探讨如何威慑国家行为体,较少涉及对非国家行为体如恐怖分子的威慑研究,即使在讨论如何威慑国家行为体而言,美国理论界也没有区分不同网络实力的对手,而试图一劳永逸用同样的网络实力威慑所有国家行为体。[②] 诚如美国学者所言,网络威慑不能预防所有的网络威胁与攻击;不能像核、常规威慑那样保护美国。[③]因此,如前所述,网络威慑理论是美国几个威慑理论中最薄弱的一个。但是,美国所进行的网络威慑理论研究无疑是在落实美国军方要求扩大威慑理论运用范围的政策,丰富了小布什政府时期所提出的"量体裁衣威慑"(tailored deterrence)理论,或者说网络威慑理论是"量体裁衣威慑"的一个领域。实际上,网络威慑的效果不可能达到核领域的水平,但这或许不是一件坏事:核威慑如此有效,因为成本巨大,如果威慑失败,相互确保摧毁就意味着共同毁灭。因此,美国战略与国际研究中心的韦纳(Sarah Weiner)就认为,尽管不能慑止低水平的网络攻击事件,但是这意味着网

---

① Charles E. Croom, Jr., "Guarding Cyberspace Global Network Operations," *Joint Force Quarterly*, No. 46, 3rd Quarter, July 2007, p. 69.

② 何奇松:《近年美国网络威慑理论研究探析》,《现代国际关系》2012 年第 10 期,第 30 页。

③ Jonathan Solomon, "Cyberdeterrence between Nation-States: Plausible Strategy or a Pipe Dream?" *Strategic Studies Quarterly*, Spring 2011, p. 24。例如,佐治亚技术研究所的杰夫·莫尔顿(Jeff Moulton)说,一个无赖国家不守规矩,美国通过在该地区部署一艘航空母舰,展示肌肉,可以慑止该国进行不可接受的行为。但是,在数字领域如何做呢?向该国工业控制系统中打几枪,也就是发起有限的分布式拒止服务攻击,会产生展示钢铁肌肉的同样效果吗?参见 Zachary Y. Fryer-Biggs, "U. S. Cyber Experts: Deterrence Not Enough," October. 21, 2012, http://www.defensenews.com/article/20121021/DEFREG02/310210001/U-S-Cyber-Experts-Deterrence-Not-Enough,2013-01-12。

络武器施加的威胁低于由其他历史性军事技术革命所产生的风险。因此,从总体上讲,网络威慑还是一个值得接受的交易。[①]也许,随着美国对特定行为体、特定的网络行为的网络威慑理论研究取得进展,美国的网络威慑理论研究将会取得较大理论成果。

根据美国理论界讨论的成果,美国国务院和国防部正式提出网络威慑战略,并且根据理论界的建议构建网络威慑体系。值得一提的是,2012 年 9 月,美国国务院首席法律顾问高洪柱(Harold Koh)在美军网络司令部于米德堡召开的一次会议上说,某些网络袭击等同于"使用武力",根据《联合国宪章》,一国有权进行自卫。这就意味着,一旦美国受到网络武器的袭击,它可以使用常规军事力量或网络武器进行反击。美国海军军事学院国际法系主任施米特认为,美国政府法律顾问站出来明确表示国际法适用于这一领域具有重要意义,表态的时机也十分重要。[②]究其实质,就是为美国对敌国的网络进攻进行惩罚报复的网络威慑张本。

党的十八大报告中强调我们要从战略高度确保包括网络安全在内的三个领域的安全。这是针对现实而提出的重大战略性问题。我国各行各业计算机网络,尤其是我军网站,每天都遭受外国网络侵扰,我国的网络安全面临着来自外部的巨大威胁与挑战。因此,我们也应该探讨、并形成具有我国特色、行之有效的网络威慑理论,构建我们的网络安全体系,并利用网络技术与能力,提高我军以打赢信息化条件下局部战争能力为核心的多样化军事任务能力。

---

① Sarah Weiner, "Searching for Cyber-Deterrence," November 26, 2012. http://csis.org/blog/searching-cyber-deterrence, 2013-01-15.

② Aram Roston, "U.S.: Laws of War Apply to Cyber Attacks," 18 September, 2012, http://www.defensenews.com/article/20120918/DEFREG02/309180012/U-S-Laws-War-Apply-Cyber-Attacks.