论网络胁迫成功的条件

刘子夜

【内容提要】 网络空间成为继海洋、陆地、天空、太空后的“第五战场”，网络武器能否发挥政治作用？网络胁迫能否成功，其成功的条件有哪些？国际关系研究者和政策制定者对此高度关注并展开了激烈讨论。然而，现有研究主要存在两点不足：一种观点认为，网络武器溯源难、易扩散、无法直接造成人员伤亡的特性限制了胁迫效果，但该观点无法对成功案例做出解释；另一种观点认为，对同一目标反复发动网络攻击或者发动可以造成巨额经济损失的网络攻击有助于胁迫成功，但该观点经不起推敲和事实检验。经验证据表明，能够损害决策者个人利益的网络胁迫最容易成功，即运用网络武器搜集有关决策者的丑闻并以之相威胁，决策者为保全个人利益不惜牺牲集体利益，被迫做出妥协。如此一来，网络胁迫成功的条件和机制得以明晰。该假设既适用于国家，也适用于非国家行为体，弥补了传统胁迫理论以国家为中心的局限与不足，是胁迫理论在信息时代下的发展和延伸。

【关键词】 网络胁迫　网络威慑　网络攻击　胁迫理论

【作者简介】 刘子夜，清华大学国际关系学系博士生。
电子邮箱：liu-zy16@mails.tsinghua.edu.cn

1832年，卡尔·冯·克劳塞维茨(Carl von Clausewitz)在《战争论》(*On War*)中写道：“战争是政治通过另一种手段的延续。”[①] 战争的根本目的并非杀戮，而是迫使敌人屈服。188年后的今天，网络空间已成为继海洋、陆地、

① Carl von Clausewitz, *On War*, trans. by Michael Howard and Peter Paret (Princeton: Princeton University Press, 1986), p. 87.

天空、太天后的“第五战场”。[①] 令人不安的是，全世界只有 9 个国家公开宣称拥有核武器，却有超过 140 个国家已经掌握或正在研发网络武器，其中近 30 个国家正式组建网络部队。[②] 此外，跨国犯罪集团、恐怖组织、黑客等非国家行为体同样具备不可小觑的网络攻击能力。“权力寓于环境”[③]，网络空间已成为国际权力寓居的新环境。网络武器能否像核武器那样强迫他国改变行为——网络胁迫能否成功？这是近年来国际关系研究者和政策制定者关心并激烈争论的议题之一。

一、网络胁迫的争论

传统胁迫理论认为，胁迫成功需要满足可信性（credibility）、保证（assurance）和成本收益核算三个条件。关于网络胁迫[④]能否成功，学界目前存在两种竞争性观点：一种观点认为，网络胁迫难以满足胁迫成功的必要条件，因此无法发挥胁迫作用；另一种观点认为，网络胁迫在特殊条件下能够满足上述条件，从而取得成功。本节将对上述观点进行梳理和回顾。

（一）可信性

传统胁迫理论认为，胁迫成功的第一个必要条件是可信性，即胁迫者有能力并且有决心实施胁迫[⑤]，劳伦斯·弗里德曼（Lawrence Freedman）将其

---

① David C. Gompert and Martin Libicki, “Cyber Warfare and Sino-American Crisis Instability,” *Survival*, Vol. 56, No. 4, 2014, p. 18.

② Emilio Iasiello, “Is Cyber Deterrence an Illusory Course of Action?” *Journal of Strategic Security*, Vol. 7, No. 1, 2014, p. 54.

③ Joseph S. Nye Jr., “Cyber Power,” paper delivered to Belfer Center for Science and International Affairs, sponsored by the Harvard Kennedy School, Cambridge, Massachusetts, May, 2010, p. 1.

④ 本文中的网络胁迫包括网络威慑和网络驱使，详见本文第二节“网络胁迫的界定”。

⑤ Vesna Danilovic, “The Sources of Threat Credibility in Extended Deterrence,” *Journal of Conflict Resolution*, Vol. 46, No. 3, 2001, pp. 341-369.

称为胁迫“魔术般的原材料”(magic ingredient)①。

胁迫的可信性离不开胁迫能力。爱德华·劳勒(Edward Lawler)等将“胁迫能力”定义为“胁迫者可能对被胁迫者造成最大伤害的程度”②。如果能力不足,无论决心多么坚定,胁迫都将失败。同核能力相比,网络胁迫能力的评估要困难得多。约瑟夫·奈(Joseph S. Nye Jr.)指出,网络武器无法像核武器那样估算其数量和当量。③ 有时,网络实力同国家实力并不一致,大国在占据更多网络资源的同时也更容易遭受网络攻击。④ 基尔·利伯(Keir Lieber)据此认为,准确衡量一国的网络实力在现阶段根本无法实现。⑤ 艾丽卡·克雷默·姆布拉(Erika Kraemer-Mbula)等提出,经验丰富且富有创造力的技术人员完全可以使用简易电子信息设备发动复杂的网络攻击⑥,但人力资源难以得到客观量化。

有能力实施胁迫不等于有决心实施胁迫。乔纳森·默瑟(Jonathan Mercer)将“决心”(resolve)定义为“一国为实现其目标而甘愿承担战争风险的程度”⑦,决心越坚定,对战争成本的耐受力也就越强。不同于军事实力、经济实力等有形属性,决心无法直接观察,被胁迫者很难判断胁迫究竟是虚张声

---

① Lawrence Freedman, *The Evolution of Nuclear Strategy* (London: Macmillan, 1989), p. 96.

② Edward J. Lawler et al., “Coercive Capability in Conflict: A Test of Bilateral Deterrence Versus Conflict Spiral Theory,” *Social Psychology Quarterly*, Vol. 51, No. 2, 1988, p. 93.

③ Joseph S. Nye Jr., “Deterrence and Dissuasion in Cyberspace,” *International Security*, Vol. 41, No. 3, 2017, p. 61.

④ Joseph S. Nye Jr., “From Bombs to Bytes: Can Our Nuclear History Inform Our Cyber Future?” *Bulletin of the Atomic Scientists*, Vol. 69, No. 5, 2013, p. 9.

⑤ Keir Lieber, “The Offense-Defense Balance and Cyber Warfare,” in Emily Goldman and John Arquilla, eds., *Cyber Analogies* (California: Naval Postgraduate School, 2014), p. 103.

⑥ Erika Kraemer-Mbula et al., “The Cybercrime Ecosystem: Online Innovation in the Shadows?” *Technological Forecasting and Social Change*, Vol. 80, No. 3, 2013, p. 548.

⑦ Jonathan Mercer, *Reputation and International Politics* (New York: Cornell University Press, 1996), p. 1.

势，还是毅然决然。[①] 为解决这一困境，可以诉诸“昂贵信号”(costly signals)。

“昂贵信号”指做出特定行为或姿态的代价足够高昂，只有决心坚定的行为体才甘愿付出这样的代价。[②] 詹姆斯·费伦(James Fearon)将释放昂贵信号的具体策略概括为“沉没成本”(sink costs)和“自缚双手”(tie hands)两种：“沉没成本”指国家首先实施代价高昂但不影响对抗结果的行为，如军队调动、军事演习等，只有决心坚定的国家才不惜预支成本。“自缚双手”指领导人公开发出威胁，如果未来承诺无法兑现，领导人的威望将严重受损。尽管这两种策略的属性不同，“沉没成本”属于“事前”(ex ante)成本，“自缚双手”属于“事后”(ex post)成本，但二者都是为了影响或操纵对于决心的心理感知。[③]

然而，昂贵信号在互联网领域缺乏有效性和可行性。首先，自缚双手策略并不可行。埃里克·加兹克(Erik Gartzke)认为，网络武器“使用则能力减损”(use and lose capabilities)[④]，公开发出网络威胁会让对方有所防备，影响胁迫效果。何奇松也指出，网络武器一旦展示，对手就有了破解机会。[⑤] 其次，沉没成本策略容易造成误判。艾丽卡·博尔加德(Erica Borghard)和肖恩·洛纳根(Shawn Lonergan)认为，运用不同技术发动网络攻击，其实施成本差异巨大。[⑥] 胁迫者可以通过预先发动网络攻击向对方展示决心，攻击成本越高，决心越大。可问题在于，攻击者只能运用已经掌握的技术手段发动网络攻击，已掌握的技术手段不等于理想的技术手段。换言之，低成本的网络攻击并不一定意味着决心不坚定，这也可能是攻击者在特定时期内唯

---

① Joshua D. Kertzer, *Resolve in International Politics* (Princeton: Princeton University Press, 2016), pp. 148-149.

② James D. Fearon, “Signaling Foreign Policy Interests: Tying Hands Versus Sinking Costs,” *Journal of Conflict Resolution*, Vol. 41, No. 1, 1997, p. 69.

③ Keren Yarhi-Milo et al., “Tying Hands, Sinking Costs, and Leader Attributes,” *Journal of Conflict Resolution*, Vol. 62, No. 10, 2018, p. 2153.

④ Erik Gartzke, “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth,” *International Security*, Vol. 38, No. 2, 2013, p. 60.

⑤ 何奇松：《美国网络威慑理论之争》，《国际政治研究》2013年第2期，第60页。

⑥ Erica D. Borghard and Shawn W. Lonergan, “The Logic of Coercion in Cyberspace,” *Security Studies*, Vol. 26, No. 3, 2017, pp. 452-481.

一的技术选择。

也有学者认为,网络胁迫在特殊条件下具备可信性。帕特里克·摩根(Patrick Morgan)根据以色列对哈马斯和黎巴嫩真主党的胁迫策略提出,在一段时间内对同一目标反复发动网络攻击可以提升"沉没成本",从而增强网络胁迫的可信性。[①] 但摩根忽视了一点,反复发动网络攻击容易引起目标警觉,一旦目标采取应对措施修补相关漏洞,将对后续胁迫无所畏惧。

(二)保证

胁迫成功的第二个必要条件是保证[②],胁迫者必须承诺不再伤害屈服者。"保证"这一概念最早由托马斯·谢林(Thomas C. Schelling)提出:"'再向前走一步我就开枪了',其隐含的保证是'如果现在停下脚步,我将不会开枪'。"[③]作为胁迫的补偿策略,保证对胁迫而言至关重要。理查德·勒博(Richard Lebow)认为,保证并非来自公开威胁,而是胁迫者对威胁的一种自我克制,旨在降低被胁迫者的恐惧和误解,避免冲突升级为战争。[④] 然而,保证在互联网领域难以奏效。

首先,网络武器的易传播性和不可控性不利于胁迫者自我克制。何奇松指出,防止核扩散的关键在于限制核材料扩散,但网络武器的构成材料是字节(byte),不可能像核材料那样得到有效控制。[⑤] 约书亚·莱德伯格(Joshua Lederberg)将网络武器类比为生物武器[⑥],二者同属于非传统武器,

---

① Patrick M. Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," National Research Council, eds., *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy* (Washington, D.C.: National Academies Press, 2010), p. 56.

② 有时也被称作"再保证"(reassurance)。

③ Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966), p. 74.

④ Richard Ned Lebow, "Deterrence and Reassurance: Lessons from the Cold War," *Global Dialogue*, Vol. 3, No. 4, 2001, p. 119.

⑤ 何奇松:《美国网络威慑理论之争》,《国际政治研究》2013年第2期,第61页。

⑥ Joshua Lederberg, *Biological Weapons: Limiting the Threat* (Cambridge: MIT Press, 1999), p. 351.

二者的杀伤力都不容轻视，二者都有可能违背使用者本意而发生大规模扩散。网络武器的易传播性和不可控性很难使被胁迫者相信自己屈服后能免遭伤害。尤其当被胁迫者的网络实力弱于胁迫者时，盲目相信胁迫者的保证无异于自杀。

其次，网络攻击同传统军事行为相比更具隐蔽性，胁迫者的进攻优势使其不具备信守承诺的动机。约翰·罗林斯(John Rollins)发现，网络攻击的受害者经常误认为自己没有遭受攻击，正如“骤雨”(Titan Rain)行动在事后数月才被受害者察觉。① 史蒂芬·毕德尔(Stephen Biddle)根据攻防理论推断，“网络空间中攻击占优”。② 网络攻击的多样性、分散性和机动性得益于网络的“互联”属性，网络防御反而需要阻断“互联”，这与信息技术的根本属性相违背。发动攻击要比停止或限制攻击容易得多，因此胁迫者根本没有信守承诺的动机。

最后，威尔·古德曼(Will Goodman)认为，国际法和国际规范尚未明确界定网络空间中可接受及不可接受的行为，即使一国遵守相关法律法规不发动攻击也无法确保该国不会成为他国网络攻击的目标。③ 正如郎平所言，“国际社会对于网络空间的治理正处于学习阶段”④，至今尚未建立起完善可行的网络规范和安全机制，这使网络胁迫者做出保证难上加难。

不过也有学者认为，网络胁迫者能够提供保证。其一，网络攻击的高门槛有助于胁迫者自我克制。沈逸和江天骄认为，实施能够危害国家安全的网络攻击，其难度远比预想得要高。⑤ 破坏数据甚至造成物理损害的网络攻击在实施难度上远高于侦察、干扰和窃取信息的网络攻击，这使胁迫者不会轻易发动大规模网络攻击。但两位学者忽视了一点，能够破坏数据甚至造

---

① John Rollins, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues, 2007* (Washington, D.C.: Congressional Research Service, 2007), p.14.

② Stephen Biddle, “Rebuilding the Foundations of Offense-Defense Theory,” *The Journal of Politics*, Vol.63, No.3, 2001, pp.741-774.

③ Will Goodman, “Cyber Deterrence: Tougher in Theory than in Practice?” *Strategic Studies Quarterly*, Vol.4, No.3, 2010, p.120.

④ 郎平：《网络空间国际秩序的形成机制》，《国际政治科学》2018年第1期，第28页。

⑤ 沈逸、江天骄：《网络空间的攻防平衡与网络威慑的构建》，《世界经济与政治》2018年第2期，第55页。

成物理伤害的网络攻击离不开侦察、干扰和情报搜集,这两种网络攻击类型在实践中很难明确区分。

其二,网络攻击中进攻并不总是占优,当防御占优时,胁迫者更有可能信守承诺。埃里克·加兹克(Erik Gartzke)和乔恩·林赛(Jon Lindsay)的研究显示,网络领域的攻防具有"确保相互欺骗"(mutually assured deception)的特征,攻击者可以伪造身份,防止事后追责和报复;防御者也可以故意设置诱饵或散布虚假信息,引攻击者误入歧途。可见,当面对低风险、低收益的目标时,攻击占优;当面对高风险、高收益的目标时,防御占优。① 有时,胁迫者并非不想伤害屈服者,而是不能继续施加伤害。加兹克和林赛误把"欺骗"当作网络攻防的固有属性,虽然网络空间具有虚拟性,但不是所有的信息和数据都可以伪造,况且攻击者和防御者同样具备识别真伪的能力。

(三)成本收益核算

胁迫成功的第三个必要条件是成本收益核算,只有当被胁迫者的抵抗成本高于屈服成本或抵抗收益低于屈服收益时,胁迫才有可能成功。② 克里斯托弗·怀特(Christopher Whyte)将网络胁迫的实施策略分为"网络惩罚"(cyber punishment)和"网络拒止"(cyber denial)两类:前者旨在增加被胁迫者的抵抗成本,后者旨在降低被胁迫者的抵抗收益。③ 这两种策略既可以针对民用目标,也可以针对军事目标,但本质上都是通过操纵对方对成本收益的心理感知来改变其行为。

但网络惩罚和网络拒止在实践中很难奏效。托马斯·里德(Thomas Rid)指出:"历史上没有一次网络攻击曾剥夺人类生命;没有一次网络攻击

---

① Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies*, Vol. 24, No. 2, 2015, pp. 343-345.

② Robert Jervis, "The Political Effects of Nuclear Weapons: A Comment," *International Security*, Vol. 13, No. 2, 1988, pp. 80-90.

③ Christopher Whyte, "Ending Cyber Coercion: Computer Network Attack, Exploitation and the Case of North Korea," *Comparative Strategy*, Vol. 35, No. 2, 2016, p. 96.

曾造成人身伤害;没有一次网络攻击曾摧毁过哪怕一座建筑物。”[①]网络攻击不能直接造成人员伤亡,这使网络惩罚无法让被胁迫者付出难以承受的抵抗成本。此外,网络攻击所造成的伤害通常是暂时的,网络拒止不能有效降低抵抗收益。罗杰·巴纳特(Roger Barnett)认为,数字信息可以无限复制,即使重要数据被恶意删除,也可以通过备份找回。[②]

也有学者对此持反对意见。艾丽卡·博尔加德(Erica Borghard)和肖恩·隆尔根(Shawn Lonergan)认为,胁迫者与被胁迫者都需要进行成本收益核算,胁迫者希望以最小代价获得最大收益。[③] 相较于传统胁迫手段,网络胁迫廉价、迅速、便捷的特征使其成为决策者钟爱的选项,但他们未能改变网络胁迫惩罚和拒止能力不足的本质。

托马斯·杜本德弗(Thomas Dubendorfer)、阿诺·瓦格纳(Arno Wagner)等学者认为,大规模网络攻击可以给目标带来巨额经济损失。[④] 特拉维斯·夏普(Travis Sharp)在此基础上构建出经济和领导力模型,认为网络胁迫带来经济损失的同时还会动摇目标的领导力,从而达到胁迫目的。[⑤]但夏普的观点不仅与事实不符,也未能揭示胁迫成功的内在机制。

(四)待解决的问题

综上,支持上述传统胁迫理论的意见经不起推敲和事实检验;反对者的

---

① Thomas Rid, “Cyber War Will Not Take Place,” *Journal of Strategic Studies*, Vol. 35, No. 1, 2012, p. 11.

② Roger W. Barnett, “Information Operations, Deterrence, and the Use of Force,” *Naval War College Review*, Vol. 51, No. 2, 1998, p. 11.

③ Erica D. Borghard and Shawn W. Lonergan, “The Logic of Coercion in Cyberspace,” *Security Studies*, Vol. 26, No. 3, 2017, pp. 460-461.

④ Thomas Dubendorfer, Arno Wagner and Bernhard Plattner, “An Economic Damage Model for Large-Scale Internet Attacks,” paper delivered to *IEEE 13th International Workshops on Enabling Technologies*, sponsored by the Infrastructure for Collaborative Enterprises, Morgantown, West Virginia, June 14-16, 2004, p. 223.

⑤ Travis Sharp, “Theorizing Cyber Coercion: The 2014 North Korean Operation Against Sony,” *Journal of Strategic Studies*, Vol. 40, No. 7, 2017, pp. 898-926.

意见可以解释网络胁迫为何失败,但无法解释网络胁迫为何成功。具体而言,网络胁迫的相关研究存在以下四点不足。

第一,概念界定不一致。一部分学者严格区分“胁迫”(coercion)和“威慑”(deterrence),认为前者旨在改变现状,后者旨在维持现状。另一部分学者坚信,胁迫包含驱使(compellence)[①]和威慑,前者强迫对方去做某事,后者强迫对方不要做某事。作为胁迫的两种表现形式,驱使和威慑犹如硬币的正反两面,其共性远大于个性。概念模糊导致相关研究自说自话,研究结论相互矛盾。

第二,研究领域过于宽泛。核威慑研究只针对核武器,网络胁迫研究则反其道而行之。这里的“网络”泛指整个互联网领域,研究对象为该领域中的所有胁迫行为,这无疑削弱了研究的针对性和说服力。

第三,胁迫成功的判定标准不统一。一部分学者将胁迫结果两分为成功与失败,此举完全排除了胁迫部分成功的可能性。另一些学者将胁迫结果视作一个渐变“光谱”,胁迫成功或失败的程度取决于胁迫者要求被满足的程度。判定标准不统一造成一个研究中的成功案例在另一个研究中反而被当作失败案例。有的判定标准过于严格造成没有成功案例可用,致使研究假设无法进行实证检验。

第四,局限于“国家中心论”。受冷战影响,传统胁迫理论以国家为中心,网络胁迫研究继承了这一特色,将国家(尤其是美国)的网络胁迫行为作为主要研究对象,这一点在国内学者的研究中尤为突出。不同于冷战时期的国际环境,互联网领域呈现出新特征:一方面,国家无法垄断网络空间的控制权;另一方面,商业实体、IT 创业者、非营利组织等非国家行为体的影响力日益凸显。“国家中心论”不免以偏概全,网络胁迫研究至今尚未建立起同时适用于国家和非国家行为体的理论框架。

二、网络胁迫的界定

冷战的兴起、发展与消亡助推了胁迫理论的发展,20 世纪 40 年代末的

① “compellence”应该翻译成“驱使”,参见:李彬:《中美对“核威慑”理解的差异》,《世界经济与政治》2014 年第 2 期,第 8 页。

学者及政策制定者在随后40年间将目光聚焦在威慑上，苏联解体则使他们的关注点开始从威慑转向胁迫。[①] 早在1966年，谢林就对胁迫的两种表现形式——威慑和驱使——进行了区分，前者“诱导对方不作为”，后者“强迫对方行动”。[②] 美、苏核力量势均力敌后，威慑研究迈入黄金时代，包括罗伯特·杰维斯(Robert Jervis)、巴里·布赞(Barry Buzan)、格伦·斯奈德(Glenn Snyder)和伯纳德·布罗迪(Bernard Brodie)在内的一批学者主张，威慑不应作为胁迫的子类，而是与胁迫并列的概念，或至少是胁迫的主要表现形式。[③] 直到20世纪90年代下半叶，亚历山大·乔治(Alexander George)、威廉·西蒙斯(William Simons)和劳伦斯·弗里德曼(Lawrence Freedman)才主张给予驱使应有的重视。[④]

苏联解体后，核武器在对外政策中的效用日益降低，学界开始逐渐意识到威慑同驱使之间存在共性。保罗·劳伦(Paul Lauren)指出，威慑和驱使都要利用威胁(threats)，其目的并非在物理上伤害对方，而是谋求影响对方意志，因此威慑者和驱使者必须要让对方相信自己“有决心和能力对对方关切的事物施以巨大伤害”。[⑤] 无论是威慑还是驱使，本质上都是操纵对方对于抵抗风险的感知，从而影响对方行为。这样一来，威慑和驱使便基于相同假定展开。

---

① Maria Sperandei, “Bridging Deterrence and Compellence: An Alternative Approach to the Study of Coercive Diplomacy,” *International Studies Review*, Vol. 8, No. 2, 2006, p. 253.

② Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966), p. 175.

③ 参见：Robert Jervis, “Deterrence Theory Revisited,” *World Politics*, Vol. 31, No. 2, 1979, pp. 289-324; Barry Buzan, *An Introduction to Strategic Studies: Military Technology and International Relations* (UK: Macmillan Press, 1987); Glenn H. Snyder, “Deterrence and Power,” *Journal of Conflict Resolution*, Vol. 4, No. 2, 1960, pp. 163-178; Bernard Brodie, *The Absolute Weapon* (New York: Harcourt Brace, 1946).

④ 参见：Alexander L. George and William E. Simons, *The Limits of Coercive Diplomacy: Laos, Cuba, Vietnam* (Boston: Little Brown, 1971); Lawrence Freedman, *Strategic Coercion: Concepts and Cases* (Oxford: Oxford University Press, 1998).

⑤ Paul Lauren, *Diplomacy: New Approaches in History, Theory, and Policy* (New York: Free Press, 1979), p. 193.

既然威慑和驱使是具有相同特征的理论,二者并列但根本对立的观点便开始动摇,有关具体案例归属问题的争论更是加剧了这一趋势。有时,威慑和驱使之间的差异会在实践中得到弥合。弗里德曼注意到,古巴导弹危机期间美国一边要求苏联立刻停止部署导弹(驱使),一边又警告苏联不要试图突破美国的海上封锁(威慑)。① 丹尼尔·拜曼(Daniel Byman)和马修·韦克斯曼(Matthew Waxman)发现,伊拉克出兵科威特后,美国的警告是威慑和驱使的综合体,不仅包括"不要入侵科威特",还包括"从科威特撤军"。② 此外,大卫·鲍德温(David Baldwin)认为:"从语义出发,任何威慑都可以用驱使术语表述;同理,任何驱使也可以用威慑术语表述。"③"不要再向前走了"既可以理解成"停止当前行为(驱使)",也可以理解成"避免在未来采取行动(威慑)"。罗伯特·奥特(Robert Art)和帕特里克·克罗宁(Patrick M. Cronin)进一步指出,"现状"(status quo)在施动方和被动方眼中是不同的,威慑者认为自己是在维持现状,却可能将目标方的回应视作改变现状。④

受此影响,网络胁迫存在两种竞争性定义。一类定义认为网络胁迫与网络威慑截然不同、根本对立,比如昆汀·霍奇森(Quentin E. Hodgson)将网络胁迫定义为"利用网络能力(cyber capabilities)驱使对手做出通常不希望做出的行动"。⑤ 另一种定义则认为网络胁迫包括网络威慑和网络驱使两种表现形式,比如克林顿·伍兹(Clinton M. Woods)就将网络胁迫定义成"通过网络武器,使用或威胁使用网络力量(cyber force)迫使对手采取特定行动或阻止对手采取行动"。⑥ 然而,这两种定义方式均存在缺陷:一方面,

---

① Lawrence Freedman, *Deterrence* (Cambridge: Polity Press, 2004), p. 111.

② Daniel Byman and Matthew C. Waxman, *Confronting Iraq: US Policy and the Use of Force Since the Gulf War* (California: Rand Corporation, 2000), pp. 5-12.

③ David A. Baldwin, "Power Analysis and World Politics: New Trends Versus Old Tendencies," *World Politics*, Vol. 31, No. 2, 1979, p. 192.

④ Robert J. Art and Patrick M. Cronin, *The United States and Coercive Diplomacy* (Washington: US Institute of Peace Press, 2003), p. 4.

⑤ Quentin E. Hodgson, "Understanding and Countering Cyber Coercion," paper delivered to 10*th International Conference on Cyber Conflict*, Tallinn, May 29-June 1, 2018, p. 73.

⑥ Clinton M. Woods, *Implementing Cyber Coercion*, Master's Thesis, Naval Postgraduate School, 2015, p. 7.

参与网络胁迫的行为体并不明确，行为体究竟是国家还是非国家，抑或二者兼而有之，上述定义没有说明；另一方面，网络胁迫涉及的其他概念诸如“网络能力”和“网络力量”同样是模糊的。更为重要的是，上述定义没有给出胁迫成功的可操作性判断标准。

事实上，网络胁迫的目的既包括阻止对手做出某种行为，也包括强迫对手采取特定行动，所涉及的行为体不仅有国家，还有跨国公司、黑客组织、个人等非国家行为体。威慑和驱使正如硬币的正反两面，我们不能只关注其中一面，而忽视另一面。

为弥补上述缺陷和不足，本文对“网络胁迫”定义如下：网络胁迫指胁迫者利用网络武器[①]强迫被胁迫者采取特定行为（网络驱使）或不要做出某种行为（网络威慑），见图 1。这里的胁迫者和被胁迫者既可以是国家，也可以是非国家行为体。网络胁迫成功与否取决于胁迫者要求被满足的程度：胁迫者要求被满足的程度越高，胁迫结果就越倾向于“成功”；胁迫者要求被满足的程度越低，胁迫结果则越倾向于“失败”。

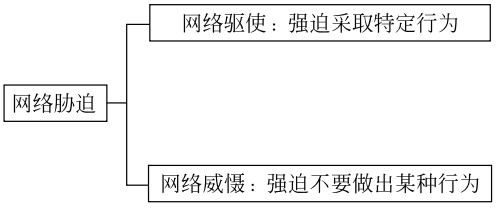

图 1　网络胁迫概念内涵示意图

值得注意的是，以下三种情况不属于网络胁迫：首先，网络胁迫不应与传统军事行动相结合，否则将难以追溯胁迫成功的具体原因。其次，网络胁迫本质上是利用威胁影响对方行为，因此网络间谍行为和盗窃行为不属于网络胁迫。最后，胁迫者的身份和意图必须明确，即被胁迫者必须知晓谁在胁迫以及为何胁迫。胁迫的根本目的是让被胁迫者按照胁迫者的要求行事。当胁迫者身份不明时，被胁迫者将失去反抗或屈服的对象，毕竟反抗或屈服无法作用于无名氏。另外，当胁迫者的意图不明时，被胁迫者难以按照

① 网络武器指能够对目标信息系统、网络、计算机及电子信息设备软硬件进行操纵、禁止访问、扰乱、降级、破坏或窃取信息的恶意代码或程序。

胁迫者的要求改变自身行为,因为根本不知道哪种行为需要改变或改变到何种程度。

三、网络胁迫的特殊性

网络胁迫具有特殊性。虽然胁迫是强迫对方违背自身意愿改变行为,但网络胁迫与核胁迫(包括核威慑和核驱使)在作用对象和适用范围上并不一致。核胁迫的作用对象通常是国家,主要目的是防止有核国家之间爆发直接战争或阻止冲突进一步升级。相较于核胁迫,网络胁迫的对象和适用范围要宽泛得多,从威胁娱乐公司不要上映侮辱领袖的电影到逼迫一国放弃核计划,网络胁迫作用的对象既可以是国家,也可以是跨国公司、新闻媒体、个人等非国家行为体。

造成上述差异的根本原因在于网络武器与核武器的属性存在本质区别。网络武器离不开传播方式(propagation method)、漏洞利用(vulnerability exploits)和有效负载(payload)三个构成要素。[①] 传播方式指网络武器传递到特定目标的途径和方法;漏洞利用指网络武器的传播和生效需要借助目标系统或应用中的特定漏洞才能实现;有效负载指网络武器的设计目的,如删除数据、远程操控、破坏计算机硬件等。

网络武器拥有核武器所不具备的特殊属性。首先,网络武器的使用者可以选择是否主动暴露自己的身份,但核武器无法做到这一点。网络武器本质上是一段代码,理论上任何网络行为体都有可能获取并使用它。具备一定技术资质的使用者可以自行研发网络武器,技术实力较弱的使用者则可以修改已有代码从而创制出衍生性网络武器。网络武器获取和使用的低门槛能让使用者长期保持匿名,除非其威胁足够巨大,否则没有必要也无须耗费庞大资源对网络攻击溯源。但在特殊情况下,网络武器的使用者会主动放弃隐藏策略,通过暗示或明示的方式暴露身份,比如为了表达不满和抗议,攻击者往往选择明示身份。核武器则不同,其获取和使用的门槛很高。

---

① Trey Herr, "PrEP: A Framework for Malware & Cyber Weapons," *Journal of Information Warfare*, Vol. 13, No. 1, 2014, pp. 87-106.

研发核武器不仅要有雄厚的工业基础和庞大的科研团队作为支撑，还要不断进行试验才有可能成功。即使破除万难拥有了核武器，“核禁忌”也使有核国家不敢轻易使用。况且对弹道导弹进行追踪和定位可在短时间内确定攻击者身份，核武器的使用者不可能匿名，自然不存在主动暴露身份一说。

其次，网络武器具有可订制性和隐蔽性，核武器则属于大规模杀伤性武器。可订制性指网络武器可以针对特定目标实施精确打击，比如“巫师行动”(Operation WizardOpium)所使用的恶意代码只对 78.0.3904.87 版本谷歌浏览器的 CVE-2019-13720 漏洞有效[①]；隐蔽性一方面指网络武器的具体功能和效力隐蔽，另一方面指网络武器的使用隐蔽。单纯从代码本身很难判断网络武器的功能和作用，2012 年日本防卫省委托富士通公司(Fujitsu)研发一种可以发现受感染计算机并对其进行“清扫”的病毒[②]，即用来反病毒的病毒。该病毒满足一般计算机病毒的一切特征，但它的最终目的却是帮助日本政府抵御网络攻击。核武器的功能则毋庸赘言，核弹头当量和弹道导弹射程都可以进行较为准确的评估。另外，网络武器的使用可以避开公众视野，只有攻击者和被攻击者了解详情。核武器既无法用以实施精确打击，也无法对公众进行隐瞒，没有国家能够对特定目标秘密实施核打击。

再次，网络武器无法直接造成人员伤亡，核武器恰好相反。网络武器的作用对象是数字信息或电子设备，数字信息的可复制性使其即使遭受攻击，也可以在短时间内恢复正常，电子设备的损坏一般也不会对人身造成伤害。核武器对人员和基础设施的破坏则是永久且不可逆的，正如马丁·利比奇(Martin Libicki)所言：“网络战最多让 GDP 跌落到 20 世纪 90 年代的水平，

---

① AMR and GReAT, “Chrome 0-Day Exploit CVE-2019-13720 Used in Operation WizardOpium,” *Kaspersky*, November 1, 2019, https://securelist.com/chrome-0-day-exploit-cve-2019-13720-used-in-operation-wizardopium/94866/, 访问时间：2019 年 11 月 9 日。

② Graham Cluley, “Why Japan's Search-and-Destroy Cyber Weapon Could Be a Very Bad Idea,” *Naked Security*, January 3, 2012, https://nakedsecurity.sophos.com/2012/01/03/japan-cyber-weapon-bad/, 访问时间：2019 年 11 月 9 日。

核战争却可以让人类社会重返石器时代。”①

最后,网络武器可用于情报搜集,核武器则不具备这一功能。网络武器必须基于特定系统或软件漏洞才能生效,因此网络武器的研发离不开情报搜集,设计者需要充分了解目标计算机的硬件配置、软件版本、系统类型甚至特定用户的使用习惯。网络武器不仅可以对目标实施干扰和破坏,还可以窃取目标计算机或移动通信设备中的重要数据与信息。由以色列科技公司NSO Group Technologies开发的间谍软件“飞马座”(Pegasus)不仅可以窃取苹果或安卓手机中的短信、电子邮件、通讯录,实时监听通话,记录网页浏览历史和按键输入内容,还可以对手机录屏。② 毫不夸张地说,一旦感染“飞马座”病毒,手机用户将没有隐私可言。

网络胁迫并未囊括互联网领域中的一切胁迫行为,而是专指利用网络武器实施的胁迫。由于武器构造及原理不同,网络武器与核武器在属性上存在巨大差异。网络武器的特殊性决定了网络胁迫的特殊性,网络胁迫成功所需要的具体条件应该有别于核胁迫。

四、网络胁迫成功的条件

本文认为,能够损害决策者个人利益的网络胁迫最容易成功。此种情况下,胁迫成功的三个必要条件——可信性、保证和成本收益核算可以同时得到满足:首先,胁迫者可以暗示或明示自己的真实身份,从而树立声誉,此举有助于增强网络胁迫的可信性。其次,网络武器的可订制性和隐蔽性有利于胁迫者做出有效保证。最后,胁迫者利用网络武器搜集被胁迫方决策者的丑闻并以之相威胁,决策者为保全个人利益,不惜牺牲集体利益满足胁迫者的要求。本节将对上述假设进行详述。

---

① Martin C. Libicki, “Cyberwar as a Confidence Game,” *Strategic Studies Quarterly*, Vol. 5, No. 1, 2011, p. 136.

② John Snow, “Pegasus: The Ultimate Spyware for IOS and Android,” *Kaspersky*, April 11, 2017, https://www.kaspersky.com/blog/pegasus-spyware/14604/, 访问时间:2019年11月9日。

（一）假设一：揭示身份有助于增强可信性

网络胁迫面临的首要难题是溯源（attribution）——“我们知道胁迫者是谁吗”？[①] 一方面，溯源有误可能导致被胁迫者向错误目标实施报复，树立新的敌人。另一方面，被胁迫者必须向第三方证明溯源的准确性和可靠性，以免牵连无辜。

溯源无效的根本原因在于网络攻击具有匿名性（anonymity），即单纯依靠技术手段很难确定攻击者的真实身份和确切位置。首先，IP 地址不足以证明攻击者的身份和地理位置，布尔伯特（W. Earl Boebert）指出：“即使找到攻击所使用的计算机，我们又如何证明攻击发生时究竟是谁在敲击键盘呢？”[②]况且，攻击者还可以采用一系列技术手段伪装或掩盖行踪，2008 年 2 月 28 日，代码托管平台 GitHub 遭受持续 8 分钟的超大规模分布式拒绝服务攻击（Distributed Denial of Service Attack，DDoS），攻击峰值时数据流量高达每秒 1.35 TB。[③] 此次攻击通过缓存服务器（memcached servers）发动，全球这样的服务器超过 10 万台，调查人员很难从中找出攻击者的真身。其次，溯源到的不一定是“主谋”，反倒有可能是“帮凶”。网络武器的获取门槛较低，国家和非国家行为体都可以研发和使用，约瑟夫·奈相信，这为利用代理人发动网络攻击创造了条件。[④] 董青岭和戴长征也认为，网络攻击“极易推卸责任或嫁祸第三方”。[⑤]

---

① Martin C. Libicki, *Cyberdeterrence and Cyberwar* (California: Rand Corporation, 2009), p. 41.

② W. Earl Boebert, “A Survey of Challenges in Attribution,” *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U. S. Policy* (Washington, D. C.: National Academies Press, 2010), p. 43.

③ Lily Hay Newman, “GitHub Survived the Biggest DDoS Attack Ever Recorded”, *WIRED*, March 1, 2018, https://www.wired.com/story/github-ddos-memcached/, 访问时间：2019 年 9 月 20 日。

④ Joseph S. Nye Jr., “Deterrence and Dissuasion in Cyberspace,” *International Security*, Vol. 41, No. 3, 2017, p. 50.

⑤ 董青岭、戴长征：《网络空间威慑：报复是否可行？》，《世界经济与政治》2012 年第 7 期，第 102 页。

其实,匿名性并非网络武器的固有属性,而是一种可供选择的攻击策略。网络武器的使用者可以根据实际需要隐藏或揭示自己的身份。当网络武器用于间谍活动或蓄意破坏时,攻击者通常隐藏身份。美国网络安全公司赛门铁克(Symantec)于 2017 年 11 月 7 日发布调查报告称,一个名叫"潮虫"(Sowbug)的黑客组织对巴西、秘鲁、阿根廷、厄瓜多尔的外交决策机构和外事部门发动网络攻击,专门搜集南美洲国家在东南亚地区的外交情报。① 该组织最早从 2015 年 5 月起开始活跃,他们行事隐秘,经常在目标网络中潜伏,有时竟长达 6 个月之久。为避免引起注意,"潮虫"将恶意代码伪装成 Windows 或 Adobe Reader 的常用文件植入目标计算机,而不会对任何正常软件造成破坏。"潮虫"甚至从不在目标国家的正常工作时间窃取信息,尽可能降低暴露风险。根据攻击方式的技术难度,赛门铁克高度怀疑"潮虫"是一个准国家黑客组织,但其真实身份不得而知。该案例中,攻击者选择隐藏身份从事网络间谍活动。

当网络武器用于胁迫时,攻击者通常会主动暴露身份,具体手段有暗示和明示两种。暗示指胁迫者以第三方名义实施胁迫,但会在代码中故意留下诸如时区、组织机构名称、自然语言符号等线索暗示身份。有时,胁迫者还会重复使用目标已知的恶意代码揭示身份。② 当然,攻击者绝不会公开承认自己与胁迫有关。这样做既可以表明身份,还可以逃避舆论谴责,摆脱道德束缚。

明示指胁迫者公开宣称对胁迫负责,此举可以赢得国内支持并积累声誉,威慑第三方。2017 年 9 月 22 日至 30 日,美军网络司令部(U. S. Army Cyber Command)对朝鲜人民军侦察总局(Reconnaissance General Bureau, RGB)发动 DDoS 攻击,警告朝鲜终止针对美国政府、基础设施和私人公司的

---

① Symantec Security Response, "Sowbug: Cyber Espionage Group Targets South American and Southeast Asian Governments," *Symantec*, November 7, 2017, https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments, 访问时间: 2019 年 9 月 20 日。

② "网络武器复用"指攻击者利用曾经使用过的网络武器发动攻击,从而达到暗示自己身份的目的。

网络活动。《华盛顿邮报》于 9 月 30 日专门就此事做出报道。[①] 有分析指出，特朗普政府出于国内政治考虑采取明示策略。在攻击发生五个星期前，特朗普签署总统令将网络司令部升级为联合作战司令部(Unified Combatant Command)，此举有助于为当局居高不下的网络战预算增强合理性，并赢得国内民众支持[②]，同时向外界释放“美国无法忍受基础设施遭受网络攻击”的信号。

胁迫者可以暗示或明示自己的身份，为树立声誉创造条件。“树立声誉”指通过一国的历史行为判断其决心。[③] 如果一国在历史上总是信守承诺，当该国发出威胁时，他国倾向于相信威胁；如果一国在过往危机中频繁退让，他国自然会怀疑其决心是否坚定。

互联网领域中，如果已知胁迫者曾发动过大规模网络攻击，其胁迫将更加可信。2010 年 9 月，印度软件公司艾普莱克斯(Aiplex Software)对民间反版权组织“海盗湾”(Pirate Bay)发动 DDoS 攻击，此举引起黑客组织“匿名者”(Anonymous)的强烈不满。随后，“匿名者”采用相同方式回击艾普莱克斯公司，迫使公司网站关停 24 小时。[④] 此举为“匿名者”树立了声誉，当其威胁美国唱片工业协会和电影协会时，没人怀疑“匿名者”是在虚张声势。“匿

---

① Karen DeYoung, “Trump Signed Presidential Directive Ordering Actions to Pressure North Korea,” *The Washington Post*, September 30, 2017, https://www.washingtonpost.com/world/national-security/trump-signed-presidential-directive-ordering-actions-to-pressure-north-korea/2017/09/30/97c6722a-a620-11e7-b14f-f41773cd5a14_story.html, 访问时间：2019 年 9 月 20 日。

② Kevin Townsendh, “U. S. Cyber Command Launched DDoS Attack Against North Korea: Report,” *Security Week*, October 2, 2017, ttps://www.securityweek.com/us-cyber-command-launched-ddos-attack-against-north-korea-report, 访问时间：2019 年 9 月 20 日。

③ Alex Weisiger and Keren Yarhi-Milo, “Revisiting Reputation: How Past Actions Matter in International Politics,” *International Organization*, Vol. 69, No. 2, 2015, p. 474.

④ BBC News, “Activists Target Recording Industry Websites,” *BBC*, September 20, 2010, https://www.bbc.com/news/technology-11371315, 访问时间：2019 年 9 月 20 日。

名者”发出“你们伪装成艺术家,其实眼中只有金钱,我们已忍无可忍”[①]的宣言后,对上述机构发动网络攻击,这又为其日后的网络活动树立了声誉。

如果在历史上曾利用网络武器窃取机密信息并爆料,则胁迫者利用丑闻进行网络胁迫的能力和决心将更加可信。2013 年 6 月,爱德华·斯诺登(Edward J. Snowden)披露“棱镜计划”(PRISM),指责美国国家安全局(NSA)从微软、雅虎、谷歌、脸书等九家互联网公司的服务器上直接搜集用户隐私。[②]“棱镜计划”曝光后,没有国家和组织怀疑美国政府的网络情报搜集能力及其利用情报“狙击”特定目标的决心。

(二)假设二:可订制性和隐蔽性有利于有效保证

传统胁迫理论认为网络胁迫无法做出有效保证的主要原因在于网络武器的易传播性和不可控性。任何新式武器在问世之初,都会遭受质疑甚至引发恐慌,网络武器也不例外。早期的计算机病毒确实容易造成大规模“感染”,这给公众留下一种刻板印象,即网络武器具有滥杀滥伤性。

实际上,网络武器同样可以用于实施精确打击。首先,网络武器能对目标发动有差别攻击。“震网”(Stuxnet)病毒曾在伊朗、印度、印度尼西亚和美国等国家被发现,但只对伊朗纳坦兹(Natanz)核设施中控制离心机运转的计算机有效,其余国家被感染设备中的病毒都处于“灭活”状态,这其实是设计者故意为之,以增强病毒靶向性。[③] 其次,设计者可以根据实际需要调整网络武器的破坏力和“杀伤”半径,避免造成过度伤害。“震网”病毒被设计成缓慢破坏离心机,而不是让所有离心机立刻瘫痪,以免引起伊朗警觉。

同普通网络攻击相比,网络胁迫的针对性更强。一方面,胁迫者、被胁

---

① Alexia Tsotsis, “RIAA Goes Offline, Joins MPAA as Latest Victim of Successful DDoS Attacks,” *TechCrunch*, September 19, 2010, https://techcrunch.com/2010/09/19/riaa-attack/, 访问时间:2019 年 9 月 20 日。

② Timothy B. Lee, “Here's Everything We Know about PRISM to Date,” *The Washington Post*, June 12, 2013, https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/, 访问时间:2019 年 9 月 20 日。

③ Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Publishers, 2014), p. 28-29.

迫者以及胁迫意图必须明确;另一方面,利用丑闻进行胁迫,只针对特定决策者或决策集团,这使网络胁迫的目标更加具体。因此,网络武器的可订制性使胁迫做出有效保证成为可能。

网络武器的另一个重要特征是隐蔽性,即网络武器的使用可以避开公众视野。胁迫者可以让决策者知晓其丑闻已被掌握,但民众对此尚不知情。实际上,网络胁迫是一种"公开的秘密"(open secret)——其保密性是相对的,不同受众对网络胁迫的知晓程度不同。① 利用丑闻进行胁迫,丑闻对决策者而言是透明的,对胁迫方和被胁迫方的民众而言却是保密的。决策者不希望丑闻公开,胁迫者也不能让丑闻公开,因为公众介入会让胁迫双方为顾及颜面不得不采取强硬立场,致使胁迫失控,甚至升级为军事冲突。

观众成本理论认为,不仅胁迫者需要支付观众成本,被胁迫者同样也要付出观众成本。胁迫者公开发出威胁的同时也限制了被胁迫者,被胁迫者在国内民众的压力下不可能轻易屈服,否则将被视为懦夫。也就是说,公开化会让被胁迫者无路可退,只能抵抗到底,否则将付出高昂的国内观众成本。② 如果胁迫秘密进行,胁迫方和被胁迫方民众对此并不知情,这样做就可以保全被胁迫者的颜面,即使被胁迫者屈服也可以借助其他理由为自己辩护,而不被视作胆小鬼,从而免除观众成本。

此外,被胁迫者基于自身利益考量,还会同胁迫者一起保守秘密,这被称作"心照不宣的合谋"(tacit collusion)。③ 1952—1953 年朝鲜战争结束,至少有 26000 名苏联军人在中国东北和朝鲜北部执行作战任务。④ "为避免冲

---

① Rory Cormac and Richard J. Aldrich, "Grey Is the New Black: Covert Action and Implausible Deniability," *International Affairs*, Vol. 94, No. 3, 2018, p. 478.

② Shuhei Kurizaki, "Efficient Secrecy: Public Versus Private Threats in Crisis Diplomacy," *American Political Science Review*, Vol. 101, No. 3, 2007, p. 543-558.

③ Austin Carson, "Facing Off and Saving Face: Covert Intervention and Escalation Management in the Korean War," *International Organization*, Vol. 70, No. 1, 2016, pp. 105-106.

④ Kathryn Weathersby, "The Soviet Role in the Early Phase of the Korean War: New Documentary Evidence," *Journal of American-East Asian Relations*, Vol. 2, No. 4, 1993, p. 438.

突升级为全面战争,莫斯科严令飞行员隐藏身份。"[①]美国早就知道苏军直接介入了朝鲜战争,令人惊奇的是,国务卿艾奇逊的顾问竟然建议政府向公众隐瞒苏联参战的事实。时任美国司法部长兼总统顾问的赫伯特·布劳内尔(Herbert Brownell)告诉历史学家乔恩·哈利迪(Jon Halliday):"我们必须把它掩藏在地毯下,否则将面临对苏开战的巨大压力。"[②]这一点同样适用于网络胁迫,为防止冲突升级,胁迫双方会达成默契,共同向公众隐瞒胁迫细节。

保证是否有效依赖于被胁迫者的心理感知,网络武器的可订制性和隐蔽性使被胁迫者相信胁迫者能够做出有效保证。在胁迫过程中,胁迫者可以避开公众视线,只让对方决策者知晓自己的丑闻已被掌握,并且保证在其屈服前不会预先曝光丑闻。由于公众对丑闻并不知情,决策者可以向胁迫者私下妥协,并借助其他理由为自己开脱,这样做既满足了胁迫者的要求,还维护了被胁迫方决策者的个人利益,更保全了决策者的颜面,可谓"一石三鸟"。

(三)假设三:以丑闻相威胁可大幅提升抵抗成本

学界普遍认为,网络胁迫无法让被胁迫者付出高昂的抵抗成本,原因在于网络武器无法直接造成人员伤亡,对目标的破坏是暂时且可逆的。网络武器的直接作用对象是数字信息和电子设备,其目的是"破坏、拒绝访问、降级和干扰"[③],网络攻击至今没有伤害人员的记录。此外,数字信息的可复制性使其即使遭受攻击,也可以在短时间内恢复正常。

如此看来,网络攻击好比"拿刀去枪战"(like bringing a knife to a gun fight)[④],很难让目标付出难以承受的抵抗成本。不过网络武器的一个重要

---

① Xiaoming Zhang, *Red Wings Over the Yalu: China, the Soviet Union, and the Air War in Korea* (Texas: A&M University Press, 2003), p. 139.

② William J. Williams, *A Revolutionary War: Korea and the Transformation of the Postwar World* (Pennsylvania: DIANE Publishing Co., 1993), p. 154.

③ *Military Cyber Operations: A Primer*, American Foreign Policy Council Defense Technology Program Brief, January 30, 2016.

④ Erik Gartzke, "Fear and War in Cyberspace," *Lawfare*, December 1, 2013, https://www.lawfareblog.com/foreign-policy-essay-erik-gartzke-fear-and-war-cyberspace, 访问时间:2019 年 9 月 20 日。

功能是搜集情报，胁迫者可以运用网络武器窃取、挖掘有关被胁迫方决策者的丑闻并以之相威胁。如果决策者不屈服，丑闻将被公开，决策者的个人名誉和形象势必受损，严重者可能因此下台并失去决策权。此种情况下，决策者为维护自身利益，更倾向于屈服。

丑闻总是同“权力、名誉和信任”[①]有关，有时甚至会断送决策者的政治生命：“水门事件”(Watergate)曝光两年后尼克松被迫下台[②]、里根因“伊朗门事件”(Iran-Contra Affair)引发美国国内强烈不满[③]、克林顿因“拉链门”(Zippergate)性丑闻成为美国历史上第二位遭受众议院弹劾的总统[④]。现代政治注重政治人物的品格，丑闻不仅能让选民对深信不疑的“正直”人物产生怀疑，还会动摇民众对政治人物所属政治团体或政治制度的信心，这种负面印象一旦形成，会对民众的政治态度和政治行为产生深远影响，并且很难在短时间内改变。[⑤]

决策者巩固决策地位的关键在于获得并维持来自下级的信任，而丑闻则在很大程度上削弱甚至摧毁这种信任。反对者或政敌还可以利用丑闻攻击涉事者，为自己在政治斗争中增加筹码。丑闻一旦曝光，决策者一方面要承受自下而上的压力，另一方面还要遭受同僚的攻击。双重压力下，决策者的执政地位很容易动摇，甚至彻底丧失决策权，这是任何决策者都不愿意看到的。

也就是说，网络武器搜集情报的特性使其可以直接威胁决策者的个人

---

① John B. Thompson, *Political Scandal: Power and Visibility in the Media Age* (New York: John Wiley & Sons, 2013), p. 241.

② Michael Schudson, “Notes on Scandal and the Watergate Legacy,” *American Behavioral Scientist*, Vol. 47, No. 9, 2004, p. 1232.

③ Richard A. Brody and Catherine R. Shapiro, “Policy Failure and Public Support: The Iran-Contra Affair and Public Assessment of President Reagan,” *Political Behavior*, Vol. 11, No. 4, 1989, p. 353.

④ Arthur H. Miller, “Sex, Politics, and Public Opinion: What Political Scientists Really Learned from the Clinton-Lewinsky Scandal,” *Political Science & Politics*, Vol. 32, No. 4, 1999, p. 721.

⑤ Norbert Schwarz and Herbert Bless, “Scandals and the Public's Trust in Politicians: Assimilation and Contrast Effects,” *Personality and Social Psychology Bulletin*, Vol. 18, No. 5, 1992, p. 577.

利益,从而放大决策者的抵抗成本,使决策者不惜牺牲集体利益来维护个人利益,向胁迫者做出妥协或让步,并按照胁迫者的要求重新做出决策。

值得注意的是,胁迫者必须提供录音、录像、照片、文件等证据,证明所获取丑闻的真实性。捏造信息或制造伪证不仅无助于胁迫成功,反而会授人以柄,为被胁迫者进行反击提供口实和帮助。

五、案例检验

本节选用五个案例验证上述假设,详见表 1。案例一为朝鲜威慑索尼公司,属于国家对非国家行为体的网络胁迫行为,取得部分成功;案例二为美国威慑俄罗斯,属于国家间的网络胁迫行为,取得完全成功;案例三是"维基解密"(WikiLeaks)驱使托克集团(Trafigura)和英国最高法院,属于非国家行为体之间及非国家行为体对国家的网络胁迫行为,取得完全成功;案例四是美军网络司令部威慑朝鲜人民军侦察总局(RGB),属于国家间的网络胁迫行为,完全失败;案例五为俄罗斯驱使爱沙尼亚政府,属于国家间的网络胁迫行为,完全失败。

表 1 案例分类表

	胁迫类型	可信性	保证	成本收益	胁迫者	被胁迫者	胁迫者类型	被胁迫者类型	胁迫结果
案例一	网络威慑	满足	不满足	满足	朝鲜	索尼公司	国家	非国家行为体	部分成功
案例二	网络威慑	满足	满足	满足	美国	俄罗斯	国家	国家	完全成功
案例三	网络驱使	满足	满足	满足	维基解密	托克集团、英国最高法院	非国家行为体	非国家行为体、国家	完全成功
案例四	网络威慑	不满足	不满足	不满足	美国	朝鲜	国家	国家	完全失败
案例五	网络驱使	不满足	不满足	不满足	俄罗斯	爱沙尼亚	国家	国家	完全失败

（一）案例一："和平卫士"威慑索尼公司

2014 年 11—12 月，朝鲜对美国索尼电影娱乐公司（以下简称"索尼公司"）发动网络攻击，威胁其不得上映讽刺朝鲜政治的喜剧电影《采访》（*The Interview*）。最终，索尼公司被迫推迟上映时间。2014 年 6 月 11 日，《采访》预告片在 YouTube 上播出。6 月 27 日，朝鲜常驻联合国代表慈成男（Ja Song-nam）致信联合国秘书长潘基文表达强烈不满和抗议。[①] 然而，索尼公司不顾朝方反对，将电影定档于圣诞节公映。

11 月 24 日，索尼公司员工的计算机屏幕上突然弹出一张恐怖图片，图片中一具血色骷髅发出威胁，如果自己的要求得不到满足，公司内部数据将被公布于众，攻击者署名为"和平卫士"（Guardians of Peace，GOP）。[②] 照片并未透露攻击者的具体要求，此时距离感恩节假期还有三天。

12 月 10 日起，索尼公司高管间的内部通信邮件陆续泄露，多名高管深陷丑闻风波。首先，总监艾米·帕斯卡尔（Amy Pascal）和制片人斯科特·鲁丁（Scott Rudin）在内部会议上发表涉及总统奥巴马的种族歧视言论。[③] 其次，帕斯卡尔在接受《纽约时报》专栏作家茉润·道得（Maureen Dowd）采访时表示"白人中年男性在奥斯卡评委会和业界顶尖人物中占据主流"。[④] 帕斯卡尔还抱怨自己遭受性别歧视，至今仍然依靠"微薄"薪水度日。但泄露的工资单据显示，帕斯卡尔的薪金同首席执行官迈克尔·林盾（Michael

---

① *Letter Dated 27 June 2014 from the Permanent Representative of the Democratic People's Republic of Korea to the United Nations Addressed to the Secretary-General*, UN General Assembly Security Council, June 27, 2014.

② Paul Ducklin, "Sony Pictures Breached-Or Was It?" *Naked Security*, November 24, 2014, https://imgur.com/qXNgFVz, 访问时间：2019 年 10 月 15 日。

③ Matthew Zeitlin, "Scott Rudin on Obama's Favorite Movies: 'I Bet He Likes Kevin Hart'," *BuzzFeed News*, December 10, 2014, https://www.buzzfeednews.com/article/matthewzeitlin/scott-rudin-on-obama-i-bet-he-likes-kevin-hart, 访问时间：2019 年 10 月 15 日。

④ Matthew Zeitlin, "Leaked Emails Suggest Maureen Dowd Promised to Show Sony Exec's Husband Column Before Publication," *BuzzFeed News*, December 12, 2014, https://www.buzzfeednews.com/article/matthewzeitlin/leaked-emails-reveal-maureen-dowd-promised-to-sony-execs-hus, 访问时间：2019 年 10 月 15 日。

Lynton)持平,达到公司最高薪资水平。显然,帕斯卡尔在薪水一事上撒了谎。令人惊讶的是,道得利用职务之便向帕斯卡尔的丈夫提前展示了《纽约时报》样刊,并表示专访绝对有利于塑造帕斯卡尔的公众形象。最后,女员工实名举报经理基思·勒·戈伊(Keith Le Goy)长期对其性骚扰的实名举报信也被曝光。① 上述丑闻使索尼公司精心营造的公共形象轰然倒塌,公司陷入空前的信任危机。

12 月 16 日,"和平卫士"明确要求索尼公司下架电影《采访》。17 日,索尼公司同意院线推迟放映该电影。② 19 日,美国联邦调查局正式认定,朝鲜实施了此次网络攻击,攻击所用的恶意代码和加密算法与 2013 年朝鲜所使用的攻击工具相同。③ 美国总统奥巴马发表公开讲话称"我们将在适当时间和地点采取适当方式进行对等回应"。④ 2015 年 1 月 2 日,美国宣布对朝鲜境内的 3 家机构和 10 名个人实施制裁。⑤

该案例中,胁迫者为朝鲜,被胁迫者为索尼公司,胁迫意图为停止上映电影《采访》。首先,朝鲜假借"和平卫士"的名义实施胁迫,但采用恶意代码复用的方式暗示身份,借此逃避道德谴责和舆论压力。2013 年 3 月 20 日,朝鲜对韩国多家银行和电视台发动大规模网络攻击⑥,朝鲜的历史行为为其

---

① Sam Biddle, "Leaked Email Alleges Racism and Sexual Harassment Horror at Sony," *Gawker*, December 12, 2014, https://gawker.com/leaked-email-alleges-racism-and-sexual-harassment-horro-1670318085, 访问时间: 2019 年 10 月 15 日。

② Linda Ge, "Sony Hack: NATO Says Theaters 'May Delay' 'Interview' Release," *The Wrap*, December 17, 2014, https://www.thewrap.com/sony-hack-nato-says-theaters-may-delay-interview-release/, 访问时间: 2019 年 10 月 15 日。

③ "Update on Sony Investigation," FBI National Press Office, December 19, 2014.

④ The White House, "Remarks by the President in Year-End Press Conference," December 19, 2014.

⑤ BBC News, "Sony Cyber-Attack: North Korea Faces New US Sanctions," January 3, 2015, https://www.bbc.com/news/world-us-canada-30661973, 访问时间: 2019 年 10 月 15 日。

⑥ Tania Branigan: "South Korea on Alert for Cyber-Attacks After Major Network Goes Down: Computer Systems of Banks and Broadcasters Are Interrupted, with Fingers Immediately Pointed at North Korea," *The Guardian*, March 20, 2013, https://www.theguardian.com/world/2013/mar/20/south-korea-under-cyber-attack, 访问时间: 2019 年 10 月 15 日。

树立了声誉。在该事件中,朝鲜分批公布内部文件,使索尼公司相信朝鲜有能力获取可能动摇公司领导层的丑闻并利用其进行胁迫的决心,胁迫具有可信性,假设一得到满足。其次,11 月 25 日至 12 月 1 日,索尼公司 3262 台计算机和 1555 台服务器上的数据被恶意删除,4 部未上映电影的原版拷贝被制作成 P2P 种子供全网免费下载,15232 名员工的社保号遭到泄露,尽管如此索尼公司仍未屈服。直到高层管理人员的丑闻被曝光后,索尼公司才决定推迟上映电影,丑闻是压倒索尼公司的"最后一根稻草",假设三得到满足。最后,电影虽然推迟上映,但最终还是以付费在线点播的方式同观众见面。也就是说,索尼公司并未完全满足胁迫者的要求,《采访》只是推迟上映,并未取消上映,此次胁迫只获得部分成功。究其原因在于假设二没有得到满足,即朝鲜未能提供有效保证。在索尼公司屈服前曝光了丑闻,这导致公司名誉和形象受损已成既定事实,屈服与否都无法挽回损失。可见,在利用丑闻进行网络胁迫的情况下,当胁迫者无法做出有效保证时,即使其他条件得到满足,网络胁迫也只能取得部分成功。

(二)案例二:美国威慑俄罗斯

2016 年 3 月中旬起,俄罗斯联邦武装力量总参谋部情报总局(Главное управление Генерального штаба Вооружённых Сил Российской Федерации)向美国民主党国会竞选委员会、民主党全国委员会、希拉里竞选团队雇员和志愿者发动了一系列网络攻击,其中包括入侵竞选委员会主席约翰·波德斯塔(John Podesta)的电子邮箱。俄方共获取包括民主党内部竞选文件、筹款数据、民调结果及通信邮件在内的约 70GB 敏感信息。[①] 经过精心筛选和编辑,俄方借助"DCLeaks"和"Guccifer 2.0"两个网站在特定时间散播上述信息,以达到抹黑希拉里个人形象的目的。

与此同时,俄罗斯互联网研究机构(Internet Research Agency,IRA)开始在社交网站上大肆进行"反希拉里"宣传。在脸书网站上,俄罗斯互联网

---

① Special Counsel's Office, U. S. Department of Justice, *Report On the Investigation into Russian Interference in the* 2016 *Presidential Election*, 2019 (California: 12th Media Services, 2019), p. 40.

研究机构以保守团体、黑人维权组织和宗教团体的名义创建公共账号,传播有关希拉里的“黑料”。[①] 在推特网站上,首先使用美国公民个人身份创建账号,再通过机器人账号伪造关注量,哄抬个人账号热度。如此一来,个人账号发布的“黑料”会被机器人账号迅速转载,产生“燎原”假象。穆勒调查报告最终认定,“俄罗斯政府全面、系统性地干预了美国 2016 年总统大选”。[②] 然而,俄罗斯外长谢尔盖·拉夫罗夫否认此项指控。

为防止 2018 年中期选举受到俄罗斯干预,美国对俄罗斯实施网络胁迫。2016 年 10 月 14 日,美国副总统拜登在接受美国全国广播公司(NBC)专访时表示:“我们正在向俄罗斯总统普京发出信号。我们有能力做到这一点,信号将被发出。在影响力最大的情况下,我们会选择时机让他知道。”[③]当主持人询问公众是否知情时,拜登回答:“我不希望公众知情。”[④]次日,NBC 后续报道指出,美国中情局已经做好网络行动准备,旨在“骚扰并羞辱克里姆林宫领导层”。[⑤] 美国退役上将詹姆斯·斯塔夫里迪斯(James Stavridis)表示,“大量资金被寡头转移到俄罗斯境外”,一旦这些信息曝光,肯定会让普京“臭不可闻”。[⑥]

克里姆林宫发言人德米特里·佩斯科夫(Дмитрий Песков)于 15 日做出回应称:“针对莫斯科和我们国家领导人的威胁是史无前例的,因为这次

---

① Special Counsel's Office, U. S. Department of Justice, *Report On the Investigation into Russian Interference in the* 2016 *Presidential Election*, 2019 (California: 12th Media Services, 2019), pp. 25-26.

② Ibid. p. 1.

③ NBC News, "Biden: 'We're Sending a Message' to Putin," October 14, 2016, https://www.nbcnews.com/meet-the-press/video/biden-we-re-sending-a-message-to-putin-786263107997, 访问时间: 2019 年 10 月 15 日。

④ Ibid.

⑤ William M. Arkin et al., "CIA Prepping for Possible Cyber Strike Against Russia," NBC, October 15, 2016, https://www.nbcnews.com/news/us-news/cia-prepping-possible-cyber-strike-against-russia-n666636, 访问时间: 2019 年 10 月 15 日。

⑥ Ibid.

威胁是由美国副总统发出的。”[①]佩斯科夫随后表示，面对美国日益增长的不可预测性和挑衅性，莫斯科将采取预防性措施维护自身利益。2018 年 3 月至 11 月，美国中期选举没有遭到来自俄罗斯的大规模网络干预。

该案例中，胁迫者为美国，被胁迫者为俄罗斯，胁迫意图为阻止俄罗斯继续干涉美国 2018 年中期选举。首先，副总统拜登通过媒体明示胁迫者身份，美国国家安全局从 2009 年起长期监听外国政要和领导人，俄罗斯没有理由怀疑美国搜集克里姆林宫丑闻并利用其进行网络胁迫的能力与决心，假设一得到满足。其次，美国副总统拜登并未向公众透露丑闻的具体内容。也就是说，只有美俄领导层了解详情，两国民众对丑闻细节并不知情。这符合网络胁迫的隐秘特征，为美国向俄罗斯做出保证创造了条件——只要俄罗斯不再干预美国中期选举，相关丑闻将不会曝光，普京的个人形象和名誉也就不会受损，假设二得到满足。事实证明，美国 2018 年中期选取期间没有遭受来自俄罗斯的大规模网络干预，此次网络胁迫取得成功，根本原因在于美国掌握了能够“骚扰并羞辱克里姆林宫领导层”的丑闻，大幅增加了俄罗斯的抵抗成本，为维护领导人的个人利益，决策者被迫做出妥协，假设三得到满足。当然，俄罗斯绝不会承认此事，美国也不会公布丑闻内容，双方达成“心照不宣的合谋”。可见，当三个假设全部满足时，网络胁迫可以取得完全成功。

（三）案例三：“维基解密”驱使托克集团和英国最高法院

2006 年 8 月 19 日晚，一艘名叫“长鼻考拉”（Probo Koala）的货船卸下 400 余吨化学废料并将其倾倒在科特迪瓦阿比让市（Abidjan）的至少 12 处地点。[②] 几天后，当地居民开始出现咳嗽、呕吐、鼻出血、皮肤过敏等症状，中国驻科特迪瓦大使马志学表示：“气味像大蒜或东西腐烂时散发出的怪味，

---

① Yahoo News, “Russia Slams ‘Unprecedented’ US Threats over Cyber Attacks,” October 15, 2016, https://news.yahoo.com/russia-slams-unprecedented-us-threats-over-cyber-attacks-114554306.html, 访问时间：2019 年 10 月 15 日。

② 世界卫生组织媒体中心：《科特迪瓦的化学废料》，2006 年 9 月 15 日，http://apps.who.int/mediacentre/news/notes/2006/np26/zh/index.html，访问时间：2019 年 10 月 15 日。

人闻了以后特别不舒服,头晕、想吐。"[①]此次化学物品倾倒事件造成约 100000 名当地居民寻求医疗帮助,共 30000 人受伤,17 人死亡,其中大部分为儿童。[②]

"长鼻考拉"货船在巴拿马注册,由托克集团英国办事处租用。事发后,托克集团表示,废料成分由水、碱性混合物及少量硫化氢构成,对人体的危害十分有限。加之阿比让当地居民长期生活在垃圾堆附近,一生都在接触有毒物质,他们的死亡与集团无关。[③] 11 月 11 日,英国利戴律师事务所(Leigh Day & Co.)向英国高院提起 1 亿英镑诉讼,指控"这是一场灾难,我们认为托克集团应对其倾倒废弃物的行为负全责"。[④] 托克集团虽然对当地居民深表同情,但否认上述全部指控。

事实上,托克集团早在 2006 年 9 月就曾撰写内部调查报告《明顿报道》(Minton Report),确认在阿比让倾倒的废料中含有剧毒化学物质。为防止报告曝光,2009 年 9 月 11 日,托克集团在卡特拉克律师事务所(Carter Ruck Lawyers)的帮助下获得"超级禁令"(super-injunction),严禁英国《卫报》刊登有关《明顿报告》的任何消息,更不能提及禁令本身。[⑤] 9 月 14 日,"维基解密"公布了《明顿报告》全文。9 月 20 日,托克集团与利戴律师事务所达成庭

---

① 新浪新闻:《欧洲毒垃圾熏倒非洲人,科特迪瓦换了政府》,2006 年 9 月 20 日,http://news.sina.com.cn/w/2006-09-20/081210062424s.shtml,访问时间:2019 年 10 月 15 日。

② David Leigh and Afua Hirsch, "Papers Prove Trafigura Ship Dumped Toxic Waste in Ivory Coast," *The Guardian*, May 13, 2009, https://www.theguardian.com/environment/2009/may/13/trafigura-ivory-coast-documents-toxic-waste, 访问时间:2019 年 10 月 15 日。

③ David Leigh, "Newsnight Sued over Toxic Waste Claims," *The Guardian*, May 13, 2009, https://www.theguardian.com/environment/2009/may/16/bbc-newsnight-trafigura-lawyers-libel, 访问时间:2019 年 10 月 15 日。

④ MAREX, "London Based Law Firm to Represent Ivory Coast Victims in Toxic Waste Case," *The Maritime Executive*, November 16, 2006, https://maritime-executive.com/article/2006-11-16london-based-law-firm-to-represent-ivo, 访问时间:2019 年 10 月 15 日。

⑤ WikiLeaks, "Minton Report: Trafigura Toxic Dumping Along the Ivory Coast Broke EU Regulations," *WikiLeaks*, September 14, 2006, https://wikileaks.org/wiki/Minton_report:_Trafigura_toxic_dumping_along_the_Ivory_Coast_broke_EU_regulations,_14_Sep_2006, 访问时间:2019 年 10 月 15 日。

外和解，愿意向阿比让市民支付约4600万美元的赔偿金，但坚称集团与倾倒事件没有直接联系。

2009年9月14日，“维基解密”创始人朱利安·阿桑奇(Julian Assange)发表公开声明，要求托克集团认罪及英国法院撤销媒体禁令。阿桑奇指责“英国的审查制度犹如私有化的封建主义”，并威胁卡特拉克律师事务所“不要轻易做出许诺”。阿桑奇呼吁网民：“磨快你们的刀，立刻投入工作。战斗远未结束，其实它才刚刚开始。”[①]10月16日晚，英国最高法院撤销了媒体禁令。[②] 11月4日，法院判决托克集团向利戴律师事务所代表的倾倒事件受害者支付总额为3000万英镑的赔偿金。[③]

该案例中，胁迫者为“维基解密”，被胁迫者为托克集团英国分公司和英国最高法院，胁迫意图为托克集团承担化学废料倾倒事件的全部责任以及英国高院取消媒体禁令。“维基解密”首先明示身份，“爆料”声誉使托克集团对其进行网络胁迫的能力和决心深信不疑。比如，2006年底，“维基解密”曾公布索马里伊斯兰党领袖哈山·达伊尔·艾维斯(Hassan Dahir Aweys)暗杀政府要员的命令；2007年11月，曝光美军关塔那摩监狱丑闻；2008年9月美国大选期间，公开共和党总统候选人麦凯恩的竞选伙伴萨拉·佩林(Sarah Palin)雅虎信箱中的电子邮件。《明顿报告》公布后更让托克集团坚信“维基解密”已经掌握内情，加上其之前的“爆料”声誉，使网络胁迫具有可信性，假设一得到满足。其次，《明顿报告》属于化学分析报告，只能证明托克集团的“废料无害论”纯属无稽之谈，并不能证明托克集团与废料倾倒直

---

① Julian Assange, “Guardian Still Under Secret Toxic Waste Gag,” *WikiLeaks*, October 14, 2009, https://wikileaks.org/wiki/Guardian_still_under_secret_toxic_waste_gag, 访问时间：2019年10月15日。

② Martin Beckford and Holly Watt, “Secret Trafigura Report Said ‘Likely Cause’ of Illness Was Release of Toxic Gas from Dumped Waste,” *The Telegraph*, October 16, 2009, https://www.telegraph.co.uk/news/uknews/6350262/Secret-Trafigura-report-said-likely-cause-of-illness-was-release-of-toxic-gas-from-dumped-waste.html, 访问时间：2019年10月15日。

③ David Leigh, “How UK Oil Company Trafigura Tried to Cover up African Pollution Disaster,” *The Guardian*, September 16, 2009, https://www.theguardian.com/world/2009/sep/16/trafigura-african-pollution-disaster, 访问时间：2019年10月15日。

接相关。“维基解密”虽然指出有“超级禁令”存在,但没有揭露禁令的具体内容。也就是说,在被胁迫者屈服前,胁迫者并未公布全部丑闻,“维基解密”做出了有效保证,假设二得到满足。最后,托克集团起初完全否认利戴律师事务所的指控,拒绝赔偿。在《明顿报告》曝光 6 天后,托克集团便与利戴律师事务所达成和解并同意支付巨额赔偿金,英国高院也随之撤销媒体禁令,可见威胁曝光丑闻是托克集团和最高法院屈服的根本原因,假设三得到满足。综上,在利用决策者丑闻进行胁迫的情况下,如果三个假设全部得到满足,网络胁迫将取得完全成功。

(四)案例四:美国威慑朝鲜人民军侦察总局

2017 年 6 月 13 日,美国国土安全部和联邦调查局发布报告指出,一个名为“隐秘眼镜蛇”(Hidden Cobra)的黑客组织自 2009 年起对美国及其他国家的新闻媒体、航空航天部门、金融和关键基础设施发动了一系列网络攻击,而该组织隶属于朝鲜人民军侦察总局。①

2017 年 9 月 22—30 日,美军网络司令部对朝鲜人民军侦察总局发动了 DDoS 攻击,旨在使目标计算机和服务器过载,中断其网络连接。9 月 30 日,一位白宫高级官员公开表示:“朝鲜应该为之前的一系列网络攻击负责,我们将采取适当措施保护网络与系统安全。”②此举被视为美国针对朝鲜实施的一次网络威慑,意在阻止朝鲜继续对美国本土的商业机构、政府机关、高校和基础设施进行网络攻击。

然而,此次威慑未能取得成功。2017 年 12 月,微软公司和脸书网站遭到朝鲜网络攻击;2018 年 1 月,谷歌应用商店(Google Play)受到朝鲜黑客攻击;2018 年 5 月,朝鲜通过互联网窃取了美国多所高校生物医学工程专业专

① “HIDDEN COBRA-North Korea's DDoS Botnet Infrastructure,” United States Department of Homeland Security, January 13, 2017.

② Karen DeYoung, “Trump Signed Presidential Directive Ordering Actions to Pressure North Korea,” *The Washington Post*, September 30, 2017, https://www.washingtonpost.com/world/national-security/trump-signed-presidential-directive-ordering-actions-to-pressure-north-korea/2017/09/30/97c6722a-a620-11e7-b14f-f41773cd5a14_story.html, 访问时间:2019 年 10 月 15 日。

家和学生的个人信息;2018 年 12 月,朝鲜对《华尔街日报》《纽约时报》《洛杉矶时报》《芝加哥论坛报》《巴尔的摩太阳报》等美国新闻媒体发动了一系列网络攻击。

此次胁迫失败的根本原因在于无法损害朝鲜领导人的个人利益,无法满足本文的三个假设。第一,美国高级官员的讲话明示胁迫者身份,朝鲜领导人相信美国完全有能力实施网络胁迫,但单纯依靠 DDoS 攻击无法损害朝鲜领导人的个人利益,因为 DDoS 攻击根本不具备情报搜集功能,从而导致可信性缺乏,假设一未得到满足。第二,媒体宣传使此次胁迫丧失了隐秘性,即使朝鲜不再对美国本土发动网络攻击,美军也不能承诺在未来停止一切针对朝鲜的网络行动。换言之,美国无法提供有效保证,假设二未得到满足。第三,胁迫无法完全阻断朝鲜的网络通信。一方面,朝鲜侦察总局特工完全可以在海外策划并组织网络活动,美国没有能力阻断全球的网络连接;另一方面,俄罗斯电信公司 TTC(TransTeleCom)在攻击结束后的第二天(10 月 1 日)便通过图们江为朝鲜开通了第二条通信光缆。这些因素致使美军无法长期阻断朝鲜侦察总局的网络通信,更没有造成目标计算机硬件损坏和数据丢失。朝鲜完全可以承受此次胁迫造成的损失,即抵抗成本小于屈服成本,假设三未得到满足。所以朝鲜没有屈服,继续对美国本土开展网络攻击。该案例表明,如果网络胁迫无法直接损害决策者或决策集团的个人利益,胁迫很难满足三个必要条件,从而导致胁迫失败。

(五)案例五:俄罗斯驱使爱沙尼亚政府

2007 年 4 月 27 日清晨,爱沙尼亚政府不顾本国俄裔移民及俄罗斯联邦第一副总理谢尔盖·伊万诺夫的强烈抗议,将青铜战士(Bronze Soldier)纪念碑及纪念碑下安葬的苏军战士遗骸从首都塔林迁往市郊的烈士公墓。苏联红军于 1947 年修建了这座 6 英尺高的青铜纪念碑,在俄裔移民看来,这座纪念碑标志着二战期间苏联红军为解放塔林所作出的巨大贡献;但在绝大多数爱沙尼亚人眼中,该纪念碑却象征着苏联对爱沙尼亚民族独立的压迫与遏制。①

---

① Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security*, Vol. 4, No. 2, 2011, p. 51.

27日上午10时,爱沙尼亚总理府、内政部、外交部、议会、经济事务与通信部的网站遭受DDoS攻击,这些网站无法正常访问。同时,执政党爱沙尼亚改革党的网站首页遭到攻击,并以总理安德鲁斯·安西普(Andrus Ansip)的名义发布了一封伪造的公开信,声称对迁移纪念碑感到后悔。28—29日,攻击规模和力度持续增强,爱沙尼亚全境的路由器和交换机都受到了不同程度影响。

5月9日,俄罗斯总统普京在卫国战争胜利日当天不点名批判了爱沙尼亚政府:"那些今天试图贬低这一宝贵历史经验的人,那些亵渎战争英雄纪念碑的人,他们正在侮辱自己的国民,并在国家和人民之间种下不和谐与不信任的种子。"①与此同时,对爱沙尼亚政府和主流媒体的网络攻击也达到顶峰,峰值时的数据请求量高达每秒5.59GB。② 一些政府和媒体网站的页面还被恶意篡改,出现诸如"被俄罗斯黑客入侵""网络戒严是爱沙尼亚的耻辱,却是我们的荣耀! 我们的自由! 我们的胜利!"③等标语。5月10日,包括塔林商业银行(Tallinn Business Bank)在内的多家银行遭受网络攻击,导致在线支付和转账业务无法正常办理。

攻击发生后,爱沙尼亚总理安西普表示:"来自俄罗斯服务器的连续网络攻击、我国驻莫斯科使领馆被围攻以及俄杜马议员呼吁爱沙尼亚政权更迭,这一切都预示着我们的国家正在遭受重击。"④但俄罗斯政府否认上述指控。不过克里姆林宫下属的俄罗斯最大青年运动团体"Nashi"⑤的政治委员康斯坦丁·戈洛斯卡科夫(Константин Голоскоков)曾在2007年公开承认对

---

① "Demonstrations Banned in Tallinn Until May 11," *Russia Today*, May 10, 2007, https://www.rt.com/news/demonstrations-banned-in-tallinn-until-may-11/, 访问时间:2019年10月15日。

② Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *WIRED*, August 21, 2007, https://www.wired.com/2007/08/ff-estonia/, 访问时间:2019年10月15日。

③ Ibid.

④ Nate Anderson, "Massive DDoS Attacks Target Estonia; Russia Accused," *arsTECHNICA*, May 14, 2007, https://arstechnica.com/information-technology/2007/05/massive-ddos-attacks-target-estonia-russia-accused/, 访问时间:2019年10月15日。

⑤ "Nashi"是俄语"наши"的拉丁字母转写,表示"我们"的意思。

此事负责:“我们给爱沙尼亚政府上了一课,如果他们采取非法行动,我们也将以适当方式回应。”①此外,俄罗斯杜马议员谢尔盖·马尔科夫(Сергей Марков)也公开表示:“别担心,袭击是我助手干的,但我不会告诉你们他的名字。”②

这场持续近20天的网络攻击其实是俄罗斯对爱沙尼亚发动的一次网络胁迫,意在驱使爱沙尼亚当局停止搬迁青铜战士纪念碑。但爱沙尼亚政府顶住压力,还是在2007年4月30日完成了全部搬迁工作。此次胁迫失败的根本原因在于未能损害爱沙尼亚领导人的个人利益,使本文的三个假设无法得到满足:首先,俄罗斯采取暗示方式揭露胁迫者身份,虽然爱沙尼亚相信俄罗斯的网络胁迫能力,但怀疑DDoS攻击能否获取足以威胁爱沙尼亚领导层的丑闻。另外,俄第一副总理伊万诺夫抵制爱沙尼亚商品的呼吁未被外交部采纳会让爱沙尼亚怀疑俄罗斯的胁迫决心,从而导致胁迫可信性不足,假设一未得到满足。其次,攻击发生后不久,在俄罗斯境内的俄语论坛上就出现了供网友免费下载的DDoS工具包,论坛还号召俄罗斯网民一起攻击爱沙尼亚政府。也就是说,即使爱沙尼亚搁置纪念碑搬迁计划,俄罗斯也不敢保证能够立刻停止网络攻击,即俄罗斯无法提供有效保证,假设二未得到满足。最后,爱沙尼亚计算机紧急事件响应小组(Computer Emergency Response Team,CERT)与来自美国和北约的网络安全专家通力合作,保证了国家关键网络正常运转,并及时对遭到攻击的政府、银行及媒体网站进行修复。网络攻击未能使政府陷入瘫痪,爱沙尼亚完全有能力承受攻击带来的损失,加之东欧多国都在竭力消除苏联的历史印记,因此抵抗成本远未超过屈服成本,假设三未得到满足。所以俄罗斯对爱沙尼亚的网络胁迫以失败告终。可见,无法损害决策者个人利益的网络胁迫很难同时满足胁迫成功的三个必要条件,导致胁迫失败。

---

① Noah Shachtman, “Kremlin Kids: We Launched the Estonian Cyber War,” *WIRED*, March 11, 2009, https://www.wired.com/2009/03/pro-kremlin-gro/, 访问时间:2019年10月15日。

② Sergei Markov, “Behind the Estonia Cyberattacks,” *Radio Free Europe*, March 6, 2009, http://www.rferl.org/Content/Behind_The_Estonia_Cyberattacks/1505613.html, 访问时间:2019年10月15日。

六、结 论

网络胁迫指胁迫者利用网络武器强迫被胁迫者采取特定行为或不要做出某种行为,包括网络驱使和网络威慑两种形式。胁迫结果取决于胁迫者要求被满足的程度:胁迫者要求被满足的程度越高,胁迫结果就越倾向于成功;胁迫者要求被满足的程度越低,胁迫结果则越倾向于失败。

网络武器的特殊性决定了网络胁迫成功的条件不同于核胁迫。首先,网络武器的使用者可以选择是否主动暴露自己的身份;其次,网络武器具有可订制性和隐蔽性;再次,网络武器无法直接造成人员伤亡;最后,网络武器可用于情报搜集。根据网络武器的特殊属性,本文认为,能损害决策者个人利益的网络胁迫最容易成功,即运用网络武器搜集有关决策者或领导层的丑闻并以之相威胁,决策者为保全个人利益不惜牺牲集体利益,被迫做出妥协。

利用丑闻进行网络胁迫,可以同时满足胁迫成功的三个必要条件——可信性、保证和成本收益核算。第一,胁迫者暗示或明示身份,为树立声誉创造条件,从而增强胁迫可信性。第二,胁迫行为避开公众视野有利于胁迫者做出有效保证。第三,当网络胁迫能够损害决策者个人名誉和形象时,决策者的抵抗成本将大于屈服成本,从而选择妥协。上述假设既适用于国家,也适用于非国家行为体。

值得注意的是,在决策者屈服前丑闻不应向公众提前曝光,否则网络胁迫只能取得部分成功,例如朝鲜威慑索尼公司。只有上述三个假设同时得到满足时,网络胁迫才能取得完全成功,例如美国威慑俄罗斯、“维基解密”驱使托克集团及英国法院。当胁迫无法损害决策者个人利益时,则很难同时满足胁迫成功的三个必要条件,最终导致胁迫失败,比如美国威慑朝鲜人民军侦察总局、俄罗斯驱使爱沙尼亚。

当然,严格检验本文假设需要充分了解网络胁迫中国家和非国家行为体的内部决策过程,这在现阶段很难做到。本文尽量选用已经解密的一手资料,有选择地使用不同来源的二手材料,两者相互印证,尽可能保证研究的客观性与可靠性。此外,胁迫成功的三个条件加上胁迫类型(网络威慑和

网络驱使)至少需要16个检验案例,但网络胁迫的隐秘性使可用案例十分有限,完全检验本文假设还有待相关材料的进一步解密和开放。最后,本文的案例检验基于观察而非试验,因此很难控制所有变量,也无法构造出真正的"反事实",这恐怕是案例研究的通病。

目前,国内学界对网络威慑的关注远多于网络胁迫,网络胁迫没有得到应有重视。其实,胁迫只是网络攻击众多目的中的一种,网络勒索是否算作胁迫?在何种情况下网络攻击等同于战争?网络军备竞赛是否会发生?网络战与信息战之间究竟存在什么关系?网络攻击会对国际关系产生何种影响?传统攻防理论是否适用于互联网领域?这些恐怕是信息时代下国际关系研究的新问题和新方向。现实中,网络攻击经常与军事、经济、外交等手段混用,如何将网络攻击的作用和机制剥离出来,这是相关研究所面临的共同挑战。

国际关系预测

东南亚国家对冲战略的变化趋势*

（对外经济贸易大学全球化与中国现代化问题研究所，
清华大学国际关系研究院对外关系定量预测组　张伟玉）

2017年12月，特朗普政府发布美国《国家安全战略报告》，将中国视为首要的战略竞争者。[①]2018年1月，美国特朗普政府发布《国防战略报告》，将美国的国防战略“从反恐转向大国竞争”，并渲染所谓的“中国军事威胁”。[②]2019年6月，美国国防部出台《印太战略报告》将中国定位为“一个修正主义大国”，将美国国家安全战略的基本关注定位为国家间的战略竞争，称要增加美国主导、同盟国和安全伙伴参与的在印太地区的国防建设和军事行动。[③]根据清华大学国际关系研究院对外关系定量预测数据显示，当前中美关系分值持续下跌，已经降至－6.7（见图1），位于－9到－6区间，处于对抗等级[④]，中美战略竞争加剧。在此背景下，学界普遍认为，东南亚国家将选择对冲战略来周旋于中美两大国之间。

* 本文系国家社会科学基金重大项目“中外关系数据库建设”（项目批准号：15ZDA069）、对外经济贸易大学中央高校基本科研业务费专项资金资助项目“国际领导与战略信誉：中美日在东南亚地区的竞争”（项目批准号：19QD24）的成果。

① “National security strategy of the united states America,” Dec 18, 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

② U.S. Deparment of Defense, *Summary of the* 2018 *National Defense Strategy National Defense Strategy of The United States of America*, Jan 19, 2018.

③ U.S. Deparment of Defense, *Indo-Pacific Strategy Report: Preparedness, Partnerships, and Promoting a Networked Region*, June 1, 2019.

④ 分值位于－9至－6区间，双边关系“对抗”；分值位于－6至－3区间，双边关系“紧张”；分值位于－3至0区间，双边关系“不和”；分值位于0至3区间，双边关系“普通”；分值位于3至6区间，双边关系“良好”；分值位于6至9区间，双边关系“友好”。“对抗”是指两国关系的性质是敌对的，而且公开称对方为自己的战略敌人，但没有直接的大规模军事冲突。参见：阎学通等：《中外关系鉴览1950—2005——中国与大国关系定量衡量》，北京：高等教育出版社，2010年，第1页。