国际政治视角下的网络安全治理困境与机制构建*

——以美国大选“黑客门”为例

鲁传颖

【内容提要】 以美国大选“黑客门”为代表的网络安全问题已经成为影响国际安全的不稳定因素之一，并对网络空间的国际治理和安全架构提出了更高的要求。从目前的研究看，国际规范、治理机制等领域的理论范式对网络安全议题具有非常强的解释力，但也面临着网络安全技术带来的挑战，需要在理论与方法上进行一定调适。以美国大选“黑客门”为例来分析，已经出现了网络空间安全从分散到融合，网络安全态势从等级化到非对称，网络空间从权力扩散向网络赋权三大趋势。因此，国际社会需要采取务实举措，推进平等参与并建立综合性机制框架来共同应对上述挑战。对于中国而言，从建设网络强国的角度来看，应该直面当前国际网络安全面临的困境，主动设置议程，推动网络空间的规范建设，维护网络空间的和平稳定，使网络空间也成为人类命运共同体。

【关键词】 黑客干预大选 维基解密 网络空间治理 网络安全

【作者简介】 鲁传颖，上海国际问题研究院副研究员

【中图分类号】 D815.5

【文献标识码】 A

【文章编号】 1006-1568-(2017)04-0033-16

【DOI 编号】 10.13851/j.cnki.gjzw.201704003

* 本文系国家社科基金青年项目“‘棱镜门’与中国参与国际互联网治理战略研究”（15CGJ001）的阶段性成果。

自 2015 年以来，网络安全事件愈演愈烈，“米拉”病毒对全球互联网关键基础设施的攻击导致美国大面积“断网”；黑客组织入侵了被誉为国际金融关键信息基础设施的环球银行金融电信协会（SWIFT），并从孟加拉银行窃取了 8 200 万美元;美国国家安全局泄漏的网络武器“永恒之蓝”（Eternal Blue）被黑客组织开发成勒索病毒“想哭”（WannaCry），对包括中国在内的 100 多个国家的军用、民用网络系统进行加密和破坏。美国大选“黑客门”在这一系列网络安全事件中具有里程碑意义，2016 年，匿名黑客组织通过曝光希拉里及其团队成员的电子邮件、通话记录、个人资料等内部信息对美国大选进行干预。[①] 截至目前，大选“黑客门”还在继续发酵，美国国家安全事务助理迈克尔·弗林（Michael Flynn）、联邦调查局局长詹姆斯·科米（James Comey）先后因牵涉此案而离职。[②] “黑客门”持续时间之长，后续影响力之大，引发争议之广泛只有 2013 年的“斯诺登事件”能够与之相比，并将对国际安全产生重要影响。不断发生的网络安全事件反映出，网络领域的国际安全制度和国际治理机制无法应对日益复杂的网络攻击和网络渗透。大选“黑客门”对于国际安全秩序造成的影响正在逐渐体现，并且呈现出一系列新的特点和趋势。国际社会必须进一步加大对网络空间的治理力度，建立相应的规范机制。同时，2015 年中国政府在第二届世界互联网大会上提出的构建网络空间命运共同体适用这一领域，但需要根据明确的目标，提出具体的治理方案。

一、网络空间安全既有理论分析的局限

大选“黑客门”主要经历了三个阶段：第一阶段主要是一系列邮件安全事件接连曝光，对整个大选进程产生了严重影响，由“希拉里邮件门”“波

[①] Kathy Gilsinan and Krishnadev Calamur, “Did Putin Direct Russian Hacking? And Other Big Questions,” *Atlantic*, January 6, 2017.

[②] Greg Miller and Philip Rucker, “Michael Flynn Resigns as National Security Adviser,” *Washington Post*, February 14, 2017, https://www.washingtonpost.com/world/national-security/michael-flynn-resigns-as-national-security-adviser/2017/02/13/0007c0a8-f26e-11e6-8d72-263470bf0401_story.html?utm_term=.8a53065a220d.

德斯塔邮件泄露”以及“民主党全国委员会邮件系统被黑客攻击”三个和美国总统竞选进程息息相关的网络安全问题组成。在竞选的关键时刻，三个事件被轮流炒作，不断有内部信息被披露到网上，不仅对希拉里的个人形象造成了伤害，也严重影响了其在选举中的表现，消耗了大量的竞选资源和精力，并为其最终败选埋下伏笔。第二阶段是美俄在大选“黑客门”问题上的博弈。2016 年 12 月底，美国总统奥巴马宣布了对黑客行为的报复举措。对于美国单方面的指控，俄罗斯的态度基本上是严厉反驳，但不与即将卸任的奥巴马政府进行纠缠。第三阶段的焦点是奥巴马离任后美国国会继续推动调查，参议院军事委员会和情报委员会都在积极推动相关的调查，[①] 并且将目标转移至特朗普的“通俄门”和阻止特朗普政府对俄关系的转圜。

美俄双方在大选“黑客门”的激烈博弈以及该事件在美国国内政治中的不断发酵，使这次事件成为一个跨越国际和国内两方面因素的国际政治议题。从理论层面来看，越来越多的国际关系学者如约瑟夫•奈（Joseph Nye）、罗伯特•杰维斯（Robert Jervis）、玛莎•费丽莫（Martha Finnemore）、江忆恩（Alastair Iain Johnston）等认为国际规范、治理机制甚至网络威慑是解决问题的关键，而非网络技术手段。[②] 从实践层面来看，当法国大选、马耳他选举也被黑客攻击后，大选“黑客门”实际上已经演变为一个重要的国际安全议题。[③] 以“黑客门”为代表的网络安全事件正在不断地破坏着国际秩序和国际安全的基础，增加了国际社会经济开放和政治信任的成本。为应对不断增加的网络安全威胁，各国加强了在网络安全领域的立法，加快了“数据本地化”和优先采购国产网络产品和设备等的速度，这不仅增加了企业的经济成本，也容易引发国家间在政治与经济贸易等领域的摩擦。

网络安全作为一项新兴的国际政治研究议程，现有的理论和方法还有待

[①] U.S. Senate Hearings, “Foreign Cyber Threats to the United States,” January 5, 2017,http://www.armed-services.senate.gov/hearings/17-01-05-foreign-cyber-threats-to-the-united-states.

[②] Joseph Nye Jr., “Deterrence and Dissuasion in Cyberspace,” *International Security*, Vol. 41, No. 3, 2017, pp. 44-71.

[③] Jamie Doward, “Malta Accuses Russia of Cyber-attacks in Run-up to Election,” *Guardian*, May 27, 2017, https://www.theguardian.com/world/2017/may/27/russia-behind-cyber-attacks-says-malta-jseph-muscat.

进一步完善。

首先，缺乏基本的网络安全技术素养会影响国际关系学者对事件性质的判断和影响的分析。以美国大选“黑客门”为例，俄美两国政府各执一词，尽管美国政府公布了一些技术分析报告，但依旧缺乏能够定性的证据；而俄罗斯政府不仅否认与自身有任何联系，普京还多次亲自对此进行回应。这样的现象在传统的国际关系领域并不多见。尽管在气候变化、核不扩散领域也会涉及很多技术细节，但国际关系学者可以通过与这些领域的技术专家合作来解决认知问题。然而在网络领域则不同，其技术门槛之高，以至于一般的技术专家无法完全理解技术细节，更无法解释清楚内幕，从而增加国际政治学者研究的难度。网络安全问题往往是以技术层面的网络安全问题与国家安全、政治安全、经济安全等结合的形式出现，由于缺乏对于网络安全技术层面的分析，国际政治领域的研究面临很大的局限。以大选“黑客门”为例，国际政治学者的分析研究往往将落脚点放在俄美双边关系和美国国内政治，对于网络安全因素则一笔带过，影响了对事件性质和影响的判定。

其次，现有国际关系理论如何应用于网络安全分析还存在一定争议。多数新兴议程出现后，总是容易出现两种极端的观点，一种观点往往认为这是一个全新的领域，需要全新的理论和方法，如网络空间的“公域说”和“网络空间独立宣言”，这种观点越来越式微；[①] 另一种观点认为原有的理论和方法依旧适用，没有本质上的变化，这种观点越来越成为主流，但在现实中往往存在问题。例如，美国国内智库在讨论应对大选“黑客门”时多采用核安全领域的威慑理论作为理论基础，但实际上网络安全领域存在归因问题（溯源能力）和威慑信号发送与接收等问题，直接套用威慑理论存在较大的理论缺陷，不能反映网络安全的实际情况。此外，也有学者倾向于从权力政治和地缘政治理论视角来看待网络空间的博弈，尽管这些传统国际关系理论范式可以作为一种分析视角来理解网络安全问题，但是如果以此来定义网络安全问题的属性，则容易忽视网络安全领域存在的很多特性，更无法提出有效的问题解决之道。

[①] 杨剑：《数字边疆的权力与财富》，上海人民出版社 2012 年版，第 44 页。

最后，国际政治视角下的网络安全问题需要更加复杂的分析方法。当前的国际政治理论缺乏对网络安全问题的系统性解释，现有的研究方法还需要根据网络安全的特点进行一定调整，增加跨学科跨领域的分析视角和思维。与其他国际政治领域的问题相比，大选“黑客门”揭示出网络安全问题具有战略性、复杂性、全局性、关联性。全球性问题一般均具有战略性和复杂性等特点，强调这些问题不仅具有重要性和优先性，同时还具有高度的专业性。核不扩散、气候变化以及极地、海洋问题多属于这一类问题。而网络安全与这些问题相比，还具有“牵一发而动全身”的特点，并且该问题还涉及政治稳定、经济发展、社会繁荣、国家安全等方方面面。因此，从国际政治视角分析网络安全问题时，要充分考虑到全局性和关联性特点。一方面，要从政治、经济、社会、安全等多维视角来分析网络安全问题的影响，避免从单一视角出发考虑问题。另一方面，网络安全与其他领域的安全问题息息相关，只有充分理解网络安全的性质和特点，并且将其作为关键要素才能更好地处理和应对这些传统领域出现的新趋势和新现象。[①] 尽管面临着一定的挑战，国际政治理论也越来越多地应用到对网络安全问题的分析和解释当中，很多国际政治理论已经成为主流的分析范式。本文重点将从国际安全、国际机制、国际规范等视角对美国大选“黑客门”事件及其影响进行分析、研究。

二、国际网络空间安全的新趋势

黑客干预大选将网络安全的认知推向了一个新的层级。传统的网络安全认知在于网络设备及其承载的数据遭到破坏或窃取所导致的安全问题，“斯诺登事件”使人们对网络空间安全的认知上升到无所不在的网络监听和国家安全的高度。美国大选“黑客门”所展现的是一种新的网络空间认知模式，它确立了新的目标，超越了大规模网络监听对于“战略信息”的获取，更加关注根据特定目标来使用这些“战略信息”。同时，它还表明网络安全的不对称性非常突出，防御的难度大幅增加。最后，它也揭示出网络安全领域正

[①] 鲁传颖：《网络空间治理与多利益攸关方理论》，时事出版社 2016 年版，第 3-9 页。

在进行的一场赋权运动，网络安全机构的力量正在上升。结合战略博弈、法律政策、技术分析等不同的分析视角，我们可以从黑客干预大选这一事件发现网络空间安全的三个重要发展趋势，即网络空间安全从分散走向融合，网络安全态势从等级走向非对称，网络空间从权力扩散走向网络赋权。

第一，网络安全从分散走向融合的趋势。黑客干预大选重新塑造了人们对网络安全的认知，拓展了网络空间安全的内涵，超越了以往不同种类的网络行动各自为政的趋势，融合为一种新国际安全冲突升级形式。黑客干预大选将目标对准了政治干预，形成了网络安全技术、意识形态攻击和政治秩序干预三位一体的新型网络行动形式。传统的网络攻击注重对关键基础设施的攻击，黑客干预大选则将目标瞄准具有战略意义的信息，并通过维基解密和社交网络进行曝光和宣传，特别是根据美国大选进程的发展对特定候选人进行爆料，形成了对一方的威慑和对选举进程的干预。

这种融合背后反映了攻击一方的战略目标已超越了以往网络安全所定义的范畴。美国前国家情报总监詹姆斯·克莱伯（James Clapper）将“干预”行为定义为超越传统间谍界限的、试图颠覆美国民主的“尝试”，“行为绝对是有预谋的，除了黑客外，他们还运用媒体和社交网络进行宣传和造谣、并用假新闻抹黑竞选人。”[①] 美国外交政策研究所研究员克林特·沃茨（Clint Watts）认为，黑客的目标不仅仅是操纵选举，更要削弱主流媒体、公众人物、政府机构的公信力。另外，黑客行动的重心是对获取的“战略信息”的使用。[②] 另一项来自无党派研究组织 PropOrNot 的调查称，黑客在窃取邮件的同时，还伴有一场大规模、长时间、有效针对美国人的宣传行动。共有 200 个疑似网站向 1 500 万美国人传播相关话题，其中一则关于希拉里的虚假负面新闻就有 2.13 亿次点击量。[③]

美国大选“黑客门”只是网络空间安全融合的起点，它给我们开启了一

[①] Brianna Ehley, “Clapper Calls Russia Hacking a New Aggressive Spin on the Political Cycle,” *Politico*, October 20, 2016, http://www.politico.com/story/2016/10/russia-hacking-james-clapper-230085.

[②] Clint Watts, “How Russia Wins an Election,” *Politico Magazine*, December 13, 2016, http://www.politico.com/magazine/story/2016/12/how-russia-wins-an-election-214524.

[③] The PropOrNot Team, “Russia is Manipulating U.S. Public Opinion through Online Propaganda,” November 30, 2016, http://www.propornot.com/p/home.html.

种更有弹性和更有想象力的网络空间安全认知和行为模式，网络安全、社交网络、意识形态宣传、政治干预，这些要素更有机地结合到一起并产生了更加严重的安全威胁，它将“战场”直接开辟在最强大的网络国家的本土，目标直指民主制度的核心区域。不管背后主使者是谁，这一现象本身，以及美国政府所采取的一系列重要的应对举措，已经明确体现出该事件的危害程度。同时，黑客干预大选对于我们如何认知网络空间风险，如何应对网络安全挑战，如何开展网络空间治理带来了更多的不确定性。

这种融合同时也反映了网络空间安全的新特点，将“战场”成功延伸到了一国境内，即“战略信息”的获取和使用，针对的目标都发生在同一个国家的网络空间中。进入 21 世纪以来，在国际安全体系中，只有极少数落后、混乱的发展中国家才会面临战争的风险，黑客干预大选则揭示出一个新的特点，即每个国家都可能面临类似于战争的风险，即使是美国这样强大的国家也不能幸免。

第二，网络安全态势从等级化走向非对称的趋势。过去网络安全的不对称性仅仅体现在特定的关键基础设施保护层面，网络强国与网络发展中国家从能力上来看还是呈现出等级化的特点。黑客干预大选打破了等级化的格局，重新定义了网络安全的非对称性。一直以来，美国和西方国家自认为在信息战方面是免疫的，互联网自由是天然与西方国家意识形态和国家利益绑定的，美国的“互联网自由战略”是最典型的代表。互联网所具有的去中心化结构、匿名性和跨国界性，被认为是对非民主国家进行意识形态宣传和政治干预的最佳平台，“阿拉伯之春”被认为是经典案例。时任美国国务卿希拉里·克林顿（Hillary Clinton）公开宣称要通过社交媒体来宣传美国的意识形态和价值观，实现对其他国家的政治干预和政权颠覆。[①] 黑客干预大选颠覆了这一传统认知，网络空间的意识形态宣传和政治干预并非等级制和单向的，而是非对称和双向的。

这种非对称性是由网络安全、社交网络和互联网自由等属性结合而产生

[①] “Secretary Clinton’s Remarks on Internet Freedom,” December 8, 2011, http://iipdigital.usembassy.gov/st/english/texttrans/2011/12/20111209083136su0.3596874.html#axzz2eIWPYNRu.

的，具有易攻、难防、扩散等特点。首先，从网络安全角度来看是难以防范的，黑客的目标不是人们传统认为的关键信息基础设施，而是政治顾问的个人邮箱和民主党全国委员会的内部网络，这些目标都难以算得上是关键信息基础设施，也难以全部被保护。其次，社交媒体取代主流媒体成为公众获取信息的主要来源，具有政治意图的黑客、维基解密和社交媒体共同组成一个新的意识形态生产和宣传生态，取代了精英和主流媒体在意识形态宣传领域的控制地位。在之前的西方国家选举中，候选人也会面临各种形式的揭老底、爆料事件，精英和主流媒体起到了“把关人”的作用，根据特定价值取向和标准进行信息传播。所谓的“外国虚假信息宣传”和特朗普的“推特治国”，都在侵蚀美国主流媒体和价值观的根基。最后，“互联网自由战略”导致自缚手脚。为了推广“互联网自由战略”，美国的法律、政策多数不涉及网络内容的传播管理，给黑客利用信息进行意识形态宣传和政治干预留下了巨大空间。网络安全、社交网络和互联网自由三大特点的融合放大了网络空间安全的非对称性。

黑客干预大选所带来的失序也许是短暂的，但其示范效应将是难以估量的。它不仅会启发更多的国家通过网络手段干预他国的国内政治，更会引发新一轮的网络空间军备竞赛，进而出台更严格的网络管制措施。这些后续的影响已经开始逐步显现，继美国大选之后，法国、马耳他大选也无法阻止黑客攻击。这强化了美欧等国通过加强信息管制来应对针对选举的黑客攻击。2016 年 12 月，美国和欧洲同步发布了《反外国虚假信息和宣传法案》，授权政府采取措施应对新型的信息战。[①] 这对于历来宣扬“互联网自由”的西方国家政府来说是前所未有的举动，这些政策会对未来网络空间的发展和治理带来负面影响和挑战。

第三，从网络空间权力扩散走向网络赋权的趋势，这会导致更多的安全议题主导国际政治，更多与安全相关的部门主导国际规则的制定。如果说网络空间发展第一阶段的主要特征是权力扩散，即网络空间治理权威的缺失导

[①] European Parliament, “MEPs Sound Alarm on Anti-EU Propaganda from Russia and Islamist Terrorist Groups,” November 23, 2016, http://www.europarl.europa.eu/news/en/news-room/20161118IPR51718/meps-sound-alarm-on-anti-eu-propaganda-from-russia-and-islamist-terrorist-groups.

致权力从国家行为体向非国家行为体扩散，从等级制走向扁平化，从中心走向节点等一系列的权力转变趋势。黑客干预大选则揭示出一个新的趋势，即一些处于网络安全治理核心区域，能够正确认知网络安全、积极掌握网络安全技术的部门，能够通过网络重新赋权，从而在权力扩散的同时，逆向集中和掌握权力。这是一轮新的网络赋权运动，它不是以平等、透明和去等级化为发展方向；相反，它呈现出某些集权的、非公开和不对等的趋势。

黑客干预大选揭示了网络赋权的三个来源：领域风险、认知能力、技术差异。首先，领域风险主要是由于某些领域具有战略性地位，相应的威胁能够对全局产生影响。例如，黑客干预大选就是从网络安全出发，对政治安全、意识形态安全甚至经济安全、个人信息安全等造成严重威胁，这些风险和威胁会提升网络安全的重要性和关注度，从而为网络安全的赋权提供了基础。其次，认知能力要求高是由于网络安全问题的全局性使其具有复杂性和跨领域、跨学科的特征，这为正确认知网络安全问题提出了很高的要求。大多数部门和个人还是从单一和传统安全的理论视角来看待网络安全，只是被动防御，而一部分能够拥有更宽广视野、更全面认知网络安全的部门和个人获得网络赋权的可能性则增加。最后，技术差异是指由于先进网络安全技术的垄断性，导致掌握技术的群体和未掌握技术的群体之间产生权力差异。上述三者既有客观因素，也有主观因素，三者之间的结合构成了网络安全甚至整个网络空间赋权发展的新趋势。

网络赋权运动加剧了部门之间权力的转移，并对国际安全体系和大国关系造成了挑战。黑客干预大选以及之前中美在网络空间问题上围绕“网络商业窃密”的博弈都显示出以美国国家安全局、联邦调查局为代表的网络情报机构在这一轮赋权运动中占得先机，而传统的情报机构以及美国国务院、美国国土安全部的地位开始下降。从黑客干预大选和中美网络博弈等事件来看，白宫都是直接采纳美国国家安全局和联邦调查局的建议，基本没有采纳美国国务院的意见，美国国土安全部的地位也岌岌可危。[①] 网络情报机构以

[①] James Lewis, “From Awareness to Action-A Cyber Security Agenda for the 45th President,” Center for Strategic and International Studies, January 4, 2017, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/160103_Lewis_CyberRecommendationsNextAdministration_Web.pdf.

及与其关系密切的网络安全公司给出的所谓“证据”成为白宫判定事件性质、采取应对措施最主要的依据。另外，从国际秩序角度来看，传统意义上的国际和外交事务是由拥有丰富经验和熟悉规则的外交部门负责，但是当各国情报和安全机构来承担这些责任，相应的机制以及信任的缺乏将对现有的国际安全架构形成挑战，大国互动关系也将重新构建。

三、国际网络空间安全治理的新要求

美国大选“黑客门”加剧了网络空间安全冲突的升级，使网络空间安全治理更加复杂化，其示范效应将会对大国关系和国际安全体系带来巨大挑战。它所展现的融合趋势增加了影响网络空间安全的变量，增加了治理的难度，不对称趋势增加了网络空间的自助防御难度，赋权趋势造成国际政治中行为体变换和游戏规则的不适用，三者从不同方面同时给网络空间安全治理带来了挑战。因此，国际社会需要采取务实举措，推进平等参与治理，建立综合性机制框架来多方面应对上述挑战。

第一，针对网络空间安全的融合趋势，国际社会要务实推进网络空间治理。相较于美国大选“黑客门”所反映的网络空间安全的威胁程度，国际社会现有的网络空间安全治理还处于起步阶段。相关的博弈还是围绕治理原则是遵从互联网自由还是网络主权，治理主体是多边还是多方，治理平台是政府间组织还是非政府组织这些基本分歧来进行。[①] 从美国大选“黑客门”的影响和后果来看，美俄各执一词并且在双边层面进行博弈，现有的国际安全体系和网络空间治理体系已经无法提供相应的争端解决机制。这再一次引起国际社会对网络空间安全秩序缺失和规则匮乏的担忧，黑客干预大选会加剧主权国家寻求单边网络安全防御的错误倾向，加剧国际网络军备竞赛，同时消解网络空间治理领域已有的合作成果，并会引起大国之间的摩擦。

国际社会应在根本性的原则、立场上采取包容态度，达成共识，推出更多务实的举措。首先，就网络空间主权原则在治理领域的具体体现达成共识。

[①] Adam Segal, *The Hacked World Order*, New York: Public Affairs, 2016, pp. 201-220.

例如，黑客干预大选事件中所发生的通过黑客技术窃取“战略信息”，利用维基解密曝光信息，利用社交媒体进行信息战等行为，都涉及对其他国家网络主权的侵犯，既不能简单地以网络自由为名为其辩护，也不能仅靠加强立法来解决问题，这涉及现存的国际秩序如何与网络空间兼容以及各国政府如何达成共识并采取一致行动等问题。因此，主权作为网络空间秩序基石的作用不可替代，对网络主权的侵犯就是对国际体系的冲击，应受到国际社会的一致谴责和制裁。其次，在涉及网络空间安全治理的核心环节上取得突破。美俄在黑客干预大选上的博弈是建立在归因能力基础之上的。归因作为一项先进和复杂的技术，具有攻防两面性，主要大国出于技术垄断的目的，不愿让国际社会分享相关技术，导致当前的集体行动缺乏依据、单方面举措缺乏合法性的困境。归因是网络安全的核心议题，国际社会可以考虑在联合国或其他多边框架下设立多国参与的归因技术中心，在敏感的网络安全博弈中提供技术细节分析，从而对不负责任的网络空间行动起到威慑作用，并促使国际社会采取一致行动对其进行制裁。[①] 最后，在建立信任措施上要有更多约束性举措，在具体议题上达成可核实、有监督，并且有惩罚机制的举措。如可推动国际社会在应对这次事件所暴露出的在他国境内社交媒体上进行意识形态宣传和政治干预问题上达成共识，并采取有约束力的举措。[②]

第二，不对称性趋势导致“区分法”不适用于建立网络空间秩序。美国和其他西方国家一直认为其在网络技术、能力以及合法性上领先于其他国家，不愿以平等地位共同建立网络空间秩序，而是通过区分的方法有选择地设置治理议程。例如，在新一届的联合国信息安全政府专家组（UNGGE）中，美方坚持只讨论国际法在网络空间中的适用性问题，而不愿根据新的情况确立新的国际法则。[③] 在大规模网络监听和网络商业窃密问题上，美国认

[①] Scott Warren, Martin Libicki, and Astrid Stuth Cevallos, *Getting to Yest with China in Cyberspace*, Santa Monica: RAND Corporation, 2016, p. 30.

[②] Kate Conger, “Microsoft Calls for Establishment of a Digital Geneva Convention,” *Tech Crunch*, February 14, 2017, https://techcrunch.com/2017/02/14/microsoft-calls-for-establishment-of-a-digital-geneva-convention/.

[③] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN General Assembly Document A/70/174, July 22, 2015.

为其对全球进行的大规模网络监听是正常的情报收集活动，不应当受到指责，而其他国家对美国企业进行的商业窃密则损害了美国的国家利益，应当受到制裁。另外，美国认为自己可以单独发展出一套网络威慑理论，通过跨域威慑的方式来保障自身安全和推动“区分”战略。

从全球治理的实践来看，规范和规则要想被国际社会广泛认可，就必须采取公正的立场，而不是有选择的依据自身利益来区别对待。“区分法”背后体现的是霸权思维和单边主义思想，并不符合网络空间秩序的要求，黑客干预大选体现了网络空间安全是无等级、非对称的，没有所谓能够自我防御的霸权国家，单边主义无法应对挑战。因此，国际社会只有采取集体行动才能加以应对。这就要求在网络空间治理中采取平等协商的方式，考虑各国的共同关切，并采取客观公正的立场推动网络空间治理进程。

第三，网络赋权趋势要求网络空间治理要有新的制度安排。网络赋权的趋势表明网络安全部门、网络情报机构、网络部队等传统意义上关注国内问题或隐藏在背后的一些部门已经冲到大国博弈和国际安全秩序的前线，成为最重要的影响力量之一。但是这些相关的网络安全部门在定位上并非传统意义上开展国际合作的部门，国际社会并没有制度性的安排来容纳这些部门。另外，网络安全技术的复杂性使得传统上擅长国际对话交流的外交部门和经济部门缺乏对上述安全部门的内部协调能力。这两方面因素叠加成为当前网络空间安全治理进程难以取得实质性突破的主要原因之一。目前网络空间安全治理进程中一个主要问题就是缺乏相关网络安全部门的参与，外交和经济部门的谈判成果难以落到实处，无论是联合国信息安全政府专家组，还是G20 之类多边机制，甚至双边合作都面临着如何落实的问题。

因此，建立综合性的国际安全制度性框架具有必要性和紧迫性。首先，各国政府应更加重视建立内部的沟通协调机制，在大国合作和国际安全合作的背景下，看待网络安全部门的作用，建立有效的跨部门对话协商机制。其次，探索建立危机管控机制。2013 年斯诺登事件发生后，因对俄罗斯收留斯诺登不满，美国中断了与俄罗斯在网络安全领域的对话。在美国大选过程中，奥巴马曾通过热线致电普京，要求俄罗斯停止通过网络干预美国大选，

但未起到任何作用。黑客干预大选事件表明危机管控机制的重要性，它能够为相关国家在网络安全领域的博弈和互动建立共识，并设立一定的底线。危机管控的缺乏将会为冲突爆发埋下隐患。最后，在有害网络信息、归因技术、漏洞信息共享等技术层面开展网络安全的务实合作。使网络空间安全的冲突和博弈从政治层面逐步回归到技术层面，更有利于问题的发现和解决。

四、中国的应对

美国大选“黑客门”反映出来的网络安全和国际安全趋势，以及国际社会在治理层面的缺失都表明，未来任何国家都可能面临同样的风险，中国作为网络空间大国也不例外。因此，对中国而言，应该客观分析事件所反映的趋势对中国网络安全和国家安全的潜在影响，从国际网络安全治理架构、大国关系以及国家网络安全能力建设出发，采取多方面的措施积极应对挑战。从大选“黑客门”、大规模网络监听等国际网络安全事件中吸取经验教训，制定完善的应对方案。

第一，中国应在国际网络空间治理机制中积极提倡新的网络规范。中国不仅是网络大国，也是网络空间治理中的重要建设者。中国一直积极主张尊重网络主权，反对任何形式的网络攻击。[①] 但是网络空间的复杂性和各方的利益争夺使国际社会在网络主权以及网络空间和平、安全上难以达成共识。尽管大选“黑客门”事件给美国等西方国家乃至国际社会带来了深刻的教训，改变了人们对网络空间安全的认知和定义，但传统思维和固定的思维模式依旧在国际社会中普遍存在，并倾向于以旧的模式来应对新的趋势和挑战。例如，美欧国家在“黑客门”事件发生后纷纷出台《反信息作战法》，成立相应的反信息宣传机构，这些举措从某种程度上看还是用传统的认知模式来看待网络空间安全的新发展，落入了单边主义和威慑战略的窠臼。这也是为什么至今依然缺乏对谁是“黑客门”背后主使形成客观结论的最主要原因，其

[①] 中华人民共和国外交部、国家互联网信息办公室：《网络空间国际合作战略》，新华网，2017 年 3 月 1 日，http://news.xinhuanet.com/politics/2017-03/01/c_1120552767.htm。

中的根本原因在于缺乏有公信力的国际机构或第三方机构的认定。同时，美国采取的报复措施也无法对所谓的对手进行有效威慑，更不能促进国际社会在相关问题上达成共识。

中国应在联合国大会、联合国信息安全政府专家组等国际机制中明确提议，在网络主权的原则之下，各国政府不应从事或者支持利用互联网从事对政治人物的网络攻击，并利用获取的信息进行虚假宣传以实现政治干预的目的。推动国际社会将上述观点作为各国网络空间的重要行为准则，纳入联合国以及其他重要的国际机制中。这样就可以最大限度避免类似事件对各国的影响，遏止网络空间安全泛化的趋势，保障各国的网络主权以及国家安全。不仅如此，中国还应当推动在联合国框架下建立针对类似事件进行调查和争端解决的机制。尽管现有的联合国机构缺乏相应的人才、资源和技术能力，但鉴于联合国具有的合法性地位，它是促使各方能够达成共识的理想选择。此外，各方对联合国究竟应该在国际网络空间安全治理中发挥什么样的作用还存在很大分歧。如何提出详细的论证方案和付诸不懈的外交努力是推动各方合作的重要因素。例如，自 1998 年起俄罗斯政府就不断向联合国大会第一委员会提交“安全背景下信息和电信领域的发展”决议草案。因受到美国的阻挠，草案一直未被联大接受，直到 2010 年，包括中国在内的很多国家加入到支持队伍中，美国政府只好接受。该决议草案成为后来中俄等国联合提交联大的“信息安全国际行为准则”的基础，甚至在某种程度上为联合国信息安全政府专家组的设立奠定了基础。[①] 俄罗斯提出方案并不懈努力对中国具有很重要的启示意义，即联合国作为一个有众多成员国的国际组织，在开展具体工作时，我们需要不断推动并积极付诸外交努力。

第二，构建与主要大国之间的信任措施。中国是外部网络干涉和虚假信息宣传最主要的受害国家之一，网上针对政府和社会的各种虚假信息和谣言层出不穷，不仅威胁政治和社会稳定，也造成了不可估量的经济损失，中国政府采取了很多举措来维护境内的互联网信息内容的安全和有序流动。很多

[①] Tim Maurer, “Cyber Norm Emergence at the United Nations-An Analysis of the UN’s Activities Regarding Cyber-security,” Belfer Center for Science and International Affairs, September 2011, http://www.belfercenter.org/sites/default/files/legacy/files/maurer-cyber-norm-dp-2011-11-final.pdf.

西方国家以所谓“互联网自由”和“自由表达”为名批评中国的政策和法规，从客观上破坏了中国与一些西方国家的互信，损害了合作的基础，加剧了双方在网络空间安全治理领域的对立。如中国的《网络空间安全战略》所言，网络空间是一个新的空间，包含了政治、经济、社会的方方面面。[①] 不仅不应该用一成不变的传统眼光来看待网络空间，也不应该因为在某些领域的分歧而损害其他领域的合作。相反，应当采取求同存异的态度，搁置在某些领域的分歧，寻找更多的合作点，通过合作来增进信任，从而更好地解决分歧。

大选“黑客门”表明，网络空间作为一个新的空间，各国虽然面临着不同的问题，但却有着共同的挑战。网络空间事关国家安全，威胁政治、经济、社会和文化，[②] 各国在网络安全的政策和治理上有不同的目标和方法是很正常的。通过建立信任措施，可以增加各国之间的互信，减少冲突。具体包括：建立相应的沟通机制，加强危机管控和避免冲突升级；增加政策的透明度，在重大政策出台前提前沟通，争取各方的理解；开展定期的对话交流，保持各方决策人员之间的定期沟通，增信释疑。中美在打击网络犯罪领域的执法合作就是最典型的案例，2015 年 9 月，习近平主席在访美期间与时任美国总统奥巴马建立了双方在打击网络犯罪领域的执法合作框架，对于化解双方在网络安全领域的对抗，稳定网络关系起到了决定性作用。[③] 此外，中国还与英国、俄罗斯等国建立了相应的合作机制。今后，应当在已有的合作机制基础上进一步发展更全面的信任建立措施，并与其他尚未建立合作机制的大国逐步形成相应的信任建立措施。

第三，加强网络安全能力建设，构建全方位的网络安全防御体系。2016 年 12 月和 2017 年 3 月，中国政府分别公布了《国家网络空间安全战略》和《网络空间国际合作战略》，虽然这两份战略报告的公布是中国网络强国战略的重要基石，但也应当看到，在这之前已经有 70 多个国家公布了网络安

[①] 国家互联网信息办公室：《网络空间国家战略》，国家互联网信息办公室网站，2016 年 12 月 27 日，http://www.cac.gov.cn/2016-12/27/c_1120195926.htm。

[②] 国家互联网信息办公室：《网络空间国家战略》，国家互联网信息办公室网站，2016 年 12 月 27 日，http://www.cac.gov.cn/2016-12/27/c_1120195926.htm。

[③] White House, “FACT SHEET: President Xi Jinping’s State Visit to the United States,” September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

全战略，美国更是早在 2009 年就公布了网络安全战略，之后又在不断推动战略的行动计划。从网络安全国防角度来看，上述两个战略都明确了中国将积极发展网络空间防御力量，特别是在《网络空间国际合作战略》中，明确提到了“网络空间国防力量建设是中国国防和军队现代化建设的重要内容……中国将发挥军队在维护国家网络空间主权、安全和发展利益中的重要作用……遏控网络空间重大危机，保障国家网络安全，维护国家安全和社会稳定”。相比较而言，美国于 2009 年就成立了网络司令部，133 支作战部队完全具备作战能力，并且正在将网络司令部升级为作战司令部。[①]

虽然从态势上来看，中国网络安全战略的起步和发展要比西方发达国家晚，但是如果比较中国的网络战略与西方国家的网络战略，可以发现中国的网络安全战略有很多优点。一方面，对网络空间安全的认知全面、深刻，不仅覆盖了政治、经济、文化、社会的方方面面，而且能够从技术、法律、政策、人才等多重视角来看待每个领域遇到的机遇与挑战。而美国等国家的网络战略更多是从传统的视角来看待网络空间，考虑的问题也比较单一。另一方面，中国的网络安全战略更加平衡和包容，不像西方国家网络安全战略那么咄咄逼人和自我标榜。中国的网络安全战略在某种意义上是一种对网络空间治理的探索，对现实和未来都保留着一定的弹性，而西方国家的网络安全战略更多是强调塑造，主张按照其理念来对网络空间进行塑造，忽视了不同国家的国情和发展阶段，对抗性较强。

总而言之，中国已经在网络空间治理中展示出了负责任大国的姿态。今后，中国应进一步加强对类似大选“黑客门”这样的网络安全事件的分析能力和应对能力，一方面推动国际社会制定相应的规范，另一方面要积极加强能力建设，保障中国网络空间的安全和秩序。

[收稿日期：2017-03-27]
[修回日期：2017-05-31]
[责任编辑：石晨霞]

[①] DOD, “Department of Defense Cyber Stretegy,” April 15, 2015, https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.