DOI：10.16513/j.cnki.qjip.2021.0012　网络首发时间：2021-05-06 15:44:18
网络首发地址：https://kns.cnki.net/kcms/detail/10.1393.D.20210506.0855.010.html

互联网如何改变国际关系*

郎　平

【内容提要】　数字时代的国际关系正在迈入一个新阶段。以互联网为代表的信息技术正在自下而上地塑造着主权国家和国际关系：互联网赋权社会，对社会单元进行权力重构，改变国家的传统权力边界；网络空间不断肆虐的网络攻击、基于信息操纵的政治战以及颠覆性技术在军事领域的应用使得国际安全形势更加复杂；围绕科技主导权、数字经贸规则以及网络空间安全规范的大国博弈更趋激烈，赋予大国竞争新的内涵。然而，互联网不会改变主权国家的政治地理学本质，不会改变国际关系以实力为基础的权力博弈逻辑，它改变的是国家的组织和行动方式以及大国竞争的内容和手段。未来的大国竞争将是一种“融合国力”的竞争，大国越是能够有效地融合各领域的国力并将其投射在网络空间，就越是能够在新一轮的科技革命竞争中获胜。

【关键词】　网络空间　大国竞争　网络安全　融合国力

【作者简介】　郎平，中国社会科学院世界经济与政治研究所研究员。
电子邮箱：langping@cass.org.cn

当今世界正处于以互联网为代表的信息技术革命快速发展的进程中。在过去的半个世纪中，以互联网为代表的信息技术在创新通信方式和提高计算效率的同时，跨越传统的国家地理边界，在全球构建了一个互联互通的

*　本文是国家社会科学基金重大项目“网络空间国际规则博弈的中国主张与话语权研究”（项目批准号：20&ZD204）的阶段性成果。感谢清华大学国际关系论坛“新科技与国际关系”研讨会线上和线下与会者给予作者的启发，特别致谢匿名评审专家以及阎学通、漆海霞、李莉、邢悦、徐进、乔燕婷、延志伟、谭亚凌等同仁对于本文提出的宝贵建议和意见，希望本文能够激发国际关系学界对数字时代国际关系新变化更深入的思考。

网络空间。网络空间深刻改变了人们的生活方式、生产方式和社会互动方式，对国家的政治、经济、社会、文化和安全秩序带来诸多的冲击和挑战。当主权国家成为网络空间治理的重要行为体，地缘政治因素逐渐渗透并显著影响着网络空间的国际治理进程；与此同时，网络空间也会反作用于主权国家的行为模式和互动结果，冲击原有的国家政治生态、国家安全和国际秩序，这在一定程度上助推了当今世界百年未有之大变局。那么，互联网如何改变国际关系？具体而言，以互联网为代表的信息技术会通过何种方式、在哪些方面改变当前主权国家主导的国际关系？有哪些主要因素决定了以互联网为代表的信息技术能够改变国际关系的程度和方向？

一、问题的提出

进入21世纪，我们正处于所谓的第四次科技革命浪潮。以互联网、大数据、人工智能和物联网为重要驱动力，人类正在逐步迈向数字化和智能化的新时代，网络空间构成了国家间互动的重要外部环境。与此同时，互联网成为当今世界百年未有之大变局的重要推动力之一：科技革命助推了大国实力对比变化，网络文化传播推动了民众权利意识觉醒，数字贸易和数字货币的崛起加速了国际贸易金融体系的重构。与以往以电力、蒸汽机和原子能为代表的工业革命不同，以互联网为代表的信息技术浪潮对国际政治的影响是由下至上的，它首先改变的是人们的思想和生活方式，接下来才逐步实现与传统工业的融合，从而加速重构经济发展、社会秩序与政府治理模式。在数字时代，信息和数据已经成为国家重要的战略资源和权力来源，也成为大国竞争的新领域和新焦点，“世界进入颠覆性变革新阶段”。这些新兴技术不是目前数字技术的渐进式发展，而是真正颠覆性变革，这些技术必将改变我们现在习以为常的所有系统，不仅将改变产品与服务的生产和运输方式，而且将改变我们沟通、协作和体验世界的方式。①

然而，随着互联网在技术上从通信网络到信息网络再到计算网络的演

① 克劳斯·施瓦布、尼古拉斯·戴维斯：《第四次工业革命——行动路线图：打造创新型社会》，世界经济论坛北京代表处译，北京：中信出版社，2018年，第23页。

进,网络空间自身的特征和属性也有了很大的变化。网络空间不仅成为国家发展和繁荣的重要驱动力,也带来了网络攻击、网络犯罪、网络恐怖主义等日益复杂的安全威胁和挑战。互联网先驱伦纳德·克兰罗克(Leonard Kleinrock)回忆:"我们在创造互联网时的想法是:开放、自由、创新和共享,因此没有对使用施加任何限制,也没有采取任何保护措施;然而,我们当时并没有预料到,互联网的黑暗面会如此猛烈地涌现出来。"①不断快速发展和迭代的新兴技术正将世界引入"一半是火焰,一半是海水"的数字时代,网络空间成为大国竞争与博弈的重要领域和重要工具。那么,演进中的互联网会如何改变国际关系?

国际关系学界对互联网与国际关系的研究始于罗伯特·基欧汉和约瑟夫·奈。在 1977 年出版的《权力与相互依赖》一书中,基欧汉和奈对网络空间中的信息治理进行了研究,他们认为,信息传播成本和时间的降低加深了全球相互依赖,而网络空间中信息资源的配置和使用会影响到国际政治的权力关系,信息自由、信息隐私、知识产权保护、网络情报收集等议题都会成为新的议题。②在 2011 年《权力大未来》一书中,约瑟夫·奈特别分析了基于网络产生的权力,他认为网络空间中的权力可以分为强制性权力、议程设置权力和塑造偏好的权力,而国家不是网络空间唯一的行为体,权力正在从国家行为体向非国家行为体扩散。③2014 年,约瑟夫·奈提出了网络空间治理的机制复合体理论,通过建立一个由深度、宽度、组合体和履约度四个维度构成的规范性框架,可以分别对网络空间的域名解析服务、犯罪、战争、间谍、隐私、内容控制和人权等不同治理的子议题进行剖析,以此来确定在特

---

① Leonard Kleinrock, "Opinion: 50 years ago, I helped invent the internet. How did it go so wrong?" *Los Angeles Times*, Oct. 29, 2019, https://www.latimes.com/opinion/story/2019-10-29/internet-50th-anniversary-ucla-kleinrock,访问时间:2020 年 11 月 8 日。

② Keohane Robert O. and Joseph S. Nye Jr., "Power and interdependence," *Survival*, Vol. 15, No. 4, 1973, pp. 158-165; Robert O. Keohane and Joseph S. Nye, *Power and Interdependence: World Politics in Transition* (Boston: Little, Brown, and Company, 1977); 罗伯特·基欧汉、约瑟夫·奈:《权力与相互依赖》,门洪华译,北京大学出版社,2012 年,第 250 页。

③ 约瑟夫·奈:《权力大未来》,王吉美译,北京:中信出版社,2012 年,第 160—176 页。

定议题下的主导行为体。①

如果说2015年以前国际关系学界的研究聚焦于网络空间的治理问题，那么2015年之后，国际关系学界则更多将关注点转向网络空间所带来的安全威胁及其对现存国际秩序的挑战。亨利·基辛格在《世界秩序》中指出，新的互联网技术开辟了全新途径，网络空间挑战了所有历史经验，并且网络空间带来的威胁尚不明朗，无法定义，更难定性；互联网技术还超越了现有的战略和学说，“在这个新时代，对于能力还没有共同的解释，甚至没有共同的理解。对于使用这些能力，尚缺少或明或暗的约束”。②亚历山大·克里姆伯格(Alexander Klimburg)认为：在不远的将来，互联网这个在很大程度上被认为是促进自由和繁荣的领域，很可能会变成一个充满征服与被征服的暗网；当前的世界正在回到某种失序的状态，战争与和平之间的界限变得模糊，国家更多地依靠除全面武装冲突之外的措施来相互制衡，互联网的架构和技术为国家间冲突提供了新的渠道和方式，对国际和平与秩序产生重大威胁。③信息革命改变了全球政治并带来又一次全球权力转移，网络和连通性成为权力和安全的重要来源；个人和私人组织都有权在世界政治中发挥直接作用；信息的传播意味着权力分配更加广泛，非正式网络可以削弱传统官僚机构的垄断地位；网络信息的快速传播意味着政府对议事日程的控制力减弱，公民面临新的脆弱性。④

可以说，数字时代的国际关系迈入了一个新阶段。与以往不同，以互联网为代表的信息技术对主权国家和国际关系的塑造是由下至上的：它赋权社会，改变了国家行为体的权力边界；它被利用或应用于军事领域，为国际安全带来了更多风险和不稳定因素；它成为大国竞争的新焦点，为大国博弈注入了新的内涵。但是，互联网不会改变主权国家的政治地理学本质，也不

---

① Joseph S. Nye Jr.，“The Regime Complex for Managing Global Cyber Activities,” *Global Commission on Internet Governance Paper Series*，No. 1，2014，pp. 5-13.

② 亨利·基辛格：《世界秩序》，胡利平等译，北京：中信出版社，2015年，第452页。

③ Alexander Klimburg，*The Darkening Web*：*The War for Cyberspace*（NY：Penguin Press，2017），p. 11.

④ Nye，Joseph S. Jr.，“The Other Global Power Shift,” *Project Syndicate*，August 6，2020，https://www.project-syndicate.org/commentary/new-technology-threats-to-us-national-security-by-joseph-s-nye-2020-08，访问时间：2020年11月8日。

会改变以实力为基础的国际政治博弈逻辑,它改变的是国家的组织和行动方式以及大国竞争的内容和手段。在当前力量此消彼长、国际秩序面临解构与重构的百年大变局下,这些改变正在同步发生和演进,它所带来的变与不变相互交织、共同作用,正在推动国际关系走向一个更加不确定的未来。

二、互联网改变国家行为体

国家是国际关系中的主要行为体,每一轮重大的科技创新都会对国家政治格局带来重大的变化,信息技术也不例外。与其他科学技术不同的是,互联网带来的不仅仅是一次科技革命,更是一场信息革命,信息成为数字社会发展的重要战略资源,并且从政治、经济、社会、文化和认知方式等多个层面重构着社会。曼纽尔·卡斯特指出,一种新的社会结构——网络社会正在兴起:知识和信息是网络社会生产力的原料,并且在网络逐渐占据支配性结构的过程中起到主要作用;网络化是这个社会不同以往的关键特色,它重构了社会,使得社会的结构充满了弹性,"这在以不断变化与组织流动为特征的社会里是一种决定性的特性",以便适应剧烈变化的外部环境。[①]网络化的逻辑正在不断冲击着原有的社会秩序,自下而上对社会单元进行权力重构,重要的是,互联网正在逐渐改变传统的国家权力边界。

(一)互联网赋权社会

互联网赋权公民和社会或许是网络时代与以往科技革命最大的不同。按照卡斯特的定义:网络社会是由基于数字网络的个体和组织网络建构而成的,通过互联网及其他计算机网络进行通信;这种历史性的特定社会结构,产生于信息和通信技术方面的新技术范式与一些社会文化变革的相互作用。[②]从技术范式来看,网络之所以能够对社会赋权是源于其革命性的传

① 曼纽尔·卡斯特:《网络社会的崛起》,夏铸九译,北京:社会科学文献出版社,2006 年,第 84 页。

② 曼纽尔·卡斯特:《传播力》,汤景泰、星辰译,北京:社会科学文献出版社,2018 年,第Ⅶ页。

播方式，即“互联网是当地的、国家的、全球的信息和传播技术以相对开放的标准和协议以及较低的进入门槛形成的一对一、一对多、多对多、多对一”[①]的万网之网。在这个人人都可以发声的扁平化网络上，网民不仅是信息的消费者，还是信息的生产者和提供者，它颠覆了传统的大众传播模式中公民个体仅仅作为信息接收者的被动地位，使得网民首次拥有了信息生产者和信息散播者的主导能力。

权力是一种关系能力，它使得某个社会行为体能够以符合其意志、利益和价值观的方式，非对称地影响其他社会行为体的决定。[②] 正是借助于网络，网络意见领袖比以往拥有了更多的、更大的塑造社会价值和构建社会机制的权力，而近年来出现的“网络自组织治理”模式就充分体现了个体权力向社区汇聚后而形成的政治影响力。克莱·舍基(Clay Shirky)认为，以往需要协作和体系化的结构才能实现的集体性活动，如今可以通过社交网络关系、常见的临时结盟、统一的目标等松散的协作方式在线发起行动。[③]在这种模式下，借助于网络提供的公共平台，世界各地原本毫无关联的普通民众和机构都可以在网络上发起合作社区，相互影响，相互帮助，建立信任；即使没有管理中心和一个体系化的结构，基于互联网的“集体行动”仍然可以实现。有学者将“社区成员所交换的信息和思想等同于军事和经济力量”，认为这已经成为政治权力的关键来源。[④]

对于社会而言，技术是中性的，权力也是如此。互联网赋权后的个体和社会一方面可以借助互联网提供的便捷工具和平台参与公共事务，实现民意的汇聚和公共利益的表达，强化公众和舆论的政治监督作用；另一方面，网络的匿名性和快速传播放大了社会阴暗面的负面效应，为敌对势力、恐怖分子和不法分子提供了新的宣传渠道，社会心理、技术平台以及政治的结合

---

① 安德鲁·查德威克：《互联网政治学：国家、公民与新传播技术》，任孟山译，北京：华夏出版社，2010年，第9页。

② 曼纽尔·卡斯特：《传播力》，汤景泰、星辰译，北京：社会科学文献出版社，2018年，第8页。

③ Clay Shirky, *Here Comes Everybody: The Power of Organizing without Organizations* (NY: Penguin Press, 2008).

④ Irene S. Wu, *Forging Trust Communities: How Technology Change Politics* (Baltimore, MD: Johns Hopkins University Press, 2015).

也可能会带来社会的撕裂和分化。随着上网的人数不断增多,网络也变得越来越复杂,基于互联网的"公民不服从"行动常常更具危险性和颠覆性,一旦被操纵或利用,就可能对社会稳定和国家安全带来重大的挑战。

(二)互联网赋权平台企业

如果说网民个体由信息消费者向生产者的角色转换使其获得了更大的政治话语权,那么作为数字时代排头兵的互联网私营企业则凭借其对数字时代关键资源的掌控能力,在国家的经济和政治生活中获得了更大的影响力和主导权。随着互联网公司和平台的不断发展和壮大,少数科技巨头所掌控的经济和社会资源几乎可以与国家相匹配,并且会对现有的经济、政治和社会秩序带来重要的冲击和挑战。

作为数字技术的创新和应用主体,互联网企业是网络社会中最重要的技术节点和信息流动节点。如果说网络权力来源于"促成最大数量的、有价值的连接以及导向共同的政治、经济和社会目标的能力"①,那么互联网企业正是网络权力的主要受益者。与传统的企业不同,互联网企业利用先进的信息技术,大力发展共享经济,一系列植根于代码和算法的新规范正在创建,并试图取代传统上由政府设定和主导的规范;借助于区块链、人工智能等新技术,互联网企业可能从根本上改变工作的本质与社会经济发展的模式,特别是会触及传统上由国家主导的贸易、金融和财政系统的运作。正是在这个意义上,互联网企业被称作"破坏性的创新者"。这些基于网络和数字技术的"破坏性的创新者"正在多个核心领域挑战国家以及国家间组织,其影响正在广泛扩散。在此情况下,国家正在失去其作为"集体行动的最佳机制"的地位。②

当前,网络安全已经成为国家面临的重大安全威胁,针对国家关键基础设施的黑客攻击行动,窃取和侵犯公民个人信息和商业机密的网络犯罪活

---

① Annie Marie Slaughter, "Sovereignty and Power in a Networked World Order," *Stanford Journal of International Law*, 2004, No. 40, pp. 283.

② Clayton Christensen et al., "Disruptive Innovation for Social Change," *Harvard Business Review*, December 2006, http://hbr.org/2006/12/disruptive-innovation-for-social-change/ar/1,访问时间:2020 年 11 月 8 日。

动，发布假消息和进行信息操纵等信息安全威胁，针对供应链和产业链的安全攻击以及网络恐怖主义活动等安全威胁与日俱增。面对日益严峻的网络安全形势，技术治网已经成为国家维护网络安全的重要支柱，应对任何一种安全威胁都离不开网络安全企业的支持。在全球层面，互联网企业特别是科技巨头更是在安全规则的制定中发挥了积极的作用。2017 年，微软公司敦促各国政府缔结《数字日内瓦公约》，建立一个独立小组来调查和共享攻击信息，从而保护平民免受政府力量支持的网络黑客攻击；[①]2018 年，微软再次联合脸书、思科等 34 家科技巨头签署《网络科技公约》，加强对网络攻击的联合防御，加强技术合作，承诺不卷入由政府发动的网络安全攻击。[②]此外，在联合国网络安全规则开放式工作组的推进过程中，微软、卡巴斯基等互联网科技巨头也纷纷提出方案和建议，就全球网络空间安全规则的制定建言献策。可以说，维护国家和全球的网络安全离不开互联网企业的参与。

由于集聚了越来越多的线上社交活动以及由此产生的数据，社交媒体已经成为网络时代文化传播和信息沟通的重要平台，是日常生活不可或缺的一部分。[③] 社交媒体打破了传统大众媒体的舆论垄断并且其影响力俨然已经超越了后者，成为网络时代的舆论场；社交媒体还可以凭借算法和人物画像等技术，具备了塑造社会行为和观念的能力，将传统上被国家政府所垄断的公权力“私有化”。有学者认为，社交媒体是在模仿生物生活的基本规则和功能，其文化基因使其作为网络社会基本的组成单元，越来越像一个

① Microsoft, “A Digital Geneva Convention to protect cyberspace,” Dec. 19, 2017, https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace, 访问时间：2018 年 12 月 5 日。

② Brad Smith, “34 companies stand up for cybersecurity with a tech accord,” April 17, 2018, https://blogs.microsoft.com/on-the-issues/2018/04/17/34-companies-stand-up-for-cybersecurity-with-a-tech-accord/, 访问时间：2020 年 11 月 8 日。

③ 截至 2019 年第一季度，推特日活跃用户同比增长 11%达 1.34 亿；到 2020 年 3 月，微博日活跃用户 2.41 亿，与上年同期相比增长 3800 万；2020 年第一季度，微信月活跃用户达 12.025 亿，同比增 8.2%。

“全球大脑”,正在重塑人类沟通、工作和思考的方式。[①]社交媒体对网络空间和社会的影响都不可忽视。拥有大量数据流量的互联网公司通过对在线内容进行过滤和算法推荐,不但会影响人们获取信息的内容和范围,还可能传播虚假和违法信息,扰乱正常的社会秩序。[②]此外,社交媒体在维护政治稳定、反恐等领域都发挥着关键的作用,有着重要的战略意义。

(三)互联网改变国家权力边界

由于互联网对社会和私营部门的赋权,国家行为体传统的权力边界也遇到了新的挑战。从绝对主权的角度来说,国家行使主权的疆域相较过去有了新的增量,一国基于国家主权对本国的网络设施、网络主体、网络行为、网络数据和信息等享有管辖权、独立权、平等权和防御权;从相对主权的角度来看,网络空间打破了国家对社会元素的垄断,实现了政治权力的再分配,国家不再是享有社会秩序制定权力的唯一主体。那些通过技术赋权的团体、公司和自组织网络,正在对传统的国家主权边界发起挑战,在商业、媒体、社会、战争和外交领域,国家的权力均在不同程度上被削弱或者转移。[③]

国家权力边界之所以在不同程度上被侵蚀,是因为网络空间的技术属性。首先,传统的国家地理边界在网络空间不复存在。作为一个开放的全球系统,网络空间没有物理的国界和地域限制,用户可以以匿名的方式将信息在瞬时从一个终端发送至另一个终端,它不仅正在打破传统意义上的地理疆域,同时也可能削弱基于领土的主权国家合法性。其次,以信息和数据为表现形式的互联网内容层不仅关系到公民的个人信息和隐私保护权利,更关系到国家主权和政治安全。然而,海量的数据大大增加了确权和甄别

---

① Oliver Luckett and Michael Casey, *The Social Organism: A Radical Understanding of Social Media to Transform Your Business and Life* (NY: Hachette Books, 2016).

② Susan Jackson, “Turning IR Landscape in a Shifting Media Ecology: The State of IR Literature on New Media,” *International Studies Review*, Vol. 21, No. 3, 2019, pp. 518-534.

③ 郎平:《主权原则在网络空间面临的挑战》,《现代国际关系》2019 年第 6 期,第 44—50 页。

的难度，而数据掌控在私营企业手中也限制了政府预判形势和管控危机的能力。再次，与传统上国家主权来源于政府自上而下的权威不同，网络权力取决于其能够“促成最大数量的、有价值的连接以及导向共同的政治、经济和社会目标的能力”，也即“个体和团体运用软实力”的能力。[①]网络化的扁平结构削弱了政府的权力，却并不必然带来权力的去中心化，反而会根据控制流量的大小在不同的节点上形成新的权力中心。

更重要的是，互联网动摇了国家垄断军事力量的基础，并在很大程度上改变了传统的战争形态。按照马克斯·韦伯的定义，国家是“这样一个人类团体，它在一定疆域内成功地宣布了对正当使用暴力的垄断权”[②]，其他任何团体或个人未经国家许可都不具有使用暴力的权利。然而，在网络空间，所有现实空间的人和事物都可以被信息化或者数字化，网络武器的生产者与使用者可以是相同的，并且很难对网络武器进行军用和民用的区分。网络武器的使用门槛大大降低，网络购买和快速传递也会加大其扩散的范围，黑客、有组织的犯罪团体和恐怖分子都可以在网络空间发起暴力行动，甚至是对国家发起网络战。网络攻击不需要派遣地面人员，不必出现流血冲突和人员伤亡，信息控制和无人机等自主作战已经成为未来新的战争形态。

综上所述，国家与私营部门和其他行为体的权力边界正在发生变化，国家不再是唯一具有巨大权力的社会行为体。诚如约瑟夫·奈（Joseph S. Nye）所言：“随着信息革命的发展，主权国家的地位会不断衰落，各类依托信息网络技术的非政府组织将拥有跨越领土边界的能力，从而改变现有的社会治理方式。”[③]一方面，政府和其他行为体的绝对权力边界都在向网络空间延伸，催生了新的权力；另一方面，国家和私营部门之间的相对权力边界发生了移动，企业对互联网关键基础设施和资源的掌控力显著增强，政府的主

---

① Anne-Marie Slaughter, “Sovereignty and power in a networked world order,” *Stanford Journal of International Law*, No. 40, 2004, pp. 283-327, https://www.law.upenn.edu/live/files/1647-slaughter-annemarie-sovereignty-and-power-in-a，访问时间：2020 年 11 月 8 日。

② 马克斯·韦伯：《学术与政治》，钱永祥等译，上海三联书店，2019 年。

③ Joseph S. Nye, “Cyber Power,” Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010, https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf，访问时间：2020 年 11 月 8 日。

权行使能力受到了很大制约。国家外部主权面临的情形也是如此,即使是在经济和安全等传统的主权管辖范围内,例如打击网络恐怖主义、网络犯罪和数字贸易规则制定等,仅仅依靠传统的政府间治理机制已难以奏效,而互联网企业和非政府间组织则在积极参与到国际规则的制定中来。

三、互联网改变国际安全

当国家主权由基于领土的地理边界延伸至基于信息技术的虚拟空间,网络空间不可避免地成为国家安全新的威胁来源;网络空间改变了国家的外部安全环境,同时也为国际安全形势增加了诸多不稳定因素,威胁的复杂性和破坏性都在增加。1991 年的海湾战争被认为是现代战争的一个重要分水岭,强大的军事力量不再是战场获胜的唯一法宝,更重要的是要具备赢得信息战和确保信息主导权的能力。美国兰德公司在 1993 年的一份研究报告中首先警告称"网络战即将到来"。[①]尽管网络空间的"珍珠港事件"并没有真的发生,但是在 2007 年爱沙尼亚危机、2008 年格鲁吉亚战争和 2010 年伊朗核设施遭受"震网"蠕虫病毒攻击之后,网络空间成为继海、陆、空、天之后的"第五战场"的想法逐渐变成了真实的存在。网络安全问题开始进入国家军事战略层面,成为一项重要的国家安全议题。

21 世纪 10 年代以来,世界开始真正进入信息时代,互联网上升为国家关键信息基础设施,国家的主权、发展与安全在各个方面都与网络空间息息相关。然而,虽然互联网能够发挥促进自由和繁荣的积极作用,但其消极影响也在不断上升:首先,网络攻击事件愈演愈烈,借助高危漏洞、黑客入侵、病毒木马等工具进行的恶意网络攻击事件频发。2019 年 1 月,Windows 系统爆出零日漏洞[②],该漏洞允许越权读取系统上全部的文件内容;2019 年全年的大流量 DDos 攻击超过 2 万次,与 2018 年相比增长超过 30%。[③]其次,

---

① John Arquilla and David F. Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy*, Vol. 12, No. 2, 1993, pp. 141-65.

② 零日漏洞,又称零时差攻击,是指被发现后立即被恶意利用的安全漏洞,具有突发性与破坏性。

③ 绿盟科技:《2019 年 DDos 攻击态势报告》,2019 年 12 月 26 日,http://blog.nsfocus.net/ddos-attack-landscape-2019/,访问时间:2020 年 11 月 8 日。

智能化、自动化、武器化的网络攻击手段层出不穷，网络攻击正在逐步由传统的单兵作战、单点突破向有组织的网络犯罪和国家级网络攻击模式演变，电力、能源、金融、工业等关键基础设施成为网络攻防对抗的重要战场。最后，人工智能、区块链、物联网等新一代信息技术快速发展，还可能与网络攻击技术融合催生出新型攻击手段。例如，量子计算可以极大降低破解加密算法的时间，人工智能技术催生了自主攻击能力，算法推荐可能衍生出有害信息传播的新模式。

在国家安全层面，网络空间正在变成一张充满征服与被征服的“渐暗的网”[①]。网络攻击肆虐致使国家关键基础设施面临着重大安全风险，利用网络环境实施的传统犯罪行为和利用网络攻防技术实施的网络窃密等犯罪行为屡有发生，利用网络对他国的政治攻击和颠覆活动愈演愈烈，恐怖组织将网络空间作为新的战场并将社交媒体作为其宣传、招募人员、组织行动的重要工具。互联网和信息技术不仅可以被用来在国家间冲突和战争中实施大规模破坏行为，而且也可以被用来支持电子战等传统军事任务，甚至是公开攻击关键基础设施和军事指挥网络的战争行为。鲍尔斯（Shawn Powers）和雅布隆斯基（Michael Jablonski）认为国家正在陷入一场“持续的以国家为中心的控制信息资源的斗争”，其实施方式包括秘密攻击另一个国家的电子系统，并利用互联网推进一个国家的经济和军事议程，其核心目标是运用数字化网络达到地缘政治目的。[②]

简言之，互联网给国际安全形势带来了三个层面的新威胁：一是日益显化的网络空间军备竞赛和针对关键基础实施的网络攻击，威胁到国家的经济和军事安全；二是网络空间的政治战，特别是社交媒体的武器化，威胁到国家的政治安全；三是人工智能等颠覆性技术不断应用于军事领域所带来的潜在安全风险。

（一）网络攻击/网络战

从计算机安全的角度看，网络攻击是指针对计算机信息系统、基础设

---

① Alexander Klimburg, *The Darkening Web: The War for Cyberspace* (NY: Penguin Press, 2017).

② Shawn Powers and Michael Jablonski, *The Real Cyber War: The Political Economy of Internet Freedom* (Chicago: University of Illinois Press, 2015).

施、计算机网络或个人计算机设备的任何类型的进攻动作;对于计算机和计算机网络来说,破坏、揭露、修改数据,使软件或服务失去功能,在没有得到授权的情况下偷取或访问任何一台计算机的数据,都会被视为计算机和计算机网络中的攻击。[①]网络攻击被认为是国家在网络空间面临的重大安全威胁,在很大程度上源于网络空间的技术和虚拟特性。由于互联网在设计之初仅考虑了通信功能而没有顾及安全性,它所采用的全球通用技术体系和标准化的协议虽然保证了异构设备和接入环境的互联互通,但这种开放性也使得安全漏洞更容易被利用,而联通性也为攻击带来了更大的便利。

不同于传统军事打击,网络攻击的特殊性在于:首先,攻击者可以无视国家的地理边界,在网络空间对其他国家的关键基础设施发动攻击,给国家经济运行和社会稳定带来极大的破坏和损失,却不致造成重大的人员伤亡和流血冲突。其次,网络攻击具有极强的隐蔽性,攻击者可以使用网络攻击程序动态切换网络接入位置并调用大量攻击设备,从而使得攻击的溯源和防护非常困难。最后,发动网络攻击的门槛相对于发动武装冲突而言要低得多,且军用和民用设施相互融合难以区分,在溯源、确定反击阈值和对等报复等方面的困难使得传统的军事威慑手段难以在网络空间奏效。

网络攻击能够对国家产生破坏力,是源于代码的武器化,即作为攻击工具的网络武器,其破坏力堪比传统的军事力量和武器。网络武器是指"用于或旨在用于威胁或对结构、系统或生物造成物理、动能或精神伤害的计算机代码"[②]。例如,据俄罗斯卡巴斯基实验室报告,2017 年全球爆发的"wannacry"病毒所使用的黑客工具"永恒之蓝"就来源于美国国家安全局的网络武器库。从 20 世纪 90 年代开始,很多学者就开始研究网络武器所具备的"网络能力"(cyber capabilities),并将其类比为非致命武器和精确制导武器。[③]与非致命武器相似,网络行动可以攻击某个计算机系统的核心部位,控

---

① IBM Services, "What is a cyber attack?" December 1, 2020, https://www.ibm.com/services/business-continuity/cyber-attack, 访问时间:2020 年 12 月 1 日。

② 托马斯·里德:《网络战争:不会发生》,徐龙第译,北京:人民出版社,2017 年,第 46 页。

③ George Perkovich and Ariel E. Levite, eds., *Understanding Cyber Conflict: 24 Analogies* (Wasington D.C.: Gerogetown University Press, 2017), pp. 47-60.

制它们或让其瘫痪。例如，窃取敏感数据以破坏计算机系统数据的机密性，输入恶意指令或破坏重要数据以破坏计算机系统的完整性，或者破坏计算机系统的可用性从而导致其在关键时刻无法接入互联网。同时，如精确制导武器一样，网络武器也可以提供一种潜在的高度精确打击能力，可以只影响特殊目标，进一步提高兵力损失交换比，让攻击发起方面临最小的伤亡风险。

目前来看，网络攻击的效果介于“外交活动和经济制裁”与“军事行动”之间，是否能够实现更大的政治与军事目标还有待观察。网络攻击固然有隐蔽性、低伤亡、灵活和精准打击等优势，但网络攻击也面临着很多局限性。首先，网络攻击行动的成功有赖于能够获得关于攻击目标充分且准确的情报，例如电力系统的控制设计、系统漏洞等，这要求行动发起者具有很高水平的情报获取能力。其次，网络攻击的目标通常是 IT 系统的软硬件，而后者是可以被不断更新和升级的，漏洞发现也会被修补，这就会使得网络攻击的效果有很大的不确定性。最后，由于网络空间的民用和军用设施常常难以区分，如果在打击军事目标时导致民用设施遭到破坏，会提高使用网络武器的政治成本，因而需要对网络攻击发起的时间、方式和地点进行审慎的评估。

按照发起者不同，网络攻击可以分为三类：第一类是作为个体的黑客，他们进行网络攻击的目的通常是宣泄个人情绪或者实施犯罪，一般不具有很大的政治和经济破坏性。第二类是有组织的犯罪集团或者恐怖主义组织，他们利用网络攻击窃取数据以实施有组织的犯罪或实施恐怖活动，对于社会的稳定和经济运行均可造成相当的伤害。第三类是国家或国家支持的组织，其发起网络攻击的目标常常是目标国的关键基础设施或军事设施，具有明确的政治和军事动机，第三类网络攻击活动日益影响着国际安全形势。例如，2019 年 3 月，美国对委内瑞拉的电力系统、通信网络和互联网发动了一次网络攻击，行动命令来自五角大楼，由美国南方司令部直接执行。[①]伊朗

① 环球网：《指责大停电是美网络攻击，马杜罗称将请求中俄等国协助调查》，2019 年 3 月 13 日，https://baijiahao.baidu.com/s?id=1627873072663719586&wfr=spider&for=pc，访问时间：2020 年 11 月 8 日。

也曾经遭受了来自美国的网络攻击。2019 年 6 月,美国对伊朗发动了网络攻击,抹掉了伊朗准军事武装用于秘密计划袭击波斯湾油轮的数据库和计算机系统,短暂削弱了其袭击油轮的能力。① 2020 年 7 月,美国总统特朗普公开证实曾于 2018 年批准了对俄罗斯互联网研究所的网络攻击,并承认该起攻击是在美俄两国政治对抗日益激烈的背景下进行的。②

尽管国际社会和学界对"网络攻击"和"网络战"的界定和认识存在分歧③,但两者之间的一个显著区别是后者仅发生在有政府主体参与的情形。按照克劳塞维茨的定义,"战争是以另一种手段进行的政治,是政治的继续,"因而政治是也应当是国家政策的工具④。因此,只有国家主导或发起的、具有明确军事动机的网络攻击行动才属于网络战范畴。尽管有学者坚持认为真正的网络战必须有重大伤亡,其效果具有毁灭性且等同于武装攻击,或在武装冲突期间发生的网络攻击才能称之为"网络战争"⑤,但是随着现实空间战争的形式逐渐由常规战争向非常规作战和混合战转变,国家间网络冲突——在网络空间发生的具有军事性质的冲突——被认为是现实世界非常规战争的网络再现,"网络战"的概念界定也随之向现实回归,通常用

---

① Julian E. Barnes, Thomas Gibbons-Neff, "US Carried out Cyberattacks on Iran," *The New York Times*, June 22, 2019, https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html, 访问时间:2020 年 11 月 8 日。

② 人民日报海外网:《俄媒:美首次承认对俄网络机构进行攻击》,2020 年 7 月 12 日,https://baijiahao.baidu.com/s?id=1671995507523151374&wfr=spider&for=pc,访问时间:2020 年 11 月 8 日。

③ "攻击"一词在国际法中受到严格限制,意味着重大的伤亡或者破坏。大多数欧洲国家认为,任何严重违反数据保密的行为都构成"网络攻击";美国认为,任何严重侵犯数据完整性以及可用性的行为都可能被视为攻击,例如通过大规模的、不可恢复的数据删除行为来彻底摧毁美国的金融系统;俄罗斯和中国则将通过网络实施"宣传战争"也认定为"网络攻击",但这种观点遭到多数西方国家的反对。Alexander Klimburg, *The Darkening Web: The War for Cyberspace* (NY: Penguin Press, 2017).

④ 詹姆斯·多尔蒂、小罗伯特·普法尔茨格拉夫:《争论中的国际关系理论(第五版)》,阎学通、陈寒溪等译,北京:世界知识出版社,2003 年,第 200 页。

⑤ Jeffrey Caton, *Distinguishing Acts of War in Cyberspace: Assessment Criteria, Policy Considerations, and Response Implications* (P. A.: US Army War College Press, 2014).

来指国家行为体采用网络攻击的方式破坏目标国的关键基础设施或军事力量，被视为21世纪新型的战争形式。①

由于现行的国际法框架无法管控网络冲突、溯源困难以及网络威慑的作用有限，国家之间因而会陷入一种“网络安全困境”：虽然两个国家都不想伤害对方，但由于彼此不信任，往往会发现发动网络入侵才是最明智的选择，而保护自身安全的手段就是威胁他国安全，最终导致冲突不断升级。②特朗普政府上台后，在“美国优先”的保守主义思想指引下，美国网络军事力量发展更加激进，试图通过“持续交手”“前置防御”将行动空间拓展到他国主权范围。俄罗斯网络作战部队隶属于俄军信息对抗体系，2017年2月，俄罗斯国防部长绍伊古表示已经建立了一支负责发动信息战的专业部队，据俄《生意人报》称，俄信息战部队的规模在1000人左右，每年约获得3亿美元的经费支持。③ 德国、巴西和以色列的网络军事化水平也不容忽视。在当前的网络空间冲突中，保护本国的关键基础设施不受网络攻击已经成为各国政府在网络安全领域面临的首要任务。

（二）信息域的政治战

与网络攻击将代码作为武器不同，网络空间的内容也会被一国利用或操纵来实现其针对他国的地缘政治目标，信息域正在成为一个越来越重要的现代政治战领域。所谓“政治战”是指利用政治手段迫使对手按自己的意志行事，它可以与暴力、经济施压、颠覆、外交等手段相结合，但其手段主要是使用文字、图像和思想。④从目标来看，政治战意在影响一个国家的政治构

---

① 也有学者将其称为国家间的“网络冲突”，认为国家间的网络冲突应被看作实施“超限战”的一个重要武器。美国在2011年宣布将把“网络攻击”行为等同于战争行为，并可以用传统军事手段进行惩罚。参见：George Lucas, *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare* (NY: Oxford University Press, 2016).

② Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (NY: Oxford University Press, 2017).

③ 新华网：《俄防长：俄已组建信息战部队》，2017年2月23日，http://www.xinhuanet.com/world/2017-02/23/c_129492633.htm，访问时间：2019年10月10日。

④ Paul A. Smith Jr., *On Political War* (Darby, PA: Diane Pub Co, 1989).

成或战略决策,因为使用的手段是非军事的,因而也常常被称为“心理战”“意识形态战”“思想战”(the war of ideas)。[①]在信息时代,政治战有了新的媒介和工具,那就是网络空间可以瞬时向全球传递的信息。2018 年 4 月,美国兰德公司发布报告《现代政治战》(Modern Political Warfare),强调信息域将是一个争夺日趋激烈甚至是决定性的政治战领域,其本质就是一场通过控制信息流动来进行的有关心理和思想的斗争,其行动包括舆论战、心理战以及对政治派别或反对派的支持。[②]

在信息域,国家面临的首要威胁是本国的信息和数据安全问题。如果说传统的情报活动是在信息传递过程中截获流动的信息,那么数字时代的常见途径就是通过互联网到计算机硬盘、移动存储介质和数据库中获取情报,例如在硬件芯片上做手脚或在软件程序中预留“后门”等。[③] 2013 年 6 月,“斯诺登事件”中曝光的“棱镜门”(PRISM)计划凸显了美国以自身的网络空间优势肆无忌惮窃取他国数据的现实,此后各国政府开始关注本国的数据安全问题,尤以 2018 年 5 月生效的欧盟《通用数据保护条例》(GDPR)为典范。特别是随着大数据时代的到来,个人信息和数据对国家安全的重要性与日俱增,特别是当大多数公民有关政治立场、医疗数据、生物识别数据等隐私数据被敌对国家或他国政府捕获后,经过人工智能大数据分析,都将会产生巨大的安全风险——信息操纵。

信息战在军事领域的应用早已有之,但近十年来,社交媒体的武器化成为现代政治战的突出趋势。信息战的基本作用机制是信息渠道,通过操纵信息,尤其是“对敌意的社会操纵”,聚集了大量互联网用户的社交媒体成为现代政治战的前沿阵地。操纵敌意社会的行为体可以利用有针对性的社交媒体活动、复杂的伪造、网络欺凌和个人骚扰、散布谣言和阴谋论以及其他工具和方法对目标国家造成损害,包括宣传、积极措施、假情报、政治战争等

① Carnes Lord, “The Psychological Dimension in National Strategy,” in Carnes Lord and Frank R. Barnett, eds., *Political Warfare and Psychological Operations: Rethinking the US Approach* (Washington, D. C.: National Defense University Press, 1989), p. 16.

② Linda Robinson et al., “Modern Political Warfare: Current Practices and Possible Responses,” Rand Corporation, 2018, p. 229.

③ 沈昌祥、左晓栋:《信息安全》,杭州:浙江大学出版社,2007 年,第 28 页。

方式。[①] 克林特·瓦茨(Clint Watts)认为,为在政治上攻击有竞争或者敌对关系的国家或颠覆其政权,竞争对手可以利用一国网民的社交媒体信息来描绘其个人的社交网络,识别其弱点,并控制偏好,进而策划各种阴谋,其手段包括新闻推文、网页匿名评论、恶意挑衅和僵尸型社交媒体账户、虚假主题标签和推特活动等。[②] 社交媒体已经成为一个虚拟的战场,攻击行为随时可能发生,政治战和心理战都在社交媒体中找到了新的展现形式。彼得·辛格(P. W. Singer)等人指出,对于这个战场,我们所有人都身处其中,无处可逃,通过社交媒体武器化,互联网正在改变战争与政治。[③]

社交媒体武器化引起国际社会的广泛关注始于2016年美国大选曝出的"黑客门"事件。自特朗普赢得大选之后,时任美国总统奥巴马指责俄罗斯政府授意并帮助黑客侵入民主党网络系统,窃取希拉里及其团队的电子邮件,交给"维基解密"等公之于众,制造希拉里丑闻,通过信息操纵干扰美国总统竞选。这起事件被认为是一次超越传统间谍界限的、试图颠覆美国民主的尝试。[④]约瑟夫·奈认为,随着大数据和人工智能的发展,互联网技术已经成为挑战西方民主的重要工具;基于信息操纵的锐实力(sharp power)正在严重冲击国家的软实力,使得西方民主制度面临危机。[⑤]黑客组织通过综合利用网络攻击、虚假信息和社交媒体操纵活动操纵美国选民,它不仅是美国网络安全领域中具有里程碑意义的事件,更给国际社会敲响了社交媒体

---

① Micheal J. Mazarr et al., "Hostile Social Manipulation: Present Realities and Emerging Trends," Rand Corporation, September 4, 2019.

② Clint Watts, *Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News* (London: Harper Collins Publishers, 2019).

③ P. W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (Boston: Eamon Dolan/Houghton Mifflin Harcourt, 2018).

④ 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,访问时间:2020年11月8日。

⑤ Joseph S. Nye, "Protecting Democracy in an Era of Cyber Information War," Harvard Kennedy School, Belfer Center for Science and International Affairs, February 2019, https://www. belfercenter. org/publication/protecting-democracy-era-cyber-information-war,访问时间:2020年11月8日。

武器化和信息操纵的警钟。

随着大数据和人工智能等新技术的发展和应用,以国家为主导、多种行为体参与、智能算法驱动、利用政治机器人散播虚假信息的计算政治宣传正在越来越多地应用在政治战中。所谓的"国家计算政治宣传",是指政府借助算法、自动化和人工管理账户来有目的地通过社交媒体网络管理和发布误导性信息的信息操纵行为。例如,操纵者可以通过制造假新闻和垃圾信息改变公众认知;通过社交机器人进行社会动员、政治干扰,进而有效干预政治舆论;算法可以模拟人际沟通,包括内容生产和传播的时间模式以及情感的表达。①新冠肺炎疫情期间,在推特、脸书等社交媒体上针对中国的政治宣传就是集中体现,研究人员发现,有关"新型冠状病毒是中国制造的生物武器"的阴谋论,在社交媒体推特经由支持特朗普的机器人账号集中传播的可能性远高于其他可能性。②由此可见,在国家安全威胁日趋多元化的背景下,信息域的政治战已经成为不容忽视的新的战争形式。

(三)颠覆性技术在军事领域的应用

信息技术仍然处于快速发展的进程中,同时也蕴含了更多的不确定性和风险。随着互联网应用和服务逐步向"大智移云"③、万物互联和天地一体的方向演进,颠覆性技术正在成为引领科技创新、维护国家安全的关键力量。颠覆性技术是能通过另辟蹊径或对现有技术进行跨学科、跨领域创新应用,对已有技术产生根本性替代作用并在其领域起到"改变游戏规则"的重要驱动作用的技术,这已经成为各国抢占战略制高点、提升国家竞争力的

---

① Samuel C. Woolley and Philip N. Howard, *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media* (NY: Oxford University Press, 2018);韩娜:"国家安全视域下的计算政治宣传:运行机理、风险识别与应对路径,"北邮互联网治理与法律研究中心,2020 年 6 月 23 日,https://mp.weixin.qq.com/s/1RA7ne5lc-hk0u8_qr9aGQ 访问时间:2020 年 11 月 8 日。

② 邢晓婧:《美媒:调查显示特朗普支持者在社交媒体上散布中国谣言》,环球网,2020 年 6 月 3 日,https://www.sohu.com/a/399422300_162522?_trans_=000014_bdss_dkmgyq,访问时间:2020 年 11 月 8 日。

③ 大数据、人工智能、移动互联网和云存储合称为"大智移云"。

关键要素，但同时也带来了更多的安全风险。①

在当前阶段，人工智能、物联网、云计算、大数据和量子计算等都是代表性的颠覆性技术，但这些颠覆性技术在应用过程中很容易引发新的安全风险，特别是应用或恶意利用颠覆性技术超高的计算、传输和存储能力，实施更为高效、有针对性、难以防守和溯源的网络攻击。例如，利用人工智能技术，攻击者可以高准确度猜测、模仿、学习甚至是欺骗检测规则，挑战网络防御的核心规则；与既有攻击手段融合，在网络攻击效率、网络攻击范围、网络攻击手段等方面加剧网络攻防长期存在的不对等局面；人工智能与区块链、虚拟现实等技术结合还可催生出新型有害信息，形成有针对性的传播目标，衍生有害信息传播新模式，并加大数据和用户隐私全面泄露的风险。②此外，随着物联网以及可穿戴设备的普及，颠覆性技术的使用很有可能使其成为全新的攻击载体，开启了利用网络能力攻击个人的大门，网络武器转变成致命性攻击武器的风险大大提升。

颠覆性技术应用在军事领域必然会给人类带来新的战争威胁。首先，量子计算技术的发展潜力将使信息控制在战争中处于核心地位。当代全球暴力的范式已经从传统的脚本战争(scripted war)1.0 向基于图像的战争 2.0 迈进，而量子计算将使得战争的语言摹本由具有确定性的文字、数字和图片进化到一种不确定的、概率的和可观察的量子战争。③理论上，量子计算机能够大大推进人工智能的突破发展，具备处理和理解海量实时监控数据的能力，那么在信息化的作战环境中，特别是面对海量的监控图片、图像和人体生物信息，掌控量子计算权力的国家会在信息控制和信息解读方面获得巨大的优势，而这在很大程度上意味着一种新的作战时代的到来。尽管量子计算的理论体系还有待完善，现阶段尚未发展出大规模、可商用的计算能力，配套的产业链和软硬件各方面都还有很多技术和产业难题没有克服，但

---

① 可参见：克莱顿·克里斯坦森：《颠覆性创新》，崔传刚译，北京：中信出版社，2019 年。

② 根据中国信息通信研究院安全研究所有关“网信领域颠覆性技术”研讨会的内容整理。

③ James Der Derian, “From War 2.0 to Quantum War: The Superpositionality of Global Violence,” *Australian Journal of International Affairs*, Vol. 67, No. 5, 2013, pp. 570-585.

其对战争甚至是国际秩序的潜在影响力是巨大的。美国国防部网络评估办公室主任安德鲁·马歇尔(Andrew Marshall)认为,如果说第一次世界大战是化学家的战争,第二次世界大战是物理学家的战争,那么第三次世界大战将是信息研究者的战争。①

如果说量子计算改变的是战争的语言摹本,那么人工智能在军事领域的应用将会在很大程度上改写战争的中枢神经系统,给战争带来重大而深远的影响。随着机器算力的提高和大数据技术的发展,人工智能在计算机视觉、语音识别、自然语言处理和机器人技术等领域的应用取得了突破性进展,并被广泛应用于军事领域,例如情报收集和分析、后勤保障、网络空间作战、指挥和控制以及各种军用自主驾驶平台等。其中,机器人的蜂拥控制可以对多个机器人进行规则编程,使其具备应对突发事件的能力,尤其是在遭遇军事威胁时可以做出实时反应,具有比人工控制的机器人更快的反应速度。人工智能对作战方式最大的影响在于其自主武器系统可以对敌方作战系统进行学习和分析,并根据敌方系统特点弥补己方漏洞或根据敌方系统弱点实施针对性打击,这也意味着该系统不仅可以在无人操作的情况下自动攻击敌方目标,而且可以大大缩短己方观察、调整、决策、行动的循环周期。② 此外,机器学习系统还可以通过模式识别技术,分析敌方战术或找出敌方隐藏目标,协助情报分析人员从海量信息中提取有价值的军事情报,提高决策的准确度。

然而,颠覆性技术自身的缺陷和不确定性也必然隐藏着巨大的安全风险。以人工智能为例,首先,在技术层面,人工智能的决策能力严重依赖于数据的完整和准确,一旦出现数据不完整或错误的情况,其数学计算的结果就可能出现偏差,决策的能力和准确度都会出现偏差。其次,在安全层面,人工智能系统一旦遭遇黑客或敌对势力的攻击造成数据损坏或系统被操纵,就可能"精神错乱",对军事行动发出错误的指令,造成难以估量的后果。

---

① 引自 Taylor Owen, *Disruptive Power: The Crisis of the State in the Digital Age* (NY: Oxford University Press, 2015), p. 172.

② Forest E. Morgan and Raphael S. Cohen, "Military Trends and the Future of Warfare: The Changing Global Environment and Its Implication for the US Air Force," Rand Corporation, 2020.

再次，在伦理和法律层面，人工智能不具备人类的价值判断能力，例如，自主作战系统只能根据数学概率识别敌我目标，无法区分战斗人员和非战斗人员，也无法对人身伤亡负法律责任。最后，在战略层面，自主武器系统无法在数学计算中加入对冲突升级、武力威慑、战略稳定等因素的战略考量，缺少对于战场上稍纵即逝的时机的把握。

由此可见，颠覆性技术发展的不确定性及其在军事领域的应用大大增加了网络战争的风险和破坏力。由于某种“未知的未知”（unknown unknowns），其蕴含的巨大风险和不确定性往往使得行为主体倾向于追求对抗的、单边的行为策略，网络空间军事化已成不争的事实。人工智能等颠覆性技术的融合正在成为网络空间攻防对抗的重要技术手段，“进攻占优”的网络攻防过程打破了传统的力量平衡，致使各国大力研发基于颠覆性技术的网络武器，网络空间军备竞赛更是愈演愈烈。[①]在颠覆性技术的驱动下，国际安全格局的力量结构面临着重新调整，大国将围绕致命性自主武器等新安全风险的国际规范制定展开新一轮的博弈。

四、互联网改变大国竞争

数字时代既是当今世界百年大变局得以形成的重要时代背景，也是大变局不断演进和深化的重要驱动力。从全球化进程来看，信息技术发展、跨境数据流动以及数字空间与现实空间的深度融合，意味着全球化进入了一个全新的数字时代。如果说传统上大国竞争的内容是争夺有限的领土和自然资源，那么数字世界最重要的资源——数据——是无限的，数字化程度越高，接入的范围越广，数据的战略价值就越大。然而，与数字世界无限延展的内在驱动力相悖，国家基于主权的权力边界是有限的，为了获得数字世界的主导权，国家主权在网络空间不断延伸和拓展，网络空间的碎片化趋势日趋显著，这又反过来抑制了数字经济扩张的内在动力。中美在网络空间的战略竞争就是在这样的背景下展开的。一方面，中美竞争和对抗的范围和

① 刘杨钺：《技术变革与网络空间安全治理：拥抱“不确定的时代”》，《社会科学》2020年第9期，第41—50页。

力度在不断加大;另一方面,数字世界扩张的自身规律和市场的张力也在发挥作用,两者此消彼长的博弈进程将在很大程度上决定未来全球格局的发展方向。

中美在网络空间日趋激烈的战略竞争,既源自中国崛起后两国之间的结构性冲突,也是特朗普政府大力推进"美国优先"战略所导致的必然结果。特朗普就任以来,网络空间在美国的国家战略定位中有了明显提升,从奥巴马政府时期将网络作为一个安全领域转变为将网络看作促进国家安全和繁荣的时代背景,加速了网络议题与经济和安全等其他领域的融合。2017 年底,特朗普政府出台的美国《国家安全战略报告》将网络安全上升为国家核心利益。2018 年 9 月,美国白宫发布美国《国家网络战略》,15 年来首次全面阐述了美国的国家网络战略,提出保护安全和促进繁荣的四大支柱①,列出了包括保护关键基础设施、保持美国在新兴技术领域的领导地位、推进全生命周期的网络安全等诸多优先事项,并且明确提出中国和俄罗斯是美国的战略竞争对手。2020 年 5 月,美国白宫发布《美国对华战略方针》指出,中国正在经济、价值观和国家安全观三个方面对美国构成挑战。

在上述顶层设计的指引下,美国开始逐步推进在网络空间与中国竞争和"脱钩"的战略意图。从 2018 年对华发起贸易争端指责中国网络窃密、强化美国外国投资委员会(CFIUS)的投资审查、成立特别工作组保护 ICT 供应链,到 2019 年扩大审查中国科技公司的范围、将包括华为在内的数十家企业列入实体清单、全面封杀和遏制华为,再到 2020 年进一步收紧对华为获取美国技术的限制、发布《5G 安全国家战略》、提出"清洁 5G 路径"和"净网计划"、发布针对 TikTok 和微信的行政令、提议修改 APEC 数据流通规则,美

① 四大支柱:通过保护网络、系统、功能和数据来保卫家园;通过培育安全、繁荣的数字经济和强大的国内创新,促进美国繁荣;通过加强美国的网络能力来维护和平与安全——与盟国和伙伴合作,阻止并在必要时惩罚那些出于恶意目的使用网络工具的人;扩展开放、可互操作、可靠和安全的互联网的关键原则,扩大美国在海外的影响力。The White House,"National Cyber Strategy of the United States of America," September 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf#:~:text=The%20National%20Cyber%20Strategy%20demonstrates%20my%20commitment%20to,steps%20to%20enhance%20our%20national%20cyber%20-%20security,访问时间:2020 年 11 月 8 日。

国的“数字铁幕”正缓缓落下，未来出现两个平行体系的可能性正在逐步上升。在大国竞争背景下，尽管中国在网络空间的实力整体上仍然与美国有很大的差距，但考虑到中国互联网企业的快速发展以及网络空间给国家安全带来的诸多挑战和不确定性，美国大力推动对华全面“脱钩”既有国家安全的考量，也有遏制中国赶超的考虑。

（一）科技主导权

科技是第一生产力，在大国战略竞争中始终发挥着至关重要的作用。科技水平不仅直接关系到国家的经济实力，而且对于国家的军事实力更为重要。互联网是在美国诞生的，美国在网络空间已经占据了先天优势，那么在下一轮以 5G、人工智能、量子计算为代表的数字技术竞争中，能够占据先机的国家可以依靠数字技术提升综合国力，成为国际格局变化的新动力。为此，打压和遏制竞争对手的发展势头、争夺科技领域的主导权就必然成为大国竞争的重头戏。阎学通认为，数字经济成为财富的主要来源，技术垄断和跨越式竞争、技术标准制定权的竞争日益成为国际规则制定权的重点；这些特点对国家的领导力提出了更高的要求，如果沿用传统的地缘政治观点来理解当前的国际战略竞争，很可能使国家陷入被动局面。①

5G 技术已经成为中美战略竞争的焦点。5G 技术的特点是超宽带、超高速度和超低延时，在军事领域，5G 技术可以提升情报、监视和侦察系统及处理能力，启用新的指挥和控制方法，精简物流系统、提高效率。② 5G 技术更好的连通性可以转化为更强大的态势感知能力，有助于实现大规模无人机的驾驶以及近乎实时的信息共享，因而具有巨大的商业和军事应用前景。③ 为此，美国除了在国内推出对华为的全面封杀，在国际上也加大对华为的围堵，一方面试图游说其盟友禁用华为的 5G 设备，另一方面也加紧抵制华为

---

① 阎学通：《数字时代的中美战略竞争》，《世界政治研究》2019 年第 2 期，第 1—18 页。

② John R. Hoehn and Kelly M. Sayler，“National Security Implications of Fifth Generation Mobile Technologies，” *Congressional Research Service*，June 12，2019，https://crsreports.congress.gov/product/pdf/IF/IF11251，访问时间：2020 年 11 月 8 日。

③ Richard M. Harrison，“The Promise and Peril of 5G，” May 2019，https://www.afpc.org/publications/articles/the-promise-and-peril-of-5g，访问时间：2020 年 11 月 8 日。

参与全球产业规则的制定。2019 年 5 月,美国联合全球 32 国政府和业界代表共同签署了“布拉格提案”,警告各国政府关注第三方国家对 5G 供应商施加影响的总体风险,特别是那些易于受国家影响或尚未签署网络安全和数据保护协议国家的 5G 通信系统供应商;美国政府表示“计划将该提案作为指导原则,以确保我们的共同繁荣和安全”。① 2019 年 9 月,美国还与波兰共同发表了“5G 安全声明”,将“布拉格提案”的内容落实到双边协议中,用双边规范将华为等中国企业排除在欧美市场之外。2020 年 7 月,英国政府决定自 2021 年起禁止该国移动运营商购买华为 5G 设备,并要在 2027 年以前将华为排除出英国的 5G 设备供应商名单。

科技革命往往有助于推动国家实力的增长和国家间权力的转移。从现实来看,一方面,实力原本强大的国家往往会具备更强的创新能力和应用能力,会更容易在新一轮竞争中占据先发优势;另一方面,重大技术创新或颠覆性技术的影响也会具有不确定性,掌握了某个关键节点优势的国家很可能在某个方面打破原有的权力格局,削弱强大国家的绝对垄断优势。因而,有报告称,尽管中国在 AI 领域取得了快速的进步,但美国的优势会进一步扩大;也有报告认为,美国传统的优势反而会让美国在数字时代处于不利的地位。②因此,我们可以看到技术对国家实力和权力的影响具有两面性,它既可能强化既有的垄断地位,也可能改变原有的权力获取路径。在既有实力差距的客观前提下,国家是否能够在科技竞争中获得更大权力更多取决于国家的变革能力和适应能力。

---

① The White House, “Statement from the Press Secretary,” May 3, 2019, https://www.whitehouse.gov/briefings-statements/statement-press-secretary-54/, 访问时间:2020 年 11 月 8 日。

② Daniel Castro, Michael McLaughlin and Eline Chivot, “Who is Winning the AI Race: China, the EU or the United States?” August 19, 2019, https://www.datainnovation.org/2019/08/who-is-winning-the-ai-race-china-the-eu-or-the-united-states/, 访问时间:2020 年 11 月 8 日;Jack Goldsmith and Stuart Russell, “Strengths Become Vulnerabilities: How a Digital World Become Disadvantages the United States in Its International Relations,” June 6, 2018, https://www.lawfareblog.com/strengths-become-vulnerabilities-how-digital-world-disadvantages-united-states-its-international-0,访问时间:2020 年 11 月 8 日。

（二）数字经贸规则

随着信息通信技术与传统制造业领域的深度融合，数字经济占比在主要大国经济总量中都占据相当的比重。根据中国信息通信研究院的《全球数字经济新图景（2019）》白皮书，2018 年，各国数字经济总量排名与 GDP 排名基本一致，美国仍然高居首位，达到 12.34 万亿美元；中国达到 4.73 万亿美元，位居世界第二；德国、日本、英国和法国的数字经济规模均超过 1 万亿美元，位列第三至六位。英国、美国、德国的数字经济在 GDP 中已占据绝对主导地位，分别为 61.2%、60.2%和 60.0%；韩国、日本、爱尔兰、法国、新加坡、中国和芬兰则位居第四至十位。2018 年，在全球经济增长放缓的不利条件下，有 38 个国家的数字经济增速明显高于同期 GDP 增速，占所有测算国家的 80.9%。①

鉴于数字经济对于国家综合国力竞争的重要性，数字经济规则的制定必然会成为大国博弈的焦点。作为一种新型的生产要素，数据已经成为数字时代重要的战略性资源。一方面，数据是人工智能、量子计算等新技术发展应用的基础和动力；另一方面，基于数据的预测与决策也在很大程度上成为许多产业向前发展的动能和保障，为数字经济发展注入新动能，并且在很大程度上助推了经济社会形态及个人生活的重构。来自麦肯锡全球研究院的研究报告指出，自 2008 年以来，数据流动对全球经济增长的贡献已经超过传统的跨国贸易和投资，不仅支撑了包括商品、服务、资本、人才等其他类型的全球化活动，并发挥着越来越独立的作用，数据全球化成为推动全球经济发展的重要力量。②联合国《2019 年数字经济报告》认为，数字化在创纪录时间内创造了巨大财富的同时，也导致了更大的数字鸿沟，这些财富高度集中在少数国家、公司和个人手中；从国别看，数字经济发展极不均衡，中美两国

---

① 中国信息通信研究院：《全球数字经济新图景（2019）》，2019 年 10 月，http://www.caict.ac.cn/kxyj/qwfb/bps/202010/t20201014_359826.htm，访问时间：2020 年 11 月 8 日。

② Mckinsey Global Institute，“Digital Globalization：The New Era of Global Flows，”February 24，2016，https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows#，访问时间：2020 年 11 月 8 日。

实力大大领先其他国家,国际社会需要探索更全面的方式来支持在数字经济中落后的国家。[①]由此可见,数字经济规则事关大国在数字经济领域的地位和权力分配,对大国综合国力竞争的重要性将愈加凸显。

目前,数字经济规则的谈判在双边、区域和全球等各层面展开。与几个世纪前大国争夺资源的竞争不同,中美竞争追求的是对全球规则制定以及贸易和技术领导地位的争夺。[②] 由于国家的实力、价值观和政策偏好不同,不同国家的政策框架难免会出现差异。基于强大的综合数字优势,美国的数字经济战略更具扩张性和攻击性,其目标是确保美国在数字领域的竞争优势地位。美国主张个人数据跨境自由流动,从而利用数字产业的全球领先优势主导数据流向,但同时又强调限制重要技术数据出口和特定数据领域的外国投资,遏制竞争对手,确保美国在科技领域的主导地位。欧盟则沿袭其注重社会利益的传统,认为数据保护首先是公民的基本人权,其次在区域内实施数字化单一市场战略,在国际上则以数据保护高标准来引导建立全球数据保护规则体系。中国的立场则更为保守,偏重在确保安全的基础上实现有序的数据流动,采取了数据本地化的政策。[③]日本的立场与欧美更为接近。在 2019 年 G20 峰会上,日本提出要推动建立新的国际数据监督体系,会议联合声明强调:"数据、信息、思想和知识的跨境流动提高了生产力、增加了创新并促进了可持续发展;通过应对与隐私、数据保护、知识产权及安全问题相关的挑战,我们可以进一步促进数据自由流动并增强消费者和企业的信任。"[④]

---

① The UNCTAD, "Digital Economy Report 2019," September 4, 2019, https://unctad.org/en/pages/PublicationWebflyer.aspx? publicationid=2466,访问时间:2020 年 11 月 8 日。

② James Andrew Louis, "Technological Competition and China," Center for International Strategic and International Studies, November 30, 2019, https://www.csis.org/analysis/technological-competition-and-china.

③ 上海社会科学院:《全球数据跨境流动政策与中国战略研究报告》,2019 年 8 月,https://www.secrss.com/articles/13274,访问时间:2020 年 11 月 8 日。

④ G20,"G20 Ministerial Statement on Trade and Digital Economy," June 2019, https://www.g20.org/pdf/documents/en/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf,访问时间:2020 年 11 月 8 日。

作为数字经济发展的核心要素，数据跨境流动既涉及个人隐私和信息保护，又涉及国家安全，因而它既是安全问题，也是贸易和经济问题。数据跨境流动需要在个人、经济和安全三者之间寻找平衡：过于强调安全，限制数据的跨境流动性，无疑会限制企业的技术创新能力，对经济增长不利；一味坚持自由流动，则必然会引发对数据安全、国家安全和主权问题的担忧。因此，围绕数据跨境流动规则的国际谈判必将是一个艰难且长期的讨价还价的过程，但它又是一项迫切的任务，因为只有通过国际合作与协调，让国家在制定本国政策框架的同时尽可能照顾到政策的外部性，在安全性和成长性之间寻求平衡，在国家与国家之间实现共识，数字经济的红利才能被各国最大程度地共享。

（三）网络空间国际安全规范

在数字时代，网络空间会影响国家的安全和发展，然而，随着网络空间的军事化和武器化加剧，如何应对复杂严峻的网络空间安全威胁以及如何规范国家间的行为，就成为各国面临的严峻挑战。尽管联合国大会从 2004 年就成立了专家组就“从国际安全角度看信息和电信领域的发展”进行研究，并且在 2015 年达成了 11 条“自愿、非约束性”的负责任国家行为规范，然而遗憾的是，由于中俄与美欧等西方国家在武装冲突法适用于网络空间这个关键节点上立场相左，各大国并未就国际规范达成一致。在缺乏国际秩序和规则约束的状况下，由于利益诉求不同，国家在网络空间的行为常常具有战略进攻性、行为不确定性、政策矛盾性等特点，使得网络空间大国关系处于缺乏互信、竞争大于合作并且冲突难以管控的状态，进而导致网络空间处于一种脆弱的战略稳定。①

2017 年联合国信息安全政府专家组谈判失败，其直接原因是有关国家在国际法适用于网络空间的有关问题（特别是自卫权的行使、国际人道法的适用以及反措施的采取等）上无法达成一致。② 美欧等西方国家支持将武装

---

① 鲁传颖：《网络空间大国关系演进与战略稳定机制构建》，《国外社会科学》2020 年第 2 期，第 96—105 页。

② 黄志雄：《网络空间负责任国家行为规范：源起、影响和应对》，《当代法学》2019 第 1 期，第 60—69 页。

冲突法适用于网络空间,认为恶意的网络行动应该受到国际法的约束和制裁。俄罗斯则认为"自卫权、反制措施等概念本质上是网络强国追求不平等安全的思想,将会推动网络空间军事化,赋予国家在网络空间行使自卫权将会对现有的国际安全架构如安理会造成冲击①"。中方认为将现有武装冲突法直接运用到网络空间可能会加剧网络空间的军备竞赛和军事化,网络空间发生低烈度袭击可以通过和平、非武力手段解决②,反对给予国家在网络空间合法使用武力的法律授权。

但从根本上看,美欧与中俄两个阵营的分野源于双方在网络空间战略利益诉求的差异。与现实空间不同的是,网络空间存在"玻璃房效应",军事实力的绝对优势并不意味着绝对的安全,一国的互联网融入程度越高,对网络空间的依赖越大,它在面对网络攻击等安全威胁时的脆弱性就越大。即使美国在网络空间的军事力量已经处于绝对领先的优势地位,但也同样面临着"越来越多的网络安全漏洞,针对美国利益的毁灭性、破坏性或其他破坏稳定的恶意网络活动,不负责任的国家行为"等不断演进的安全威胁和风险。③为此,特朗普政府推出了"持续交手"④"前置防御"⑤和"分层

---

① Andrey Krutskikh, "Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS's Question Concerning the State of International Dialogue in This Sphere," June 29, 2017, https://www.mid.ru/en/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/2804288, 访问时间:2020 年 11 月 8 日。

② Ma Xinmin, "Key Issues and Future Development of International Cyberspace Law," *China Quarterly of International Strategic Studies*, Vol. 2, No. 1, 2016, pp. 119-133.

③ The White House, "National Cyber Strategy of the United States of America," September 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf#:~:text=The%20National%20Cyber%20Strategy%20demonstrates%20my%20commitment%20to,steps%20to%20enhance%20our%20national%20cyber%20-%20security, 访问时间:2020 年 11 月 8 日。

④ "持续交手"是指在不爆发武装攻击(armed attack)的前提下,打击对手并获取战略收益。

⑤ "前置防御"是指在网络危害发生前,提前收集对手的信息,使对手放弃攻击行动,"从源头上破坏或阻止恶意网络活动,包括低烈度武装冲突"。

威慑”[①]的进攻性网络安全战略，放开了美军在采取进攻性网络行动方面的限制，扩大了美军防御行动的范围，使其能够更自由地对其他的国家和恐怖分子等对手开展网络行动，而不受限于复杂的跨部门法律和政策流程。基于美国自身的网络安全战略，美国在国际规则制定中的利益诉求非常明确，即尽可能获得在网络空间采取行动的法律授权，特朗普政府并没有动力去达成一个约束自己行动能力的国际规则。例如，对伊朗授权使用网络攻击手段的实践就是美国在未来网络空间展开军事行动的体现。中俄不可能认同美国的立场和诉求。

特朗普政府进攻性的网络空间安全战略不仅加剧了自身的安全困境，而且导致大国间的战略竞争面临失控的风险。尽管 2019 年联合国网络空间安全规则的谈判进程进入了政府专家组（UNGGE）和开放工作组（OEWG）“双轨制”运行的新阶段，但客观上看，近几年的谈判前景并不乐观：首先，在大国无战争的核时代，大国战略竞争不可能通过霸权战争来决定权力的再分配，但是却可以通过网络空间的战争来实现这一目标，从而使得网络攻击越来越多地被用作传统战争的替代或辅助手段，信息战和政治战的重要性将明显上升。其次，由于技术发展带来的不确定性以及网络空间匿名性、溯源难的特性，网络空间所蕴含的不安全感会促使国家去尽可能地探究维护安全的各种路径，特别是网络空间军事能力建设。但在网络空间军民融合、军备水平难以准确评估的情况下，即便能够达成一些原则性、自愿遵守的国际规范，网络空间的军备竞赛还将在事实上持续，直到未来触及彼此都认可的红线。换言之，在网络空间军事力量没有达到一个相对稳定和相对确定的均势之前，网络空间的大国竞争将始终处于脆弱的不稳定状态。

---

① 2020 年 3 月，根据“2019 年国防授权法案”授权成立的美国“网络空间日光浴委员会”（CSC）发布报告，提出“分层网络威慑”的新战略，核心内容包括塑造网络空间行为、拒止对手从网络行动中获益、向对手施加成本三个层次，并提出六大政策支柱以及 75 条政策措施。迄今该战略是否会被美国政府采纳还未有定论，但却在很大程度上可以看出美国网络威慑战略的走势。

五、结论

当今世界仍然处于互联网引领科技革命的早期阶段,数字时代作为一个背景元素正在渗透至国家政治、经济和社会生活的方方面面,或早或晚,国家体系的各个节点必须进行新的调适以适应新的现实,而最终呈现的结果将是网络力量与传统力量的融合。国家权力尽管遭遇多方的挑战,但它必然会试图掌握从网络空间中衍生出来的各种权力,以达到某种新的权力平衡;网络空间冲突正在成为大国在战争与和平之间较量的"灰色地带",而胜负的结果在某种程度上仍然有赖于国家实力在网络空间的投射。国家必须在新的时代背景中谋求自身的发展和安全,此时大国格局的基础不仅有赖于传统的国家实力,还有赖于国家在网络空间的力量,特别是两者力量的有机融合以及是否能够彼此促进和强化。无论是从国家内部还是从大国竞争的角度看,一项重大的"权力再平衡"正在进行中,国家的力量正在强势进入网络空间。

尽管如此,在不确定中锚定确定性,特别是在当今国际政治经济格局加速演进、深刻调整的背景下,未来的大国竞争将是一种"融合国力"的竞争:哪个国家能够更有效地融合各领域的国力并将其投射在网络空间,哪个国家就能够在新一轮的科技革命竞争中获胜。这种融合性首先体现在网络议题本身的融合特征上。基于互联网技术和国家行为而衍生的治理问题常常会兼具技术、社会与政治的多重属性,技术、经济和政治议题彼此关联或融合,无论是数据安全还是网络窃密,这些议题往往同时涉及国家在意识形态、经济、政治、安全和战略层面的多重利益和博弈。其次表现为竞争手段的融合。由于信息技术在各领域的应用以及地缘政治因素的强力介入,网络空间的碎片化趋势已经成为必然,这决定了大国对网络空间话语权的争夺将在多领域多节点展开,在客观上对一国政府融合、调配各领域资源的能力提出了更高的要求。

诚如尼尔·弗格森(Niall Ferguson)在其著作《广场与高塔:网络和权力,从共济会到脸书》中所言,我们生活在一个网络化的世界中,等级和网络

的世界相交并产生互动。[①]互联网不会从根本上改变世界，而是与世界既冲突又融合，在无政府世界的丛林中推动构建新的国际秩序。作为当今世界最大的两个经济体，中美两国的战略竞争聚焦于网络空间，未来的国际秩序走向在很大程度上取决于两国“融合国力”的竞争。因此，与后冷战时代技术、经济和安全议题的竞争进程相对独立不同，“政经分离”的现象在数字时代会越来越难以维系，数字时代的“融合国力”竞争比拼的不是各领域实力的综合相加，而是国家在不同领域实力的融合，这需要政府各部门之间更有效地相互协调与配合，而这最终取决于政府的治理能力、变革能力以及国际领导力。

① Niall Ferguson, *The Square and the Tower: Networks and Power, from the Freemasons to Facebook* (NY: Penguin Press, 2018).