外交评论　2020 年 第 3 期

DOI:10. 13569/j. cnki. far. 2020. 03. 069

网络空间军事化及其国际政治影响

杨　楠

摘　要　网络空间军事化是指各国将网络空间相关的资源及技术持续投入军事和安全领域以实现战略目标的过程。近年来，国际网络空间军事化的速度明显加快，各国先后通过一系列举措来完善网络安全战略规划，扩张网络军事组织体系，并在物理、应用和人文层面强化自身的进攻性网络行动能力。网络空间军事化对国际政治领域造成了较为明显的影响，网络空间威胁被“过度安全化”，“网络军备竞赛”提上日程，“网络恐怖主义”如影随形。为了应对这种复杂局面和态势，各国开始发展在网络空间的威慑能力，积极投入网络空间国际规则的制定，并致力于推动关键基础设施保护由传统国内治理模式转向有限度的国际合作。探讨网络空间军事化及其国际政治影响，分析各国以及国际社会的应对方式及其限度，对于深入理解当前网络空间国际治理的现状及其困境具有重要意义。

关键词　网络空间军事化　网络安全　网络空间治理　国家网络战略　国际政治　震网攻击

2010 年，伊朗核设施受到了“震网”（Stuxnet）病毒感染，造成大量离心机被摧毁，核研发进程受到影响。震网攻击是历史上首个通过网络对关键基础设施造成物理伤害的现实案例，一经媒体报道，即在全球范围内掀起轩

＊　杨楠，中国社会科学院美国研究所博士后、助理研究员（北京 100720）。

＊＊　本文是第 66 批中国博士后科学基金面上项目“‘全政府’视阈下美国网络空间战略管理与协调体系研究”（项目编号：2019M660916）的阶段性成果。感谢中共中央党校国际战略研究院樊吉社教授在本文撰写过程中给予的指导和帮助。文中错漏由笔者自负。

然大波。[①] 作为一种武器化的网络工具，震网病毒本身的精密程度、入侵过程中的隐蔽性及潜在杀伤力陡然增加了国家的不安全感，促使攻防、威慑和战争等经典安全概念在网络领域得到再度延展。而震网攻击事件本身则改变了国际行为体之间的传统冲突形式，打开了所谓“网络战”（cyber warfare）的“潘多拉魔盒”，将“进攻性网络行动”（offensive cyber operations）与“网络防御”（cyber defense）等概念置于国际舞台的聚光灯下。[②]

震网攻击事件既是国际安全领域的一次“范式转换”，也是自冷战结束以来网络空间生态发展演进的集中写照。随着信息通信技术（Information Communication Technology，ICT）的长足进步，网络空间作为一个战略领域的重要意义日趋凸显。在国际治理机制滞后甚至趋于失灵的状态下，基于政治目标的军事行为开始逐渐取代原有基于经济目标的犯罪行为，构成网络安全议题的核心要素，其直接结果便是传统地缘政治格局因难以溯源的进攻性网络行动而趋于模糊，行为体间的低烈度网络冲突频发。在这种背景下，各国际行为体基于典型的现实主义逻辑，以加强能力建设和诉诸战略博弈的方式捍卫自身利益，并积极争取在该领域的权力。这种无序状态成为当前国际政治领域的一个重要注脚，即“网络空间军事化”（militarization of cyberspace）。

作为一种实际发生的趋势，国际社会的网络空间军事化在震网攻击事件后逐步凸显，并随时间推移而日益加深。不过，国内外学界有关网络安全的理论性探索对其着墨不多，而各类实证研究大多从网络空间军事化进程的某个侧面展开，缺乏对这一趋势的全局性思考与理性反思。那么，网络空间军事化的实质是什么？在当前网络空间国际规则模糊、全球治理范式尚不明确的背景下，这种趋势给当前国际政治环境带来何种影响？对这些问题的回答是拓宽现有安全认知、完善全球公域建设的应有之意。实际上，网络空间军事化是安全困境的产物，既是当前网络空间不安全状态的重要诱因，也是其导致的结果。为证实这一观点，本文将首先梳理网络空间军事化的具体表现与特征，进而分析网络空间呈现这一趋势的原因以及给国际政治格局带来的影响，最后探讨国际社会缓解这一趋势负面影响的手段及其限度。

---

① Amit Sharma，“Cyber Wars：A Paradigm Shift from Means to Ends”，*Strategic Analysis*，Vol. 34，No. 1，2010，p. 62.

② 参见 Ted Koppel，*Lights Out：A Cyberattack，A National Unprepared，Surviving the Aftermath*，Crown Publishers，2015；Bruce Schneier，*Click Here to Kill Everybody：Security and Survival in a Hyper-connected World*，W. W. Norton & Company，2018。

一、网络空间军事化：问题与研究

网络空间军事化是指各国将与网络空间相关的资源、技术持续投入军事和安全领域以实现战略目标的过程。[①] 尽管互联网因军用需求而生，军事与安全也始终是其发展演进过程中的一个重要维度，但人类最初将网络视为潜在的战略空间，进而构建军事理论学说的尝试则始于冷战末期。作为当代信息技术的先行者，美国的计算机联网规模在里根政府时期迅速扩展，许多专家学者也延续了自托马斯·杰弗逊时代就有的“跨域”（cross-domain）思维传统，[②] 开启了将网络空间视为实现国家利益、诉诸国际冲突之“战场”的猜想。1991 年爆发的海湾战争则为这种猜想提供了现实性依据。基于美军对伊拉克军事控制与通讯系统展开的“电子战”，军事理论家开始对冲突性质及手段的迭代进行深入思考，并系统探讨了瘫痪敌方通信网络、获取“制信息权”（information dominance）在未来战争中的重要意义。[③] 与此同时，兰德公司的研究人员也预见到借助网络实现国家利益的另一种方式，即通过控制信息流来影响对象国民众或政治精英预期的“软军事行动”。尽管这种观念在当时略显“超前”，但其战略逻辑却在 1999 年北约干涉南联盟的行动后清晰可辨。[④] 总之，开启网络空间的军事化进程在早期被视为一种难能可贵的“战略机遇”。

进入 21 世纪，技术的迅速发展与全球扩散使得各类风险交织，创造了一个“失控的世界”，并为人类带来更多的不确定性。[⑤] 网络空间也是如此。在互联网技术扩散并商业化后，“市场导向”令网络科技研发以牺牲安全为代价，换取更

---

① 目前，国内外学界对于“网络空间军事化”这一趋势缺乏明确、统一的界定。有学者曾对这一概念的多个内涵进行辨析。参见 Boguslaw Olszewski，“Militarization of Cyber Space and Multidimensionality of Security”，*Journal of Science of the Military Academy of Land Forces*，Vol. 48，No. 2，2016，pp. 104-120。总体而言，相关定义包含了这一趋势的三个核心特征：（1）政府将资源和技术向军事部门倾斜；（2）是一种长期且持续的过程；（3）同时涵盖进攻性与防御性的战略目标。本文对这一概念的界定有鉴于此。

② Kris Osborn，“Cross-Domain Fires：US Military's Master Plan to Win the Wars of the Future”，*The National Interest*，July 19，2016，https://nationalinterest.org/blog/the-buzz/cross-domain-fires-us-militarys-master-plan-win-the-wars-the-17029. 有关当代美国网络安全理念在冷战末期的源起，参见 Christopher Fuller，“The Roots of the United States' Cyber（In）Security”，*Diplomatic History*，Vol. 43，No. 1，2019，pp. 157-185。

③ John Arquilla and David Ronfeldt，“Cyberwar Is Coming!” in John Arquilla and David Ronfeldt，eds.，*In Athena's Camp：Preparing for Conflict in the Information Age*，Rand Corporation Press，1997，pp. 23-60.

④ Jonathan Zittrain，“‘Netwar’：The Unwelcome Militarization of the Internet Has Arrived”，*Bulletin of the Atomic Scientists*，Vol. 73，No. 5，2017，pp. 300-304.

⑤ 安东尼·吉登斯：《失控的世界》，周云红译，江西人民出版社，2001 年。

加优良的性能。这一态势阻碍了信息安全业的发展，使网络空间的“安全赤字”进一步增加，最终导致“信息科技系统越复杂，漏洞就越多，就越难以控制和管理”。[①] 在这种情况下，此前如约瑟夫·奈所述“因网络优势而带来战略优势”的“信息利剑”成为一把“双刃剑”。[②] 各国开始评估自身关键信息基础设施面对各类网络军事行动的脆弱性，并提出了旨在增加自身耐受力的“弹性”（resilience）治理理念以期将损失降至最低。[③]

随着人类对网络空间军事化的论述由“进攻性叙事”转为“防御性叙事”，学界开始以更为理性的视角探讨如何对进攻性网络行为予以限制，进而抑制网络空间军事化。相关研究大多基于对网络军事化诱因的追溯来探寻其相应对策。以汉森为代表的哥本哈根学派认为，军事化的趋势源于“威胁感知”。风险的未知、对技术的依赖以及防御手段的局限均会迫使行为体对网络空间进行“安全化”，并寻求增强自身的进攻性网络能力以确保安全。[④] 利比奇等人则认为，军事化进程是由“理性驱动”的，即网络空间的不对称特质打破了常规战争中的“成本—收益”平衡，并创造了永恒的“进攻方优势”，从而诱惑行为体参与到这一“潮流”之中。[⑤] 尽管这些研究对网络空间军事化背后的原因做出了理论解释，但却难以给出对等且切实的应对方案。

在“如何管控网络空间军事化”尚无定论的情况下，震网攻击却率先令“网络战略轰炸”成为现实。[⑥] 出于对现实的震惊及对未来的忧惧，学界近年来的探讨转而呈现出卡维尔蒂所述的“震网化”（stuxnetification），即在承认网络空间军事化已成既定现实且无法避免的基础上，密切关注如何降低这种趋势所

---

① 阿兰·柯林斯主编：《当代安全研究》（第三版），高望来、王荣译，世界知识出版社，2016年，第532页。

② Joseph Nye, Jr., and William Owens, “America's Information Edge”, *Foreign Affairs*, Vol. 75, No. 2, 1996, pp. 20-36.

③ Myriam Dunn Cavelty, “Systemic Cyber/in/Security: From Risk to Uncertainty Management in the Digital Realm”, *Swiss Re Risk Dialogue Magazine*, September 15, 2011; Lewis Herrington and Richard Aldrich, “The Future of Cyber-Resilience in an Age of Global Complexity”, *Politics*, Vol. 33, No. 4, 2013, pp. 299-310; Ana Juncos, “Resilience as the New EU Foreign Policy Paradigm: A Pragmatist Turn?” *European Security*, Vol. 26, No. 1, 2017, pp. 1-18; James Brassett and Nick Vaughan-Williams, “Security and the Performative Politics of Resilience: Critical Infrastructure Protection and Humanitarian Emergency Preparedness”, *Security Dialogue*, Vol. 46, No. 1, 2015, pp. 32-50.

④ Lene Hansen and Helen Nissenbaum, “Digital Disaster, Cyber Security, and the Copenhagen School”, *International Studies Quarterly*, Vol. 53, No. 4, 2009, pp. 1155-1175.

⑤ Martin Libicki, “Sub Rosa Cyber War”, in Christian Czosseck and Kenneth Geers, eds., *The Virtual Battlefield: Warfare*, IOS Press, 2009, pp. 55-65; Ilai Saltzman, “Cyber Posturing and the Offense-Defense Balance”, *Contemporary Security Policy*, Vol. 34, No. 1, 2013, pp. 40-63.

⑥ Spencer Ackerman, “With Stuxnet, Did the U. S. and Israel Create a New Cyberwar Era?” Wired, January 16, 2011, https://www.wired.com/2011/01/with-stuxnet-did-the-u-s-and-israel-create-a-new-cyberwar-era/.

造成的损失。[①] 对此，有学者尝试通过对网络空间军事行动的局限性进行客观描述，来改变国际社会基于威胁的叙事模式。[②] 或者力图证实网络军事行动“收益远小于成本”，来破除各行为体对网络不对称优势的笃信。[③] 同时，国际法学界也始终致力于对所谓“网络战规制”的探讨，从另一侧面延缓网络军事化进程。尽管这些理论解释有助于帮助人们洞悉网络空间军事化的内涵，却无力改变国家所处网络空间冲突日趋加剧、“网络军控”遥不可及的现实。正是在这种情势下，网络空间军事化进程“愈演愈烈”，最终成为当代国际政治的重要特征。

二、网络空间军事化的趋势与特征

本世纪初，各国决策界开始意识到网络空间作为战略领域的重要意义，并逐步将与网络空间相关的资源和技术向军事及国防方面倾斜，为可能出现的“网络战”做好准备。震网攻击事件成为助推这一进程的“催化剂”与“导火索”。2010 年后，网络空间军事化速度明显提升，并呈现新的演变特征和趋势，其中，各行为体战略规划的完善、军事组织体系的扩张以及进攻性网络行动能力的强化是反映这一进程的三个核心特质。

（一）网络空间战略规划的完善

行为体对自身网络安全战略的调整契合了全球政治、经济与社会发展的客观需要。冷战结束后，各类网络安全战略的关注重心一度在于保护数字隐私、促进经济贸易及抑制网络犯罪。近十年，军事及国防要素在各国网络安全战略体系中所占比重稳步增加，成为网络空间军事化的基础和前提。涉及网络空间军事化的安全战略大体上可被分为三类，即提供总体战略框架、统筹网络空间威慑能力并厘定威胁响应模式的“国家网络战略”（national cyber strategy）、细化自身在网络空间进攻与防御能力的“网络军事战略”（military cyber strategy）以及旨在防止关键基础设施遭受网络威胁并提供弹性方案的“关键基础设施保护战略”（critical infrastructure protection strategy）。根据美国战略与国际研究中

① Myriam Dunn Cavelty，“The Militarisation of Cyberspace：Why Less May Be Better”，4th International Conference on Cyber Conflict，2012，p. 147.

② Thomas Rid，“Cyber War Will Not Take Place”，*Journal of Strategic Studies*，Vol. 35，No. 3，2012，pp. 5-32；Sean Lawson，“Beyond Cyber-Doom：Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats”，*Journal of Information Technology and Politics*，Vol. 10，No. 1，2013，pp. 86-103.

③ Emilio Iasiello，“Cyber Attack：A Dull Toll to Shape Foreign Policy”，5th International Conference on Cyber Conflict，2013，pp. 451-468.

心（CSIS）和联合国裁军研究所（UNIDIR）发布的指数报告，截至 2019 年底，世界范围内已有 78 个国家发布了国家网络战略、31 个国家发布了网络军事战略、63 个国家发布了关键基础设施保护战略。[①] 其中，有 19 个国家形成了同时涵盖上述三类规划的“战略体系”，可以被视为网络空间军事化进程的主要推动者。[②] 值得注意的是，纵观全球各国，以“防御”为核心理念的“关键基础设施保护战略”大部分都于 2010 年前出台，而以“积极防御”和“进攻”为要旨的“国家网络战略”和“网络军事战略”却几乎都在 2010 年后发布或更新，印证了近十年来网络空间军事化的客观现实（如图-1 所示）。

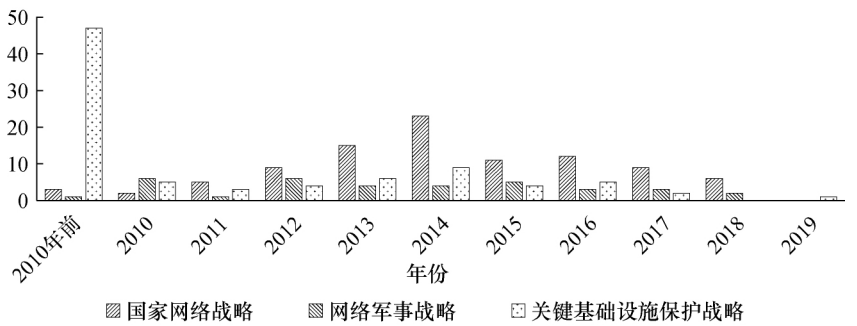

图-1　网络战略与网络空间军事化[③]

如果将网络空间军事化的总体趋势视为全球各国对安全战略持续进行完善的综合结果，那么相对而言，三类国家在推动该趋势的过程中发挥了更为重要的作用。

首先，尽管网络空间具有“去地缘化”的特质，但作为传统地缘政治大国的美国、俄罗斯和中国在这一新兴领域所做的战略规划仍具有较强的导向意义。近年来，三国均明显增加了军事与国防要素在安全战略体系中的比重，并实现了战略重心由常规安全向军事安全的调整，成为全球网络空间军事化的“风向标”。2011 年以来，美国国防部先后通过三份《网络安全战略报告》，完成了从“被动防御”到“主动防御”再到“防御前置”的演进，并倡导通过开发“网络武器”、部署威慑体系以及“提前制止”恶意网络行动等方式来确保自身安全，

① Center for Strategic and International Studies，“Global Cyber Strategies Index”，CSIS Report，January 2020，https://www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/global-cyber-strategies-index.

② 分别为加拿大、中国、捷克、丹麦、爱沙尼亚、拉脱维亚、立陶宛、芬兰、法国、格鲁吉亚、德国、匈牙利、荷兰、俄罗斯、西班牙、瑞典、土耳其、英国与美国。

③ 资料来源：Center for Strategic and International Studies，“Global Cyber Strategies Index”。

体现出愈发强势和主动的进攻性姿态。[①] 相比之下，俄罗斯的网络安全战略则以“威胁”为驱动力，以“防御”为主要特质。该国于2014年和2016年先后公布与更新《联邦网络安全战略构想》及《联邦信息安全学说》，定位了自身面临的各类网络风险，并强调通过将信息战力量嵌入军事与大战略体系来抵御这些风险。[②] 同时，面对北约“咄咄逼人”的威慑与演习，俄罗斯也将网络产品供应链安全和维持互联网独立纳入战略构思，以“战时思维”来应对可能性挑战，2019年的“断网”行动无疑是该战略理念的集中体现。与俄罗斯相似，中国网络空间战略规划的源起及成熟同样源自对外部威胁的感知。在大国网络竞争日趋激化、美国对华网络施压加剧、“污名化”行动频繁发生的背景下，中国政府开始将捍卫网络安全视为维护国家安全的前提要件，并在2016年底公布了首个《国家网络空间安全战略》，明确提到“个别国家强化网络威慑战略，加剧网络空间军备竞赛，世界和平受到新的挑战”，主张在“和平利用网络空间”的基础上，建立与中国国际地位相称、与网络强国相适应的网络空间防护力量，从而维护网络空间这一国家主权的“新疆域”。[③]

其次，作为信息技术研发与实践的“先行者”，欧洲各互联网国家同样高度重视网络安全的国防价值，助推网络空间军事化向纵深迈进。一方面，以英国、法国、德国以及瑞典等国为代表的传统工业化国家均形成了网络空间军事化的战略体系，对自身在网络空间的进攻、防御与威慑能力进行统筹及规划。鉴于国情及战略重心的差异，各国网络空间的军事性要素区别较大，所呈现的姿态也不尽相同。例如，英国在《2016-2021年国家网络安全战略》中侧重防御而淡化主动的军事行动，法国的《国防与国家安全战略评估》则十分注重为传统军事行动注入网络作战要素，而后还在该战略的指导下发布了进攻型网络作战条令。[④] 值得注意的是，一些中立国也分别发布了军事化网络安全战略，如瑞典在2017年先后发布《国家安全战略》和《网络安全战略》，提及建设“稳健的”

① 有关特朗普政府的美国网络安全战略转向与政策调整，参见李恒阳：《特朗普政府网络安全政策的调整及未来挑战》，《美国研究》，2019年第5期，第41—59页。

② James Wirtz, “Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy”, in Kenneth Geers, ed., *Cyber War in Perspective: Russian Aggression Against Ukraine*, NATO CCDCOE Publications, 2015.

③ 中国国家互联网信息办公室：《国家网络空间安全战略》，2016年12月27日，http://www.cac.gov.cn/2016-12/27/c_1120195926.htm。

④ Regner Sabillon, Victor Cavaller, and Jeimy Cano, “National Cyber Security Strategies: Global Trends in Cyberspace”, *International Journal of Computer Science and Software Engineering*, Vol. 5, No. 5, 2016, pp. 67-81.

(robust) 网络国防能力，以应对愈发严重的“混合威胁”(hybrid threats)。[①] 另一方面，以格鲁吉亚、匈牙利和波罗的海三国为代表的中东欧国家因长期作为网络冲突的“战场”而迅速演化出相对成熟的网络安全战略。例如，爱沙尼亚政府、银行及媒体在 2007 年遭受了广泛且深度的网络袭击，被国际战略界视为世界历史上首次国家层面的“网络战”。该国旋即在 2010 年将加强网络国防能力理念融入当年出台的《国家安全理念》与《国防战略》两份报告中，成为国际社会最早发布军事化网络空间战略的国家之一。[②]

最后，出于安全和保密方面的考虑，有一些强敌环伺的区域性国家并未明文公布与国防军事相关的网络安全战略，并试图借此隐匿自身的战略意图。尽管如此，这些国家在网络空间进行宏观统筹规划的能力和实力却难以被国际社会所忽视。伊朗和朝鲜无疑是此类国家的代表。长期以来，发展网络空间的国防军事能力始终是伊朗政府的要务，而其中亟待解决的问题便是确定其在未来构建该领域战略能力的总体方向与具体路径。震网攻击事件“加深了伊朗政府对网络在‘不对称战争’中重要意义的理解”，促使其意识到网络军事能力应当成为其军事战略中的重要“支柱”。[③] 此后，伊朗在网络安全方面的能力建设遵循了较为明显的战略逻辑，即同时强化自身在网络空间的攻击与防御能力，以应对来自美国和各地缘政治对手的“网络战”威胁。与伊朗相似，朝鲜的网络安全战略也可被视为该国军事战略框架下的“衍生品”。鉴于朝鲜与国际互联网的低连接度以及该国关键基础设施与网络的低连接度，其战略重心更侧重于网络攻击能力而非防御能力的发展与强化。[④]

(二) 网络军事组织体系的扩张

主要互联网国家在竞相将军事要素纳入安全战略规划的同时，开始寻求在各自军事体系内建立支撑这些战略的实体机构，从而实现对网络空间军事行动的指挥、协调与保障，贯彻其战略意图。爱沙尼亚国际防卫与安全中心研究员皮雷·贝尔尼克将这些“有形力量”统称为网络军事组织 (military cyber

① Government Office of Sweden, “National Security Strategy”, January 2017, pp. 18-20, https://www.government.se/4aa5de/contentassets/0e04164d7eed462aa511ab03c890372e/national-security-strategy.pdf.

② Government of Estonia, “National Security Concept of Estonia”, May 12, 2010, https://www.eda.europa.eu/docs/default-source/documents/estonia---national-security-concept-of-estonia-2010.pdf; Estonian Ministry of Defense, “National Defense Strategy”, 2010, https://www.kaitseministeerium.ee//sites/default/files/elfinder/article_files/national_defence_strategy.pdf.

③ Hadi Ajili and Mahsa Rouhi, “Iran's Military Strategy”, *Survival*, Vol. 61, No. 6, 2019, pp. 145-146.

④ Jenny Jun, Scott LaFoy, and Ethan Sohn, “North Korea's Cyber Operations: Strategy and Responses”, CSIS Report, December 2015.

organizations，MCOs)，指出各国创设这些机构的目的在于“集中曾经分散的组织，精简过去重叠的能力，消除冗余的人员和职能，最终使自身在网络这一新兴领域中实现有效的军事化运作”。[①] 近年来，各国先后投入大量资源对自身网络军事组织体系进行强化、扩张，成为反映网络空间军事化进程的一个重要侧面。

网络军事行动流程繁复、隐蔽性强，具有较强的跨部门特质，进攻性网络行动尤其如此。一些国家的战略界逐渐意识到组建统一指挥协调机制的重要性。在中美俄三国中，美国率先建立了网络司令部，并基于其网络空间战略理念的演化进行持续的组织革新与职能扩张，最终在特朗普政府时期升级为美军一级联合作战司令部。[②] 同样，作为全球范围内较早将网络技术诉诸实践的国家，以色列在 2003 年便建立了名为“C4I 司令部”（C4I Command）的统筹机制，并在 2011 年通过在其内部增设网络国防司强化其在网络空间的军事协调能力。[③] 依据麦克斯·施密茨的最新研究，包括英国、法国与德国在内的 16 个主要北约国家均在 2010 年前后着手建立统筹性的网络军事组织，大部分在近五年内得到了实质性发展和扩张。[④] 震网攻击后，伊朗先后增设了网络空间最高委员会与网络防御司令部，系统性地强化自身网络军事能力，以应对外界的干扰和威胁。[⑤] 截至目前，大部分国家的网络空间战略指挥协调机制并非“凭空建立”，而是基于对现有机构的重组与合并，意味着此类机制的发展需求与具体实践之间还存在一定程度上的脱节，使得一些原本宣称以“防御”为目的而建立的统筹机构暴露出较强的攻击性，引发其他国家的不安全感。对此，包括中国在内的一些国家对是否应当建立此类机制并对其赋权始终保持相对谨慎的态度。

与网络空间战略统筹机制相对应的则是具体负责贯彻战略意图的网络部队（cyber army）。近年来，世界各国对自身网络空间作战力量的扩充有目共睹。美国在成立网络司令部的同时开始稳步扩充网络部队。2015 年，该司令部战力已

---

① Piret Pernik，“Preparing for Cyber Conflict：Case Studies of Cyber Command”，ICDS Report，December 2018，p. 2，https：//icds. ee/wp-content/uploads/2018/12/ICDS _Report _Preparing _for _Cyber _Conflict _ Piret _Pernik _December _2018-1. pdf.

② Max Smeets and Herbert Lin，“A Strategic Assessment of the U. S. Cyber Command Vison”，in Herbert Lin and Amy Zegart，eds.，*Bytes*，*Bombs*，*and Spies*：*The Strategic Dimensions of Offensive Cyber Operations*，Brookings Institution Press，2019，pp. 81-104.

③ Yaakov Katz，“IDF Sets Up New Cyber-defense Division”，*The Jerusalem Post*，June 28，2011，https：//www. jpost. com/defense/idf-sets-up-new-cyber-defense-division.

④ Max Smeets，“NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations：A Framework for Analysis”，11th International Conference on Cyber Conflict，2019，p. 7.

⑤ Collin Anderson and Karim Sadjadpour，*Iran's Cyber Threat*：*Espionage*，*Sabotage*，*and Revenge*，Carnegie Endowment for International Peace Press，2018，pp. 17-28.

超过 3000 人。其下设的网络任务部队（Cyber Mission Force，CMF）多达 60 余支。而后，在“主动防御”网络安全战略理念指导下，其规模迅猛扩增，2018 年达到 6187 人和 133 支任务部队的“满编状态”。[①] 对于中国来说，建立并强化专门适用于信息作战的力量是“网络强国”战略的重要组成部分。2015 年，中国人民解放军成立战略支援部队，其独立承担包括网络攻防、电子对抗和信息通信等多项作战职能。此外，俄罗斯的特种信息部队、日本网络防卫队以及伊朗伊斯兰革命卫队网络部队等都在近年来持续扩充自身规模，增强网络实战能力，实现对自身常规军事力量的支援，并对潜在的恶意网络行动形成威慑。

为了增强战略统筹机构与网络部队之间的协同能力，各国陆续举行网络攻防实战演习，逐步丰富其内容，并注重提高演练的频率。其中，美国的“网络风暴”、北约的“锁盾”以及俄罗斯的“网络反恐”等演习均已常态化，并根据威胁的变化及时调整演练科目。与此同时，源自军队的战略文化也逐步被私营部门或跨国公司所吸纳。例如，2019 年底，美国网络司令部联合哈佛大学贝尔福中心开展了名为“选举战斗工作者”（Election Battle Staff）的封闭培训，通过实战模拟、战棋推演等具体课程实现对选举管理人员的动员，由此造成的紧张备战状态由军队外溢至民间。[②]

在大多数国家中，网络安全公司、企业与第三方机构等私人部门是网络产品与服务的主要提供者。在当前与网络空间军事化相关的诸多探讨中，这类至关重要的组织却往往被忽略。近年来，各国政府在发展和应用进攻性网络能力时，一般同时面临法律和道义上的束缚、冲突升级失控的危险以及技术人力资源缺失三项掣肘。因而，在政府主导下，越来越多的私人部门开始接受来自政府与军方的外包任务，成为当前网络军事组织体系中的重要组成部分。洛克希德·马丁公司的研究报告显示，近年来各大网络安全私人部门已愈发深入地参与国家网络军事行动之中，形成了一种“网络杀伤链”（cyber-kill chain），为本就脆弱的国际网络安全环境增加了更多不确定性。[③] 随着网络安全人才流动性的

① Joe Gould，“Constructing a Cyber Superpower”，DefenseNews，June 27，2015，https://www.defensenews.com/2015/06/27/constructing-a-cyber-superpower/；U.S. Congress，“Statement of Admiral Michael Rogers，Commander United States Cyber Command Before the Senate Committee on Armed Services”，February 27，2018，p. 9，https://www.armed-services.senate.gov/imo/media/doc/Rogers_02-27-18.pdf.

② Defending Digital Democracy Project，“The Elections Battle Staff Playbook”，Harvard University Belfer Center Report，December 2019，https://www.belfercenter.org/sites/default/files/2019-12/Battle%20Staff.pdf.

③ Eric Mutchins，Michael Cloppert，and Rohan Amin，*Intelligence-driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*，Lockheed Martin Press，2011.

增强，越来越多的私人部门已具备媲美政府和军方的能力，成为网络工具武器化的重要节点，而与官方合作的日趋深化则加速了破坏性网络技术向社会层面的流散。例如，近年来位于澳大利亚的网络安全公司 Azimuth Security 因获得向“五眼联盟”提供技术支持的机会，而在短期内实现了从初创公司到网络军事技术“巨头”的跃升。[①] 在这种情况下，政府和军方越来越乐于借助私人部门实现“网络代理人战争”，私人部门也因利益驱使不断投入军事网络工具的研发，增强自身竞争力。私人部门已成为网络空间军事化的重要推动者，而国际社会对这种合作的监管和约束尚处真空。

（三）进攻性网络行动能力的强化

依据美国国会研究局的分类，国家军事组织诉诸的网络行动（cyber operation）一般包括进攻性网络行动、防御性网络行动以及信息网络管理三个部分。[②] 其中，进攻性网络行动是国家在网络空间投射自身力量的重要方式，体现出较强的侵略特质，是网络空间军事化的关键组成部分。目前，各国分别从与网络空间相关联的物理、应用和人文三个目标层面增强这一能力。

1．物理层面：以实现物理损害为目标

震网攻击所代表的高级持续性网络攻击不仅向世界呈现了新的国际冲突方式，同时也将关键信息基础设施的脆弱性暴露无遗。一方面，该案例加剧了各国的恐惧与不安，使全世界认识到通过网络攻击工业控制系统的方式在理论上有助于取得较为显著的战略效果，这无疑为网络工具武器化提供了发展范式。另一方面，随着技术的发展、军民一体化程度的加深，各国对关键基础设施的依赖性愈发增强，但能采取的防御手段并从攻击中得以缓解的方式却十分有限。由此，在网络空间冲突规制缺失的国际环境下，各大互联网国家陆续投入到此类战略工具的研发和应用之中，传统安全领域的攻防平衡被逐步侵蚀。

与此同时，各行为主体也不吝将这些工具逐步应用于实践。自 2010 年以来，关键基础设施受到威胁的频率持续上升，于 2019 年达到峰值。[③] 尽管这些攻击大部分没有超越震网病毒的烈度，但却在世界范围内引发了与震网攻击相

① Joseph Cox and Lorenzo Franceschi-Bicchierai，“How a Tiny Startup Became the Most Important Hacking Shop You've Never Heard of”，Vice，February 7，2018，https://www.vice.com/en_us/article/8xdayg/iphone-zero-days-inside-azimuth-security.

② Catherine Theohary，“Defense Primer：Cyberspace Operations”，CRS Report，January 14，2020，https://fas.org/sgp/crs/natsec/IF10537.pdf.

③ Stephen Cobb，“Trends 2018：Critical Infrastructure Attacks on the Rise”，welivesecurity，May 30，2018，https://www.welivesecurity.com/2018/05/30/trends-2018-critical-infrastructure-attacks/.

同的影响。2013 年，位于全球人口最稠密区域的纽约鲍曼水坝计算机控制系统被入侵，直到 2016 年，美国司法部才对七名伊朗黑客提出指控。[①] 2015 年与 2016 年，乌克兰首都基辅的电网系统先后两次遭到名为“黑暗能量”的恶意软件攻击而停摆，其背后被公认蕴含了颠覆性的政治因素。[②] 2019 年，此类事件更是此起彼伏。先是委内瑞拉遭遇大面积停电，为本就动荡不宁的委国内局势平添了更多不确定性。[③] 而后，美国对伊朗石油、金融与武器系统发动大规模网络攻击，作为对伊朗先前在霍尔木兹海峡击落其无人机的回应。[④]《纽约时报》还爆料称，美国早在 2012 年就已将恶意代码植入俄罗斯电网系统中。[⑤] 2020 年初，中国网络安全公司 360 根据维基揭秘网站提供的线索，捕获了美国中情局对中国多个政府部门与企业长达 11 年的网络攻击渗透。[⑥]

尽管震网攻击事件告一段落，但既有战略逻辑仍被各行为主体所沿用。随着 5G、人工智能以及物联网等高技术的长足发展，加之伦理约束在网络空间长期缺失，主要网络国家开始依据自身地缘政治利益来诠释这种逻辑，导致这些工具呈现出更强的隐蔽性、更广的攻击范围。与此同时，各国际行为体自身遭受攻击的几率也大幅提升，有些甚至蕴含了引发常规军事冲突的风险。在近年来有关网络战的公开文章中，一多半将关键信息基础设施作为主要论述对象，其中大部分研究认为冲突的关键点在于民用而非军用设施（如图-2 所示），这无疑是客观现实的重要写照。可以预见的是，利用网络对关键信息基础设施造成物理打击仍是各国未来网络空间军事化能力建设的首要目标。

---

① “Cyber Brief: Iranian Cyber in America”, National Security Archive, March 28, 2018, https://nsarchive.gwu.edu/news/cybervault/2018-03-28/cyber-brief-iranian-cyber-america.

② Andy Greenberg, “How an Entire Nation Became Russia's Test Lab for Cyberwar”, Wired, June 20, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/.

③ Joe Parkin, “Venezuela: Widespread Blackouts Could Be New Normal, Experts Warn”, *The Guardian*, July 23, 2019, https://www.theguardian.com/world/2019/jul/23/venezuela-blackouts-new-normal

④ Julian Barnes, “U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say”, *The New York Times*, August 28, 2019, https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html

⑤ David Sanger, “U.S. Escalates Online Attacks on Russia's Power Grid”, *The New York Times*, June 15, 2019, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

⑥ 360 Core Security, “The CIA Hacking Group (APT-C-39) Conducts Cyber-Espionage Operation on China's Critical Industries for 11 Years”, March 2, 2020, http://blogs.360.cn/post/APT-C-39_CIA_EN.html

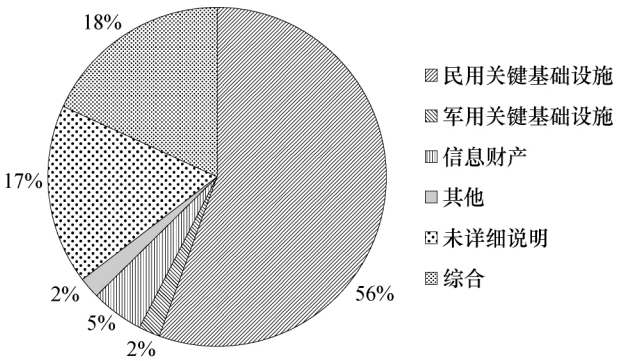

图-2　网络战所意指的战略目标①

2．应用层面：以造成数据损失为目标

利用互联网实现对目标数据、知识产权和情报等信息的搜集、窃取或破坏的网络间谍行为（cyber espionage）是网络空间军事化的早期尝试。与传统间谍行动“非战争行为”的属性相同，网络间谍至今同样处于国际法与国际规制的“灰色区域”，因而被众多国际行为体视为一种重要的战略工具。

震网攻击事件后，由于自身技术水平及归因困境，伊朗对攻击发起者难以做出对等回应。相比之下，网络间谍行为在实施报复行为的同时，会有助于抑制冲突升级，因而成为伊朗的首要战略选择。自2010年以来，这种聚焦于数据层面的冲突成为美伊“网络纠缠”最突出的表现形式。2012—2013年，包括JP摩根、美国银行以及纽约证券交易所在内的一系列美国金融机构陆续遭到黑客攻击，网页和信息被篡改，正常服务受到干扰。2014年，美国一家赌场遭受网络攻击，大量会员的个人资料被窃取。名为“沙蒙”的病毒先后在2012年和2017年入侵了阿美石油公司，清除了超过三万台以上的计算机数据，并用一张焚烧美国国旗的图片改写了硬盘的主引导记录。2020年初，伊朗革命卫队指挥官苏莱曼尼遇刺后，“美国联邦图书馆计划”网站迅速遭到黑客篡改。② 上述网络攻击均被美国归因为伊朗黑客所为，究其动因皆出于对美国侵略行径的回应。

① **资料来源**：Sean Lawson and Michael K. Middleton，“Cyber Pearl Harbor：Analogy，Fear and the Framing of Cyber Security Threats in the United States，1991—2016”，*Peer-Review Journal of the Internet*，March 4，2019，https：//firstmonday. org/ojs/index. php/fm/article/view/9623/7736 # author。

② Marie Baezner，“Iranian Cyber-activities in the Context of Regional Rivalries and International Tensions”，ETH Zürich Center for Security Studies Report，May 2019，pp. 5-8，https：//css. ethz. ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20190507 __MB __HS __IRN% 20V1 __rev. pdf.

而伊朗的网络军事能力也正是在这一时期获得了长足进步。[①]

同一时期，技术扩散也是网络空间军事化在数据层面的重要特征。自2011年以来，名为“Gauss”（高斯）、“Flame”（火焰）和“DuQu”的间谍软件先后给世界各国造成重大损失。网络安全专家指出，这些具备强大信息搜集能力的软件与震网病毒在精密程度和代码编排上有着高度的相似性，可能是由某些国家政府机构提供大量资金和技术支持而研制的网络战工具。[②] 此外，2017年席卷全球的勒索病毒“WannaCry”（想哭）和“NotPetya”也被认为是在美国国家安全局“网络武器”的基础上改造而成。

近年来，以数据为打击对象的网络空间军事化进程总体呈现三种趋势。其一，随着网络技术在国际社会的对称性流动，网络间谍行为已经变得更先进、高效和专业，甚至在某些特定时期取代了传统的人力资源情报活动。其二，网络间谍行为已逐步发展成为各国公认甚至是首选的不对称工具。[③] 相比针对关键基础设施的攻击，这种网络军事行为烈度低，不易诱发大规模冲突。其三，一些非国家行为体很可能借助相关的技术扩散参与全球网络空间军事化进程，给网络安全增添了更多不确定性因素。

3．人文层面：以改变心理预期为目标

政治宣传是一种古老且始终活跃于国际政治历史发展中的战术，其目的在于影响社会大众对某一政府或政策的立场及态度，并使特定人士或团体从中获益。近年来，随着国际互联网连接程度的加深，以及人工智能与大数据等信息技术的日渐成熟，这种在冷战后一度销声匿迹的颠覆行为再度出现，并成为现代政治战的重要一环。[④] 行为体借助互联网中各类社交媒体等媒介，有选择性和有针对性地散播虚假消息（disinformation）与错误信息（misinformation），从而改变受众的心理预期。

尽管网络信息武器化的趋势在近些年刚刚出现，但已对国际政治造成重要影响。北约和欧盟单方面声称，俄罗斯曾在2014—2017年通过《今日俄罗斯》

① Council on Foreign Relations，“The Cyber Competition Between the United States and Iran Matters Less than You Think”，February 26，2015，https://www.cfr.org/blog/cyber-competition-between-united-states-and-iran-matters-less-you-think.

② Bruce Sterling，“Flame/Stuxnet/Duqu Are Attacking Kaspersky”，Wired，June 10，2015，https://www.wired.com/beyond-the-beyond/2015/06/flamestuxnetduqu-attacking-kaspersky/.

③ David Mussington，“Strategic Stability，Cyber Operations and International Security”，Center for International Governance Innovation Report，May 2019，https://www.cigionline.org/articles/strategic-stability-cyber-operations-and-international-security.

④ Linda Robinson and Todd Helmus，*Modern Political Warfare：Current Practices and Possible Responses*，Rand Corporation Press，2018.

与卫星通讯社等媒体集中对波罗的海三国发动了一次有组织的政治宣传活动，同时指责俄罗斯试图通过负面叙事与散布虚假信息等方式，加剧这一地区民众和社会对北约的离心倾向。[①] 2016 年美国大选后，美国情报界断言，选举遭受了来自俄罗斯的“影响力行动”，即企图通过改变选民的信息环境来间接地影响选民决策。[②] 干涉事件导致选举结果的合法性下降，不仅引发了民众的质疑与恐慌，而且在某种程度上动摇了美国民主制度的根基。2018 年，始现于刚果（金）的埃博拉疫情呈现国际扩散的趋势，随之在互联网出现大量有关病毒的虚假信息，加剧了其国内武装冲突和暴力活动，这也成为此后世卫组织将疫情升级为全球卫生紧急事件的重要原因。[③]

相比以物理和数据为打击目标的网络工具，信息武器化更能体现网络战中行动的隐蔽性和影响的广泛性，但常常成为网络空间军事化进程中被忽略的一环。在互联网的回声室效应下，大量信息因难以证伪而被纳入阴谋论，导致很多目标国家当前无法应对此类风险。近年来，世界各主要互联网国家纷纷建立应对这一战术的组织机制，如美国国务院的“全球参与中心”以及北约应对混合威胁卓越中心，恰恰充分体现出此类军事化进程已开始引发国际社会的广泛重视。

三、网络空间军事化的国际政治影响

近年来，网络空间军事化程度日趋加深，但国际社会却没有行之有效的应对策略阻止或延缓这一进程。这种现实给国际政治环境带来了持久而深刻的影响。

（一）网络空间威胁“过度安全化”

“9·11”事件后，以美国为首的主要互联网国家出现了夸大网络空间威胁的倾向，而震网攻击及随后的网络空间军事化则在某种程度上加重了这一趋势。

① Aleksander Król，“Russian Information Warfare in the Baltic States：Resources and Aims”，Warsaw Institute Report，July 20，2017，https：//warsawinstitute. org/russian-information-warfare-baltic-states-resources-aims/.

② United States Office of Intelligence，“Assessing Russian Activities and Intentions in Recent U. S. Elections”，National Security Archive，January 6，2017，p. ii，https：//www. dni. gov/files/documents/ICA _ 2017 _ 01. pdf.

③ David Fidler，“Disinformation and Disease：Social Media and the Ebola Epidemic in the Democratic Republic of the Congo”，Council on Foreign Relations Report，August 20，2019，https：//www. cfr. org/blog/disinformation-and-disease-social-media-and-ebola-epidemic-democratic-republic-congo.

有学者认为，网络工具武器化与新兴技术的扩散给网络安全领域增加了额外的“恐惧风险”（dread risks），令国际社会普遍处于“过度忧虑”状态。[①] 其中，政界、媒体和企业成为相关威胁“过度安全化”（hyper-securitization）的主要推手。

近十年来，尽管美国网络军备规模持续扩大，相关技术也取得长足进步，但大部分国家安全高官始终在公开场合保持较为谨慎的姿态，并声称美国的网络防御能力不足以应对层出不穷的威胁。[②] 除美国外，欧洲各国政要也纷纷有意夸大网络安全威胁，强调应对这些威胁的紧迫性。媒体也在网络威胁“过度安全化”中扮演了重要角色。早在1996年，“网络珍珠港”的类比便首次出现在新闻媒体上。[③] 震网病毒出现以及网络军事化程度加深无疑为这一假设提供了现实论据。以美国媒体为例，如图-3所示，“网络珍珠港”一词在“9·11”事件后的2001—2003年，以及震网攻击事件发酵的2011—2012年均在媒体上有高曝光率，且后者的频率明显高于前者。2011年后，大量有关“网络战”的文章和著作陆续问世，[④]“数字9·11”、“网络闪电战”乃至“数字末日”等词汇层出不穷。此外，出于经济利益考量，大量互联网产业公司也加入渲染网络安全威胁的队伍中。有专家公开表示，震网攻击“仅仅是个开始……一系列‘模仿作品’将会陆续问世”。[⑤] 技术人员为外部威胁“背书”的举动被某些研究人员视为“网络—工业共同体”的诞生。[⑥]

---

① 刘建伟：《恐惧、权力与全球网络安全议题的兴起》，《世界经济与政治》，2013年第12期，第43—59页。

② 例如，2012年时任美国国家安全局局长亚历山大和国防部长帕内塔对于美国面临网络威胁的强调。参见 Josh Rogin，“NSA Chief：Cybercrime Constitutes the ‘Greatest Transfer of Wealth in History’”，*Foreign Policy*，July 9，2012，https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/；U.S. Department of Defense，“Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security”，October 11，2012，https://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136。

③ Sean Lawson，“On This Date in Cyber Doom History：An Example of Getting It So Wring for So Long”，*Forbes*，June 25，2016，https://www.forbes.com/sites/seanlawson/2016/06/25/on-this-date-in-cyber-doom-history-an-example-of-getting-it-so-wrong-for-so-long/#5d74094b56b7.

④ 例如，Richard A. Clarke and Robert Knake，*Cyber War：The Next Threat to National Security and What to Do About It*，Ecco Press，2011；Fred Kaplan，*Dark Territory：The Secret History of Cyber War*，Simon & Schuster Press，2017；David E. Sanger，*The Perfect Weapon：War，Sabotage，and Fear in the Cyber Age*，Crown Press，2018。

⑤ Alexis C. Madrigal，“Stuxnet？Bah，That’s Just the Beginning”，*The Atlantic*，December 16，2010，https://www.theatlantic.com/technology/archive/2010/12/stuxnet-bah-thats-just-the-beginning/68154/.

⑥ 有关“网络—工业共同体”的论述，参见 David Talbot，“The Cyber Security Industrial Complex”，MIT Technology Review，December 6，2011，https://www.technologyreview.com/s/426285/the-cyber-security-industrial-complex/。

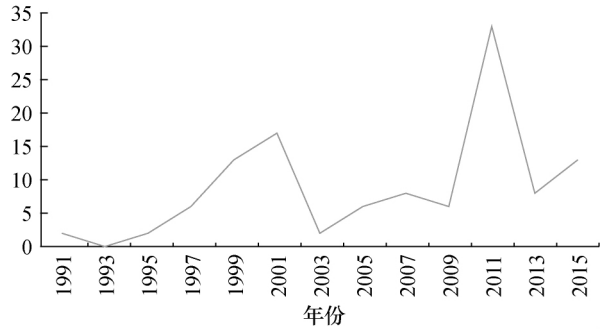

图-3　美国主要媒体提及“网络珍珠港”次数（1991—2015）①

2010年后，尽管大部分网络攻击的技术含量并未超过震网病毒，但上述三个群体仍热衷于持续不断地渲染威胁，加大了民众的恐惧心理。在这种网络“威胁通胀”（threat inflation）的环境下，人们难以就客观事实做出准确而独立的判断，多倾向于听信政客和媒体的宣传与逻辑，“网络不安全”的论断被普遍接受。

（二）“网络军备竞赛”已现雏形

网络空间的军事化导致国家间呈现出一种“预防式的”军事对抗：各国力图在“网络军事装备”质量与数量方面取得相对优势，从而获得战略先机。由此可见，当前国际社会出现所谓“网络军备竞赛”已是不争的事实。

尽管各国战略界对如何“赢得”这样一场竞赛理解有别，但在具体行动上却是殊途同归。首先，鉴于网络空间是一个新兴的战略领域，国家不得不在原有军事预算的基础上增加额外的资金配比。同时，战略重心的差异决定了各国政府及军方利用资金的侧重点。对大部分国家来说，维系网络军事组织的日常运作以及保护关键信息基础设施安全都是必不可少的投入，而意图强化自身进攻性网络行动能力的国家则会投入更多资金致力于网络军备的研发与试用。拿美国来说，在“主动防御”的战略理念下，其针对军事网络安全的资金投入持续上涨，2020财年的预算更是飙升至96.4亿美元，比去年的87.3亿美元上涨了近10%。②

其次，与常规军备竞赛相似，各国也意图通过各种方式扩充自身“网络武器”的储备。一般而言，主要互联网国家通过维持一定程度的研发投入来发现并定位各类“零日漏洞”，并在此基础上研制进攻性网络工具。而对于网络资源和基础设施有限的国家来说，其更倾向以相对低廉的价格从私人部门甚至黑市

① 资料来源：Sean Lawson and Michael K. Middleton，“Cyber Pearl Harbor：Analogy，Fear and the Framing of Cyber Security Threats in the United States，1991—2016”。

② Aaron Boyd，“What DOD Plans to Do With $9.6 Billion in Cyber Funding”，Nextgov，March 14，2019，https://www.nextgov.com/cybersecurity/2019/03/what-dod-plans-do-96-billion-cyber-funding/155564/.

购买并储备这些安全漏洞。[①] 近年来，随着国际社会“网络军备竞赛”加速，一些主要互联网国家也开始涉足这一“灰色”与“黑色”市场，导致安全漏洞出现明显溢价。在强势国家的参与下，本属于弱势国家的“不对称优势”在逐渐减小，反倒加剧了战略竞争中的力量失衡。[②]

最后，对网络安全人才的争夺也是“网络军备竞赛”的重要组成部分。在开放且由利益驱动的网络安全人才市场中，企业始终比政府具备更强的吸引力，令全球各国当前都面临人力资源短缺的重要挑战。据国际信息系统安全认证协会（ISC²）预计，截至 2022 年，全球网络安全人才会出现 180 万个岗位空缺。[③] 在人工智能与自主网络武器尚未成熟的情况下，各国开始投入大量资源参与人才“争夺战”。而为了尽快填补这些空缺，以美国为首的一些国家开始“另辟蹊径”，将重点放到加强与私人部门的联系上。2013 年爆发的“棱镜门”事件非但没有减缓这一趋势，反而坚定了美国政府扶持各类国防承包商的意愿。2016 年，前任网络司令部司令官迈克尔·罗杰斯就曾在参议院军事委员会的听证会上公开表示，在当年招募的 1372 名新成员中，包括 409 名政府外合同制雇员，占总人数的三分之一。[④]

由此可见，世界各国争相发展网络攻防能力的势头逐步上升，美国因其进攻性网络安全战略预设和高额军费投入成为这一趋势的重要推手。如果缺乏长期且行之有效的“网络军控”，那么，网络军备竞赛势必会比常规军备竞赛更容易失去控制。

（三）“网络恐怖主义”引发广泛担忧

网络空间军事化的一个重要方面就是技术向非国家行为体的不对称性流动，引发人们对所谓“网络恐怖主义”迫在眉睫的担忧。如同“恐怖主义”本身存在歧义一样，“网络恐怖主义”概念至今仍缺乏明确界定。[⑤] 早期网络恐怖主义行为是指传

---

① 兰德公司的研究报告对网络安全漏洞“黑市”的经济模式及其对国家战略选择的影响进行了细致探讨。参见 Lillian Albon, Martin Libicki, and Adrea Golay, *Markets for Cybercrime Tools and Stolen Data: Hacker's Bazzar*, Rand Corporation Press, 2014; Lillian Albon and Timothy Bogart, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*, Rand Corporation Press, 2017。

② Irv Lachow and Taylor Grossman, “Cyberwar INC.: Examining the Role of Companies in Offensive Cyber Operations”, in Herbert Lin and Amy Zegart, eds., *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, p. 390.

③ The International Information System Security Certification Consortium, “IT Professionals Are a Critically Underutilized Resource for Cybersecurity”, ISC² Report, September 13, 2017, https://www.isc2.org/-/media/068AEB6CF4CE40948327ECC011A6DC7A.ashx.

④ U.S. Congress, “Statement of Admiral Michael Rogers, Commander United States Cyber Command Before the Senate Committee on Armed Services”, April 5, 2016, p. 1, https://www.armed-services.senate.gov/imo/media/doc/Rogers_04-05-16.pdf.

⑤ Marco Marsili, “The War on Cyberterrorism”, *Democracy and Security*, Vol. 15, No. 2, 2018, pp. 1-4.

统恐怖主义组织利用网络散播极端主义思想及言论。而“网络恐怖主义者”概念一再泛化，涵盖了利用互联网进攻网络站点等企图的黑客主义者（hacktivism）。①

理论上讲，在技术充足的条件下，恐怖分子很有可能将民用电网、航空、公共交通、金融机构或通信网络等作为袭击对象。这一群体热衷破坏，但自身资源匮乏。上述无差别的攻击效果能在保证自身隐蔽的情况下，用较少的资源引发更多的恐慌，与恐怖主义行为的传统思维逻辑高度契合。2010 年末震网攻击事件发酵后，基地组织的线上论坛 Al-Shamukh 旋即发布大量“檄文”，声称要沿用震网攻击的方式对以美国为首的西方国家工控系统进行“灾难性”打击。虽未提及进攻方式，但却给国际社会带来“长期且挥之不去的忧惧”。②

近年来，虽然全球各国经历过难以计量的网络攻击，但没有一次造成“灾难性”后果。尽管如此，国际社会的恐惧感却始终挥之不去。对此，技术界试图破除这种恐惧，对恐怖分子发动网络袭击的可能性进行了前瞻性研究。作为历史上唯一的现实性案例，震网攻击事件再次成为重要的分析基础。震网病毒复杂的设计和耗费巨大资源的运作模式充分证明，非国家行为体发动高烈度网络战争的能力是极其有限的。③ 在这种情况下，激进分子更倾向于利用最简单的方式造成最直接的损伤，因此“网络恐怖袭击”在当下的可能性并不高。④

四、网络空间军事化对策及其局限

近年来愈演愈烈的网络空间军事化佐证了一个重要论断，即网络安全领域的挑战“从来都是政治和经济而非科技层面的”。⑤ 即使解决问题的科技手段已然存在，但相关的组织或个人都很难恰当地使用这种手段。于是，世界各国积

---

① 例如，20 世纪初在互联网兴起、提倡人权和政府透明的政治性黑客组织“匿名者”。参见 Carole Cadwalladr，“Anonymous：Behind the Masks of the Cyber Insurgents”，*The Guardian*，September 8，2012，https：//www. theguardian. com/technology/2012/sep/08/anonymous-behind-masks-cyber-insurgents。

② Thomas Chen，*Cyberterrorism After Stuxnet*，U. S. Army War College Press，2014，p. 14.

③ 针对非国家行为体在网络战争中发挥的作用，目前学界各执一词。有人认为非国家行为体资源有限、能力不足，在一段时间内难以具备发动大规模网络袭击的能力，即网络战“不是弱者的武器”。参见 Jon R. Lindsay，“Stuxnet and the Limits of Cyber Warfare”，*Security Studies*，Vol. 22，No. 3，2013，p. 389。也有人指出，非国家行为体长期保持在网络冲突中的存在，已经实质性地影响网络空间秩序，并间接塑造了网络国际规则。参见 Nicolo Bussolati，“The Rise of Non-State Actors in Cyberwarfare”，in Jens David Ohlin，Kevin Govern，and Clair Finkelstein，eds.，*Cyber War：Law and Ethics for Virtual Conflicts*，Oxford University Press，2015，pp. 102-126。

④ Michael Kenney，“Cyber-Terrorism in a Post-Stuxnet World”，*Orbis*，Vol. 59，No. 1，2015，p. 128.

⑤ 弥尔顿·穆勒：《网络与国家：互联网治理的全球政治学》，周程等译，上海交通大学出版社，2015 年，第 195 页。

极构建网络空间治理体系，完善自身在网络空间的抗御力，促进网络空间规则的制定，并推动关键基础设施由传统国内治理模式走向有限度的国际合作治理。

（一）国家网络威慑能力：理念套用与技术掣肘

威慑的本质是通过增加不对称优势来提高诉诸冲突的成本，达到防止对手潜在进攻的目的。鉴于网络空间与国际社会相似的无政府状态，相关学者一直试图将传统核威慑观念引入该领域。网络工具的潜在杀伤力使其被视为“具有与原子弹和远程轰炸相似的战略能力”，各国也寄希望于再次利用威慑这一核时代的理念来确保安全。[①] 当前，“以威慑求安全”已成为诸多互联网国家适应网络空间军事化的重要选项。

一方面，通过持续增强基础防御能力，实现网络空间的拒止威慑（deterrence by denial）被视为各国“最不坏的选择”。[②] 此前，主权国家往往将提高网络空间防御能力的重心置于信息层面，包括保障安全信息、定期维护信息系统以及发展反病毒工业技术等等。相应手段即在国家层面设立计算机应急应对小组，或在国际层面统一信息安全标准等。在网络空间军事化进程不断加速的影响下，互联网国家对网络空间防御的理解超越了信息层面，对实体设施保护的关注力度明显增强。人们认识到有关网络空间的风险不能完全消除，相关防御措施大部分都是由“风险管理”的理念所引导。在这种情况下，国家通过增设预案、加强管理等方式增强自身应对网络威胁的弹性，并尝试借助常态化演习来进一步提升关键基础设施在遭受重大打击后的恢复能力。

另一方面，鉴于网络空间被公认为是“易攻难守”领域，一些国家在构建防御体系时试图超越单纯的防御，基于惩罚威慑（deterrence by punishment）实现以攻代守，从而迫使敌对国减少对自身的侵略行动。这方面美国体现得尤为明显。奥巴马任内，美国政府始终致力于通过叠加武力与威胁换取网络空间的安全。特朗普执政后，进一步诠释了美国网络部队中的进攻性战略文化传统。[③] 在这种理念影响下，美国不仅执着于保持互联网域内的相对攻击优势，而且努力尝试建构与其适配的军事能力，打造跨域威慑体系。[④] 这种转变在本质上与其长期主导的自由主义传统大相径庭，在某种程度上削弱了国际社会对制定网络空间国际法律及规则的信心。美国的进攻行为甚至引发其他国家的效仿，造成

① John Arquilla，“Deterrence After Stuxnet”，Communications of the ACM，August 4，2015，https://cacm.acm.org/blogs/blog-cacm/190371-deterrence-after-stuxnet/fulltext.

② William J. Lynn III，“Defending a New Domain”，*Foreign Affairs*，September/October 2010.

③ Eric Sterner，“Retaliatory Deterrence in Cyberspace”，*Strategic Studies Quarterly*，Spring 2011，p. 70.

④ 罗曦：《美国构建全域制胜性战略威慑体系与中美战略稳定性》，《外交评论》，2018年第3期，第38页。

负面影响。2019年初，以色列以一次定点空袭回应了此前哈马斯针对它的网络攻击，成为人类历史上首次将跨域威慑转化为实践的案例。[①]

然而，在难以精确定位恶意网络行为发起者的情况下，拒止威慑耗资巨大且效度不高，惩罚威慑更是无从谈起。“溯源困境”长期被视为威慑这一旧有管控理念在网络空间推行的最大障碍。[②] 对此，各国技术人员长期致力于研发新的科技，试图提升溯源的准确度和速度。而对于战略研究者来说，当务之急是依据网络空间特性对传统的威慑框架予以更新。目前，已有学者提出将拒止威慑与惩罚威慑相融合，演化出一套基于“欺骗威慑”（deterrence by deception）理念的网络空间防御模式。[③] 该模式旨在利用“蜜罐”等虚假手段误导对方进攻错误目标，阻止其获利并造成额外消耗，同时或许能解决长期困扰网络安全界的归因问题。实际上，“欺骗威慑”本质上既是一种“以模糊促安全”的防御形式，同时又有助于国家在维护自身道义的基础上诉诸烈度相称的报复，以缓解网络空间军事化所带来的安全困境。然而，这种战略意图在具体贯彻过程中将有很大可能因技术性问题而受到限制。

（二）网络空间国际规则：制定与制约

近十年恰逢网络空间从国内规制迈向全球治理的重要阶段。此前，网络犯罪跨国化程度加剧，国家间数字鸿沟进一步加大，而相应的国际规则却明显缺失。震网攻击造成的负面影响不亚于一次小规模战争，而国际层面的法律法规都无法对制造并投放震网病毒的罪魁祸首进行制裁。根据《战争法》（武装冲突法）对“暴力”的界定，一个国家只有“使用动能武器破坏或摧毁其他国家物理财产”或“在其他国家领土内造成人类伤害或死亡”，才称得上是诉诸战争行为。[④] 显而易见，这一概念过于侧重物理损害，忽视愈发依赖信息和通信技术的国家可能受到非物质的损害方式。因此，通过网络攻击物理设施的手段在很长时间内被视为一种不受束缚的国际冲突模式。

鉴于网络空间军事化带来的不安全感，国际社会开始严肃审视旧有国际法律以人为中心的暴力观，并思考如何对网络冲突与武装冲突之间的“门槛”进

① Lily H. Newman, “What Israel's Strike on Hamas Hackers Means for Cyberwar”, Wired, May 6, 2019, https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/.

② Forrest Hare, “The Significance of Attribution to Cyberspace Coercion: A Political Perspective”, 4th International Conference on Cyber Conflict, 2012, p. 128.

③ Erik Gartzke and Jon R. Lindsay, “Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace”, *Security Studies*, Vol. 24, No. 2, 2015, pp. 316-348.

④ 《联合国宪章》第一章第2条第4款，https://www.un.org/zh/sections/un-charter/chapter-i/index.html。

行界定等规范性问题。尽管学界建议将道德问题扩展到物质世界之外，并引入“信息伦理”作为克服法律有限暴力概念的一种手段，[①] 但国家间缺乏相应的网络安全共识，以及国际社会长期缺乏非侵略性运用网络空间的规范成为问题的关键。当前，尽可能消除或缩小国际法律与网络空间安全之间的“灰色区域”成为规范国际网络空间的重要目标。

然而，在针对《战争法》以及联合国宪章第51条（自卫权）是否适用于网络空间这一原则性问题上，中俄与美欧之间产生了根本性分歧。在第2016—2017届联合国信息安全政府专家组（UNGGE）会议上，美欧各国基于此前G7峰会的《七国集团网络空间原则和行动》（G7 Principles and Actions on Cyber），意图将《战争法》和自卫权引入网络空间，把传统意义上的战争行为与网络战挂钩。这样，这些国家可以利用自身强大的军事能力回应网络攻击，维系“网络霸权”。以中俄为代表的网络“后起国”一致认为，这种以一概全的行为无助于缓解当前网络空间军事化的趋势，甚至会让网络军备竞赛愈演愈烈。这些国家确信，得到美欧各国支持的报告草案第34段试图模糊“动网”与“动武”之间的本质差异，将网络空间转变为军事行动的新疆域，使单边武力行为合法化。双方分歧最终导致谈判破裂。[②] 此外，各国溯源能力的差异也是谈判难以为继的原因之一。尽管网络空间军事化日益加剧，在无法界定网络行动“进攻”或“自卫”性质的状况下，全球政策框架的问世还需主要互联网国家的长期磨合。

（三）关键基础设施保护：国内治理与国际合作

自20世纪90年代起，世界各国逐步将关键基础设施保护议程纳入自身战略规划框架，确保其安全、持续的运营进而成为国家安全目标的组成部分。随着时间推移及科技发展，这一战略要素在两个方面出现了根本变化。其一，关键基础设施与互联网之间的相互依赖日趋加深。其二，这些设施的私有化程度加大，政府管辖权下降。然而，这种变化并未深化人们对关键基础设施的理念与认知。由于关键基础设施并未遭受破坏性后果，各国政府进行保护的动力不足，与之相关的理论探讨与实战演习极其有限。

如果说震网攻击给关键基础设施的脆弱性敲响了警钟，那么随之出现的网络空间军事化进程则将“关键基础设施保护”从国内安全事务上升为国际议题。震网攻击平息后的一次调查显示，世界范围内有七成的关键基础设施公司在此

① Samuli Haataja and Afshin Akhtar-Khavari, “Stuxnet and International Law on the Use of Force: An Informational Approach”, *Cambridge International Law Journal*, Vol. 7, No. 1, 2018, pp. 99-121.

② 徐培喜：《米歇尔Vs.米盖尔：谁导致了UNGGE全球网络安全谈判的破裂？》，《信息安全与通信保密》，2017年第2期，第10—12页。

前至少经历过一起非法网络入侵，[①] 其内部存在的诸多隐患暴露无遗。其一，人们意识到关键基础设施存在安全隐患。民用设施的市场化导向使其长期缺乏应有的维护，导致网络运行故障时常发生，随时有可能将自身漏洞暴露于世，直接损害国家安全。其二，以美国为首的西方社会意识到关键基础设施存在运营隐患。建立在信息交换基础之上的旧有“公私伙伴关系”只取得了“有限的成功”。[②] 政府是否应当加强监管、如何监管、在不同设施中怎样协调现有政策等问题仍亟待解决。其三，内涵界定不清、相关法律不足同样是其存在的重要隐患。为克服这些顽疾，世界各国进一步完善了关键基础设施的国内治理体系，并在此基础上逐步拓展有限的国际合作范式。

互联网国家间的国情和政策差异较大，对关键基础设施的国内治理基本上从三个角度展开。第一，各国政府尝试推动自身与负责管理关键基础设施的机构融合，使双方合作关系更为紧密。在以美国为首的西方互联网国家，传统的公私合作伙伴关系难以解决“网络安全—经济利益”的困境，即互联网市场的激烈竞争、开发防御措施的巨大成本导致产品安全性持续下降，使得防御性措施难以匹配进攻性网络威胁的发展。[③] 有人指出，单纯的投资并不能解决任何问题，政府应当承担更多网络防御的公共成本，而私人企业也应当让渡更多的权力。[④] 对于中国来说，尽管政府和企业之间缺乏相关合作范式，但鉴于大部分关键基础设施都属于国有企业，有关信息及资源的交换渠道更为顺畅，因此在加强关键基础设施治理方面具备天然优势。对此，有学者认为应当通过对关键基础设施实施“动态指定—主体架构—过程控制”三个步骤来推进公私合作与治理。[⑤]

第二，以政府为主导、多部门参与的演习活动逐渐成为拓宽关键基础设施风险应对措施的重要渠道。这些演习逐渐囊括针对基础设施的各类攻击，包括

---

① Kimberly A. Whitler, “70% of Firms Report a Cybersecurity Incident: Why Marketers Should Care”, *Forbes*, February 11, 2017, https://www.forbes.com/sites/kimberlywhitler/2017/02/11/70-of-firms-report-a-cyber-security-incident-why-marketers-should-care/#b644ed830062.

② Myriam Dunn Cavelty and Manuel Suter, “Public-Private Partnerships Are No Silver Bulled: An Expanded Governance Model for Critical Infrastructure Protection”, *International Journal of Critical Infrastructure Protection*, Vol. 2, No. 4, 2009, p. 181.

③ Dale Peterson, “Offensive Cyber Weapons: Construction, Development, and Employment”, *Journal of Strategic Studies*, Vol. 36, No. 1, 2013, p. 123.

④ **有关西方国家关键基础设施管理进程中经济与安全的关系，参见** Ross Anderson and Tyler Moore, “The Economics of Information Security”, *Science*, Vol. 314, No. 5779, October 27, 2006, pp. 610-613; Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*, Praeger Press, 2013。

⑤ **陈越峰：《关键基础设施保护的合作治理》，《法学研究》，2018 年第 6 期，第 175—193 页。**

应对每日恶意软件、处理“零日漏洞”、“鱼叉式攻击”、“水坑攻击”或排除高级持续性威胁等。近年来，美国已经陆续开展了一些相关演习，如 2009 年国土安全部主导的“阿罗拉计划”（Aurora Project）以及上文提到的“网络风暴”、“锁盾”。这些演习有助于检验关键基础设施针对潜在网络攻击的防范能力、事件响应速度、消息流通的安全性与顺畅性。

第三，各国也开始意识到加强关键基础设施内部管理的重要性。欧洲刑警组织在 2016 年的报告中指出，关键基础设施的一个重要弱点源于其内部人员安排失当。[①] 震网攻击同样证明，关键基础设施防御的重要一环便是对人的管理，如果人力防御机制出现漏洞，内外网络间的物理隔绝则形同虚设。对此，卡维尔蒂指出，关键基础设施应当被视为一种“开放城市”理念的重要部分。对于其网络防御不仅需要“城墙守卫”，更重要的是建立和完善内部的“警察队伍”以及“反叛乱小组”。[②]

互联网空间已成为全球重要公域，关键基础设施安全的治理是否可以跨越国家界限，由有限国际合作实现“集体的安全”？震网攻击爆发后，联合国专家对信息科技带来的国家安全问题进行了系统研究，并指出了关键基础设施国际治理的必要性。[③] 为此，各国决策者也尝试在国内治理的基础上进行有限度的国际合作。自 2010 年起，东盟、欧盟、北约、美洲国家组织、亚太经合组织等区域性机制先后利用现有机制框架积极加速合作进程。总体来看，这些努力在某种程度上增强了关键基础设施的网络防御，在国家层面与企业层面实现了有限的信息共享，同时为他国网络安全建设提供了一定程度的援助。这种利用“制约性要求”的模式有效填补了目前国际法缺失背景下关键基础设施合作的空白。同时，一些国际组织也意识到关键基础设施的重要性，纷纷制定相应的保护措施，如国际原子能机构、国际民航组织等开始注重其成员国的能力建设。除了区域和国际组织，诸如管理公用水域或工业事故影响的“软法律”或公约也增强了对关键基础设施的保护。

---

① Europol, “Attacks on Critical Infrastructure”, https://www.europol.europa.eu/iocta/2016/attacks-on-ci.html

② Myriam Dunn Cavelty and Reimer A. Van Der Vlugt, “A Tale of Two Cities: Or How the Wrong Metaphors Lead to Less Security”, *Australian Journal of International Affairs*, January 2015, p. 22.

③ United Nations, “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security”, June 24, 2013, https://undocs.org/A/68/98.

结　语

进入21世纪以来，网络技术在经历迅猛发展后具备了成为武器的能力，为全球带来了更多的风险及不确定性。各国在感知自身存在脆弱性的同时，已经意识到网络作为一个战略空间的重要意义。从这个意义上讲，网络空间的军事化似乎是一种必然的结果。尽管各国承认这一趋势会给国际政治生态带来负面影响，并分别出台了各类应对措施，但在国际法律规制及监管机制长期缺失的状态下，国际社会对于如何消解当前的安全困境仍莫衷一是，“网络军控”则更显渺茫。

当前这种“僵持不下”的局面也为网络空间的未来发展提出了一系列问题。首先，随着全球越来越多的关键基础设施成为“两用目标”，带有军事意图的网络攻击将大概率导致民事损失。一旦发动攻击的行为体因“走投无路”而不再考虑道德伦理，此类攻击的杀伤性则必然趋于无限大，造成的后果更难以预料。那么，从国际社会道德和伦理角度出发，如何界定发动网络攻击的门槛？其次，在网络安全产业市场中，以盈利而非安全为核心导向的运作模式意味着互联网公域存在难以避免的技术滞后与安全漏洞。短期来看，这种情况似乎是不可逆的。那么，在科学与技术层面，国家如何避免自身遭受网络军事化带来的负面影响？最后，“网络军备竞赛”不仅给各国情报机构和军方提供了在网络领域加大行为尺度的动机，同时也使人们对现有国际规则在网络时代的有效性产生了怀疑。那么，从国家宏观战略的角度来看，如何将国际法律和国家规范进行有机结合，从而实现“网络军控”？未来国际社会将难以回避直面这些问题。

技术因人之需要而生，人却赋予这些技术更多的不确定性。鉴于科技本身并不具备道德，建立克制、协调的国际法律和规范是降低未来国际网络不安全的重中之重。近年来，新兴冲突模式所导致的摩擦事件频发，反映了这一领域因规则缺失而引发的无序和混乱。诚然，网络空间“永远无法靠蛮力破门而入”。[①] 积极构建并完善网络秩序法规，提升互联网空间稳定性，进而缓解网络空间军事化带来的对峙情势，是确保网络国际公域长期安全的应有之意。

（责任编辑：李　丹）

① Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, Cambridge University Press, 2007, p. 31.

researchers have paid attention to the geopolitical background of the initiative and institutional competition among great powers. This paper focuses on the new institutional features of the LMC. Compared with the existing international institutions such as the Greater Mekong Sub-region Economic Cooperation (GMS), the LMC has two new institutional features: wider issue scope and higher level of centralization. Besides regional economic cooperation issues, the LMC also put regional security cooperation and water resources cooperation issues on its agenda. Meanwhile, the LMC is a leaders-driven institution and is working hard to build its independent international secretariat, whereas the GMS serves only as a functional ministerial-level institution and uses the ADB as its secretariat. Applying the rational design theory, this paper argues that the increasing severity of distribution problem and enforcement problem in the international cooperation in the Mekong sub-region has led to the establishment of the LMC with new institutional features.

Key words: Lancang-Mekong Cooperation (LMC), Greater Mekong Sub-region Economic Cooperation (GMS), regional security cooperation, water resources cooperation, wider issue scope, higher level of centralization, rational design theory

Militarization of Cyberspace and Its Impact on International Politics

YANG Nan

Abstract: The militarization of cyberspace refers to the process where countries continuously invest resources and technologies of cyberspace in military and security domain to achieve strategic goals. In recent years, the speed of militarization of cyberspace has significantly increased. Countries around the world have adopted measures to improve cyber security strategic planning, expand cyber military organization systems, and strengthen offensive cyber operations capabilities in physical, application, and humanistic dimensions. The militarization of cyberspace has made a significant impact on international politics, including the "hyper-securitization" of threats in cyberspace, the emergence of "cyber arms race", and the haunting "cyber-terrorism". In response to these complicated situations, countries have begun to develop deterrent capabilities in cyberspace, actively invested in the for-

mulation of international rules and laws in cyberspace, and committed themselves to promoting the transformation of critical infrastructure governance from domestic models to limited international cooperation models. It is of great significance to probe into the development of cyberspace militarization, and to understand the validity and limits of existing solutions.

Key words: militarization of cyberspace, cyber security, governance of cyberspace, national cyber strategy, international politics, Stuxnet

Power Competition and the Evolution of the U. S. Tech Policy Towards China

HUANG Qixuan

Abstract: The international technology policies of the U. S. serve its strategic competition with other great powers. The more direct and urgent the strategic competition becomes, the more likely it is for the U. S. to relax technology import and export control to its partners to build and strengthen a coalition against strategic competitors. Since the 1970s, the U. S. technology policy towards China has experienced a transformation from control-relaxation to control-tightening. The US-USSR security competition forced the U. S. to tighten technology export control to Soviet Union while relaxing restrictions to China. The US-Japan economic competition compelled the U. S. to tighten its technology import control to Japan while easing the restrictions to China. Such U. S. policies have provided opportunities for China to improve its technological capabilities. However, when the pressure of strategic competition from the Soviet Union and Japan receded gradually, the U. S. technology policy towards China have undergone profound changes. At present, the U. S. is trying to exercise comprehensive tightening of high-tech imports and exports control to China, particularly by launching a trade war with China and suppressing China's high-tech industries. The U. S. technology control towards China will be a major obstacle for China's technological upgrading in the long run.

Key words: power competition, Sino-U. S. relations, technological competition, security competition, economic competition, technology import and export control, Sino-U. S. trade friction