美国太空系统网络安全能力构建 *

何奇松

【内容摘要】 太空与网络紧密相连、相互依赖、相互促进。太空系统具有军民两用属性，其通信越来越依赖网络，各技术环节都有被潜在对手或黑客利用网络进行攻击的可能，其面临的巨大网络安全风险逐渐受到美国重视。自特朗普政府以来，美国政府强化应对太空系统网络安全问题的相关政策，包括发布指导性政策指令和安全备忘录，与产业界合作确立安全标准和共享安全威胁信息，通过立法将太空系统纳入关键基础设施，以期将太空系统的网络标准从自愿遵守变为强制性义务。美国军方以零信任构架方式采购卫星部件，建设太空系统的网络靶场，并组建太空网络攻防部队。美国强化太空系统网络安全的目的在于构筑美国应对他国反太空武器能力，确保太空产业供应链与工业控制系统的安全，防止太空技术扩散到非盟国，并建立以美国规则为基础的太空秩序。中国需要加强太空系统供应链安全，倡导太空系统网络安全治理规则，构建太空系统网络安全架构与国际太空系统网络治理规则，从国家安全高度谋划太空系统与网络空间一体化的系统集成。

【关键词】 美国太空政策　太空系统　网络安全　太空竞争

【作者简介】 何奇松，华东政法大学政治学与公共管理学院教授（上海，邮编：201620）

【中图分类号】 D815　　**【文献标识码】** A

【文章编号】 1006-1568-(2022)03-0134-22

【DOI 编号】 10.13851/j.cnki.gjzw.202203008

* 本文系国家社科基金项目“国际太空新竞争及太空命运共同体研究”（21BGJ021）的阶段性成果。感谢上海政法学院教师周顺博士的修改建议和文字润色，感谢匿名审稿专家的建设性修改意见。

太空与网络是两个不同领域，分别被称为第四空间与第五空间，对当今政治、经济、军事、社会都产生了极为重要的影响。网络空间与太空系统已进入无缝隙整合期，两者相互依赖又相互促进。太空系统的通信越来越依赖互联网，甚至有观点认为未来的太空理论将严重依赖网络理论。[①] 同样，网络空间建立于物理空间、数据处理和通信系统基础之上，未来的网络空间也将依赖太空系统的有形基础设施。美国将太空与网络分别纳入国家大战略，但太空系统的基础设施长期未被纳入网络关键基础设施之列。[②] 2020 年 9 月，特朗普曾签署“太空政策指令-5”（Space Policy Directive-5, SPD-5），要求加强太空系统的网络安全；[③] 2020 年 12 月，美国政府公布《美国国家太空政策》（National Space Policy of the United States of America），再次强调加强太空系统网络安全的重要性，将防止太空系统遭受网络攻击作为重中之重。[④] 拜登政府执政后，先后发布三道行政令与安全备忘录，强调供应链、工业控制系统等方面的网络安全。由此，作为反太空武器能力的重要构成部分，美国开始打造太空系统网络安全能力。美国政府、军方与产业界在共同努力，强化太空系统的网络安全。

一、美国对太空系统网络安全的评估

太空系统既是军民两用技术，又与网络关键基础设施紧密相联。美国政府和军方高度依赖这一系统，且依赖程度远超任何其他国家。网络空间的安全威胁也是太空系统的安全威胁，随着过去十年太空商业化的快速发展，美国政府和军方开始重视太空系统的网络安全问题。美国对太空系统网络安全

① Matthew Mather, “How Space and Cyberspace Are Merging in the 21st Century Battlefield,” Discover Sci-Fi, June 7, 2017, https://discoverscifi.com/space-cyberspace-merging-21st-century -battlefield/.

② 参见美国国土安全部网络与基础设施安全局（CISA）网站：https://www.cisa.gov/critical-infrastructure-sectors。

③ “Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems,” White House, September 4, 2020, https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/.

④ “National Space Policy of the United States of America,” White House, December 9, 2020, https://trumpwhitehouse.archives.gov/wp-content/uploads/202 /12/National-Space-Policy.pdf.

问题的评估，是以基于西方学界的理论讨论与产业界的实践为基础的。

（一）太空系统网络安全威胁的类型

网络空间依赖太空系统，包括卫星、地面站点以及卫星与地面站点之间、卫星与卫星之间的通信链路。在理论上，网络空间面临的安全问题同样会在太空系统中出现。根据美国战略与国际研究中心（Center for Strategic and International Studies, CSIS）的界定，太空系统网络攻击的目标是数据本身以及使用、传输和控制数据流的系统。对卫星的网络攻击可以用来监视数据通信模式、拦截数据，也可以在系统中插入虚假或损坏的数据。这些攻击可以针对地面站点、终端用户设备或卫星本身实施。[①] 因此，就太空系统的网络攻击而言，可以分为对卫星本身的攻击、对运载火箭的攻击、对卫星与地面站点链路的攻击、对卫星之间的链路的攻击以及对卫星地面站点的攻击。

鉴于太空系统的独特性，太空系统网络安全问题不完全等同于网络空间的安全问题。包括对定位导航系统（GPS）的干扰与欺骗在内，对定位导航授时系统的网络攻击是太空系统独有的网络攻击方式。干扰技术是指破坏定位导航卫星的发射器，使定位导航系统的终端用户无法接收数据，从而影响定位导航卫星的精度。欺骗指使用一个虚拟信号扭曲或者替换所需要的信号。[②] 欺骗包括多种方式，一种是破坏卫星接收器并改变卫星的输出信号；另一种是将虚假信息注入对方的 GPS 信号模拟器，或者使用软件定义（Software-Defined）进行欺骗。[③] 就卫星本身而言，从预购、生产、在轨运

① Todd Harrison, et al., “Space Threat Assessment 2021,” Center for Strategic and International Studies, April 2021, p. 5, https://aerospace.csis.org/wp-content/uploads/2021/03/CSIS_Harrison_SpaceThreatAssessment2021.pdf.

② David Livingstone and Patricia Lewis, “Space, the Final Frontier for Cybersecurity?” Chatham House, September 22, 2016, p. 18, https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf.

③ 美国得克萨斯州大学奥斯汀分校一个科研小组就曾以上述欺骗手段，成功骗过一架无人机上的 GPS 信号，并将其捕获；该小组也顺利完成了以虚假信号使船舶偏离正常航线的试验。Gregory Falco, “Job One for Space Force: Space Asset Cybersecurity,” Belfer Center for Science and International Affairs, Harvard Kennedy School, July 2018, p. 8, https://www.belfercenter.org/sites/default/files/files/publication/CSP%20Falco%20Space%20Asset%20-%20FINAL.pdf; Colin Lecher, “Texas Students Hijack a U.S. Government Drone in Midair,” Popular Science, June 29, 2012, https://www.popsci.com/technology/article/2012-06/researchers-hack-government-drone-1000-parts/; and David Livingstone and Patricia Lewis, “Space, the Final Frontier for Cybersecurity?” Chatham House, September 22, 2016, p. 19.

转直至终结（包括拖入坟墓轨道、进入大气层燃烧、成为有源或无源废弃卫星）的整个寿命周期，都有可能遭受网络攻击。

（二）网络攻击太空系统造成的危害

对太空系统进行网络攻击，会造成多方面后果。[①] 首先，从国家安全角度而言，对太空系统的网络攻击将影响军事行动的成效。太空系统是军队C4ISR[②] 的重要组成部分，用网络攻击太空系统，无疑对军队的 C4ISR 造成影响，降低军队的作战效能，甚至关系到战略、战役、战术的成败及战争的胜负。其次，从民事、民生角度而言，太空系统便利了经济、金融、社会等各方面运转，对商用太空卫星的攻击无疑将对民生、民事活动等产生影响。再次，从知识产权保护角度而言，对太空系统的网络攻击会导致窃取技术和数据。美国经常指责一些行为体通过对太空系统进行网络攻击，窃取其包括航天技术在内的知识产权。最后，从太空利用角度而言，如果通过网络攻击破坏运载火箭、载荷、卫星发射场等设备，将严重影响国家进入太空的能力，对国家经济、金融、社会等构成威胁，甚至对军事安全、政治安全产生影响，进而危及国家生死存亡。

太空系统遭受网络攻击的后果，一方面取决于该太空系统的国家、所有者、运营者、操作者抵御网络攻击的能力，另一方面取决于发动网络攻击者的能力与意图。对于前者而言，如果建立了强大的抵御攻击的能力，包括足够的弹性与冗余，损失则相对较小。对于后者而言，网络能力与造成的后果存在正相关关系；在能力不变的情况下，攻击意图的大小或强弱则决定了攻击的力度及其造成的损失。如果国家行为体决心让核大国的预警卫星失灵，就会产生灾难性后果，可能引发核战争，因为预警卫星是战略核力量的重要助手，攻击预警卫星可能被视为核打击的前奏，有可能让对手按下核按钮。

① 根据英国查塔姆研究所（Chatham House）的研究报告，对太空系统进行网络攻击可能产生降低国家安全或防务能力，降低通信、观测及导航能力，撞击、销毁或挟持航天器，毁损运载火箭、有效载荷，损坏或删除卫星传送的数据，截取包括敏感知识产权在内的通讯等后果。David Livingstone and Patricia Lewis, “Space, the Final Frontier for Cybersecurity?” Chatham House, September 22, 2016, p. 13.

② C4ISR 系统是指挥（command）、控制（control）、通信（communication）、计算机（computer）、情报（intelligence）及监视（surveillance）与侦察（reconnaissance）的英文单词的缩写。C4ISR 系统是现代军队的神经中枢，是军力的倍增器。

（三）美国各界呼吁加强太空系统网络安全

美国政府与军方最初并未意识到太空系统网络威胁的严重性，也没有制定统一的太空系统的信息安全标准。这具体体现在三方面。首先，2013 年美国政府正式确立的 16 个关键基础设施没有涵盖太空系统。被纳入关键基础设施之列的领域会受到联邦政府的各种“关照”，包括隶属于商务部的国家标准与技术研究院（National Institute of Standards and Technology）制定关键基础设施的网络安全标准，国土安全部网络与基础设施安全局（Cybersecurity and Infrastructure Security Agency, CISA）具体负责联邦政府的网络安全。其次，美国政府有关部门没有制定商业卫星统一的信息安全标准等。军方和美国国家航空航天局（National Aeronautics and Space Administration, NASA）根据自己的需求对卫星系统的网络安全标准进行设计、制造。军方或者政府其他部门预先租用尚未入轨的商业卫星，商业公司则根据国家安全系统委员会（Committee on National Security Systems）的商业卫星信息安全标准订购卫星；国家海洋和大气管理局安全委员会（National Oceanic and Atmospheric Administration, NOAA）负责管理商业遥感卫星系统的许可证。其他商业卫星的信息安全标准却没有任何一个政府部门负责。再次，基于上述两点，商业卫星公司由于成本因素较少考虑网络安全问题。而政府有关部门没有发布卫星部件网络安全的指南或标准，为生产商利用网络安全的漏洞提供了空间。理论上，如果一颗卫星由不同生产商提供的部件越多，那么给对手提供的网络攻击机会也就越多。

2010 年前后，美国和西方国家从太空与网络对国家安全的重要性着手，开始评估太空系统的网络安全问题。[①] 随着太空商业化的迅猛发展及其在军事领域的广泛运用，有关太空系统的网络安全问题成为智库、军方、咨询公司、网络安全公司关注的焦点。尤其是 2018 年美国组建太空军之后，各类智库和学术期刊发表了一系列评论、学术文章、研究报告等。网络媒体上的专家评论文章大多认为美国没有做好太空系统的网络安全准备。[②] 专业人士

① Madelyn R. Creedon, “Space and Cyber Shared Challenges, Shared Opportunities,” *Strategic Studies Quarterly*, Vol. 6, No. 1, Spring 2012, p. 3.

② Shaun Waterman, “Space Is Cybersecurity's New Frontier,” Afcea International, May 1, 2020, https://www.afcea.org/content/space-cybersecuritys-new-frontier.

的学术论文、研究报告则不仅论述了太空系统网络安全产生的原因、方式，也提出了改进的办法。[①] 美国各界对太空系统网络攻击的认知也没有太大差别，只是评估方式或角度不同。[②] 新冠肺炎疫情的大流行导致 NASA 以及一些私人机构的工作人员居家办公，这为潜在对手或黑客进行网络攻击提供了便利条件。

二、美国加强太空系统网络安全的目的和行动

美国相关领域人士呼吁重视太空系统的网络安全，美国政府、国会与军方也为此花费巨大精力。美国的太空战略等因素决定了其目的和行动。

（一）维持太空军事霸权

自人类进入太空时代以来，美国就开始从军事方面谋划太空运用，为其军事霸权服务，并提出与发展了制天权理论。冷战结束后的历次局部战争中，美国凭借其太空优势很快赢得了军事胜利，使美军更痴迷于制天权理论。冷战结束以后美国始终强调太空行动自由，并欲在危机时剥夺对手的太空行动自由。太空控制与行动自由，就是一枚硬币的两面。美国所确立的太空控制与行动自由，包括太空态势感知在内的十大太空作战行动能力与指挥控制在

① Gregory Falco, “Job One for Space Force: Space Asset Cybersecurity,” Belfer Center for Science and International Affairs, Harvard Kennedy School, Vol. 79, 2018, https://www.belfercenter.org/sites/default/files/files/publication/CSP%20Falco%20Space%20Asset%20-%20FINAL.pdf; Gregory Falco, “The Vacuum of Space Cyber Security,” AIAA SPACE and Astronautics Forum and Exposition, September 19, 2018, https://www.researchgate.net/publication/327678396_The_Vacuum_of_Space_Cyber_Security; Gregory Falco ,“Cybersecurity Principles for Space Systems,” *Journal of Aerospace Information Systems*, Vol. 16, No. 2, 2019, pp. 61-70; and Gregory Falco, “When Satellites Attack: Satellite-to-Satellite Cyber Attack, Defense and Resilience,” Aerospace Research Center, November 2, 2020, https://www.researchgate.net/publication/340335070_When_Satellites_Attack_Satellite-to-Satellite_Cyber_Attack_Defense_and_Resilience.

② 美国的有关部门认为，各国将网络安全战争转移到卫星上只是时间问题，瞄准卫星的目的是企图干扰对商业和安全至关重要的通信或信息流。美国太空军负责技术与创新的金伯利·克里德（Kimberly Crider）少将认为，太空系统很可能成为“网络冲突的下一个战场”。轨道安全联盟（Orbital Security Alliance, OSA）董事长哈里森·考迪尔（Harrison Caudill）则指出，太空系统的网络安全问题是“国家安全的噩梦”。 Paul Ferrillo, “Protecting Space-Based Assets from Cyber Threats,” Homeland Security Today , October 17, 2020, https://www.hstoday.us/subject-matter-areas/infrastructure-security/protecting-space-based-assets-from-cyber-threats/; Shaun Waterman, “Space Is Cybersecurity’s New Frontier,” May 1, 2020。

内的七大联合功能。[①]

要实现上述目标，需要解决包括网络安全在内的各种漏洞与风险。首先，太空军需要有强化太空系统网络安全的理由，因此美国总是夸大中、俄对其太空系统造成的网络安全威胁，以此强化美国太空军应该全力解决太空系统的网络安全问题的主张。[②] 其次，太空军强调网络作战能力。2020 年太空军公布的作战条令强调，网络作战作为其使命之一，要确保太空军在整个冲突时期能访问和利用太空，明确进攻性行动不仅限于敌方反太空系统，还可以针对敌方利用太空领域的所有能力，其中包括陆地和网络目标。[③] 这就是太空军组建“太空德尔塔 6”（Space Delta 6）的原因。

当然，在此过程中，美国将充分利用网络技术与数字技术优势。除了制定与实施各种网络安全标准外，美国打造太空系统的网络安全体系的重中之重是借助数字工程技术，构建太空系统的“数字孪生”（Digital Twin）[④] 系

① 2020 年 6 月公布的《太空防务战略》将美国太空战略目标表述得极为清晰：谋求全面太空军事优势，为美国赢得大国竞争下的战略、战役与战术各层级的军事胜利。2020 年 8 月公布的太空军作战条令再次强调了太空军的最基本职能，即确保太空作战自由。参见张茗：《美国太空安全战略转向及其对中国的影响》，《社会科学》2020 年第 9 期，第 17 页；“Space Power: Doctrine for Space Force, Space Capstone Publication,” US Space Force, August 2020, p. 28, https://www.peterson.spaceforce.mil/Portals/15/Space%20Capstone%20Publication_10%20Aug%202020.pdf。

② 例如，美国时常指控中国黑客攻击美国（军事）卫星，也指控俄罗斯对其 GPS 进行网络攻击。美国智库先进国防研究中心（Center for Advanced Defense Studies, C4ADS）称，2016 年 2 月到 2019 年 3 月，美国 GPS 在俄罗斯周边受到干扰的次数达到 9883 次，受影响的船只达到 1311 艘。在美国将军大卫·戈德芬（David Goldfein）看来，“该领域（网络攻击太空系统）投资最多的国家是中国与俄罗斯。” “Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria,” C4ADS, March 2019, p. 15, https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5c99488beb39314c45e782da/1553549492554/Above+Us+Only+Stars.pdf； Kathryn Waldro, “Space: The Last Frontier for Cybersecurity,” *The Hill*, July 28, 2018, https://thehill.com/opinion/cybersecurity/399224-space-the-last-frontier-for-cybersecurity/。

③ “Spacepower: Doctrine for Space Force, Space Capstone Publication,” p. 47; p. 36.

④ 数字孪生是由美国密歇根大学的迈克尔·格里夫斯（Michael Grieves）教授于 2002 年提出的“信息镜像模型”（Information Mirroring Model）概念演变而来的。2009 年，美国空军研究实验室（Air Force Research Laboratory, AFRL）提出“机身数字孪生”（Airframe Digital Twin），数字孪生自此成为专业名词。2010 年，美国国家航空航天局（NASA）在《建模、仿真、信息技术和处理路线图》中把数字孪生运用到太空领域，此后这个概念运用到各个领域。参见“Modeling, Simulation, Information Technology and Processing Roadmap,” NASA, April 2012, https://www.nasa.gov/pdf/501321main_TA11-MSITP-DRAFT- Nov2010-A1.pdf。简单地说，数字孪生是一组由虚拟信息构成、模仿物理实体结构和行为的计算机模型，并在寿命周期内动态更新数据，保持与物理实体同步。它实现了现实物理系统的信息映射到网络空间，也就是在网络空间可视化现实的物理系统信息。

统，把太空军建设成首个数字化军种，实现美军数字化战略。太空军力求准确把握包括网络安全在内的各种安全风险，赢得决策先机，强调太空军与网络司令部在数字化转型过程中构成“密不可分”的一体，[①] 以避免潜在对手的网络攻击。

（二）构筑太空供应链安全、防止太空技术扩散

如果说从作战层面消除太空系统的网络安全问题是美国军方的战略考虑，那么美国政府与军方加强太空系统的网络安全标准，则是出于构筑太空供应链安全的考虑，目的在于防止先进技术泄露到非盟国。同时，在大国竞争背景下，加强高科技供应链安全具有战略意义。美国以加强太空系统的网络安全为由，已经禁止从中国进口卫星相关产品或软件。加强太空系统的网络安全，强调系统部件以及工业控制系统的网络安全，是特朗普政府与拜登政府加强太空供应链安全的重要举措。

同样地，美国加强太空供应链安全也是以从中国进口的卫星相关部件及软件对太空安全与国家安全造成威胁为借口的。为加强供应链安全，美国扩大《沃尔夫修正案》（Wolf Amendment）的适用范围，禁止私人太空公司与中国合作。2011 年的《沃尔夫修正案》禁止获得联邦政府资助的民用航天实体机构与中国开展科学合作。[②] 这个条款的目的在于阻止美国先进太空技术转移至中国。美国政府为强化本国的供应链安全与工业控制系统安全，把禁令适用范围扩大到所有太空实体（不论是否得到联邦政府资助），禁止太空相关的实体与中国科学家、企业进行科学与技术合作。2021 年 6 月，NASA 局长尼尔森（Bill Nelson）明确表态要让《沃尔夫修正案》永久化。[③]

为保障美国太空供应链安全，美国太空军通过 2017 年成立的太空企业联盟（Space Enterprise Consortium, SpEC）购买太空企业的产品与服务。2021

① Abraham Mahshie, “Dickinson: Space Command and Cyber Command ‘Inseparable,’ ” *Air Force Magazine*, July 27, 2021, https://www.airforcemag.com/dickinson-space-command-cyber-command-inseparable/.

② “Trouble in the Stars: The Importance of US-China Bilateral Cooperation in Space,” *Harvard International Review*, October 27, 2019, https://hir.harvard.edu/trouble-in-the-stars-the-importance-of-us-china-bilateral-cooperation-in-space/.

③ Skye Witley, “NASA Head Seeks New Funding for Annual Moon Landings ‘Over a Dozen Years,’ ” *Global Security*, June 23, 2021, https://www.globalsecurity.org/space/library/news/2021/space-210623-voa01.htm.

年，太空军与该联盟签订了 10 亿美元合同。[①] 太空军通过太空企业联盟把大部分合同授予非传统供应商，促进其提高包括网络安全在内的各种安全标准，同时也鼓励企业自主创新，不再从国外尤其是非盟国进口相关技术或服务，保证美国太空产品或技术的供应链完整与安全。更重要的是，美国通过这种方式培育太空新技术与新工艺，可以为美国赢得全面太空技术优势，以更好地服务其太空军事霸权。

（三）确立美国主导的太空规则与秩序

美国希望通过打造太空全面技术优势，封堵包括网络安全在内的各种风险漏洞，确立其主导的太空规则，构建有利于美国的太空秩序。目前，太空多极化趋势极为明显。美国认为太空多极化趋势打破了冷战时代美苏称霸太空的局面，各国拥有多种反太空武器与能力，提出了诸多太空规则倡议，挑战了美国太空规则制定权，对美国利益造成威胁。[②] 在这种情况下，美国希望打造完整的太空产业链与更加先进的太空技术，解决太空系统的网络安全问题，并从“实力地位”出发建立以美国的规则为主导的太空秩序。拜登政府执政以来多次强调建立基于规则的国际秩序。在太空治理方面就是建立以美国为主导的太空规则与秩序。以探索月球规则为例，2020 年 10 月，美国政府推出《阿尔忒弥斯协定》，[③] 试图以此取代冷战时代签订的《月球协定》。到 2022 年 4 月，包括美国在内的 18 个国家签署了该协定。它们企图垄断月球资源的开采，以保护开采区安全（Safety）为由谋求月球主权。为实现这一图谋，美国正推进地球静止轨道到月球轨道之间的地月空间控制战略。[④] 就太空军备控制而言，美国不反对太空武器化，而是主张对太空行为进行控

① Nathan Strout, “Space Force Expects $1 Billion in Contracts in First Year of Space Enterprise Consortium Reloaded,” *Defense News*, September 9, 2021, https://www.defensenews.com/battlefield-tech/space/2021/09/08/space-force-expects-1-billion-in-contracts-in-first-year-of-space-enterprise-consortium-reloaded/.

② “The National Intelligence Strategy of the United States of America 2019,” The Office of Director of National Intelligence, https://www.dni.gov/files/ODNI/documents/NationalIntelligenceStrategy2019.pdf, p. 4.

③ “The Artemis Accords,” NASA, October 13, 2020, https://www.nasa.gov/specials/artemis-accords/img/Artemis-Accords-signed-13Oct2020.pdf.

④ “A Primer on Cislunar Space,” U.S. Air Force, https://www.afrl.af.mil/Portals/90/Documents/RV/A%20Primer%20on%20Cislunar%20Space_Dist%20A_PA2021-1271.pdf?ver=vs6e0sE4PuJ51QC-15DEfg%3d%3d.

制。[①] 美国由此推出了太空交通管理概念，怂恿与支持英国在联大提出“负责任太空行为”倡议等。凡此种种，美国企图借助其在太空攻防能力与太空武器在内的全面太空技术优势，谋求构建美国主导的太空规则与秩序。

三、美国打造太空系统网络安全规则的举措

冷战结束以来，美国历届政府视网络安全为国家安全的重要领域，制定了一系列与网络安全相关的战略和具体举措。从特朗普政府时期开始，美国各界密切配合，回应对太空系统网络安全所做的评估，力求实现其战略目标。

（一）美国政府指导太空工业重视太空系统网络安全

第一，特朗普政府颁布“太空政策指令-5”（SPD-5），要求相关部门采取最佳网络安全政策。2020 年 9 月，时任总统特朗普签署“太空政策指令-5”，即《太空系统网络安全原则》。[②] 该指令认为，影响太空系统运行的网络攻击包括“欺骗传感器数据、损坏传感器系统、干扰或发送未经授权的命令以进行指导和控制、输入恶意代码、进行拒止服务攻击”等。为此，该指令要求太空系统根据网络工程来开发与运作，太空系统网络安全遵循网络空间的最佳做法与行为规范，进行逻辑或物理隔离，定期升级补丁等。该指令还要求运营商和所有者从“可靠的供应商”采购零部件，识别可能被非盟友恶意使用的零部件，试图强化工业控制系统的网络安全与供应链安全。

第二，颁布《国家太空政策》，在盟国与公私伙伴关系中构筑太空系统的网络安全屏障。2020 年 12 月颁布的《国家太空政策》强调，美国要制定战略以应对潜在的对手对美国及其盟友的关键基础设施的太空分系统进行的有目的干扰或攻击。[③]《国家太空政策》特别要求加强与太空相关的科学、技术、工业基地供应链的安全性、完整性与可靠性；加强国内公私合作、国

① 参见王国语：《美国〈外空防务战略〉对外空军控国际规则博弈的影响分析》，《太平洋学报》2021 年第 3 期，第 94—106 页。

② “Memorandum on Space Policy Directive-5 — Cybersecurity Principles for Space Systems,” White House, September 4,2020, https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/.

③ “The National Space Policy of the United States of America,” p. 9.

际盟友合作，消除对非盟友供应商的依赖，以确保供应链的安全。[①]

第三，颁布网络安全行政令与备忘录，消除公私网络安全威胁的信息共享屏障，强化工业控制系统的网络安全与供应链安全，封堵卫星部件生产中的网络安全漏洞。科洛尼尔（Colonial Pipeline）石油运输管道遭到网络攻击之后，拜登政府于 2021 年 5 月 12 月颁布“改善国家网络安全”行政令，[②] 要求联邦政府改善整个国家的网络安全，包括提高网络安全标准，强制采用多因素身份验证与加密，使用安全云服务与零信任架构（Zero-Trust Architecture），改善软件供应链安全等。2021 年 7 月，拜登总统签署“改善关键基础设施控制系统网络安全”的国家安全备忘录，[③] 要求工业控制系统网络威胁的可视化，以便及时探测、发出警告，保护美国关键基础设施。2022 年 1 月，拜登总统签署国家网络安全备忘录，责令国家安全部门应切实遵守 2021 年 5 月的网络安全行政令，并规定具体时间表与实施指南。[④] 这些行政令、备忘录直接或间接提升了太空系统的网络安全标准。

美国政府通过上述方式，从国家顶层逐步将太空系统纳入关键基础设施范围，把太空系统的网络安全纳入关键基础设施的网络安全标准，同时消除网络安全的信息共享屏障，将供应链、工业控制系统纳入网络安全基线。

（二）确立太空系统网络安全标准，共享网络安全威胁信息

第一，针对太空系统没有网络安全标准化框架的现状，美国国土安全部与商务部等部门合作制定了有关网络安全标准。国土安全部网络和基础设施局视“太空政策指令-5”等为加强太空系统网络安全的机会，设立跨部门工作组，加强与使用太空系统的工业部门及政府部门（如 NASA、NOAA 等）

① “The National Space Policy of the United States of America,” pp.7-8.

② Briefing Room, “Executive Order on Improving the Nation’s Cybersecurity,” White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

③ Briefing Room, “National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems,” White House, July 28, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems.

④ Briefing Room, “Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems,” White House, January 19, 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/.

之间的协调，尤其是与商务部的国家标准与技术研究所（National Institute of Standards and Technology）以及商务部的商业太空办公室（Office of Space Commerce）合作，制定有关标准与最佳规范。首先，商务部从太空军接管商业太空态势感知工作。太空态势感知不仅涉及太空碎片等问题，也包括太空系统的网络安全问题。美国商务部与国家海洋和大气管理局（NOAA）合作，为商业卫星与太空供应商制定了太空数据开放式存储库（Open Architecture Data Repository of Space Data）。其次，商务部专门制定太空系统网络安全标准，即 NIST800-160。[①] 这个标准将系统安全工程方法、实践与技术引入到太空系统和软件工程中。再次，商务部为全球定位导航系统特制网络安全规范文件。[②] 文件要求使用定位、导航、授时信息的用户，提供信息需求（Request for Information, RFI）以利管理。

第二，国土安全部与产业界共同努力，为太空领域提供威胁信息共享服务与设立网络安全标准。2019 年美国国土安全部在科罗拉多斯普林斯国家网络安全中心（National Cybersecurity Center in Colorado Springs）组建了太空信息共享与分析中心（Space Information Sharing and Analysis Center, Space ISAC）。作为信息交流与推行最佳实践的平台，以及企业与政府直接沟通的渠道，该中心致力于推动美国与盟友之间在太空领域的协作。这是商业太空领域对抗网络威胁的重要举措。[③] 当然，还有专门致力于太空安全的机构也在为网络安全劳心费力。例如，轨道安全联盟（Orbital Security Alliance）

① 该标准由第一卷《系统安全工程》（Systems Security Engineering）扩大到第二卷《发展网络弹性系统》（Developing Cyber-Resilient Systems）。后者 2021 年 12 月公布修订版。上述两个文件分别参见下列美国商务部国家标准与技术研究院网站：https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final；https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/draft。

② Michael Bartock, et al., “Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services,” NISTIR 8323, NIST, U.S. Department of Commerce, https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8323.pdf.

③ 另外，该中心组建了太空系统漏洞实验室（Space Systems Vulnerability Laboratory），检测、分析与改善太空系统的网络安全漏洞。Sandra Erwin, “Space Industry Group Focused on Cybersecurity to Begin Operations in Spring 2020,” *Space News*, January 23, 2020, https://spacenews.com/space-industry-group-focused-on-cybersecurity-to-begin-operations-in-spring-2020/.

为小型太空公司量身定做了一套详细的商业太空系统安全指南。[①] 该指南提出了网络安全准则，要求采用多因素身份验证。[②]

第三，专门机构举办太空系统网络安全培训并提供安全认证服务。太空网络安全培训与认证的迫切需要促使一些培训机构开设了太空系统网络安全培训课程。除了 ISAC 等机构承担部分培训任务外，国际太空与安全专家学会（International Society of Space and Security Specialists, IS4）也开展了太空系统网络安全培训工作。作为国际注册太空和安全专业人员协会的成员，国际太空与安全专家学会是全球唯一一家太空网络安全认证机构。

（三）尝试将太空系统网络标准从自愿遵守变为强制施行

针对太空系统未纳入关键基础设施领域的问题，2021 年 6 月，美国众议院民主党议员泰德 •刘（Ted Lieu）与共和党议员肯 •卡尔弗特（Ken Calvert）提出两党提案《太空基础设施法案》（Space Infrastructure Act），旨在将太空系统纳入国土安全部第 17 个关键基础设施部门。一旦该法案通过，国土安全部的网络安全标准将在太空系统领域得到贯彻。[③] 同时，国会试图把太空系统的网络安全标准从自愿性要求变为强制性义务。马克 • 华纳（Mark Warner）等三名参议员提交了一项两党提案，即《国土安全部工业控制系统能力增强法案》（DHS Industrial Control Systems Capabilities Enhancement Act）。[④] 该法案已经获得通过，赋予国土安全部更大权限，在关键基础设施领域与工业控制系统领域全面推广网络安全标准。

美国颁布、执行上述强化太空系统的网络安全措施的一个重要内容，是加强太空系统部件、工业控制系统与太空网络系统的供应链安全。首先，制定严格的质量保障准则。政府、私人实体采购太空系统部件，除了严格执行

① Harrison Caudill and Chris Wake eds., “Commercial Space System Security Guidelines,” Orbital Security Alliance, https://osa-public.s3.us-west-1.amazonaws.com/guidelines/space_cyber_guidelines-v1.0.1.pdf.

② Shaun Waterman, “Space Is Cybersecurity's New Frontier,” May 1, 2020.

③ Jeff Foust, “House Bill would Designate Space as Critical Infrastructure,” *Space News*, June 4, 2021, https://spacenews.com/house-bill-would-designate-space-as-critical-infrastructure/.

④ “Warner, Rubio, Peters, Portman Introduce Bipartisan Legislation to Secure Critical Infrastructure Networks Against Cyber-Attacks,” U.S. Senate, July 22, 2021, https://www.warner.senate.gov/public/index.cfm/2021/7/warner-peters-portman-rubio-introduce-bipartisan-legislation-to-secure-critical-infrastructure-networks-against-cyber-attacks.

政府的有关网络安全标准外，还要执行 NASA 有关太空供应链的质量保障准则（Quality Assurance Discipline）。为此，2013 年 NASA 组建供应链风险管理（Supply Chain Risk Management）机构，并与联邦调查局合作以识别、评估和消除试图进入该机构供应链的网络间谍或破坏风险。2019 年 10 月，供应链风险管理机构组建安全与任务保障办公室（Office of Safety and Mission Assurance, OSMA）具体负责执行质量保障准则。其次，按照美国标准加强与盟国太空供应链合作。这个任务由 NASA 安全与任务保障办公室的国际航空航天质量小组（International Aerospace Quality Group, IAQG）来完成。该机构负责管理、协调与公布太空系统供应链的质量管理系统（Quality Management Systems），即 AS9100。2020 年 4 月，NASA 通过 AS9100，只有采纳这一标准的盟国产品才有可能进入美国市场。

上述措施提升了美国太空供应链的可视化与控制力，增强了美国与伙伴国的太空攻防领域合作。然而，在美国和盟国太空系统网络安全提升的同时，非盟友国的太空系统则因严格的出口管制而难以进入美国及其盟国的市场。

四、美国太空军的太空系统网络安全措施

政府、国会、产业界为美国的太空系统网络安全制定了最低安全标准，而作为美国太空霸权的基石，军方的太空系统网络（包括军方自身的太空系统与租用的商业太空系统）则需要一个更高、更全面的安全标准。

（一）太空军实施数字化转型

美国的军队、情报系统大量使用卫星，对太空系统的依赖程度远超任何国家，因此保护太空系统的安全至关重要。作为军方太空系统的最大用户，保护太空系统安全是太空军的重要职能之一。为了便于快速决策，不论是进攻还是防御，太空军致力于打造数字化军种，目的就是保护美国太空系统的网络安全。自 2018 年太空军成立以来，美国就开始谋求将太空军变为数字化军种。[①] 2021 年 5 月太空军司令部公布的《数字军种构想》力图把太空

① 在美国军方看来，太空就是一个“大数据环境”，把太空军变成数字化军种是必然

军构建为创新、数字化的主导军种。[①] 为此，太空军采用数字工程系统建立数据云，将数据储存在特定空间。一方面，军方、政府、产业界合作，在数据平台中审查各种程序，便于采购决策；另一方面，数据云便于战地司令部利用数据快速决策，为美军获取战略、战役、战术先机，从而赢得军事胜利。

美军希望把太空军变成世界上首支数字化军种，作为美国数字化现代化战略的试验田。[②] 军方视数据为支柱，要求太空军做到“在任何时间、任何安全级别、世界任何地方”随时可用，[③] 并利用可视化数据，封堵包括网络安全在内的漏洞与安全风险，做出适当的攻防决策以赢得军事胜利。

理论上，数字化的太空军又为潜在对手提供了网络攻击的机会。这需要太空军全方位加强太空系统的网络建设。在数字化转型过程中，太空军把太空系统的网络安全作为关键一环。为此，太空军太空与导弹中心（Space and Missile Systems Center, SMC）从采购方面着手相关工作。[④] 2020 年 10 月，太空与导弹中心选择三个项目作为试点，其中两项是下一代通信卫星项目，一项是可适应多种任务的模块化卫星总线，目的是通过严格的安全标准，保证卫星与地面站点不受包括网络攻击在内的各种干扰。简言之，太空军用这种方式设计、开发了一种可以抵御网络攻击的军用太空硬件。

在太空系统的实际采购过程中，太空军实行零信任制度。零信任将网络

的，也是必须的。Nathan Strout, “Space Force Wants to Be the World’s First Fully Digital Service,” C4ISRNET, May 6, 2021, https://www.c4isrnet.com/battlefield-tech/space/2021/05/06/space-force-wants-to-be-the-worlds-first-fully-digital-service/.

① “U.S. Space Force: Visionfora Digital Service,” U.S. Space Force, May 2021, https://www.spaceforce.mil/News/Article/2597623/space-force-unveils-its-vision-for-a-digital-service/.

② 2019 年 7 月，美国国防部公布《国防部数字现代化战略》；2020 年 10 月 8 日，国防部公布《国防部数据战略》，要求几个军种向数字化转型，力求在作战速度和规模上利用数据提高作战优势和效率。参见：“DoD Digital Modernization Strategy,” U.S. Department of Defense, July 12, 2019, https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF; “DoD Data Strategy,” U.S. Department of Defense, September 30, 2020, https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF。

③ Amanda Miller, “What ‘Digital Force’ Really Means — and How to Build One,” *Air Force Magazine*, August. 27, 2021, https://www.airforcemag.com/what-digital-force-really-means-and-how-to-build-one/.

④ 该中心 2021 年 8 月正式改组为太空系统司令部（Space System Command），具体负责太空系统采购事宜。其创建了新虚拟测试环境，将数字工程技术应用于太空，以获取物理世界的真实信息。其中“数字孪生”技术发挥了重要作用，使用计算机生成 3D 模型，使工程师与士兵能够进行虚拟实验与测试太空系统。

安全防御从基于网络的安全边界（防火墙、VPN 和入侵检测系统等）转移到用户身份、设备和个人资源。用户每次访问都需进行验证、认证、授权和加密。由此，用户的身份成为新的安全边界。太空军为国防承包商设立网络安全成熟度模型认证（Cybersecurity Maturity Model Certification, CMMC），保护受控的非保密信息，帮助承包商实现 IT 基础架构现代化。①

（二）强化太空系统的攻防能力

第一，组建太空系统靶场。太空与导弹中心/太空系统司令部所做的上述工作，只是力图从采购角度封堵包括网络安全在内的各种风险，但并不能保证卫星上天后以及卫星系统的地面站点不受网络攻击。为解决这一问题，太空与导弹中心/太空系统司令部设立了太空网络测试靶场（Space Cyber Test Range），以检测太空系统与地面站点的网络安全漏洞，并找到解决办法。该靶场为太空军测试、评估、训练提供了可靠、真实的网络空间环境，为国家网络靶场（National Cyber Range, NCR）基础设施开发了新颖的数字环境。实际上，该靶场就是专门针对太空系统的独特性而量身定制的测试工具，目的是找到正在开发、建造的新型卫星的网络漏洞。该靶场预计 2022 年全面投入使用，2023 年具备全面行动能力。②

第二，多手段提升保护太空系统网络安全的能力。即便有了太空网络靶场，经由太空军太空与导弹中心/太空系统司令部数字化、标准化采购系统购买的卫星仍可能存在网络靶场检测不出的安全漏洞。因此，太空军发起太空网络攻击游戏邀请赛，同时邀请网络安全公司参与建设太空军的网络靶场。就前者而言，军方希望通过黑客找到卫星系统的网络漏洞。例如，2020 年 5 月，美国空军向黑客发出邀请，参加“攻击卫星”（Hack-A-Sat）黑客大赛，以期发现军事卫星和地面站点的安全漏洞。美国军方通过这种方式，一边招募优秀人才，一边向太空工业系统宣传网络安全意识，希望他们能与军方、政府密切配合，努力消除系统的网络安全风险。就后者而言，军方与

① 以上内容参见 Ryan Heidorn, “Hasten CMMC Compliance Through Zero-Trust,” *National Defense*, August 2021, pp. 16-17。

② Shaun Waterman, “Hacking the Space Force: Critical Space Capabilities are Vulnerable to Digital Attack,” *Air Force*, August 2021, pp. 45-46.

私企签订合同，要求其帮助建设太空网络靶场或开发网络游戏，以期发现太空系统的网络安全隐患。例如，位于华盛顿的曼科技公司（ManTech）已获得军方合同，将开发网络太空战游戏产品，帮助军方发现太空系统的漏洞和软件错误。[①] 总之，美国在保护太空系统网络安全方面，始终贯彻军民融合思路，充分挖掘民间力量为军事服务。

第三，组建太空系统的网络攻防军力。不论是数字太空网络靶场，还是网络太空战游戏，都是未雨绸缪的行为。太空军也为现实中太空系统的网络安全漏洞做好准备，组建“太空德尔塔 6”，专门应对太空系统的网络安全威胁，确保太空军的网络安全。该部队的主要任务是通过卫星控制网络，提供持续的太空利用以及组织网络太空作战的能力。2020 年 7 月，该部队在原空军基础上组建完毕。为提升其太空系统网络保护能力，太空军从其他军种调入了诸多网络人员。为保证美军整个网络系统的安全，真正实现跨域作战任务，2021 年 4 月美军筹划组建了一个专门的联合网络中心，以促进美国太空军司令部、网络司令部与战略司令部之间网络作战能力的整合。[②]

（三）培训太空系统网络人才

为了确保数字化转型顺利，美国的太空军需要大量数字化人才。太空军一方面招募此类人才，另一方面也对存量与增量人员进行培训。根据吉姆 •克里德（Kim Crider）少将透露的消息，未来招聘的太空军战士必须拥有数字化专业学位；此外，太空军还为现有人员提供在线学习平台，并跟踪他们的数字技术水平的进展。[③] 值得注意的是，太空军利用空军的数字大学（Digital University）培养人才。美国空军为了推动数字化空军战略，组建了在线数字大学，加强对一线 IT 和网络安全士兵的培训。[④] 太空军也顺势借助该大学

① Sandra Erwin, “ManTech’s Cyber Warfare Technology Adapted for Space Systems,” *Space News*, May 4, 2020, https://spacenews.com/mantechs-cyber-warfare-technology-adapted-for-space-systems/.

② Sarah Coble, “Space Command to Launch Dedicated Cyber Center,” April 26, 2021, https://www.infosecurity-magazine.com/news/space-command-to-launch-dedicated/.

③ Sarah Sybert, “USAF Launches Digital University to Enhance IT & Cybersecurity Training; Master Sgt. James Crocker Quoted,” Executive Gov, August 21, 2020, https://executivegov.com/2020/08/usaf-launches-digital-university-to-enhance-it-and-cybersecurity-training-master-sgt-james-crocker-quoted/.

④ Jason Miller, “Space Force to Require all of Its Employees to be Digitally Fluent,” *Federal News Network*, August 21, 2020, https://federalnewsnetwork.com/defense-main/2020/08/space-

来培训数字化人才。

实际上，美军强化太空系统的网络安全，与其将太空视为军事作战域（Operational Domain）紧密相关。2011 年，美军即认为太空已进入“拥挤”（Congested）、“竞争”（Contested）与“对抗”（Competitive）的“3C”时代。[①] 但美国认为自己在太空的所谓“战略克制”并未换来俄罗斯、中国等的克制，因此美国需调整太空政策。[②] 2018 年 3 月，特朗普政府发布《国家太空政策》，明确强调太空是一个战争作战域（War Fighting Domain），要求美军把保护延伸到私人太空资产。[③] 美国政府也要求北约为其政策背书。[④] 从“3C”到“作战域”的转变，表明美国对太空安全环境的认识已经发生重大转变，给予巨大安全关切。尤其是随着俄罗斯与中国太空实力的日益上升，美国认为太空安全越来越具有不确定性，风险与威胁程度越来越高，直接威胁到美国的太空霸权与太空规则制定话语权。为此，美国认为需要封堵太空系统的网络安全漏洞，以提升美军跨域威慑与作战能力。

五、美国强化太空系统网络安全的影响、启示与应对

太空与网络彼此依赖，是国家政治、经济、金融、社会与军事的关键基础设施。美国依赖网络空间与太空系统的程度远超其他任何一国，高度依赖就意味着要承担巨大的安全风险。就太空系统而言，美国也面临网络安全风

---

force-to-require-all-of-its-employees-to-be-digitally-fluent/.

① “National Security Space Strategy,” Unclassified Summary, U.S. Department of Defense, January 2011, https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2011_nationalsecurityspacestrategy.pdf.

② 参见 Theresa Hitchens and Joan Johnson-Freese, “Toward a New National Security Space Strategy: Time for a Strategic Rebalancing,” Atlantic Council, June 17, 2016, http://www.atlanticcouncil.org/images/publications/AC_StrategyPapers_No5_Space_WEB1.pdf。

③ “President Donald J. Trump is Unveiling an America First National Space Strategy,” White House, March 23, 2018, https://trumpwhitehouse.archives.gov/briefings-statements/president-donald-j-trump-unveiling-america-first-national-space-strategy/.

④ 2019 年 11 月，北约峰会强调太空是一个作战域；2021 年 6 月，北约峰会公报向世界宣布，如果一国对北约成员国的太空资产发动攻击，北约将启动集体防御条款；2022 年 1 月，北约的太空政策再次强调了这一点。“Brussels Summit Communiqué,” NATO, June 14, 2021, https://www.nato.int/cps/en/nato hq/news_185000.htm?selectedLocale=en; “NATO’s Overarching Space Policy,” NATO, January 17, 2022, https://www.nato.int/cps/en/natohq/official_texts_190862.htm.

险，从太空系统的地面系统与运载系统，到在轨运行与部件生产，都存在被潜在对手、黑客利用网络进行攻击的可能。封堵太空系统网络安全漏洞，为美国所急需，为此，将太空系统列为关键基础设施并强制私人太空公司遵守网络安全标准等就具有必然性。

太空实力是美国霸权的坚实技术与军事基础，太空领域出现重大漏洞与安全风险，无疑会动摇美国霸权。因此，随着商业太空技术与服务的广泛应用，强化太空系统的网络安全是美国的必然之举。在此过程中，美国政府、国会、军方与私人实体结成伙伴关系，力图封堵太空系统的各种网络安全漏洞。虽然一个国家采取措施强化太空系统网络安全属于主权范围内的权力，但美国却将所谓中国与俄罗斯攻击其太空系统网络安全作为托词，来掩盖其谋求太空（军事）霸权的实质。

（一）美国太空系统网络安全政策的影响

美国借助强化太空系统的网络安全，一方面意在构筑应对他国的反太空能力，从而赢得大国竞争背景下的战略、战役与战术各层面的军事胜利。另一方面旨在强化本国的太空产业供应链安全与工业控制系统安全，实现制造业复兴目标，增强本国的经济与科技竞争力，并防止非盟国窃取其太空系统的先进技术。此外，美国希望借着强化太空系统网络安全的机会，谋取制定太空规则的主导权。对霸权国而言，以本国主导的规则形成的秩序是霸权体系的重要组成部分，也是其核心利益。因此，美国希望太空系统网络安全措施能巩固与提升其在太空领域的领导地位，形成全面太空优势，并将此整合进美军作战系统，使美军能够在全域作战并赢得军事胜利；继而以此为基础，制定美国主导下的太空治理规则，构建符合其利益的太空秩序与太空格局。

美国力图封堵太空系统网络安全漏洞也会对全球太空格局产生重要影响。简单地说，一旦美国解决了太空系统的网络安全问题，建立起强大的太空系统网络攻防能力，其太空行动将更加自由，将对其他国家太空资产形成更大的挑战与威胁。基于安全困境的逻辑，迫使别国发展相应的反制措施，太空军备竞赛就很难遏制，太空治理规则也将难以确立。太空领域的国际行为体为强化太空攻防能力，必然制定相应的战略来发展太空实力。2021 年 9

月英国公布《国家太空战略》，旨在制定太空规则，实施太空控制，促进太空系统发展，使英国成为太空领域的领导者。[①] 随着各国太空实力的提升，为谋求有利于自己的太空治理规则，各种治理规则和倡议将相互竞争，给太空治理共识的达成增加实际障碍。

事实上，美国强化太空系统网络安全，也会推动“颠覆性技术”的发展，进一步提升美国科技实力。在科技发展预期中，美国将太空与网络一体化集成作为推动科技发展的重要手段。2016 年 8 月，美国空军太空司令部认为未来 10—30 年在太空与网络空间的交叉领域需要攻克多项关键技术难题，其中包括人工智能、认知电子战与先进数据技术分析等 3 大类共 11 项核心技术，系统集成太空与网络以提升美国整体战场态势感知、指挥与控制能力、作战效能。[②] 同时，美军正式研发新技术，改善 GPS 的定位与导航、授时能力，解决传统 GPS 易遭网络攻击的问题。[③] 所有这些举措可能会导致未来在太空与网络态势感知、太空与网络攻防技术以及太空操作等方面出现“颠覆性技术”。例如，太空探索技术公司（SpaceX）的“星链”卫星在一定程度上让美国跨越 5G 时代迈入 6G 时代。这些技术即使仍不是“颠覆性技术”，但也足以提升美国科技实力，为美国在太空技术、网络技术等高技术方面与中国进行精准脱钩奠定基础。此外，美国强化与盟国的太空产业链安全国际合作，意在构筑所谓的“民主国家科技联盟”，遏制中国高新技术的发展。

（二）美国太空系统网络安全政策的启示与应对

第一，中国应加强包括制造太空系统的工业控制系统安全在内的太空系统网络安全。太空资产事关政权稳固、国家安全、经济安全、金融安全等。从理论上讲，太空系统与网络空间系统更加紧密的结合意味着太空系统遭受

① “National Space Strategy,” U.K. Government, September 27, 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1020617/national-space-strategy.pdf

② USAF Space Command, “Air Force Space Command Strategic S&T Challenges,” U.S. Air Force, August 23-24, 2016, https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/airforce/Combined_Innovation_Summit_Charts_for_Space_Cyber.pdf.

③ Theresa Hitchens, “SASC Wants Alternative GPS by 2023,” *Breaking Defense*, June 29, 2020, https://breakingdefense.com/2020/06/sasc-wants-alternative-gps-by-2023/.

网络攻击的可能性进一步增大。因此，中国没有理由不重视太空系统的网络安全。2019 年《新时代的中国国防》白皮书传递了中国努力强化太空系统网络安全的信号，“太空是国际战略竞争制高点，太空安全是国家建设和社会发展的战略保障。着眼和平利用太空，中国积极参与国际太空合作，加快发展相应的技术和力量，统筹管理天基信息资源，跟踪掌握太空态势，保卫太空资产安全，提高安全进出、开放利用太空能力。”① 加快发展相应技术和力量，跟踪太空发展态势的要求，就包含应对太空系统所面临的网络安全威胁。要确保太空系统网络安全，就必须强化中国的工业控制系统的安全，以及强化与太空产业供应链。伊朗浓缩铀的离心机受到“网震”病毒攻击，导致其核工业遭受巨大损失，这告诫我们必须高度重视太空系统生产、运行的工业控制系统的安全。太空供应链的安全也应立足于国内，依靠国外提供太空系统的部件或服务，都会对中国太空系统造成潜在安全威胁。

第二，中国也应将太空系统与网络空间进行一体化系统集成，提升太空系统的网络攻防能力。太空系统与网络空间高度依赖、相互渗透，太空系统与网络空间一体化的系统集成已成为趋势。未来的战争一定是海、陆、空、网、天、电一体化的军事较量。现代战争不仅是暴力的对抗，也是信息的对抗。太空与网络在信息收集、处理、分发等方面具有无与伦比的优势，可谓信息流决定着军事行动的成败。鉴于太空已经成为作战域，中国需要从战略高度思考太空与网络安全问题，即不能仅将太空力量作为其他军兵种的战略支援力量来对待，更应从独立作战角度进行谋划。这需要将太空系统与网络技术进行一体化系统集成，并整合进其他军兵种的武器系统，形成陆、海、空、网、天、电的一体化威慑能力与整体作战效能。解决这个问题的关键，仍需要从顶层设计出发，举国上下合力，推动“颠覆性技术”的发展。

第三，中国要在太空系统的网络安全规则上发出自己的声音。太空系统用于军事领域，已经对国际人道法造成了诸多困境。太空武器化、太空战场化无疑让包括外层空间相关法律在内的现有国际法面临更大挑战。有关行为体试图在此领域发声，力图说明太空军事利用的法律适用问题。例如，2016

① 国务院新闻办公室：《新时代的中国国防》，新华网，2019 年 7 月 24 日，http://www.xinhuanet.com/politics/2019-07/24/c_1124792450.htm。

年 5 月，加拿大麦吉尔大学法学院航空与空间法研究中心发布《外空军事利用国际法适用手册》（Manual on International Law Applicable to Military Uses of Outer Space, MILAMOS），试图规范太空的军事利用；[①] 北约卓越合作网络防御中心（Cooperative Cyber Defence Centre of Excellence, CCDCOE）先后制定了两版《塔林手册》，试图解决网络空间这个灰色领域的武装冲突问题。不论是利用太空系统对网络进行攻击，还是利用网络攻击太空系统，都使灰色地带问题更为凸显。为保证太空事业和平发展以及长期可持续利用，国际社会应发出倡议以规范太空系统的网络行为。《2021 年中国的航天》白皮书同样表示，“加强国际空间法研究，积极参与外空国际规则制定”[②]。在规范太空系统网络安全行为方面，积极发出中国倡议，是中国作为太空大国的体现。在此过程中，中国要坚持多边主义立场，在联合国框架下开展相关太空外交，努力推动磋商，为形成目标共识贡献中国智慧，在太空领域推进人类命运共同体建设。

[责任编辑：孙震海]

① 有关信息参见该中心网站：https://www.mcgill.ca/milamos/。

② 国务院新闻办公室：《2021 中国的航天》，2022 年 1 月 28 日，http://www.cnsa.gov.cn/n6758823/n6758838/c6813086/content.html。