乌克兰危机中网络空间对抗的影响及启示*

武　琼

【内容提要】　俄乌冲突爆发后，双方在网络空间展开激烈较量。俄乌冲突中的网络空间对抗主要体现在两方面：一方面，国家级网络部队和非国家级黑客组织“选边站”；另一方面，围绕主流媒体及社交平台的控制和争夺日益激烈。俄乌网络空间对抗产生三方面的影响：第一，双方的战略稳定性受到冲击；第二，影响战争形态和作战样式；第三，外溢效应迫使各国筑牢网络安全防护屏障。面对俄乌冲突中的网络空间对抗，中国应从中汲取经验教训，可采取以下四项应对措施：其一，利用大数据技术从海量数据中筛选出敏感数据，建立己方数据优势；其二，推进人工智能人才的引进和培养；其三，加强认知战力量建设；其四，提升网络空间防御能力和威慑能力，保护关键信息基础设施的安全。

【关 键 词】　俄乌冲突　网络战　认知战　人工智能　非国家行为体

【作者简介】　武琼，南京大学国际关系研究院博士研究生。

2022 年 2 月 24 日，俄罗斯总统普京宣布开展特别军事行动，乌克兰危机全面升级。两国在网络空间展开激烈争夺，其实际热度丝毫不亚于战场前线的硝烟弹雨。既有研究主要集中在俄乌冲突中网络空间的武器化运用、深度伪造技术的使用、社交平台的争夺及对全球网络安全空间的影响等四方面①。这些研究成果对理解俄乌网络空间对抗及其影响具有重要的启示意义，但仍有继续补充与完善

* 本文受“南京大学优秀博士研究生创新能力提升计划 B”的资助。

① 卞学勤、于德山：《俄乌冲突中社交网络传播的伦理失范及反思》，载《传媒观察》2022 年第 4 期；郎平：《从俄乌冲突看网络空间武器化倾向及其影响》，载《中国信息安全》2022 年第 6 期；严明：《对俄乌冲突中网络空间对抗的思考》，载《中国信息安全》2022 年第 6 期；苗争鸣：《认知博弈：俄乌冲突中深度伪造技术的应用》，载《中国信息安全》2022 年第 6 期；范勇鹏、韩沁雯：《俄乌冲突网络信息战的特征与启示》，载《中国信息安全》2022 年第 6 期；李恒阳：《俄乌冲突网络对抗及其对网络空间安全的影响》，载《中国信息安全》2022 年第 6 期。

的空间：一是既有研究虽然关注到俄乌冲突中网络空间对抗的全球影响，但针对其在国际关系和国际战略层面（如新型战争形态及其影响）影响的分析仍需加强；二是面对俄乌网络空间对抗，中国网络安全应对策略的研究有待拓展。鉴于此，本文首先探讨俄乌冲突中网络空间对抗的主要表现，之后分析俄乌冲突网络空间对抗的主要影响，最后讨论俄乌网络空间对抗带来的启示。

一　俄乌冲突中网络空间对抗的主要表现

作为与陆、海、空、天并列的第五空间，网络空间已成为俄乌双方展开博弈和斗争的重要阵地。随着冲突的持续进行，两国的网络空间对抗也随之进入白热化阶段。

（一）国家级网络部队和非国家级黑客组织“选边站”

近年来，世界主要国家纷纷创建网络空间部队，加快研发网络空间作战装备，以谋求战略主动权。在俄乌冲突中，国家级网络部队相继登场，并在网络空间展开一系列的激烈对抗。

第一，来自俄罗斯的国家级网络部队。2022 年 4 月 12 日，乌克兰计算机应急响应小组（CERT－UA）和网络安全公司 ESET 发布公告称，黑客组织“沙虫”（Sandworm）使用一款名为“Industroyer2”的恶意软件攻击乌克兰的电力设施。“Industroyer2”是一个完全模块化的平台，具有多个工业控制系统（ICS）协议的攻击载荷，通过把详细的信息硬编码配置在程序主体中，驱动恶意软件操作①。据《华尔街日报》报道，这种恶意软件与 2016 年一次电网攻击中使用的恶意软件相似，被认为是俄罗斯总参谋部情报总局下辖的黑客组织“沙虫”的作品②。安迪·格林伯格认为，“沙虫”实际上为俄罗斯军情部门服务，是一支高度复杂、技术精湛、由国家支持的网络部队，拥有破坏力最强的恶意软件，能对电力、能源、交通等关键信息基础设施实施进攻性网络攻击③。虽然俄罗斯政府对此予以否认，但西方国家却认为，隶属于俄罗斯军方的“沙虫”是对乌克

① ESET Research，“Industroyer2：Industroyer reloaded”. https：//www. welivesecurity. com/2022/04/12/industroyer2－industroyer－reloaded/，访问时间：2022 年 8 月 10 日。

② Dustin Volz and Robert McMillan，“In Ukraine，a ‘Full－Scale Cyberwar’ Emerges”. https：//www. wsj. com/articles/in－ukraine－a－full－scale－cyberwar－emerges－11649780203，访问时间：2022 年 8 月 10 日。

③ Andy Greenberg，*Sandworm：A New Era of Cyberwar and the Hunt for the Kremlin’s Most Dangerous Hackers*，New York：Doubleday，2019.

兰实施网络攻击的幕后黑手。

第二，来自乌克兰和美国的国家级网络部队。俄乌冲突爆发后，乌克兰网络警察部队对俄罗斯联邦调查委员会、联邦安全局及国有银行实施网络攻击，且成效显著①。乌克兰“IT 军队”实际上也具有一定的国家级黑客组织色彩。面对俄罗斯的特别军事行动，乌克兰政府号召平民加入乌克兰“IT 军队”，以保护乌克兰境内的关键信息基础设施，并对俄罗斯执行网络攻击任务。从表面上看，乌克兰“IT 军队”是民间黑客组织，但苏黎世联邦理工学院安全研究中心高级研究员斯蒂芬·索桑托认为，乌克兰“IT 军队”是一支目标清晰、指挥明确、组织严密的黑客军队，其核心成员与乌克兰国防和情报系统关系密切，或者可能就是由其国防和情报系统的人员组成的②。乌克兰“IT 军队”内部的高级管理人员在接受记者专访时曾表示，该组织的核心领导权掌握在乌克兰“专业人士”手中；其成员虽然来自世界各地，但大多数为乌克兰人③。也有中国学者认为，俄乌冲突中的一些黑客组织看似是民间组织，但显然在组织和意识形态上跟政府部门有密切关联④。乌克兰“IT 军队”组建后不久就对俄罗斯实施了网络攻击。俄罗斯网络安全公司卡巴斯基（Kaspersky）的数据显示，2022 年第二季度分布式拒绝服务攻击（DDoS）的持续时间约为 3 000 分钟，较 2021 年第二季度平均 30 分钟的数值增长近 100 倍⑤。俄罗斯外交部指出，以乌克兰“IT 军队”为首的黑客组织定期对俄关键信息基础设施发动分布式拒绝服务攻击。

此外，美军网络司令部和国家安全局正在派遣国家级网络部队介入俄乌冲突。2022 年 6 月 1 日，美军网络司令部司令兼国家安全局局长保罗·中曾根（Paul Nakasone）上将在接受记者采访时表示，美国正在派遣网络部队对俄罗斯实施进攻性网络行动以支援乌克兰。中曾根虽然未说明详细内容，但基于进攻性

① Bill Toulas，“Ukraine says its ‘IT Army’ has taken down key Russian sites”. https：//www. bleepingcomputer. com/news/security/ukraine - says - its - it - army - has - taken - down - key - russian - sites/，访问时间：2022 年 8 月 10 日。

② Stefan Soesanto，“The IT Army of Ukraine：Structure，Tasking，and Ecosystem”. https：//css. ethz. ch/content/dam/ethz/special - interest/gess/cis/center - for - securities - studies/pdfs/Cyber - Reports - 2022 - 06 - IT - Army - of - Ukraine. pdf，访问时间：2022 年 8 月 10 日。

③ Dina Temple - Raston and Sean Powers，“Inside the IT Army of Ukraine，‘A Hub for Digital Resistance’”. https：//therecord. media/inside - the - it - army - of - ukraine - a - hub - for - digital - resistance/，访问时间：2022 年 9 月 3 日。

④ 范勇鹏、韩沁雯：《俄乌冲突网络信息战的特征与启示》。

⑤ “Crypto - collapse and rising smart attacks：Kaspersky reports on DDoS in Q2”. https：//www. kaspersky. com/about/press - releases/2022_☞rypto - collapse - and - rising - smart - attacks - kaspersky - reports - on - ddos - in - q2，访问时间：2022 年 9 月 3 日。

网络行动的敏感性，该言论还是一度引发外界广泛热议。事实上，中曾根也曾私下透露，对俄罗斯实施进攻性网络活动能使其无法开展更有效的网络攻击[①]。美军网络司令部前法律顾问加里·科恩（Gary Corn）和加里·布朗（Gary Brown）等人表示，中曾根所说的进攻性网络行动应该包括侦察和攻击活动的结合。即使美国对俄罗斯采取的网络行动属于武力攻击行为，也不会给俄罗斯攻击美国提供借口[②]。

俄乌冲突催生出一种前所未有的网络游击战形式：大批非国家行为体可以在没有国家军事机构协调的情况下自主展开网络行动[③]，其参战程度之深令人叹为观止。

第一，支持俄罗斯的非国家级黑客组织，主要包括 Conti、Zatoichi、Killnet、XakNet 等[④]。以 Killnet 为例，“许多俄罗斯民众将 Killnet 视为英雄，该组织擅长使用视频或图像在社交平台宣扬攻击战果，意在让欧洲人为他们明确支持乌克兰而付出代价，并惩罚西方政府的反俄情绪。”[⑤] 在以往的网络攻击中，Killnet 主要使用分布式拒绝服务攻击发送大量请求，从而导致计算机系统超载或瘫痪，使之无法提供正常的网络服务。2022 年 5 月 16 日，Killnet 以“恐俄症”为由，正式宣布向美国、英国、德国、意大利、罗马尼亚、拉脱维亚、爱沙尼亚、立陶宛、乌克兰、波兰十个国家发起网络战。2022 年 8 月 10 日，Killnet 宣布入侵洛克希德·马丁公司网站，并导致该公司的员工授权系统、NASA 卡和 RSA 授权系统崩坏，公司所有求职者的资料被黑[⑥]。

第二，支持乌克兰的非国家级黑客组织，主要包括匿名者（Anonymous）、

① Erica D. Lonergan，“The Cyber – Escalation Fallacy”. https：//www. foreignaffairs. com/articles/russian – federation/2022 – 04 – 15/cyber – escalation – fallacy，访问时间：2022 年 9 月 20 日。

② Kim Zetter，“What It Means that the U. S. Is Conducting Offensive Cyber Operations Against Russia”. https：//zetter. substack. com/p/what – it – means – that – the – us – is – conducting，访问时间：2022 年 9 月 20 日。

③ Janosch Delcker，“Ukraine’s IT army：Who are the cyber guerrillas hacking Russia?”. https：//www. dw. com/en/ukraines – it – army – who – are – the – cyber – guerrillas – hacking – russia/a – 61247527，访问时间：2022 年 9 月 20 日。

④ Emma Vail，“Russia or Ukraine：Hacking groups take sides”. https：//therecord. media/russia – or – ukraine – hacking – groups – take – sides/，访问时间：2022 年 9 月 20 日。

⑤ Antoaneta Roussi，“Meet Killnet，Russia’s hacking patriots plaguing Europe”. https：//www. politico. eu/article/meet – killnet – russias – hacking – patriots – plaguing – europe/，访问时间：2022 年 9 月 20 日。

⑥ “Russian Killnet Hacker Group Targets Lockheed Martin Services”. https：//sputniknews. com/20220810/russian – killnet – hacker – group – targets – lockheed – martin – services – 1099443981. html，访问时间：2022 年 10 月 7 日。

幽灵安全（Ghostsec）、反对西方（ATW）、SHDWsec 等[①]。以匿名者为例，据统计，其至少已经攻击 2 500 多个俄罗斯网站。被其攻击的单位主要有军队、中央银行、航天部门、油气公司、物业管理公司、广播公司、IT 公司、律师事务所等，泄露出的数据相当庞大，可能需要数年时间予以核查[②]。2022 年 6 月 4 日，匿名者宣布入侵俄罗斯顶级律师事务所 Rustam Kurmaev and Partners，并从中窃取电子邮件、法庭文件、客户文件等大量数据，目前，被盗数据已被公开在 DDoSecrets 上[③]。匿名者对俄罗斯的网络攻击活动主要分为四类：一是公开重要数据，攻击并发布从俄罗斯国家航天集团、俄罗斯能源公司等实体机构获取的数据。二是攻击在俄罗斯开展业务的公司，通过发动分布式拒绝服务攻击来增加公司在俄罗斯运营的风险。三是劫持媒体服务，通过入侵俄罗斯国家电视台来破坏俄罗斯的审查制度。四是开展宣传，通过俄罗斯社交网站 VK 发送反战和亲乌克兰消息等[④]。

（二）围绕主流媒体及社交平台的控制和争夺日益激烈

主流媒体及社交平台凭借其庞大的用户群体、海量的媒体数据和极快的更新速度成为描述战争进程，影响战争走向的无形利器。基于此，在该领域的争夺日趋激烈。

第一，西方国家、国家集团、大型互联网企业对俄罗斯国营媒体下达全面“封杀令”。西方国家和国家集团利用数字技术优势和媒体话语权，全面封堵俄罗斯的战争宣传。美国、澳大利亚、西班牙、法国、德国、加拿大、英国、拉脱维亚等西方国家纷纷宣布对俄罗斯国营媒体实行封锁，禁止今日俄罗斯（RT）、俄罗斯卫星通讯社（sputnik）在其境内播出。欧盟要求欧盟国家不得转播今日俄罗斯和俄罗斯卫星通讯社电视频道和卫星运营商的节目。大型互联网企业也积极配合美国等西方国家的对俄制裁。谷歌、元（Meta）等企业遵循欧盟禁令，在欧洲

① Emma Vail，“Russia or Ukraine：Hacking groups take sides”. https：//therecord. media/russia – or – ukraine – hacking – groups – take – sides/，访问时间：2022 年 10 月 7 日。

② Monica Buchanan Pitrelli，“Hacktivist group Anonymous is using six top techniques to ‘embarrass’ Russia”. https：//www. cnbc. com/2022/07/28/how – is – anonymous – attacking – russia – the – top – six – ways – ranked – . html，访问时间：2022 年 10 月 7 日。

③ Octavio Mares，“Major Russian law firm is hacked；terabytes of stolen data”. https：//www. security newspaper. com/2022/06/06/major – russian – law – firm – is – hacked – terabytes – of – stolen – data/，访问时间：2022 年 10 月 7 日。

④ Monica Buchanan Pitrelli，“Hacktivist group Anonymous is using six top techniques to ‘embarrass’ Russia”. https：//www. cnbc. com/2022/07/28/how – is – anonymous – attacking – russia – the – top – six – ways – ranked – . html，访问时间：2022 年 10 月 7 日。

范围内禁止访问今日俄罗斯和俄罗斯卫星通讯社，关闭其在欧洲的优兔（YouTube）、脸书（Facebook）、Instagram 的官方账号，并限制俄罗斯官方媒体的广告投放。面对美国等西方国家咄咄逼人的进攻态势，俄罗斯也不甘示弱，采取一系列反制措施：一是封锁脸书，加大对优兔、Telegram 在俄罗斯境内发布信息的审查力度，将“元”列入恐怖主义和极端主义组织名单，全力推荐俄版脸书 VK、俄版优兔 Rutube、俄版抖音 Yappy；二是签署俄罗斯联邦刑法修正案，对故意散布有关俄军的假信息者，最高可判处 15 年监禁；三是封禁美国之音、英国广播公司、自由欧洲电台、拉脱维亚“美杜莎”（Meduza）新闻网、德国之声等媒体，谴责这些机构故意传播有关俄乌冲突的虚假信息；四是打击使用 VPN 的行为，宣布建立数据库，收集手机 IMEI 代码①。

第二，借助主流媒体及社交平台发布鱼龙混杂的消息。一是通过主流媒体发布有关信息。俄罗斯主要通过国内主流媒体向民众揭露“亚速营”犯下的各种战争罪行、美国在乌克兰设立生物实验室来宣扬战争的合法性，争取舆论支持。俄罗斯卫星通讯社报道称，“亚速营”是乌克兰国民警卫队的一个作战单位，由乌克兰内务部直接领导，具有新纳粹主义和白人至上主义特征。“亚速营”成员曾在顿巴斯地区打击亲俄武装时犯下各种令人震惊的战争罪行，包括禁锢和迫害当地居民②，所以这支部队的存在是俄罗斯实施特别军事行动的主要动因之一。

二是利用社交平台发布各种博人同情或暴力恐怖的信息，如一名乌克兰女孩在基辅防空洞中演唱电影《冰雪奇缘》主题曲《放手》（Let It Go），大量乌克兰民众躲在地铁站避难，布恰事件的画面等。需要指出的是，泽连斯基擅长利用社交平台来发布“仇俄”和“反俄”的信息。泽连斯基曾发布过一段巧妙剪辑过的视频。这段视频开始部分展现出俄乌冲突前乌克兰在经济建设、社会发展和人民生活呈现出的欣欣向荣景象。然而，画面随即一转，切换至具有强烈视觉冲击效果的战争画面。这段视频的中后半部分记录俄军在使用导弹袭击乌克兰城市后，现场火光四起、浓烟滚滚、爆炸声不断的画面，并从不同角度拍摄大量因战争而受伤的当地平民和流离失所的儿童。

① Matt Burgess，“Russia Is Quietly Ramping Up Its Internet Censorship Machine”. https：//www. wired. co. uk/article/russia - internet - censorship - splinternet，访问时间：2022 年 10 月 7 日。

② “Evidence Suggests US May Have Supported Neo - Nazi Azov Battalion”. https：//sputniknews. com/20220309/evidence - suggests - us - may - have - supported - neo - nazi - azov - battalion - 1093714960. html，访问时间：2022 年 10 月 19 日。

与此同时，大量移花接木、断章取义的虚假信息正在社交平台上广泛传播。例如“蛇岛十三勇士”面对大军压境拒不投降，乌克兰男子上战场前挥泪告别妻女，俄军攻破美军在乌克兰的实验室并解救数千名儿童等。一则乌克兰男子泪别妻女、准备上前线与俄军作战的视频刷爆社交平台，仅一天内播放量便达到 700 万次。但事实是，该名男子为顿巴斯地区的一名亲俄人士。为确保家人安全，他选择将其送往俄罗斯，自己则投入到与乌军的战斗中。再如一则俄军攻破美军在乌克兰的实验室并解救数千名儿童的视频也在社交平台上流传。但实际上，该视频是 2018 年因叙利亚内战而受伤的儿童正在医院接受治疗的影像，与俄乌冲突毫无关系。

三是利用高技术手段制造并传播虚假信息。其一是利用社交机器人散布虚假信息。社交机器人是指在社交平台中模仿正常用户自主进行操作并发布文本、图片、音频、视频等内容的自动化程序体。2022 年 3 月 28 日，乌克兰国家安全局通报，自俄罗斯实施特别军事行动以来，乌克兰国家安全局已经发现并关闭五个社交机器人农场。这些拥有超过 10 万个社交平台账户的机器人农场主要在哈尔科夫、切尔卡瑟、捷尔诺皮尔和扎卡帕蒂亚四个地区运作，旨在通过散布虚假信息来制造恐慌，影响社会局势的稳定①。2022 年 8 月 2 日，乌克兰国家安全局表示，已关闭在基辅、哈尔科夫及文尼察运营的机器人农场。这些机器人农场依靠 100 万个社交平台账户大肆传播虚假信息，旨在破坏乌克兰的社会和政治局势②。

其二是借助视频合成技术传播虚假信息。俄乌冲突爆发后不久，一段关于“基辅幽灵”的视频在社交平台上广泛传播。一名乌克兰空军飞行员在开战首日便击落 6 架俄军战机，并创下单人击落 40 架俄军机的“战果”，被外界称作“基辅幽灵”。乌克兰前总统波罗申科、乌克兰国防部、国家安全局和空军积极转发相关视频，并不断渲染其空中“战绩”。乌空军司令部更是表示，“基辅幽灵”是乌克兰人的“超级英雄传奇”，是乌军第 40 战术航空旅全体飞行员的“集体

① “Since war started，SSU shuts down 5 enemy’s bot farms with over 100，000 fake accounts”. https：//ssu. gov. ua/en/novyny/z - pochatku - viiny - sbu - likviduvala - 5 - vorozhykh - botoferm - potuzhnistiu - ponad - 100 - tys - feikovykh - akauntiv，访问时间：2022 年 10 月 27 日。

② “SSU shuts down million - strong bot farm that destabilized situation in Ukraine and worked for one of political forces（video）”. https：//ssu. gov. ua/en/novyny/sbu - likviduvala - milionnu - botofermu - yaka - rozkhytuvala - obstanovku - v - ukraini - na - zamovlennia - odniiei - z - politsyl - video，访问时间：2022 年 10 月 27 日。

形象”[①]。然而，路透社和德国之音等媒体核查发现，“基辅幽灵”击落俄军战机的视频实际上来自于一款名为“数字战斗模拟世界”（DCS）的计算机游戏，并利用视频合成技术对其中的片段进行了拼接处理[②]。

其三是利用深度伪造技术制造虚假视频。深度伪造技术是指通过深度学习算法篡改原始声音、图像和视频的智能处理技术。俄乌冲突发生后，有关普京和泽连斯基的虚假视频在社交平台上疯传。社交平台上曾出现一段关于普京的虚假视频。在这段假视频中，普京表示，我们将与乌克兰达成和平协议；乌克兰与顿涅茨克和卢甘斯克接壤，这是世界公认的边界；我们还签署一份五年路线图，让克里米亚成为乌克兰境内的一个独立共和国。同时，一段关于泽连斯基的虚假视频也在社交平台上流传。视频内容是呼吁乌克兰士兵放下武器，向俄罗斯投降，回到家人身边。事实上，普京和泽连斯基从未说过这些话。视频中，两人的音频和嘴部动作是使用深度学习算法完成的[③]。

二　俄乌冲突网络空间对抗的主要影响

作为欧亚大陆上重要的地缘战略棋手国和地缘政治支轴国[④]，俄乌冲突中的网络空间对抗不仅加剧两国冲突，对全球网络空间安全形势的影响也正在日益显现。

（一）双方的战略稳定性受到冲击

战略稳定性这一概念来源于冷战期间美苏两个超级大国相互核威慑的互动实践。冷战结束后，战略稳定性的概念内涵呈现出不断发展与深化的趋势。就广义层面而言，战略稳定性是指在国际体系中互动关系较为稳定、行为模式可以预期、难以出现进攻占优诱因的基本态势。其中，网络空间的战略稳定性非常重要，关系到各国的国家安全、国土安全，与全球的和平与发展也息息相关。随着

① Laurence Peter，“How Ukraine’s ‘Ghost of Kyiv’ legendary pilot was born”. https：//www. bbc. com/news/world – europe – 61285833，访问时间：2022 年 10 月 27 日。

② Reuters Fact Check，“Fact Check – Animation miscaptioned as if to show video of Ukrainian fighter jet shooting down Russian plane”. https：//www. reuters. com/article/factcheck – animation – ukrainianjet – idUSL1N2V035G；Ines Eisele，“Fact check：Ukraine’s ‘Ghost of Kyiv’ fighter pilot”. https：//www. dw. com/en/fact – check – ukraines – ghost – of – kyiv – fighter – pilot/a – 60951825，访问时间：2022 年 10 月 27 日。

③ Rachel Baig，“Fact check：The deepfakes in the disinformation war between Russia and Ukraine”. https：//www. dw. com/en/fact – check – the – deepfakes – in – the – disinformation – war – between – russia – and – ukraine/a – 61166433，访问时间：2022 年 10 月 27 日。

④ Zbigniew Brzezinski，*The Grand Chessboard*：*American Primacy and Its Geostrategic Imperatives*，New York：Basic Books，1998，pp. 20 – 79.

网络信息技术的快速发展和不断普及，网络空间超级大国通过发起网络挑衅性行动、网络先发制人打击甚至是摧毁性网络攻击等手段来影响局势，改变对手的行为，但同时也会削弱战略稳定性，影响国家和国际安全①。

俄乌冲突爆发前，俄罗斯持续加大对进攻性网络力量的战略投入，其综合网络实力②和网络攻击能力③不可小觑。俄罗斯军事专家和高级将领认为，鉴于网络空间安全的重要性，若要取得相对于竞争对手的网络空间优势，采取先发制人的打击是其中的重要一环，甚至是最有可能取得胜利的途径。时任俄罗斯导弹和炮兵学院副院长亚历山大·拉赫曼诺夫中将曾指出，俄军在地区冲突中应采取“以网络为中心”的战争模式，一旦发生冲突，要先发制人地压制或摧毁敌人的网络系统来实现信息优势④。俄罗斯武装力量总参谋长瓦列里·格拉西莫夫认为，为配合地面部队的进攻作战，俄军在地区冲突中应首先采取隐蔽的军事手段，包括实施进攻性网络攻击行动和特种部队秘密突袭。其中，开展进攻性网络攻击行动有助于在短时间内摧毁敌国重要的军民两用基础设施，削弱其战争潜力⑤。俄乌冲突爆发当日，俄罗斯国家级网络部队成功部署的破坏性恶意软件比世界其他网络强国在特定年份通常使用的总和还要多，主要攻击目标为乌克兰政府和军队、国防工业企业、能源和电力等关键部门。此后，俄罗斯以网络工具库为后盾，持续在基辅和哈尔科夫等城市部署破坏性恶意软件。随着俄乌冲突的持续进行，俄罗斯的国家级网络部队会处于永久战备状态，并根据上级通知随时支持在乌克兰战场上的战术和战略目标⑥。

---

① 刘杨钺：《网络空间国际冲突与战略稳定性》，载《外交评论》2016 年第 4 期；周宏仁：《网络空间的崛起与战略稳定》，载《国际展望》2019 年第 3 期。

② 贝尔弗科学与国际事务研究中心（Belfer Center for Science and International Affairs）利用 32 个意图指标和 27 个能力指标，对 30 个国家的网络能力进行综合评估。根据计算，俄罗斯的综合网络实力位列全球第四。参见 Julia Voo and Irfan Hemani et al.，“National Cyber Power Index 2020，” *Belfer Center for Science and International Affairs*，September 2020，pp. 1 – 2.

③ 美国情报专家丽贝卡·科弗勒（Rebekah Koffler）在《普京剧本：俄罗斯击败美国的秘密计划》一书中透露，俄罗斯在过去三十年里一直在发展进攻性网络能力。迄今为止，俄罗斯已拥有逻辑炸弹、网络蠕虫、特洛伊木马等各式网络武器，其网络武器在智能性、自主性、攻击力、对敌渗透速度等方面可与美国媲美。俄罗斯的网络攻击小组“从进入目标的计算机系统到利用漏洞破坏工业控制系统”仅需 18 分钟 49 秒。参见 Rebekah Koffler，*Putin’s Playbook：Russia’s Secret Plan to Defeat America*，Washington. DC.：Regnery Gateway，2021，pp. 127 – 163.

④ Alexander A. Rakhmanov，“Network Centric Control Systems：Natural Trends，Problems，and Solutions”，*Military Thought*，Vol. 20，No. 1，2011，pp. 100 – 111.

⑤ Valery Gerasimov，“The Value of Science Is in the Foresight：New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations”，*Military Review*，January – February 2016，pp. 23 – 29.

⑥ David Cattler and Daniel Black，“The Myth of the Missing Cyberwar”. https：//www. foreignaffairs. com/articles/ukraine/2022 – 04 – 06/myth – missing – cyberwar，访问时间：2022 年 11 月 9 日。

面对俄罗斯实施的网络攻击，乌克兰仅凭一国的力量难以抵抗。事实上，乌克兰网络防护手段相当滞后。为增强网络防御能力，乌克兰政府 2015 年以来开始与美国等西方国家展开网络空间安全合作。在北约、美军欧洲司令部、美国陆军和海军的帮助下，乌克兰国防部和内务部等重要部门的网络防御能力得到实质性提升①。美国等西方国家的网络技术支持在保卫乌克兰网络空间安全方面发挥了不可替代的作用。俄乌冲突爆发后，虽然西方国家没有大规模派遣地面部队前往乌克兰作战，但在网络空间，西方国家政府及技术和网络安全公司直接与俄罗斯对垒，并致力于采取措施保卫乌克兰境内的关键信息基础设施及其数据安全。根据尼克·比克罗夫特的研究，这主要体现在以下六方面：一是派遣网络安全人员前往乌克兰，如美军网络司令部执行“前出狩猎”（hunt forward）行动、欧盟启动网络快速反应小组；二是远程开展网络安全操作，如美英资助私营部门向乌克兰提供网络安全服务、网络安全公司为乌克兰用户提供安全服务；三是共享攻击活动、敌方战术和战略评估等情报，如美国政府部门与乌克兰共享网络情报、网络安全公司建立与乌克兰快速共享情报的机制；四是提供培训、机构建设和政策协调等，如美国与乌克兰展开联合培训、吸纳乌克兰加入北约合作网络防御卓越中心（CCDCOE）；五是提供硬件和技术措施以解决网络漏洞，如西方国家政府捐助硬件、SpaceX 公司提供“星链”（Starlink）卫星通信设备；六是通过云服务增强稳健性和韧性，如帮助乌克兰将公私机构数据迁移到云端②。

俄罗斯军方高层最初预计俄乌冲突是一场能以势如破竹般的“闪电战”而迅速结束的短期战争，所以俄并未对乌克兰发起破坏性的网络攻击行动，主要是希望能保持乌克兰关键信息基础设施完好无损，以便在冲突结束后使用。然而，随着陷入持久战和消耗战，俄罗斯的国家级网络部队正在对乌克兰的关键信息基础设施展开全面进攻性网络攻击。一场“全方位网络大战”（Full－Scale Cyberwar）正在笼罩乌克兰③。至此，俄乌在网络空间的战略稳定性已严重失衡，且呈现日益加剧之势。

---

① Nadiya Kostyuk and Aaron Brantly, “War in the borderland through cyberspace: Limits of defending Ukraine through interstate cooperation”, *Contemporary Security Policy*, Vol. 43, No. 3, 2022, pp. 498－511.

② Nick Beecroft, “Evaluating the International Support to Ukrainian Cyber Defense”. https://carnegieendowment.org/2022/11/03/evaluating－international－support－to－ukrainian－cyber－defense－pub－88322, 访问时间：2022 年 11 月 9 日。

③ Dustin Volza and Robert McMillan, “In Ukraine, a ‘Full－Scale Cyberwar’ Emerges”. https://www.wsj.com/articles/in－ukraine－a－full－scale－cyberwar－emerges－11649780203; Dustin Volz, “Hackers Linked to Russia Launched Hundreds of Cyberattacks in Ukraine, Microsoft Says”. https://www.wsj.com/articles/hackers－linked－to－russia－launched－hundreds－of－cyberattacks－in－ukraine－microsoft－says－11651078821, 访问时间：2022 年 11 月 18 日。

（二）影响战争形态和作战样式

随着人类社会进入数字时代，俄乌网络空间对抗给国际安全领域带来的深远影响正在改变传统的战争形态和作战方式。非国家行为体的深度介入、认知战的广泛运用及网络空间和物理空间的密切结合不仅会彻底改变传统的战争模式，还会在未来的战争中发挥出越来越大的影响力。

第一，非国家行为体介入网络空间正在塑造新型作战样式。与国家行为体相比，非国家行为体不仅不受规则的限制，其战略和战术选择也更加多元和丰富。这意味着非国家行为体具备以小博大和以弱胜强的资本。作为弱势一方，非国家行为体可通过挑衅、动员、消耗等方式同国家行为体对抗，从而导致战争形态发生变化①。在俄乌冲突中，以大型互联网企业、小型科技企业和民间黑客组织为代表的非国家行为体不仅显著影响战场进程，改变国家军事力量的对比态势，还拓展传统战争形态的空间领域，打造新的战争样式②。以非国家级黑客组织为例，在包括网络战在内的常规军事冲突中，战争双方基本遵循一种被称为“指挥—控制”的作战样式，即指挥官在执行任务时不仅要确定军事目标，还对作战部队拥有监督和指挥权。如果没有这样的指挥结构，国与国间的冲突可能变成一场混战，因为不同单位甚至个人都会自主选择攻击目标。但在俄乌冲突中，支持乌克兰的网络志愿军和亲俄黑客组织会自行决定、计划和执行对两国关键信息基础设施的任何打击。乌克兰网络志愿军对俄罗斯的网络攻击会促使亲俄黑客组织发起报复。同样，亲俄黑客组织对乌克兰的网络攻击也会促使乌克兰网络志愿军展开复仇行动③。《华盛顿邮报》的追踪调查显示，这些非国家级黑客组织具有三个特点：一是自愿实施各种网络攻击行动，不要求得到任何回报；二是自己提供相关基础设施，并在工作和家庭生活以外的时间实施各种网络攻击行动；三是没有得到乌克兰或其他政府机构的指导或帮助④。

就俄乌冲突而言，非国家级黑客组织的广泛介入已成为俄乌网络空间对抗的重要组成部分。网络安全专家约瑟夫·马克斯和亚伦·沙弗认为，已知的针对俄

① 左希迎：《非常规战争与战争形态的演变》，载《世界经济与政治》2020 年第 3 期。

② 李岩：《从俄乌冲突看非国家行为体的作用与影响》，载《现代国际关系》2022 年第 4 期。

③ Elisabeth Braw，“Ukraine’s Digital Fight Goes Global”. https：//www. foreignaffairs. com/articles/ukraine/2022 - 05 - 02/ukraines - digital - fight - goes - global，访问时间：2022 年 11 月 18 日。

④ Joseph Menn，“Hacking Russia was off - limits. The Ukraine war made it a free - for - all”. https：//www. washingtonpost. com/technology/2022/05/01/russia - cyber - attacks - hacking/，访问时间：2022 年 11 月 18 日。

罗斯和乌克兰的网络行动大部分是由非国家级黑客组织自愿实施，而非直接为两国政府工作。按照目前的发展趋势，非国家级黑客组织将会在未来的冲突中发挥决定性作用，尤其是当公众广泛同情其中一方，使大量掌握网络技术的黑客愿意提供帮助的时候①。前瑞典军事情报局局长、退役少将古纳尔·卡尔森（Gunnar Karlson）预测，未来将会在网络空间看到更多这样的自由影子战争。难以负担大规模武装力量的国家可以通过号召志愿者加入影子军队的方式来低成本地发动战争。对年轻一代而言，这将会成为很自然的参与方式②。与传统层面上国家通过调动整体力量和资源来协调一致指挥组织军事行动不同的是，派别复杂且组织指挥结构松散的非国家级黑客组织正在打造一种新的作战方式：在任何时间、任何地点、任何位置自主对目标实施网络攻击，即使这样的攻击行动有可能会违反国际规则和国内法律。

第二，以社交平台为载体的认知战正在影响战争进程和关键走向。随着5G、大数据、人工智能等新一代信息技术的快速发展和广泛运用，作战空间正在由物理域和信息域加快向认知域转变。认知空间正在成为大国战略竞争的主战场。与传统军事任务不同的是，“认知战是将人的思想作为战场，其不仅试图改变人们的观念，还企图改变其思维方式和行为模式。成功的认知战将塑造和影响个人和群体的信念和行为，从而支持进攻方的战术和战略目标。在极端情况下，认知战可能分裂整个社会，以削弱敌方的抵抗意志。”③

网络空间内的认知战已成为俄乌冲突的重要部分。俄乌正在以社交平台为基础，干扰对方视听、搅乱对方思想、引导国际舆论，堪称是一种新型战争形态和高级作战样式④。在俄乌冲突期间，各方在发布真实信息以宣扬本方立场，定义战争合法性的同时，也发布了大量虚假信息诱使对手作出战略误判，构建有利于己方的国际舆论环境。具体而言，通过图片、视频等形式大肆制造并向对手传递虚假信息，可以在社交平台带来以讹传讹式的扩散，此举有助于对敌人的思维、

① Joseph Marks and Aaron Schaffer，“In cyber conflict，Ukraine has an underdog advantage over Russia”. https：//www. washingtonpost. com/politics/2022/05/02/cyber - conflict - ukraine - has - an - underdog - advantage - over - russia/，访问时间：2022年11月18日。

② Elisabeth Braw，“Ukraine's Digital Fight Goes Global”. https：//www. foreignaffairs. com/articles/ukraine/2022 - 05 - 02/ukraines - digital - fight - goes - global，访问时间：2022年11月18日。

③ Kathy Cao and Sean Glaister et al.，“Countering cognitive warfare：awareness and resilience”. https：//www. nato. int/docu/review/articles/2021/05/20/countering - cognitive - warfare - awareness - and - resilience/index. html，访问时间：2022年11月18日。

④ 李明海：《认知域正成为未来智能化混合战争主战场》，载《环球时报》2022年3月17日。

意志、心理等无形目标进行软杀伤，并传播己方的情感态度和价值观念，塑造利于己方的公众舆论氛围，从而达到影响对手指挥决策，甚至干扰战争进程或走向的目的。尤其是随着 5G 网络的快速发展和社交平台的广泛应用，这些错误和虚假信息将会以前所未有的速度在各种社交平台快速传播。正如彼得·辛格和艾默生·布鲁金所指出的，社交平台曾经是一个令人感到轻松和愉悦的联系场所，但现在却已演变为一个高度武器化的战场。不管是世界上实力强大的主权国家，还是微不足道的普通民众，社交平台正在成为他们手中的利器。为此，他们会在社交平台上大量传播并广泛扩散包含阴谋和谎言在内的各种虚假信息，以营造有利于本国的舆论环境，并以软手段战胜对手①。

从“基辅幽灵”、“蛇岛十三勇士”、乌克兰男子被征召上战场含泪告别妻女等虚假视频在社交平台上的广泛传播可以发现，乌克兰与西方国家正在“没有硝烟的战场”上里应外合，把反俄挺乌的信息视为重要武器，煽动乌克兰人对俄罗斯的仇恨和愤怒情绪，以此在第一时间博取国际社会的同情和支持。事实证明，在俄乌冲突中，依托于高度发达的西方主流媒体和各大社交平台，乌克兰在认知战中占尽优势，而“俄罗斯正在输掉认知战”②。《纽约时报》对此评论道，俄乌冲突爆发以来，乌克兰不断开展一系列相当经典的宣传攻势，如塑造战场英雄、宣传民众苦难等，此举至少能起到四方面效果：一是破坏俄罗斯的国际形象；二是塑造乌克兰站在道德制高点的坚强幸存者的国家形象；三是与俄罗斯专注于影响本国民众不同，乌克兰通过操纵大量虚假信息和未经证实的信息来争取国内及国际社会的支持；四是策应乌军在前线作战③。

此外，深度伪造技术通过社交平台对俄乌冲突的广泛介入值得高度关注。诚然，由于技术限制，关于泽连斯基劝降乌军的视频画质一般且制作粗糙，难以达到以假乱真的效果。然而，深度伪造专家尼娜·希克（Nina Schick）表示，尽管这段视频制作十分粗陋，但在不久的将来，情况会发生改变。人们会相信伪造出

① P. W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media*, New York: Eamon Dolan/Houghton Mifflin Harcourt, 2018, pp. 19 – 261.

② David Acosta, “Are We Informationally Disadvantaged? The Realities of Information War in Ukraine”. https://smallwarsjournal.com/jrnl/art/are – we – informationally – disadvantaged – realities – information – war – ukraine, 访问时间：2022 年 11 月 22 日。

③ Stuart A. Thompson and Davey Alba, “Fact and Mythmaking Blend in Ukraine’s Information War”. https://www.nytimes.com/2022/03/03/technology/ukraine – war – misinfo.html; Megan Specia, “‘Like a Weapon’: Ukrainians Use Social Media to Stir Resistance”. https://www.nytimes.com/2022/03/25/world/europe/ukraine – war – social – media.html, 访问时间：2022 年 11 月 22 日。

的任何人或物。这是一种新武器，也是假信息的一种有效形式①。美国法学专家罗伯特·切斯尼和丹尼尔·西特龙指出，在不久的将来，不仅制作利用深度伪造技术篡改的视频会越来越容易，而且这些视频还能够达到让人深信不疑的效果。在社交平台的推波助澜下，用户往往不会去核实这些信息的真实性，最终结果就是谎言比任何时候传播得都快②。有鉴于此，随着深度学习算法的日益优化，政治对手或战场敌人可以利用深度伪造技术制造高度逼真且外界难以辨别的音频/视频，如国家领导人或军队资深将领的虚假命令音频或暴力行动视频，政府官员和政党组织领导人的负面音视频等。届时，谁能掌握先进的深度伪造技术，谁就能在战场上更快地干扰和破坏敌方的判断与决策，瓦解敌方的抵抗意志，从而引发决策失误、士气低落、军心涣散，最终实现攻心夺志的战略目标。

第三，网络空间与物理空间的紧密结合正在催生新型“混合战”。随着大数据、人工智能、物联网和云计算等新科技的快速发展，网络空间正处于与物理空间深度互动的阶段③。在俄乌冲突中，网络空间与传统陆、海、空作战域的快速融合正在超越过去低强度、目的相对单一的网络战，不仅是整个战场不可分割的组成部分，还成为助力乌克兰地面抵抗的新型“混合战”④。事实上，正是依托低延时和高稳定的网络信息服务，俄乌才能在战场上有针对性地部署和运用智能化指挥系统和无人化作战系统，从而迅速定位重要目标并对其实施精准打击。

一是借助智能化指挥系统提升战场决策能力。智能化指挥系统在某种程度上以软件的形式存在，而软件的正常运行离不开持续和稳定的网络服务。俄乌冲突爆发后，两国分别使用“自动控制系统”（ACS）和“德尔塔系统”（Delta）分析处理从战场上收集的海量作战数据，并将其转化为有价值的情报，从而辅助指挥员走出“数据海洋”，快速制定科学合理的决策方案。俄军使用的“自动控制系统”主要通过智能算法自主分析处理从战场上获得的海量原始数据，以从中挖掘出关键军事情报，从而缩短俄军指挥官的决策循环周期，帮助制定方案，如自主对攻击目标进行优先排序或确定打击敌方目标所需要的军事装备。乌克兰主要

① Jane Wakefield，“Deepfake presidents used in Russia – Ukraine war”. https：//www. bbc. com/news/technology – 60780142，访问时间：2022 年 12 月 7 日。

② Robert Chesney and Danielle Citron，“Deepfakes and the New Disinformation War”. https：//www. foreignaffairs. com/articles/world/2018 – 12 – 11/deepfakes – and – new – disinformation – war，访问时间：2022 年 12 月 7 日。

③ 鲁传颖：《网络空间大国关系面临的安全困境、错误知觉和路径选择——以中欧网络合作为例》，载《欧洲研究》2019 年第 2 期。

④ 方兴东、钟祥铭：《算法认知战：俄乌冲突下舆论战的新范式》，载《传媒观察》2022 年第 4 期。

使用“德尔塔系统”处理原始作战数据。该系统可以从笔记本电脑登录使用，并安装“态势感知”智能软件，结合来自无人机、卫星的图像构建交互式地图，以追踪敌人①。根据战场态势感知变化，乌军指挥员能根据重要军事情报确定最佳伏击地点、最优进攻路线、己方和敌方部队的所在位置，从而精准指挥和协调控制前线作战部队。

需要指出的是，以美国为首的西方国家正在利用人工智能系统分析处理海量战场数据，并将其传输给乌克兰的军事单位，以帮助乌军建立战场优势。美国情报官员表示，俄罗斯发起特别军事行动之后，美国国防部及时向乌克兰提供关于俄军行动的详细情报，其中包括俄军的战略部署及导弹和炸弹攻击的主要目标、确切时间和具体地点，俄军的军事指挥所、弹药库及行军路线，从俄秘密作战计划中收集的俄军调动情况等。基于保密原因，美国官员并未透露情报共享的具体细节②。美国对外关系委员会研究员劳伦·卡恩对此表示，美国正在利用人工智能系统分析海量数据，并生成俄罗斯战术和战略模型，以支援乌克兰作战③。

二是使用无人化作战系统打击重要军事目标。在俄乌冲突中，两国主要使用无人机、精确制导导弹等无人化作战系统对敌展开打击。以无人机为例，无人机因其操作简便、机动性强、作战效率高、隐蔽性能突出等优势而颇受大国青睐。然而，无人机若想在战场上执行前沿侦察、高空监视和火力打击等任务，就需要有可靠且稳定的网络通信服务。俄罗斯在战场上主要使用以“猎户座”（Orion）“前哨－R”（Forpost－R）“天竺葵－2”（Geranium 2）为代表的无人机。2022 年 3 月 4 日和 13 日，俄罗斯分别使用“猎户座”和“前哨－R”无人机打击乌克兰“艾达尔”（Aidar）营观察指挥所和多管火箭系统。2022 年 9 月 17 日，乌

① Gemma Parry and Alex Hammer，“Elon Musk’s satellites help Zelensky dominate the skies：US billionaire’s internet system is allowing Ukrainian drones to pound Putin’s helpless tanks”. https：//www.dailymail.co.uk/news/article－10630625/Elon－Musks－internet－allowing－Ukrainian－drones－pound－Putins－helpless－tanks.html；Alia Shoaib，“Inside the elite Ukrainian drone unit founded by volunteer IT experts：‘We are all soldiers now’”. https：//www.businessinsider.com/inside－the－elite－ukrainian－drone－unit－volunteer－it－experts－2022－4，访问时间：2022 年 12 月 7 日。

② Ken Dilanian and Courtney Kube et al.，“U.S. intel helped Ukraine protect air defenses，shoot down Russian plane carrying hundreds of troops”. https：//www.nbcnews.com/politics/national－security/us－intel－helped－ukraine－protect－air－defenses－shoot－russian－plane－carry－rcna26015；Julian E. Barnes and Helene Cooper et al.，“U.S. Intelligence Is Helping Ukraine Kill Russian Generals，Officials Say”. https：//www.nytimes.com/2022/05/04/us/politics/russia－generals－killed－ukraine.html；Julian E. Barnes and Helene Cooper，“Ukrainian Officials Drew on U.S. Intelligence to Plan Counteroffensive”. https：//www.nytimes.com/2022/09/10/us/politics/ukraine－military－intelligence.html，访问时间：2022 年 12 月 7 日。

③ Lauren Kahn，“How Ukraine Is Remaking War”. https：//www.foreignaffairs.com/ukraine/how－ukraine－remaking－war，访问时间：2022 年 10 月 19 日。

克兰第92机械化旅炮兵指挥官罗迪翁·库拉金（Rodion Kulagin）指出，过去一周里，俄罗斯使用“天竺葵-2”无人机对哈尔科夫地区东北部的乌军装甲和炮兵阵地实施“蜂群”式打击。这是俄军首次在战场上大规模部署自杀式无人机，并对乌军造成严重破坏①。

乌克兰在战场上主要使用“旗手-TB2”（Bayraktar-TB2）、“弹簧刀-300”（Switchblade-300）、“凤凰幽灵”（Phoenix Ghost）等无人机攻击俄军的重要目标。2022年4月14日，俄罗斯国防部表示，“莫斯科”号导弹巡洋舰因起火引起弹药爆炸，导致船体受损，后在拖曳回港口途中失去稳定性而在狂风大浪中沉没于黑海。然而，乌克兰官员和军事专家则表示，“旗手-TB2”无人机使用其配备的微型激光制导导弹率先发起攻击，打击该舰防空系统，随后协助“海王星”（Neptune）反舰导弹击中该舰②。

（三）外溢效应迫使各国筑牢网络安全防护屏障

由于网络空间打破了传统意义上的地理疆域，国与国间网络攻击而引发的局部性甚至全球性危害早已屡见不鲜③。为应对俄乌网络空间对抗引发的外溢效应，各国及国际组织纷纷提高安全级别。作为冷战结束后俄罗斯采取的最大规模的国际军事行动④，俄乌网络空间对抗已经对北约国家产生明显的外溢效应。北约负责情报和安全的助理秘书长大卫·卡特勒和北约网络威胁分析部门首席分析师丹尼尔·布莱克认为，俄乌冲突爆发后，俄罗斯的网络攻击行动已经对北约国家产生明显的外溢效应，并由此影响到关键部门的正常运行和民用互联网连接⑤。如在俄乌冲突爆发当日，黑客组织对卫星通信公司Viasat展开网络攻击。虽然此次的袭击目标应是主要针对乌克兰境内的军事目标，但同时也导致德国、法国、匈牙利、希腊、意大利、波兰等北约国家的约1.3万名互联网用户出现网络服务中断，并致使德国等国约5 800台风力漩涡机的调制解调器离线。法国太

① Yaroslav Trofimov and Dion Nissenbaum，“Russia's Use of Iranian Kamikaze Drones Creates New Dangers for Ukrainian Troops”. https：//www. wsj. com/articles/russias-use-of-iranian-kamikaze-drones-creates-new-dangers-for-ukrainian-troops-11663415140，访问时间：2022年12月7日。

② David Hambling，“Ukraine's Bayraktar Drone Helped Sink Russian Flagship Moskva”. https：//www. forbes. com/sites/davidhambling/2022/04/14/ukraines-bayraktar-drones-helped-destroy-russian-flagship/，访问时间：2022年12月10日。

③ 2017年6月，一款名为“Petya”的恶意软件最初用于攻击乌克兰一家公司，但后来快速扩散至俄罗斯、美国、英国、法国等全球范围内的60多个国家，造成的经济损失达上百亿美元。

④ 赵会荣：《乌克兰危机的多维探源》，载《俄罗斯东欧中亚研究》2022年第4期。

⑤ David Cattler and Daniel Black，“The Myth of the Missing Cyberwar”. https：//www. foreignaffairs. com/articles/ukraine/2022-04-06/myth-missing-cyberwar，访问时间：2022年12月10日。

空司令部司令米歇尔·弗里德林（Michel Friedling）少将证实，覆盖欧洲的卫星网络 Viasat 在遭遇网络攻击后，其成千上万的终端无法运行①。

面对俄乌网络空间对抗带来的外溢风险，北约正在通过实施网络安全演习、举行网络安全会议、建立网络空间支援部队等方式提升北约国家的网络空间作战能力。2022 年 4 月 19～22 日，在北约合作网络防御卓越中心的组织下，包括北约国家和乌克兰在内的 32 个国家参加“锁盾”（Locked Shields）演习。北约合作网络防御卓越中心的负责人雅克·塔里恩（Jaak Tarien）表示，“锁盾”演习的具体细节不便公开，但其中一些情景反映出与俄乌冲突有关的担忧。如首次在演习中演练了电网遭到攻击的情况②。5 月 18 日，北约高级网络协调员在布鲁塞尔首次举行会议，主要讨论俄乌冲突后的战略环境及其对网络空间安全的影响，以及进一步加强北约的网络空间作战能力③。6 月 29 日，北约官员透露，随着俄乌冲突的外溢效应日渐显现，北约计划建立联合网络安全小组，以在其成员国发生大规模网络攻击时快速部署，并保护各成员国的网络安全④。

需要说明的是，美国是北约的主要领导国，一旦北约国家因大规模网络攻击而引发社会动荡或政局不稳，将直接损害美国在欧洲的战略利益。因此，美国正在利用其成建制的网络空间作战部队和体系化的进攻性网络武器装备库帮助北约国家在网络空间实现“弱者变强、强者更强”。一方面，俄乌冲突爆发后，美国网络司令部在立陶宛、克罗地亚等北约国家持续执行“前出狩猎”行动，旨在通过识别恶意网络活动来提升关键信息基础设施的网络防御能力。另一方面，美国继续向北约内部的亲密盟友提供进攻性网络武器。俄乌冲突爆发前，美国便已将网络攻击武器交付给英国、加拿大等国使用。俄乌冲突爆发后，美国等西方国家不断渲染俄罗斯在网络空间的威胁，因此，美国可能会继续向北约内部的亲密盟友提供进攻性网络武器。美国及其领导的北约正在加快推动网络空间作战力量

① Tanmay Kadam，“Blasting Satellites，Crippling Attacks – Russia’s Invasion Of Ukraine Has Given A Clear Glimpse Of Future Wars – Top French Officer”. https：//eurasiantimes. com/russias – invasion – of – ukraine – has – given – a – clear – glimpse – of – future – wars/，访问时间：2022 年 12 月 10 日。

② Catherine Stupp，“NATO Cyber Exercise Proceeds Against Backdrop of Ukraine War”. https：//www. wsj. com/articles/nato – cyber – exercise – proceeds – against – backdrop – of – ukraine – war – 11650480793，访问时间：2022 年 12 月 13 日。

③ “First meeting of NATO national cyber coordinators”. https：//www. nato. int/cps/en/natohq/news _ 195493. htm，访问时间：2022 年 12 月 13 日。

④ Antoaneta Roussi and Laurens Cerulus，“NATO aims to take on Russia with its own cyber military – industrial complex”. https：//www. politico. eu/article/nato – plans – to – build – a – cyber – military – industrial – complex – russia – china – hacking/，访问时间：2022 年 12 月 13 日。

建设，提升网络空间作战能力。此举将加剧全球网络空间军事化进程，对地区甚至全球安全格局产生极大的负面影响。

一些国家虽然远离欧洲大陆，但仍然对俄乌网络空间对抗引发的外溢效应持高度警惕态度，并纷纷采取应对措施。一方面是要求国内企业采取必要措施来保障关键信息基础设施不受攻击破坏。俄乌冲突爆发后，澳大利亚网络安全中心（ACSC）、美国网络安全和基础设施安全局（CISA）、新加坡网络安全局（CSA）等机构纷纷要求国内企业提升网络空间安全防护级别，以保护关键信息基础设施免受干扰和破坏。澳大利亚网络安全中心表示，俄乌冲突爆发后，澳大利亚面临的网络攻击风险正在快速增加。各大运营商要为破坏性恶意软件、勒索软件、鱼叉式网络钓鱼等潜在的网络威胁作好准备①。另一方面是强化与国家或国际组织的网络安全合作。最具代表性的是韩国和日本于2022年5月和11月分别加入北约合作网络防御卓越中心。在俄乌冲突如火如荼之际，韩国和日本两个东北亚国家高调宣布加入北约合作网络防御卓越中心，一度引发外界的高度关注。在韩国加入北约合作网络防御卓越中心后不久，该中心随即表示，俄乌冲突凸显出防范网络空间威胁的重要性，加强包括韩国在内的各成员国间的技术合作和情报共享对应对日趋严峻的网络空间安全形势至关重要②。

三　乌克兰危机中网络空间冲突的启示

俄乌危机中的网络空间对抗给全球各国上了一堂现实版的网络较量课。在世界百年未有之大变局快速推进的背景下，网络空间安全威胁已成为中国面临的主要挑战之一。基于此，我们应从俄乌网络空间对抗中总结经验、汲取教训，并及时采取网络安全措施防患于未然。

（一）利用大数据技术从海量数据中筛选出敏感数据，建立己方数据优势

俄乌冲突中不断发生的数据泄露事件凸显出数据安全保护的重要性。网络安

① “Russian State－Sponsored and Criminal Cyber Threats to Critical Infrastructure”. https：//www.cyber.gov.au/acsc/view－all－content/advisories/russian－state－sponsored－and－criminal－cyber－threats－critical－infrastructure，访问时间：2022年12月13日。

② “The CCDCOE held a flag－raising ceremony for new Members”. https：//ccdcoe.org/news/2022/the－ccdcoe－held－a－flag－raising－ceremony－for－new－members/，访问时间：2022年12月14日。

全的核心是数据安全，数据安全关系到国家安全、国民经济发展和社会和谐稳定，其战略价值正在不断提升。与此同时，以数据窃取、数据泄露、数据非法使用为代表的数据安全问题正在日益凸显。个人身份信息、面部识别数据、关键地理位置等数据皆属于敏感数据。其他国家获取这些数据后即能利用深度学习算法对其进行分析处理，从中寻找关于社会经济发展和军事战略方针的薄弱环节，并制定有针对性的作战计划。因此，有关部门应利用大数据技术从海量数据中挖掘出与国防军工、核心技术、重要地理位置等领域有关的敏感数据，并全力保证其在中国境内存储和管理，防止被秘密携带出境。

（二）推进人工智能人才的引进和培养

当前，人工智能人才整体匮乏。以深度伪造技术为例，俄乌冲突期间，各种深度伪造视频持续在各个社交平台上肆虐，而负责检测的分析师人数却极度匮乏。根据达特茅斯大学计算机科学教授哈尼·法里德（Hany Farid）的说法，随着深度伪造视频很快发展到高度逼真的程度，防守者在这种形势下将无计可施。开发虚假内容的人数可能比负责检测和鉴别深度伪造视频的人数要多 100～1 000 倍①。因此，引进和培养人工智能人才已是迫在眉睫。一方面要大力引进与神经网络、机器学习、自然语言处理等领域有关的国际高端人才、青年领军人才和顶尖创新团队，加强对原创性、前瞻性、引领性科研成果的重大攻关力度，全面提升人工智能技术创新水平②。另一方面要建立涵盖初等教育、中等教育和高等教育的多层次人工智能人才培养体系。在中小学阶段，引入人工智能普及教育，设置相应的人工智能课程，重点培养学生的计算思维、设计思维、创新思维。在高校阶段，应打造完整的人工智能核心知识课程体系，保证学生掌握系统的人工智能基础理论，同时也应实现学科交叉融合，为学生生成个性化、高效化的学习方案。

（三）加强认知战力量建设

在俄乌冲突中，从利用智能机器人散布各种虚假信息，到由“数字战斗模拟世界”游戏剪辑出来的所谓“基辅幽灵”，再到通过深度伪造技术篡改的俄乌领导人讲话的虚假视频，说明认知战已经在网络空间打响，并成为影响俄乌冲突走向的重要因素。为避免在认知战中处于不利地位，可开展以下两方面工作。

① Richard Fontaine and Kara Frederick，“The Autocrat's New Tool Kit”. https：//www. wsj. com/amp/articles/the－autocrats－new－tool－kit－11552662637，访问时间：2022 年 12 月 14 日。

② 武琼：《韩国人工智能战略的实施路径及发展前景研究》，载《情报杂志》2021 年第 4 期。

第一，利用大数据、人工智能等尖端技术赋能认知战能力建设，全面增强软杀伤力。美国哈佛大学肯尼迪政府学院前院长约瑟夫·奈认为，在信息时代，成功不仅取决于谁的军队战斗力强，更取决于谁的故事更有说服力①。在数字时代，若要最大化地释放认知空间的战斗力，最优途径莫过于借助大数据、人工智能等前沿技术为指挥官和前线作战人员提供强大的技术支撑。有研究指出，将大数据、人工智能等先进技术运用于认知战中，有助于优化认知战的作战理念，充分发挥最大作战威力②。基于此，可利用智能算法从海量原始数据中快速提取高价值情报，减轻作战人员的认知负荷；利用大数据技术绘制目标对象在心理特征和思维习惯等方面的认知场景图；利用虚拟现实技术构建逼真的数字化战场环境，加大作战人员的心理韧性训练，提升战场心理素质等。

第二，打造一批具有国际影响力的社交平台，增强中国在国际舆论场上的影响力。近年来，新华社、人民日报、中央广播电视总台等主流媒体海外影响力日渐提升。相较之，社交平台则是中国在海外开展外宣的薄弱环节。社交平台是营造外部舆论环境和提升中国国家形象的重要平台。以 Tik Tok 为例，作为一家全面打开美国市场的中国科技公司，Tik Tok 成功的关键是“它能利用强大的智能算法来为用户主动推送轻松活泼的短视频，并建立起一个如蝴蝶效应般的用户自制视频传播网络，这是其他大型互联网企业较少达到过的”③。未来一段时期，中国网络企业可以在效仿 Tik Tok 模式的基础上，将传递中国声音、讲好中国故事作为对外传播的重中之重，以帮助中国提升在国际舆论场上的正面形象。

（四）提升网络空间防御能力和威慑能力，保护关键信息基础设施的安全

在俄乌冲突中，黑客组织围绕金融、电信等领域的关键信息基础设施展开一系列的网络攻击，以此削弱对方的抵抗能力。关键信息基础设施是维护国家网络空间安全，保证国民经济稳定运行和社会高质量发展的重要载体。一旦遭到大规模攻击或严重破坏，会在金融、交通、电力、能源等领域引发连锁反应，进而对

① Michael Cox and Doug Stokes, *US Foreign Policy*, Oxford: Oxford University Press, 2012, p. 98.

② Koichiro Takag, “New Tech, New Concepts: China's Plans for AI and Cognitive Warfare”. https://warontherocks.com/2022/04/new-tech-new-concepts-chinas-plans-for-ai-and-cognitive-warfare/, 访问时间：2022 年 12 月 14 日。

③ Georgia Well and Yang Jie et al., “TikTok's Videos Are Goofy. Its Strategy to Dominate Social Media Is Serious”. https://www.wsj.com/articles/tiktoks-videos-are-goofy-its-strategy-to-dominate-social-media-is-serious-11561780861, 访问时间：2022 年 12 月 14 日。

国家安全、国计民生和公共利益造成严重影响。鉴于此，中国可从以下两方面推进。

第一，借助人工智能提升网络空间防御能力。网络空间国防力量建设是中国国防和军队现代化建设的重要内容，遵循一贯的积极防御军事战略方针。因此，中国应以人工智能技术为后盾，加快构建全天候、全方位、全覆盖的网络空间防御体系，增强网络安全实时监测、联动处置、追踪溯源能力建设，防范遏制系统漏洞、黑客攻击、网络入侵、信息破坏等网络安全风险事件。如利用深度学习构建“网络攻击链”模型，及时发现攻击者可能实施的网络入侵行为，并快速形成网络反击预案；同时，运用海量数据对深度神经网络进行模型训练，利用训练好的模型提高对新型恶意木马程序和高级持续性威胁（APT）攻击的检测准确率和反应速度，并不断根据实时数据加快模型实现升级换代，从而加强网络空间防御能力，保护关键信息基础设施免遭恶意入侵破坏。

第二，研发“杀手锏”武器，增强网络空间威慑能力。单纯的消极防御无疑是给网络入侵者提供可乘之机。在网络空间必须坚持积极防御，通过慑防一体夺取制网权，把网络威慑列入积极防御范畴[①]。因此，中国应强化人工智能对网络安全的赋能作用，通过发挥人工智能在态势感知、威胁检测和持续监控等方面的作用，以研发出更具战略威慑力的非对称性“杀手锏”武器。作为维护国家安全的新型作战力量，战略支援部队应加快开发集战略性、针对性、威慑性于一体的“杀手锏”网络武器装备，并将其作为提升网络空间威慑能力的倍增器。

（责任编辑　聂侯诚）

① 张仕波：《战争新高地》，国防大学出版社 2016 年版，第 67 ~ 85 页。