海峡都市報 报料：智慧海都 95060
2022年10月27日 星期四 责编/刘虎 美编/杰清 校对/卓敏

编前 经过数十年的发展，网络空间已经成为人类社会生产生活的重要领域，成为继“陆、海、空、天”后的第五维战场。近年，美国等发达国家争相出台网络空间战略，组（扩）建网络战部队，实施网络攻防行动，在网络战建设、发展、运用等方面的举动值得世人关注。

韩国军队10月24日开始首次参加美国主导的“网络旗帜”多国联合网络攻防演习，演习将持续至28日。除美国和韩国，还有英国、加拿大、澳大利亚、新西兰等总计25个国家参加。

目前，网络态势监控、网络攻防、密码破译等领域的武器系统，已在网络空间优势国家出现智能化雏形。随着人工智能技术的发展，网络武器智能化的趋势将越来越明显。

N 新华社 环球时报 解放军报 参考消息 中国国防报

网络战 离我们并不遥远

美军网络司令部（资料图）

美网络战部队大幅扩充

美军网络司令部2011年起每年举办“网络旗帜”多国网络战联演。“网络旗帜”联演由战术层面的网络安全攻防演习和研讨会两部分组成，参演方将共享有关信息并找出最有效的应对方法，验证效果，以熟练掌握识别、分析、共享、消除、阻止网络威胁等作战程序。韩国国防部24日说，韩国军队当天开始首次参加美国主导的“网络旗帜”多国联合网络攻防演习，演习将持续至28日。韩国国家情报院今年4月第二次参加北大西洋公约组织合作网络防御卓越中心（CCDCOE）主办的全球最大规模国际网络安全攻防演习“锁盾”。5月，这一韩国情报机构正式加入设在爱沙尼亚首都塔林的CCDCOE，成为该组织第一个亚洲成员。

据俄媒援引美国《陆军时报》报道，本世纪20年代末，美国陆军网络战部队人员数量将是现在的两倍。美国陆军发言人表示，网络和电子战部队人数将从3000人增加到略高于6000人。报道称，包括现役军人、预备役军人以及国民警卫队在役人员在内，美国陆军网络战部队专家总人数将从5000人增加到7000人。

《陆军时报》指出，美国陆军要求在2023财年拨款166亿美元，用于支持网络和IT部门。这笔资金的绝大部分（约98亿）将用于军队网络现代化，大约20亿资金将被用于进攻性和防御性网络建设，以及网络安全领域研发工作。

美军最早将网络空间武器运用于实战。在美国未来联合作战愿景中，网络空间不仅是独立的作战域，还是统筹和赋能联合全域作战的基础。美军在太空战“施里弗”演习中，太空作战与网络战的融合就是重要内容之一。

多国强化网络战力量建设

近年来，组建、整合、扩充专业化网络战力量已在外军中形成风潮。

日本于2018年提出“多次元统合防卫力量”概念，即在重视陆、海、空联合作战基础上，加强太空、网络和电子战等领域作战能力。经过不断演变，日本逐渐形成所谓“跨域联合作战构想”，要求网络战在跨域联合作战中发挥作用。今年3月，日本防卫省整合现有网络战力量，建立新的“网络防卫队”，编制增至540人，未来进一步增至千人规模。不少媒体猜测，千人规模的网络战编制形成后，日本可能效仿美国组建自卫队网络战司令部。同月，日本联合多国举行线上网络战演习。这是日本首次主办多国网络战演习，折射出其提升网络战能力的迫切心态。

俄罗斯2013年成立专业信息战部队，网络战是其重要职能。近期，数位欧洲军事网络防御部队负责人一致认为，俄罗斯在对乌克兰发动进攻的过程中，在运用数字作战能力方面远不及预期。法国网络防御力量负责人评论称，计算机攻击与俄罗斯地面军事攻势脱节。

英国2020年也宣布即将创建国家网络部队。在此基础上，外军对网络战力量普遍进行了体系化设计和布局。在网络战领域内，网络攻击、网络防御、网络运维等力量密不可分；在外部，网络战力量与信号侦察、电子战等信息作战力量一体建设、融合发展。如美军网络司令部司令兼任国家安全局局长，网络攻防与信号情报侦察相互融合。日本自卫队专门设立一级司令部，统管太空、网络、电子战事务。

值得注意的是，外军的军方力量构成了网络战力量的“正规军”，民间网络安全公司、科技公司、黑客组织等也成为重要的网络攻防力量，备受重视。臭名昭著的“索伦之眼”“方程式组织”等黑客组织都与美军有千丝万缕的联系，近年来伊朗、俄罗斯、委内瑞拉遭遇网络攻击，都有“方程式组织”的影子。印军也在考虑吸纳其丰富的IT业人才组建网络战后备部队，以进一步壮大其网络战力量。

网络战『暗器』

“宝库7号”

网络武器是用于网络攻防的特殊武器，可以是病毒、漏洞，也可以是拒绝服务攻击、钓鱼攻击等攻防技术，或者是网络攻防系统平台。据斯诺登和“维基解密”的披露，美国情报机构及美军已建设形成了体系化的攻击性网络武器库，有的武器威力堪称网络空间的“大规模杀伤性武器”。

今年7月中旬，美国纽约市一个联邦陪审团裁定，中央情报局前软件工程师乔舒亚·舒尔特向维基揭秘网站泄露该机构“最有价值”的黑客工具，犯有盗取及输送国防信息罪。舒尔特可能面临数十年牢狱生活。据检方指控，舒尔特原先为中情局精英黑客小组工作，偷取中情局的黑客工具库“宝库7号”文件，并在辞职后将其发送给维基揭秘网站，2017年3月被中情局发现。“宝库7号”据信结合多种计算机病毒、恶意软件、木马程序等，用于侵入并破坏目标电脑和技术系统，是中情局从事网络战的重要武器。这一泄密事件揭露了中情局如何侵入海外用户的苹果和安卓智能手机系统，或在网络电视机植入窃听程序，以刺探外国情报。

“酸狐狸”

网络系统平台方面，美军构建了全球最完整的网络战系统平台，包括联合网络指挥与控制、统一平台等指控管理系统，IKE项目等网络战规划与执行基础系统，“舒特”等网络战与火力战一体的武器系统。

今年6月底，国家计算机病毒应急处理中心和360公司披露美国国家安全局（NSA）下属的又一款网络攻击武器——“酸狐狸”漏洞攻击武器平台。相关专家表示，“酸狐狸”平台是NSA下属计算机网络入侵行动队（CNE）的主战装备，攻击范围覆盖全球，重点攻击目标指向中国和俄罗斯，美国的做法不能不让人怀疑其正在积极为发动更大规模的网络战做准备。据介绍，“酸狐狸”平台是NSA下属的特定入侵行动办公室（TAO）对他国开展网络间谍行动的重要阵地，现已成为CNE的主力装备。该武器平台主要用于突破位于受害目标办公内网的主机系统，并植入各类木马、后门等程序以实现持久化控制。“酸狐狸”平台采用分布式架构，由多台服务器组成，按任务类型分类，包括垃圾钓鱼邮件、中间人攻击、后渗透维持等。报告披露，“酸狐狸”平台明确将在中国和俄罗斯的计算机杀毒软件作为“技术对抗”目标。而且美国在国际互联网上专门部署了针对中国和俄罗斯的网络间谍活动服务器，用于植入恶意程序并窃取情报。

印刷：晋江市梅岭南路507号福建日报社（泉州）印务有限公司 电话：0595-82033695