2021年上半年全球网络空间发展态势综述

Original Cismag 信息安全与通信保密杂志社 3 days ago

收录于话题
#网络空间 1 #勒索软件 1 #网络安全 1

2021年上半年，在日益不稳定的全球网络安全格局中，大规模针对性网络行动大幅增加，数据泄露、勒索软件、安全漏洞不断升级发展，网络安全已成为国家安全的重要因素。为此，各国持续加强网络顶层设计、加速网络空间军事竞争、加快网络安全技术赋能，网络强国建设已经从“粗放式”发展延伸至“精细化”耕耘的新阶段。

Vol.1
安全态势篇

新冠疫情所致远程办公和云端迁移潮，为网络罪犯开辟了新的途径。2021年上半年，在远程工作状态影响下，世界各地的网络攻击急剧上升，网络钓鱼、勒索软件、人为错误操作等导致的数据泄露不断增加，全球范围内的网络威胁依旧不断。

（一）全球网络空间局部矛盾冲突接连不断

2021年上半年，全球网络空间局部冲突依旧不断，国家级网络攻击频次不断增加，攻击复杂性持续上升，同时国家级网络攻击正与私营企业技术融合发展，网络攻击私有化趋势明显。网络攻击与社会危机交叉结合，全球网络对抗在底线试探中向新阶段发展。

基于SolarWinds供应链攻击事件，美国表示将对俄罗斯网络实施报复性攻击，美俄网络大战或已正式拉开序幕。上半年，对美国造成重大影响的网络攻击活动被曝均来自于俄罗斯，如俄罗斯APT组织攻击Colonial Pipeline公司致使美国输油动脉中断、全球最大肉食品加工商JBS 停工等。

中东地区地缘政治仍是APT活动的主要推力。1月，伊朗黑客连环攻击80多家以色列公司，获取国防承包商内部数据；4月，以色列再次针对伊朗伊朗纳坦兹核设施进行网络攻击，导致核设施断电、离心机受损严重；5月发生的巴以冲突中，以色列通过网络设施定位，多次配合使用导弹集中轰炸了哈马斯的军事情报网络设施基地。

（二）超大规模数据泄露趋于常态化

2021年上半年，全球数据泄露整体形势依旧严峻，泄露事件频次、数量屡创新高，每个事件的平均泄露数量增加了131%。从泄露行业看，重点针对社交媒体、医疗保健、金融保险、公共管理等；从泄露类型看，个人身份信息泄露高居首位。Imperva网站预测，2021年将发生约1500起数据泄露事件，超400亿条数据泄露。

3月，印度最大数字支付运营商之一的MobiKwik遭遇黑客攻击，泄露了约1亿用户的个人信息，包括电话号码、邮箱、签名、交易日志、密码以及个人身份证明等；3月，以色列大选投票应用Elector受网络攻击影响，超过650万以色列选民信息遭大规模公开泄露，包括选民姓名、电话号码、住址等，超2/3的以色列公民受这次泄露影响；4月，来自106个国家的超5亿Facebook用户隐私数据被公布于黑客论坛上，内容涉及电话号码、姓名、家庭住址、个人简历及电子邮件等；5月，黑客攻击了日本富士通公司开发的信息共享平台PrijectWEB，窃取了多个政府部门的数据。

（三）勒索软件攻击水平全面升级

2021年上半年，受比特币等虚拟货币飙涨刺激，DDoS勒索攻击抬头，以能源供应商、医疗卫生、交通食品为代表的关键公共需求运营商已经成为勒索软件团伙的主要攻击目标。攻击者已从大规模、通用、自动化攻击转变为更具针对性的攻击，勒索软件的运营模式升级为“三重勒索”。美国已将勒索攻击提升至与恐怖袭击同等级别。

3月，计算机巨头弘基受勒索软件REvil攻击，勒索赎金高达5000万美元，创勒索软件赎金新纪录；5月，挪威IT技术公司Volue遭遇勒索软件攻击，导致挪威国内200座城市的供水与水处理设施的应用程序关闭，影响范围覆盖全国约85%的居民；5月，美国最大燃油运输管道商科洛尼尔（Colonial Pipeline）公司遭网络攻击而暂停输送业务，美国18个州进入紧急状态；6月，全球最大肉类加工企业JBS遭受网络攻击，多个生产设施被迫停产，致使美国市场近四分之一供应量造成影响。

（四）重大安全漏洞缺陷不断涌现

随着网络犯罪团伙日益职业化，安全漏洞数量、验证程度增加明显。2021年上半年，漏洞数量持续增长，漏洞影响面逐步扩大，超高危漏洞比率大幅增加，威胁形势依旧严峻。

3月，微软Exchange Server电子邮件服务器被爆4个重大零日漏洞，攻击者通过漏洞无需身份验证或可访问个人电子邮件账户。全球数十万台Exchange服务器被攻击，大量企业、政府部门被感染，超6万家组织受影响。

5月，高通公司MSM芯片中发现了一个高危安全漏洞，全球约40%的手机都使用了该芯片。攻击者可以利用该漏洞获取手机用户的身份信息、短信、通话记录、监听对话甚至远程解锁SIM卡，且无法被常规系统安全功能检测。

5月，纽约大学安全研究员发现FragAttacks（碎片聚合攻击）Wi-Fi超级安全漏洞，该漏洞可追溯到1997年以来的所有Wi-Fi设备，包括计算机、智能手机、智能汽车等。通过该漏洞，黑客可窃取敏感用户数据并执行恶意代码，进而接管整个设备。

Vol.2
战略法规篇

2021年上半年，美英日等国持续发布网络空间战略政策、法案条令，着力加强网络建设顶层规划，谋求在全球网络空间激烈竞争格局中占据优势。

（一）拜登政府登台，强化网络安全

随着拜登政府的登台，穿插在SolarWinds供应链攻击事件处理行动前后，是美国网络安全策略的更迭。拜登政府延续特朗普政府的网络战略与政策，把网络安全提升为政府的头等大事，着重强化基础设施网络安全、供应链安全。

3月，美国政府发布《国家安全战略临时指南》，这是拜登上台后颁布的第一个联邦层级战略文件。该指南提出将网络安全列为国家安全首位，增强美国在网络空间中的能力、准备和弹性，通过鼓励公私合作、加大资金投资、加强国际合作、制定网络空间全球规范、追求网络攻击责任、增加网络攻击成本等方式保护美国网络安全，同时特别强调国家网络人才库多样化的重要性。

5月，总统拜登签署《关于加强国家网络安全的行政命令》，旨在通过保护联邦网络、改善美国政府与私营部门间在网络问题上的信息共享及增强美国对事件发生的响应能力，从而提高国家网络安全防御能力。美国政府将通过使用零信任架构、加快安全云服务的发展、数据采用多因素认证和加密、发布加强软件供应链指南、成立网络安全审查委员会等措施，实现网络安全现代化的目标。

（二）英国颁布新政，重塑网络安全愿景

2021年上半年，英国面对新冠疫情、地缘政治与脱欧挑战，连续发布两份国家安全战略报告，强调提速国家网络部队的建设，大力增强网络攻击能力。

3月，英国政府发布《竞争时代的全球英国：安全、国防、发展与外交政策综合评估》，报告将网络列为核心安全问题。根据文件，即将发布的网络战略优先事项包括：一是加强英国的网络生态系统，加深政府、学术界和业界之间的合作伙伴关系；二是建立弹性和繁荣的“数字英国”，实现经济的数字化转型，增强网络安全；三是引领网络空间关键技术，包括微处理器、安全系统设计、量子技术和新形式数据传输等；四是与其他政府、业界合作，促进自由、开放、和平与安全的网络空间；五是发现、破坏和威慑对手，将构建无缝系统以大规模和快速检测网络威胁，利用所有杠杆向对手施加代价，阻止损害英国利益的能力。同时，该战略首次提出将网络空间纳入核威慑理论，英国有权动用核武器反击网络攻击。

同月，英国防部发布《竞争时代的国防》，阐述了不断变化的战略环境及战场形势，承诺未来四年增加14%国防投资，对网络武器进行全球化升级，研究开发先进技术。该文件是冷战结束以来英国最全面的军事现代化战略文件。

（三）日本推陈出新，建设自由安全网络空间

面对日益严峻的网络威胁、数字化挑战以及即将到来的东京奥运会，日本内阁网络安全中心（NISC）于5月发布《下一代网络安全战略纲要》、《网络安全研发战略》，进一步推进数字社会建设，构建网络防御体系，以期建立自由公共安全的网络空间。

《下一代网络安全战略纲要》以提高经济社会活力、建立安全数字社会与国际安全参与为目标，设立“数字厅”作为数字化改革的指挥部门，借助企业力量推动多层次网络防御体系构建，提高网络攻击的防御、威慑和态势感知能力，全面加强国际网络合作。

《网络安全研发战略》提出基于网络事件进一步理解和分析网络攻击技术，通过产学官生态系统的构建，重点发展物联网、人工智能、量子技术及密码技术。

Vol.3
力量建设篇

2021年上半年，美英等国持续优化管理机构机制，以期建立高效的管理体系。同时，不断完善网络部队机制和力量建设，新建、扩充或重组网络空间作战力量，将网络力量扩展至太空领域，谋求全面提升网络空间作战能力。

（一）优化机构机制，强化关键领域管理水平

随着拜登政府权力过渡的逐步完成，美国正在进行相应的机构调整和机制改革，顶级网络安全人才的空缺将逐渐填补。1月，美国务院成立网络空间安全和新兴技术局（CSET），重点推动美国开展网络空间安全和新兴技术相关工作，并在日益严峻的国家安全问题上与盟友和伙伴国开展合作；4月，拜登政府提名前美国家安全局（NSA）克里斯•英格利斯（Chris Inglis）担任首任国家网络总监，负责协调整个联邦政府机构的攻防行动。

同时，美军设立科研加速机构，提高自身“造血”能力。3月，美国防部启动一个研究中心，专注将计算和通信整合到军队大型网络系统，旨在研究用于快速态势感知的网络化可配置指挥、控制和通信，其首要任务就是研究下一代计算和通信的大规模网络化系统；4月，美国防部最高信息技术办公室正在考虑成立一个综合管理办公室，负责加速采用零信任网络安全架构，为国防部的零信任网络实现制定战略路线图，并在国防部、任务伙伴、国防工业基地和盟友内部分享最佳实践。

2月，英国政府宣布成立网络空间安全委员会（UK Cyber Security Council），负责民事网络安全任务的培训和专业影响。该委员会致力于推动英国网络空间安全专业建设，特别关注网络安全人才培养、职业发展引导、职业道德制定、思想领导力和影响力塑造。

（二）优化部队建设，提升网络攻防力量体系

2021年上半年，为适应网络空间安全新需求，美英等国建立太空网络空间作战力量，不断调整部队架构和体系，强化战术层次梯队力量建设，谋求联合全域作战优势，推动网络部队建设全面和深度发展。

美网络司令部近期正在调整期工作重点和资源分配，明确将工作重心从反恐转向具有“持续对抗”性质的大国竞争，并将关注对象从恐怖组织转向中俄等对手国家。同时，美网络司令部将进一步扩充、融合网络作战部队人员数量，进一步提升新形势下的网络作战能力。

面对未来太空竞争，美国太空部队和太空司令部正加速发展网络战力量，致力于夺取太空主导权。当前，美国太空部队正在招募第一批网络战士，将网络人员从空军转移到其队伍中，以保护信息系统和任务；2月，总部位于施里弗空军基地的“太空三角洲6”部队正式将40名士兵转移至太空部队，负责执行空军卫星控制网络、网络作战，以保护太空作战、网络和通信。同时，美军正在建立太空司令部联合网络中心，旨在与网络司令部加强联系，促进网络行动整合。

英国紧随其后，于4月正式成立太空司令部，指挥控制国防部所有太空能力，包括英国太空作战中心、“天网”卫星通信系统、英国皇家空军菲林代尔斯基地和其他赋能能力。同时，最新军事战略透露，英国政府将斥资发展和部署创新作战能力，包括卫星、电子战、网络战、无人机等。

Vol.4
技术装备篇

2021年上半年，世界主要国家持续加大新兴技术投资力度，强化5G、量子信息、人工智能等颠覆性技术的研发和应用，尤其重视零信任在保障信息安全中发挥的重要作用，并充分借助业界技术和能力，加强网络装备的研发，以大幅提升网络作战能力、夺取未来网络对抗的主动权。

（一）驱动赋能技术发展，打造网络安全引擎

1、全面拥抱采纳推行零信任

当前，零信任架构已经成为美国政府首选的网络安全战略，尤其是拜登政府5月的行政命令，强调政府部门向云技术的迁移应在可行的情况下采用零信任架构。2021年上半年，美国陆续发布零信任部署文件，加速零信任实施，促进网络安全转型。

2月，美国家安全局发布《拥抱零信任安全模型》，展示了遵循零信任安全原则，确保关键联邦机构内的关键网络和敏感数据的安全。5月，美国防信息系统局发布《初始国防部零信

任参考架构》，为国防部大规模采用零信任设定了战略目的、原则、标准及其他技术细节，旨在增强国防部网络安全并在数字战场上保持信息优势。

2、持续拓展开发5G技术应用

2021年上半年，世界各国在加速5G技术的大规模军事应用测试、部署的同时，积极探索基于太空的5G全球网络，以确保5G技术的鲁棒性、安全性及弹性，减少作战中的系统漏洞。

1月，北约合作网络防御卓越中心（CCDCOE）推出与部队机动性相关的5G网络安全研究项目，将从技术、法律、战略和实战等多个维度进一步深化对5G发展影响的理解。该项目将绘制欧洲商用5G网络的规划布局图，并为北约在平日军力部署和战时军事行动提供最安全有效的优化建议。

2月，美太空军太空及导弹系统中心发布了"5G太空数据传输（SDT）"项目征求书，寻求使5G网络、射频与微波接入、移动支持以及相关大数据功适用于太空系统，实现军队与指挥机构间快速且安全的数据传输。

4月，美空军与Phosphorus Cybersecurity公司签订小企业创新研究（SBIR）合同，为美国空军开发适用于5G装备的网络安全解决方案，将公司的企业平台调整得适合于美国国防部的5G环境，并通过其技术解决方案来自动保障物联网设备的网络安全。

3、推动量子技术的国防研究

2021年上半年，世界各国持续加码量子技术研究，进一步加大量子技术的国防开支。通过提供资金支持、建立研究工作组、加速技术标准制定、支持量子技术商业化应用等方式，促使量子技术发展进入良性循环，最终实现经济发展、国家安全。

4月，DARPA推出"量子基准（QB）"项目，旨在重塑关键的量子计算指标，使这些指标可以测试，并估计达到关键性能阈值所需的量子和经典资源。

4月，美陆军科学基金资助的量子计算研究取得突破性进展，其中路易斯安那州立大学通过机器学习技术纠正了由光子构成的量子系统中的失真信息，成果可用于量子通信、量子密码学和量子传感等；芝加哥大学建立了量子通信新方法，通过通信电缆发送纠缠的量子比特将两个网络节点连接起来，成果为大规模量子网络的应用铺平了道路。

5月，法国泰雷兹集团（Thales）和澳大利亚塞内塔斯公司（Senetas）合作推出全球首个抗量子网络加密解决方案，以保护客户数据，使之免受未来的量子攻击。

4、探索人工智能集成应用

当前，世界各国加速人工智能的军事应用，使智能化要素渗透于作战的全过程，以期在激烈的军事竞争中占据优势。当前，美国防部联合人工智能中心（JAIC）正考虑将其人工智能技术开发平台——联合通用基础（JCF）与国防部及各军种主导的其他平台相连接，以建立统一系统，推动未来军事人工智能发展。

1月，美人工智能公司SparkCognition和无人机空域管理公司SkyGrid宣布合作，将在无人机上部署基于人工智能的网络安全产品，保护无人机在飞行过程中免受零日漏洞攻击。SparkCognition公司的"深层铠甲"网络安全产品利用机器学习技术为终端提供多层保护，可以抵御99%的未知威胁。

4月，JAIC发布"人工智能开发数据准备（DRAID）"项目，寻求人工智能数据准备的数据采集、标记、模型训练的整个生命周期服务，旨在全面使用国防部数据资源，推动国防部所有人工智能活动。

5月，DARPA推出"用于适当可拓展性的增强设计（EDGE）"项目，旨在创建一套人机界面设计工具，并将其纳入系统设计流程。这些工具将优先用于量化、支持和测试态势感知。

6月，美国防部启动"人工智能与数据加速（ADA）"计划，力图快速推进联合全域指挥控制（JADC2）等相关概念深入发展。为此，美军组建了作战数据团队、技术团队，通过集成人工智能技术帮助各司令部快速整理、分类、管理数据，实现基础网络更新，确保美军在跨域多国作战环境中，提升全面作战能力。

（二）强化网络装备研发，催化作战有效落地

随着网络作战在军事领域的重要性日益凸显，世界主要国家均将网络武器研发视为战略竞争的新高地。2021年上半年，美欧等国不断加强态势感知、训练测试、安全防御等网络武器研发，提高基于网络信息体系的作战能力。

1、打造增强战场态势感知管理系统

当前，美军正在从技术层面进行体系研发，构建在大规模动态网络环境中实时网络空间战场态势感知系统。

4月，作为美国网络作战关键系统的IKE项目正式移交美国网络司令部。项目可为美网络任务部队提供网络指挥控制和态势感知能力，并利用人工智能和机器学习技术帮助指挥官理解网络战场、支持制定网络战略、建模并评估网络作战毁伤情况。项目可视为美国网络司令部联合网络指挥控制项目的试点项目，并将成为未来网络指挥控制的核心及基础。

2、搭建虚拟网络靶场环境

当前，美欧等国积极建设网络靶场平台，旨在构建精确复制真实场景的虚拟网络环境，为军方网络作战培训和网络安全测试提供支持。

2月，卡塔尔计算研究所（QCRI）选定意大利莱昂纳多公司提供网络靶场和培训系统构建，以支持安全运营。该靶场可模拟网络攻击，以便用户评估数字基础设施的恢复能力。

4月，美陆军宣布正在为城市构建一种定制的便携式网络攻击演习平台，以保护电信或供水服务系统等关键基础设施，使其免受网络攻击。该平台具备场景构建能力，能为军方提供数据库制定决策，其它城市也可根据自身需求对其进行调整。首个测试版平台预计于第三季度推出，预计于2023年第四季度提供全面运行。

3、强化安全防护装备研发

当前，美澳等国充分借助业界技术和能力，加强网络安全装备的研发，从全局视角提升对安全威胁的发现识别、理解分析、响应处置能力。

1月，美国防创新单元（DIU）授予CounterCraft公司交易协议，以检测和提供网络威胁的情报。该公司的平台产品可利用蜜罐进行高级网络防御，引诱、帮助红色团队识别黑客。

2月，澳大利亚国家科学机构（CSIRO）、新南威尔士州政府、澳大利亚计算机协会（ACS）等多家机构合作开发了一款隐私保障工具——个人信息因素（PIF），可评估任意数据集内的个人数据风险，建立起有针对性的高效保护机制。该工具可确保关键数据集中的敏感个人信息通过严密检查后再公开共享，比如用于跟踪新冠疫情蔓延的数据集。

3月，美陆军“网络探索2021”演习中测试了由埃森哲公司开发的一种高度机密的工具。作为攻击性网络行动的安全措施，该工具使用了截取到的或逆向工程的代码，利用模式识别来模糊美军网络战士留下的数字签名，从而避免美军攻击行动被溯源。该工具将同时供地面战术部队和美国网络任务部队使用。

4月，美网络司令部寻求承包商支持，扩展现有的文件共享安全工具WOLFDOOR的基础架构，并满足不断增长的任务需求和对数据流请求的增加。承包商将维护、复制和扩展数据共享基础架构，改善系统的安全性，减少支持人员在多个地点的冗余，同时为各个站点提供可伸缩性和增强的安全性支持。

（三）探索前沿项目研究，维护网络空间壁垒

2021年上半年，以DARPA为代表的国防科技研发机构持续加大网络空间安全尖端技术投入，围绕通信网络、信息系统、供应链安全等领域开展项目，寻求军事应用和大幅提升作战能力的技术途径。

3月，DARPA授予CACI国际公司和Perspecta Labs公司合同，要求其为"宽带安全和受保护发射机与接收机（WiSPER）"项目开发安全射频发射机和接收机技术，以实现下一代安全军用战术无线电系统。

3月，DARPA推出"自动实现应用的结构化阵列硬件（SAHARA）"项目，旨在扩大美国国内制造能力的使用范围，以应对阻碍国防系统定制芯片安全开发的挑战。该项目将与英特尔公司、佛罗里达大学、马里兰大学和德克萨斯A&M大学的学术研究人员合作，设计自动、可扩展、可量化的安全结构化专用集成电路（ASIC），同时还将探索新型芯片保护，支持零信任环境下的硅制造。

3月，法国空客公司、日本富士通公司和法国泰雷兹公司携手组建ICELUS团队，开展英国陆军"陆上环境战术通信和信息系统（LE TacCIS）"项目的应用程序、基础设施和网络产品和服务的设计与集成工作。LE TacCIS由多个子计划和项目组成，旨在提供陆上环境中的下一代战术军事通信系统，以支持敏捷通信信息系统的及时决策。

3月，欧洲防务局选择泰勒斯公司启动关于"网络编程和编排技术（Softanet）"项目，将为通信网络使用最新虚拟化技术提供更深入的见解。这是为可部署战术网络的发展以及采用可编程网络技术、软件定义网络（SDN）模型和5G做准备的重要一步。

Vol.5
作战演习篇

为提高网络空间的实战能力，国外军事强国纷纷建设网络靶场，组织多国、多部门、多情景的网络演习，以检验网络部队作战水平、发展攻防战术。2021年上半年，美欧等国除按惯

例开展年度大型网络演习外，致力于发展多域作战，特别瞄准太空战场，开展了多场网络演习。

（一）举行专项技术演习，发展联合作战概念

美军新兴联合作战概念特别强调增加太空和网络空间，以充分利用两者在交战规则、机动方式和作战效果等方面的优势。目前，美军正积极开展相关演习，以提升全军联合作战能力。

1月，美空军启动“红旗21-1”演习，美空军、陆军、太空部队及其他盟国部队的数百名人员参与本次演习，通过实战、虚拟和构造方阵，开展了空中、太空和网络空间的一体化作战和训练。本次演习的非动能演习将地面和空中资产的电子战火力与进攻性网络火力结合使用。

3月，美国陆军举行“网络探索2021”演习活动，旨在测试连级以下多域作战的新概念。与往年不同，本次演习活动与陆军“远征战士实验”活动合并开展，从而达到强化协同的效果，更好地推动多域作战。本次演习中，共有14家供应商带来了15种技术，涉及网络态势感知、电子战、战术无线电等。

（二）举行网络攻防竞赛，发现漏洞培养人才

立足攻防实践升级安全、提升军事基础能力的需求，美军积极举办网络攻防竞赛活动，组织人员在仿真场景中开展攻防演练，以达到发现安全漏洞、培养网络人才、提升实战经验的目的。

2月，美网络安全和基础设施安全局（CISA）和可持续能源公司AVANGRID进行联合虚拟桌面演习，测试、确定该公司自新冠疫情以来实施的安全程序与其他必要程序，以确保未来的安全运营和业务连续性。桌面演习测试了短期及长期恢复计划、业务连续性、内部信息共享和沟通情况，以应对持续的新冠疫情。

4月，第20届美国国家安全局网络演习（NCX）大奖赛顺利举行，来自美国军事学院、海军学院、海岸警卫队学院、诺里奇大学等多个学院团队参与了本次比赛。比赛以虚拟方式进行，以各种特色场景形式开展，包括取证、网络政策、密码学、逆向工程以及传统网络战斗演习方面的挑战，旨在测试针对网络发展计划的平民实习生、培训网络战士。

4月，美国防部宣布在HackerOne平台上推出“国防工业基地漏洞披露计划（DIB-VDP）”，邀请HackerOne社区安全人员远程测试，致力于缓解或修复国防工业基地（DIB）承包商信息

系统、网络或应用程序中的漏洞。

5月，美空军与网络安全社区合作，宣布启动第二版黑客事件“太空安全挑战：Hack-A-Sat”。此次比赛中，安全研究人员将解决应用于太空系统的各种网络安全挑战，并展示开发针对这些系统的保护机制的最佳方法。

（三）举行国际联盟演习，增强网络行动协同

美欧将联盟关系从现实世界推动到网络空间，通过加强在网络空间的合作，在新兴作战领域建立集体作战优势，力图掌握未来作战主导权。当前，美欧等国积极举行联合网络演习活动，促进盟国之间在网络空间的练兵协作。

2月，为进一步深化欧盟各成员国军方计算机应急响应小组（MilCERT）的合作，欧洲防务局（EDA）组织举行首次网络实战演习，来自17个欧盟国家和瑞士的200多名专业人员通过线上方式远程接入演习平台。该演习旨在团结各国MilCERT力量，强化网络事件管理动态过程中信息共享的地位，并将其视为现代网络防御的关键要素之一。

4月，北约举行年度“锁定盾牌”演习。此次演习号称全球规模最大的网络防御实战演习，涉及30个国家、2000多名网络安全专家和决策者。本次演习旨在考验相关国家保护重要服务和关键基础设施的能力，并强调网络防御者和战略决策者需要了解各国IT系统之间的相互依赖关系。

6月，来自美国、英国、加拿大的17个团队约430名人员参加“网络旗帜21-2”演习。此次演习使用了持久网络训练环境（PCTE），模拟了印太地区常见威胁，同时也纳入了勒索软件等常见场景，旨在重新确定网络防御团队的成功要素，以改进现实世界的网络防御。

Vol.6 结　语

回顾2021年上半年，全球网络空间政治和军事领域力量持续发展，太空网络安全建设重要性进一步凸显，网络空间规则主导权和话语权争夺更加激烈。面对美国网络威慑实施、网络预算节节攀升，我国进一步增强网络防御手段、优化装备建设、研发自主技术已迫在眉睫。

（作者：信息中心郝志超）