兵器广角

1月5日，奥地利外交部和内政部联合发表声明说，自当地时间4日23时起，奥地利外交部电脑系统遭到有针对性的网络攻击，至5日白天网络攻击仍在持续。

这让人不由得联想到去年3月委内瑞拉发生的全国大停电。委内瑞拉政府当时称停电是美国策划的“电磁和网络攻击”，但随即遭到否认。

这些事件，一再把网络攻防武器推入公众视线。

网络攻防武器是什么？有专家曾形象地把它比作网际“特工”，意思是它既可以长期“潜伏”于网络中获取对手情报、观察对手动向，也可以在事态恶化或战时闻令而动，修改对手指令，瘫痪对手通信和控制系统，甚至攻击对手实体攻防系统，在关键时刻发挥决定性作用……

本期，就请专家带我们走近神秘的网络攻防武器，一探究竟。

网络攻防武器：潜能惊人的“网际特工”

■吴敏文 程天昊

图①：2007年的“果园行动”中，借助“舒特”机载网络攻击系统，以色列空军10余架F-15和F-16战机突入叙利亚领空，对预定目标实施了精确轰炸。图为以军的F-16战机。图②：DDOS攻击成为时下网络攻击的重要方式之一。

科学研究发明催生的“破坏者”

网络攻防武器的源头是计算机病毒。从技术本质上讲，计算机病毒与其他程序没有什么不同。

两者的不同体现在功用上，正常程序维持与顺畅计算机、网络的运行，计算机病毒则是破坏计算机、网络的正常运行。显然，“破坏者”的定位与功能，为计算机病毒军事化、成为网络攻防武器提供了可能。

世界上第一台电子计算机叫ENIAC，由美国陆军阿伯丁弹道实验室和美国宾夕法尼亚大学莫尔学院于上世纪40年代联合研制成功。ENIAC“块头”很大，造价为48万美元。这在当时堪称“天价”。

当时的电子计算机发明者们，无论如何也想不到：这么昂贵的技术发明，会有人想方设法去破坏它。也正是因为如此，最初的电子计算机无论从软件上还是从硬件上都是不设防的。

1983年，正在攻读博士学位的美国人弗雷德·科恩研制出一种在运行过程中可以自我复制的破坏性程序，并将其命名为计算机病毒。科恩的发现，证实了计算机既能通过程序保证运行，也可以因此“自废武功”。

此后，计算机病毒事件不断出现。

1988年，美国康奈尔大学一年级学生罗伯特·莫里斯编写出“蠕虫”病毒程序。这个只有99行的病毒程序，以极强的自我复制和传播能力迅速蔓延，导致美军的MIL网和ARPA网中6000台计算机受到感染，与之联网的欧洲计算机也深受影响，造成直接经济损失近亿美元。

后来，“CIH病毒”出现。这是第一种能够破坏计算机硬件的恶性病毒，可使计算机硬盘数据丢失，并可致计算机主板损坏。3个多月里，“CIH病毒”在全球蔓延并造成空前破坏。

计算机病毒的种种表现，昭示了一个堪称冷酷的事实：计算机及其程序具有多大的正面功用，其病毒程序就具有多大的破坏能力。

基于其惊人的破坏作用，计算机病毒后来渐渐被用于军事目的，并最终发展为网络攻防武器。

军事应用推波助澜赋予更大“破坏力”

1989年，美国军方正式提出“计算机病毒是一种新型电子战武器”的理论。

1990年，美国军方悬赏55万美元，试图研制一种新型计算机病毒。这种计算机病毒的研制要求是，可通过无线电通信系统潜入敌方计算机系统，在传递中修改敌方命令，甚至可以摧毁敌方通信线路和控制系统。

海湾战争时期，计算机病毒被用于实战。

战前，美国特工偷偷将植入病毒的同类芯片，置换进伊拉克从法国进口的打印机里。战争中，美军遥控激活预置病毒，成功瘫痪了伊拉克的防空系统和指挥中心。

科索沃战争中，北约特别是美军计算机黑客多次对南联盟政府及其军队的指挥控制网络实施攻击。1999年4月，南联盟也多次有组织地攻击北约的计算机网络系统，使美军“尼米兹”号航母互联网系统瘫痪3个小时。南联盟黑客还向北约网站发送带有“梅利莎”“病牛”“幸福1999”等病毒的电子邮件，使北约网站遭到不同程度的破坏。

“过载”病毒是俄罗斯研制和使用过的一种“蠕虫”病毒。它能在传播中高速自我复制，对特定目标进行饱和式攻击，造成目标服务器阻塞和瘫痪。2007年4月，爱沙尼亚的互联网就曾遭到“过载”病毒攻击。

这一时期被称为网络攻防武器的计算机病毒时代。

计算机病毒投送方式包括无线注入、芯片预置、网络扩散等。

其攻击特点是：主要攻击网络系统的某个局部而非整个网络；攻击的目的主要是弱化对方网络功能、占用对方网络资源；攻击的对象是计算机终端或者网络本身，而不是与之相联的受控实体等。

这个阶段有代表性的网络攻击武器还有网络“蠕虫”、“特洛伊木马”、逻辑炸弹、计算机“陷阱”等。

网络攻防武器的发展渐成体系

随着信息网络时代的全面到来，在一些国家，网络攻防武器正式列装，成为军队武器库的组成部分。有的西方发达国家军队的武器库中，已有数千种计算机病毒和其他网络攻防武器。网络攻防武器不仅用于攻击信息网络系统，也能通过网络攻击，破坏受控的工业制造、预警探测、防空反导、指挥控制等实体系统。与此同时，包括网络侦察、网络攻击、网络防御在内的网络攻防武器装备体系逐渐形成。

网络侦察武器，是对被侦察对象的网络信息进行侦察的网络武器系统，如“高级侦察员”系统、“网络飞行器”系统和“爱因斯坦计划”。

“高级侦察员”系统被用于寻找对手信息网络体系入口。它可以探测、跟踪和定位对手的雷达站、微波塔楼、蜂窝电话、卫星地面站和其他通信链接点，然后朝对手信息网络注入错误数据流、植入己方可控制的算法程序包，根据需要摧毁对手信息网络。

“网络飞行器”可以按照研制人员制定的策略，在无线网络和有线网络中穿梭，不留痕迹地收集网络态势情报，实施相应攻击，并具有特定情况下的自毁能力。

“爱因斯坦计划”是美国政府的网电监控系统，它可以感知通过网关和互联网接入点的数据流，检测恶意代码和异常活动，及时发现威胁和入侵，保护己方的网络空间安全。

网络攻击武器，是破坏对手信息网络系统和网络信息、削弱其使用效能的网络武器。为人们熟知的有“舒特”攻击系统，除此之外还有“震网”病毒、“黑暗力量”等。

“舒特”攻击系统可以检测与识别多种辐射源，利用对手的防空系统漏洞，发送假目标信息进行欺骗和误导，甚至接管和关闭对手的防空系统。以色列的F-15和F-16战斗机群有过在实战中成功运用“舒特”攻击系统的案例。

“震网”病毒是针对工业控制系统的计算机“蠕虫”病毒。“震网”病毒通过“摆渡”方式感染与互联网物理隔离的内部网络，直至系统损坏。“震网”病毒于2010年7月曾袭击伊朗核设施，导致伊朗浓缩铀工厂内约五分之一的离心机报废。

“黑暗力量”是一种攻击工业自动化控制系统的病毒，通过对Word文档内嵌入病毒的方式来展开攻击。乌克兰电厂系统就曾两次受到这种病毒攻击，造成大面积停电事故。

网络防御武器，是用于保护己方信息网络系统和信息数据安全的网络武器。除用于计算机网络防御的常规防护设备外，网络防御手段还有“网络诱骗”系统和“网络狼”软件等。

“网络诱骗”系统主要用来检测、追踪和确认潜在的网络入侵者。美军的“网络诱骗”系统会自动建立虚假网络，诱使对手攻击并浏览虚假网络情报，同时向系统管理员通告入侵者的行踪。

“网络狼”是一种分布式网络攻击智能嗅探软件，它可实时收集、记录各种网络入侵事件，审查、提取、浓缩入侵图样并向管理员报告，能把误警、虚警发生次数大大降低。

此外，还有网络攻击告警系统，这类系统可以及时向系统管理员提供情况、发送告警信息。

（作者单位：国防科技大学、空军工程大学）

供 图：张 曦 阳 明

本版投稿信箱：jfjbbqdg@163.com

兵器控

品味有故事的兵器

■本期观察：孙 阳 王宁川 龚 豪

现代海战中，如何对军舰进行有效防护是重要课题。为此，各国纷纷着手研制舰艇防御武器并对其优化。今天我们就给大家介绍三款舰载近空防御武器系统。

“卡什坦”近防系统

俄罗斯“卡什坦”舰载近防系统是一种弹炮结合系统。它的炮塔上装有两个四联装导弹发射筒和两门6管30毫米机关炮，并且集成了一体型火控系统。

它采用模块化设计，整个系统由指挥模块、作战模块、导弹存储和再装填系统、防空导弹和炮弹组成。指挥模块用于探测和发现目标，可同时跟踪多个目标，为作战模块提供相关数据。作战模块接收到数据，火控计算机会同步处理目标信息，自动选择最佳作战模式。

作战时，“卡什坦”会发射防空导弹拦截远距离处的来袭目标，多管小口径机关炮则负责对付近距离处的来袭目标，在适当放弃精度的情况下编织出密集的火力网。凭借这种配合，“卡什坦”不仅能用来防御精确制导武器、飞机和直升机的打击，也能用来攻击海上小型目标。

“守门员”近防系统

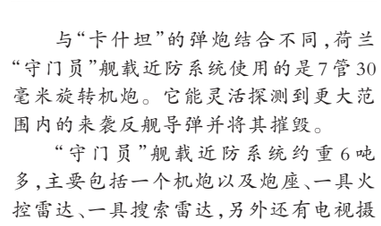
与“卡什坦”的弹炮结合不同，荷兰“守门员”舰载近防系统使用的是7管30毫米旋转机炮。它能灵活探测到更大范围内的来袭反舰导弹并将其摧毁。

“守门员”舰载近防系统约重6吨多，主要包括一个机炮以及炮座、一具火控雷达、一具搜索雷达，另外还有电视摄影机、无线电发射接收机、电子控制舱、系统界面等。通过系统界面，它可与舰上的作战、火控系统相连。

它的炮塔拥有独立的水平旋转基座，可连续360度水平旋转，炮身俯仰角范围为-25至+85度。这有助于它持续对周围环境进行广域搜索。即使在受到强杂波干扰情况下，它也能探测到高速目标。

“守门员”舰载近防系统可以追踪多个目标并按照威胁程度依次接战，还能同时做出毁伤评估，获得舰上其他战斗系统的支援。

“梅罗卡”近防系统



西班牙“梅罗卡”近防系统是世界上炮管数目最多的近防系统。该系统没有采用国际上流行的转管炮布局方式，而是将12根单管炮分成上下两排，每排6管，再由钢箍固定而成，看上去十分威武。

在架构上，它采用的是国际上通用的三位一体架构，即跟踪雷达、搜索雷达置于炮架上，与火炮成为一体。该炮每根单管口径20毫米，射程达到3000米。独特的设计使其火力强大，弥补了转管炮因一管卡壳而全炮“罢工”的不足，提高了快速反应拦截能力。

但该炮也存在不足。为了避免因后坐力太大影响射击效率，该炮射击时需要分成4组，4组依次射击完毕后才能一次性装填好12枚弹药。这显然会对该炮的实际速射火力产生不利影响。

安-225：实至名归的“空中巨无霸”

■赵艳斌 梁智勇

提到安-124“鲁斯兰”运输机，许多军迷估计不会陌生，这款运输机无论出现在哪个机场，都会招来众多惊讶和赞叹的目光。但与安-225相比，它则是名副其实的“小兄弟”。作为运输机界的“老大”，“梦幻”运输机安-225，被称为“空中巨无霸”。

安-225和安-124都是乌克兰安东诺夫设计局的杰作。安-225当时是以安-124为基础研制的新款运输机，所以两者之间保持了高度通用性，但也有差异。为了减轻重量，安-255取消了安-124货舱后斜坡的设计，这使得它的后机身构型更加流畅，有利于减小飞行阻力。它用H型双垂尾取代了安-124的单垂尾，以便增加运输机的气动效率和舵面稳定性。它的主起落架增加了两副额外的串联双轮组件。

为了运输“暴风雪”号航天飞机长59米的主火箭推进器，安-225安装有6台涡扇发动机，安-124只有4台。它的机身比安-124加长了15米，在机翼之前和之后的机身都有所增长，最终机长达到84米。这使它的载重达250吨。

“暴风雪”号航天飞机项目遇冷后，安-225的发展陷入低谷期。不过随着当今超大超重货运市场的兴起，安-225迎来了“新生”。2002年，安-225被美国雇佣，向驻阿曼美军送去总重量180多吨的快餐；2004年，它将重达247吨的货物，从捷克运输到了乌兹别克斯坦……

尽管安-225的运输能力举世无双，但它目前承接的业务一直处于“吃不饱”的状态。主要原因有三方面：一是为了增强安全性和可靠性，它需要长时间停飞进行大量维护或升级；二是安-225运营成本高，直接运营成本几乎是安-124的两倍；三是安-225庞大的体积和重量对起降场地要求高，目前全球范围内能满足安-225起降条件的机场寥寥无几，还涉及到复杂的调度问题。

由于缺乏资金，安-225一共生产了两架，第二架至今还未接通动力系统。但是其他货机不能匹敌的运输能力使它仍在全球货运市场占有一席之地。一方面，它能完成其他货机无法完成的重型运输工作，比如重量为150吨的单件货物。在空运总量相同的货物时，安-225只要飞一架次，安-124也许要飞两架次，对于有些业务来说总体上还算是经济划算的。

兵器观察