新闻热线：010—58884062
E-mail:adaxuqian@126.com
■责编 许 茜
科技日报
2019年7月31日 星期三

三个典型案例解构网络战

发生在第五维空间的战争 离你并不遥远

本报记者 **张 强**

随着信息和网络技术的飞速发展，互联网已渗透到人类生活的方方面面，并对国家安全、军事斗争以及战争形态产生了重大而深远的影响，网络空间已成为与陆、海、空、天并列的第五维空间领域。

作为互联网的起源地，美国早在上世纪90年代就提出了网络战的概念。而近年来出现的“舒特”攻击、“茉莉花革命”等事件，更是给世界带来极大的震撼和冲击。

为了让更多读者了解这种与人们生活密切相关的作战形式，科技日报记者特意选取了3个网络战经典案例，并特邀专家进行点评，从不同角度梳理网络战的现状和发展。

案例一 “震网”病毒 曾是最复杂、精妙的网络武器

2016年2月，美国纪录片《零日》在柏林电影节举行全球首映。这部影片围绕美国针对伊朗发动的网络战展开，以“震网”计算机病毒攻击伊朗核设施这一件事为蓝本。

位于伊朗南部的布什尔核电站是伊朗首座核电站，设计装机容量为1000兆瓦。按照伊朗官方的计划，该核电站应于2010年10月并网发电。然而，到了第二年2月，布什尔核电站不但没有发电，还卸载了反应堆中的核燃料。这其中一个重要原因，就是其遭到了美国和以色列的网络攻击。

据称，起因是2006年伊朗宣布恢复已中止2年多的核燃料研究工作，此举引起国际社会的强烈反响，由此伊朗遭到了美国的网络攻击。相关报道称，由于被一种靠U盘传播的蠕虫病毒感染，布什尔核电站内的监控录像被篡改。监控人员看到的是正常画面，而实际上该核电站离心机在失控情况下在不断加速，最终导致设备损毁。

2010年6月，“震网”病毒首次被发现。截至当年9月底，伊朗国内至少有3万台电脑感染了“震网”病毒。“震网”病毒由美国和以色列相关研究人员联合研发，可以通过移动存储介质和网络进行传播，专门攻击德国西门子公司开发的基础设施控制系统。布什尔核电站采用的控制系统就来自西门子公司。有专业人士称，这种病毒是当时被发现的最精妙、最复杂的网络武器，没有之一。

据西方媒体报道，“震网”病毒导致伊朗约1000台离心机瘫痪，令伊朗核发展计划拖后了至少2年。

专家点评：

从打击效果可以看出，“震网”病毒展示出网络武器的巨大威力，拖延了伊朗核发展计划，打乱了政府决策，发挥了不流血便可毁坏战略设施的惊人效能。此后，利用网络病毒实施攻击成为敌对国家间一种常见的对抗方式和战斗样式，网络病毒也成为各国竞相追逐的新型武器。

2018年，美国再次对伊朗的基础设施实施了网络病毒攻击，最近又对伊朗的情报部门和导弹发射系统实施网络攻击。虽然相关网络武器未被公开，但从后续反应推测，伊朗的网络侦攻防能力已有明显提升。未来，通过网络病毒实施网络攻击的事件还会出现，许多已建立网络军队的国家将研发更先进、复杂的网络病毒，创新网络攻击方法，网络军备竞赛将愈演愈烈。

（点评专家系军事科学院战争研究院研究员王桂芳）

案例二 “果园行动” 将网络战与常规战结合的典范

2007年9月6日，以色列对位于叙利亚东北部的城市代尔祖尔的阿尔奇巴核设施发起“果园行动”袭击，此战被业界评为，将网络战与常规战完美结合的典范。

虽然这次袭击发生在十余年前，但直到2018年，以色列才公开证实了2007年秘密轰炸叙利亚核设施的传闻。

2007年9月6日凌晨，7架以色列空军F-15I重型战斗轰炸机在G550电子战飞机和地面特种部队的空地支援下，趁着夜幕闪电袭击了代尔祖尔附近沙漠地区的核反应堆建筑群，当时该核反应堆建筑已进入最后施工阶段。

行动中，G550电子战飞机启动了网络攻击系统，先后压制了叙利亚边境的防空系统和“神秘工厂”附近的防空导弹系统，使叙利亚防空系统的信息获取、传递和处理的功能彻底瘫痪，即使其武器平台毫发无损也发挥不出作用。

据称，以军在此次空袭行动中使用的G550电子战飞机上搭载了“舒特”网络攻击系统和网络瞄准技术（NCCT）系统。其中，“舒特”网络攻击系统可以入侵敌方通信网络、雷达网络以及计算机系统，尤其是与一体化防空系统有关的网络系统。

这使得以色列的G550电子战飞机成功入侵敌方雷达网络，替代敌方雷达操作员控制雷达。于是，以方操作员就可以控制敌方雷达避开以方飞机，以方也就不必使用隐身飞机或采取更多的规避动作。这种控制即使被敌方操作员知道，其夺回控制权也非易事。

这场代号为“果园行动”的闪电空袭非常成功，以色列F-15I战斗机投下的精确制导炸弹彻底摧毁了代尔祖尔附近沙漠地区的核设施建筑群。

专家点评：

“果园行动”是以色列在叙利亚战争中，针对叙核设施动用“舒特”网络攻击系统，以网电一体的形式配合空军常规打击的一次成功战例，呈现了处于技术高端国家的绝对军事优势及作战效能。该战例最可怕之处在于，处于技术低端的国家对这场行动浑然不知。类似行动后来在美国、俄罗斯等国的实战中频繁出现，已成为一种常态化的联合作战样式，未来还会在实战中不断完善。以色列在发起“果园行动”10年后公布该行动，表明以色列有了更加先进的网络作战方式，同时此举也对处于技术低端的敌对国家形成了强大的威慑。该行动促使更多国家探索网络武器与常规武器、网络军队与常规军队的有效融合，生成新质战斗力，以最小代价获取最大的作战效能。

（点评专家系军事科学院战争研究院研究员王桂芳）

案例三 勒索病毒 NSA“网络军火”首次实现民用化

2017年，一次大规模的勒索病毒网络攻击席卷全球，短短3天便影响了全球近百个国家，我国校园网和多家能源企业、政府机构也不幸中招。

研究人员发现，该病毒正是利用美国国家安全局（NSA）黑客武器库泄露的黑客工具“永恒之蓝”开发的。由此，被称为黑客武器“军火商”的黑客组织“影子经纪人”浮出水面。

据报道，“影子经纪人”盗走的黑客工具远不止“永恒之蓝”，该组织声称其入侵了NSA的黑客武器库，获取了大量的互联网攻击工具。

当时，“影子经纪人”明目张胆地在推特上表示，他们将免费提供一些网络攻击和黑客工具的下载，而这些攻击武器均来自另一黑客团队——“方程式组织”。据称，“影子经纪人”盯上“方程式组织”的原因是，“方程式组织”帮政府干活，其隶属于NSA，被称为NSA的网络“武器库”。

有业内人士表示，“方程式组织”是全球最顶尖的黑客团队。2010年毁掉伊朗核设备的“震网”病毒，也被指出自“方程式组织”之手。

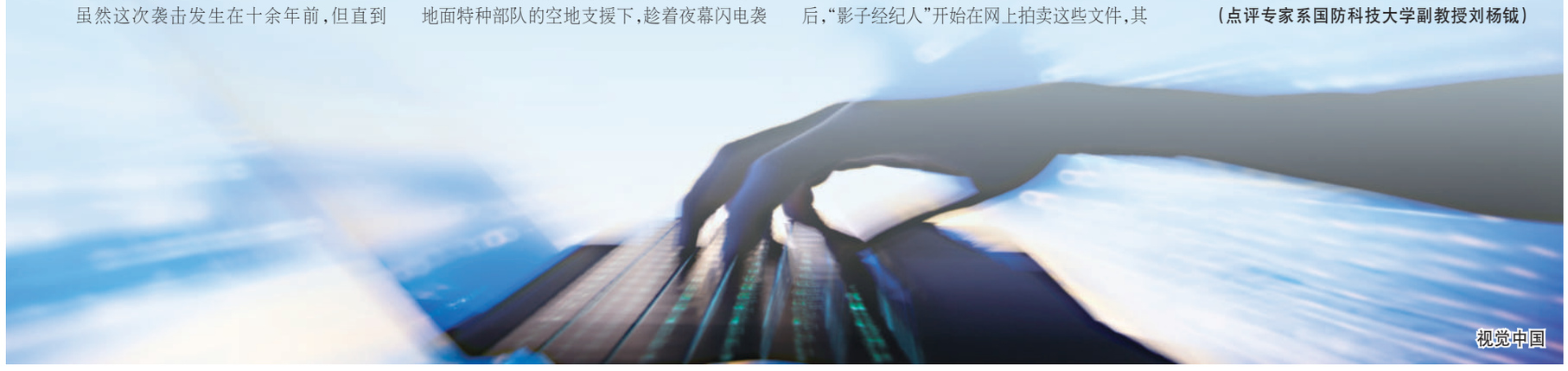
在声称盗取了“方程式组织”的攻击武器之后，“影子经纪人”开始在网上拍卖这些文件，其中就包括“永恒之蓝”。勒索病毒就是不法分子利用“永恒之蓝”开发的蠕虫病毒，这是NSA“网络军火”民用化的全球第一例。

专家点评：

如果说“震网”病毒和“果园行动”体现的是国家层面的网络交锋，那么勒索病毒事件则反映了网络战的另一个侧面——网络武器的扩散会给国际安全带来严重危害。当前，不少国家正公开或半公开地推进网络空间军事化措施，导致网络空间军备竞赛日趋激烈。但随之而来的，就是对网络武器和网络冲突的管控难度日益增加。

网络武器本质上是可复制、可转移的程序代码，使用这类武器发起攻击的门槛相对较低。除了国家行为体之外，黑客、犯罪团伙、恐怖组织等各类非国家行为体都有可能运用网络武器为非作歹。美国国家安全局开发、囤积的黑客武器库，恰恰为这些攻击者提供了便利条件，可以说是国际社会安全稳定的严重隐患。因此，如果不能尽快形成国际规范，约束网络空间军事化、武器化的脚步，类似勒索病毒的事件将会层出不穷，而且还可能愈演愈烈。

（点评专家系国防科技大学副教授刘杨钺）



视觉中国

IP根来了，假IP再难坑你

第二看台

本报记者 **朱 丽**

“当前，国际上有一个重要性不亚于域名根的机制——IP根正在形成。未来，IP根或将重塑国际互联网治理格局。”在近日举办的第16届中国网络安全年会上，域名国家工程研究中心主任毛伟表示，IP根是个新概念，它有望解决“路由劫持”问题。

那么，究竟什么是IP根？它在互联网中扮演着什么角色？

IP根：最顶级的IP地址验证机构

要解释IP根，就要先从IP地址说起。如果把个人电脑比作电话，那么IP地址就相当于电话号码。可现实中却存在很多假冒的电话号码，引用户误入歧途，由此带来隐私泄露甚至财产损失风险。

“然而长期以来，我们未形成IP地址认证机制。”毛伟介绍道，网络攻击者可利用这一漏洞，冒充他人的IP地址，截获误入歧途的流量，这一操作被称为“路由劫持”或“路由泄露”，发布假冒IP地址的过程就像伪基站发布诈骗短信。

如何解决路由劫持问题？毛伟表示，RPKI（互联网码号资源公钥基础设施）作为公认的互联网地址安全认证体系解决方案，有望成为下一阶段网络空间安全和互联网治理的核心技术。简单来讲，RPKI证书就像为IP地址颁发的“认证证书”，通过对IP地址进行第三方认证，来增强IP地址的安全性、可靠性。

2017年，全球五大IP地址注册管理机构（RIR）及中国互联网络信息中心，开始在分配IP地址时，同时签发RPKI认证证书，用于验证IP地址的分配信息。这些IP地址信息的分配及验证机构，处于全球IP地址树的“根部”。也就是说，IP根是整个IP地址认证体系的入口，是最顶级的IP地址验证机构。

部署应用进入关键阶段

这种强认证机制，虽然解决了路由劫持问题，但也带来新的潜在风险：如果认证机构出现认证错误，那该怎么办？

2017年，域名国家工程研究中心技术专家和RPKI发明人联合起草了国际标准IETF RFC 8211，在技术上系统梳理了RPKI部署应用后治理架构改变带来的风险和挑战。2018年，域名国家工程研究中心技术专家再次牵头起草了国际标准IETF RFC 8416，提出了本地验证机制的解决方案，从而可避免全球RPKI的错误数据干预本地网络运行。

这一系列国际标准的不断推出，使路由认证和IP根运行机制日臻完善。在毛伟看来，现在的认证技术已非常成熟，正进入部署应用的关键阶段。

数据显示，截至2019年6月30日，被RPKI签名认证的IP地址数量呈爆发式增长趋势，全球IPv4地址空间的RPKI覆盖率已达17%，包括美国的AT&T、日本的NTT、德国的DECIX等在内的运营商，以及亚马逊、微软、脸书等网络内容服务商，都开始依赖RPKI验证彼此间的通信。在我国，华为、中兴、新华三等设备制造商也开始在路由器上支持基于RPKI数据的路由起源验证。

“当前全球范围内开展的RPKI部署应用，是一次触及互联网‘互联互通根基’的安全升级行动，是互联网由‘可用’向‘可信’演进的新阶段。”毛伟说，在这个推进过程中，中国不应该缺位。

为推广RPKI，毛伟建议，我国相关单位可依托其职能定位，发挥积极作用。例如，网络运营商可升级其IP地址管理系统以支持RPKI，启动基于RPKI的路由认证试点；互联网服务提供商可使用RPKI技术，来保护其关键服务地址空间。

行业观察

电视开机率仅30% 众厂商逆势扎堆推新图啥

左鹏飞

近日，华为子品牌荣耀宣布正式进入智能电视领域，将于8月上旬发布首款产品。今年以来，TCL、索尼、三星、夏普等厂商已先后推出8K超高清电视。

在彩电行业持续多年低迷的背景下，众多企业为何逆势出招？未来电视机行业又将如何发展？

为抢占机遇厂商逆势而动

技术的快速发展，打破了电视原有的信号接收模式，将“老电视”原有的视频接收模式变为智能电视跨时空的随机欣赏模式，改变了受众的视频观看习惯。同时，在智能手机的冲击下，目前我国电视日均开机率仅有30%，且用户年龄普遍在40岁以上。

此外，彩电行业发展形势日趋严峻，利润率逐年降低。2019年上半年我国彩电市场总售量为2200万台，同比下降2.7%；零售额规模仅有640亿元，同比下降11.8%。但2019年华为荣耀、TCL、索尼等电视厂家却扎堆推新，在笔者看来，出现这一现象的原因主要有两点：

一是“5G+8K”带动相关行业发展。2019年是我国5G商用元年，也是8K元年，5G推动万物互联时代的到来，8K让4倍于人眼的超高清技术变为现实。在“5G网络+8K分辨率”的推动下，相关应用正加速涌现，而电视也是重要应用场景之一，这一技术变革为彩电行业带来了新机会。因此，一批传统家电企业、信息技术企业纷纷在2019年逆势出招。

二是抢占智能家居生态入口。2018年我国智能家居行业规模在1700亿元左右，行业报告预测，未来几年全球智能家居市场将以15%的年复合增长率继续增长，而围绕智能家居的入口之争从未停息。电视作为智能家居场景的关键一环，在新场景形成和发展过程中具有天然优势，企业自然不愿错过抢占这一入口的机会。

不是电视而是显示设备

虽然技术和智慧家居，能为电视带来新的市场机遇，但不可否认，传统电视的消费群体已经越来越小。由于智能手机娱乐功能的日益增强，加上手机的便携性，渐渐被手机替代的电视正一步步沦为一种家庭摆设。尤其是在年轻人组成的家庭中，这一现象体现得更为明显。

同时，由于彩电厂商间残酷的价格争夺战，单品彩电的利润空间也变得越来越小。相关报告显示，2017年中国彩电行业主要企业的平均利润率仅为1.3%。在彩电行业持续低迷的背景下，如果还是以传统思维去做电视，即便用上“互联网”“5G”这些新瓶子，厂商做出来的，可能还是旧酒。

诚如华为消费者业务CEO、华为常务董事余承东所说，华为做的不是电视，而是拥有电视功能的大屏设备。这一设备将立足于AI（人工智能）时代，专注体验升级。可见，这一轮逆势推新的厂商，想要做的其实不是电视，而是一种显示设备，或者说是超大屏的手机。

不可否认，彩电在内容显示方面具有显著优势。在内容呈现上，大屏电视具备音箱、手机等产品不具备的先天优势，可以更好地服务于未来智慧家庭。据了解，包括创维、康佳在内的传统家电企业都已经开始在这方面进行布局。

而这种显示优势，尤其在AR/VR领域、大型游戏体验方面就会体现得更为明显。不同于手机游戏，大型游戏对硬件要求比较高，云端化与彩电的高清显示功能相结合，将会使玩家的操作更便捷、娱乐体验更逼真。

或成为智慧家庭连接枢纽

没有传统的产业，只有传统的思维。

近年来，很多行业在技术革新和新商业模式推动下获得了新的发展，电视机也可以在智慧家庭方面大有作为。信息通信技术的进步，不仅推动着彩电的硬件升级，更从内容、形式、渠道等多个维度深刻改变着电视。即在高品质制造基础上，融合互联网元素，从供给侧发力，为用户提供个性化电视机。

以后的电视机不仅要满足观众观看节目的需求，更要实现功能性转变。具体来说，笔者认为，在未来5到10年内，电视机将呈现以下两大发展趋势。

一是成为智慧家庭生态的中心。由于电视在音频、视频方面的表现功能，可以在该设备上进行声控、点击等多种操作，加上用户已积累的使用习惯，智能电视更有条件成为智能家居相关设备，如冰箱、洗衣机、空调等电器的连接枢纽，成为智慧家庭生态的中心。

二是成为连接智慧家庭的基本节点。在三网融合进程不断加快的背景下，电视在连接家庭内外互联网方面具有的显著优势，将在万物互联时代得到放大和强化。根据现状预测，电视将是未来家庭内外物联网连接的最佳入口，将有可能成为连接一个个智慧家庭的基本节点。

（作者系中国社会科学院数量经济与技术经济研究所助理研究员）

图片来源于网络