军界瞭望

本报副刊部主编 | 第 389 期 | 2016 年 5 月 13 日 星期五 责编:钱 卫 视觉:竹建英 编辑邮箱:qianw@xmwb.com.cn

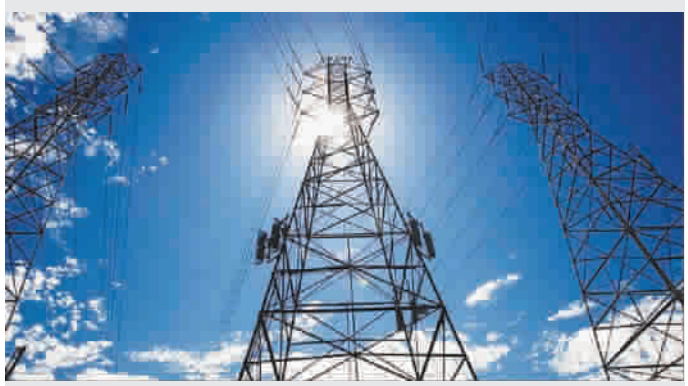
南海舰队战备巡逻 提升海区管控能力

近日,由南海舰队导弹驱逐舰合肥舰、兰州舰、广州舰,导弹护卫舰三亚舰、玉林舰,综合补给舰洪湖舰等 6 艘舰艇组成舰艇编队赴远海展开战备巡逻实兵对抗训练,随舰搭载各型直升机 3 架及数十名特战队员。据了解,这次训练紧贴舰队使命任务, 强化主战兵力远海作战运用,强化舰机协同反潜、合同攻击、防空反导、特种作战等重难点问题专攻精练,扎实提高实战能力。

■ 5 月 5 日,编队中的合肥舰在西沙海域与驻巡的韶关舰演练驱离行动 图 CFP

严防电力设施遭破坏,美欲研制“网攻预警”

去年 12 月 23 日, 乌克兰发生世界首例因遭受黑客攻击而造成的大面积停电事故。近日,有美国调查分析机构就该次停电事故发布调查报告。美国爱达荷国家实验室的安迪·巴克曼指出:围绕电力等军民两用基础设施的网络攻击将变得越来越多,涉及的范围也将越来越广。有消息称,为了防范此类事件在美国境内上演,美国政府和军方机构正在急寻对策。



■ 对任何组织来说,因网络攻击导致的严重停电事故都是一场噩梦

“电网攻击”危害巨大

在乌克兰电力公司遭黑客攻击前,美国政府和军方都坚信黑客奈何不了本国电网。美国爱迪生电力研究所的专家斯科特·阿隆森曾信心十足地表示:“从未发生过对电网安全性有影响的网络攻击,断电事件从未发生过。”但时隔不久,乌克兰电力公司就遭了殃。乌克兰方面发布的报告显示,因监控管理系统遭到入侵, 至少有 3 个电力区域被攻击, 导致 7 个 110 千伏变电站和 23 个 35 千伏变电站出现故障,约 8 万用户因此断电。

“北美供电信息分析中心”(E-ISAC) 于 5 月 2 日发布调查报告称,攻击乌克兰电网的黑客早在事故发生的 6 个月前就控制了 3 家乌克兰供电公司的部分系统,之后黑客悄悄收集各种登录证书(用于身份识别和加密传输数据的密钥),并在一台接一台的计算机上提升操作权限,最后入侵关键的电网控制系统、配电所和变电站。当停电事故发生后,这三家公司努力恢复供电,却发现大量数据被恶意程序删除,事故调查和善后工作受到阻碍。值得一提的是,其中一家电力公司的呼叫中心也被黑客攻陷,令部分饱尝断电之苦的用户无法报修。

美国电力通讯委员会研究员娜蒂娅·巴托尔表示,随着越来越多的电力公司在电网监控管理系统中采用广泛趋同的第三方软件,以及更多的智能仪表和自动控制系统,在给企业管理带来便利的同时, 也给黑客创造了机会。

基础设施成为标靶

美国国土安全部曾委托爱达荷国家实验室于 2007 年 3 月进行代号“欧罗拉”的测试行动,验证网络攻击能对发电机造成怎样的物理损害。测试标靶是 1 台独立的 2.25 兆瓦发电机, 测试人员通过网络攻击手段控制了发电机的计算机控制系统, 通过遥控操作使得发电机内的断路器非正常启闭, 导致发电机内部压力不断上升。测试开始 3 分钟后,发电机就喷出了浓烟。最终,这台发电机炸裂开来。英国劳埃德保险公司与剑桥大学风险研究中心的一项研究认为,如果有 50 台大型发电机被网络攻击破坏, 那么造成的经济损失将超过 2400 亿美元。

也许是意识到针对电力系统的网络攻击可能造成灾难性后果,自 2009 年起,美国国土安全部与国防部联手追踪针对美国基础设施的网络攻击, 据称已收集到约 900 份报告, 其中针对电力公司和发电厂的网络攻击占 40%。总的来看,对基础设施的网络攻击可以分为三类:攻击网站及服务终端、监控重要信息流、攻击生产控制系统。其中,最后一种攻击的影响最大, 且有较大的战略意义。比如,为了阻挠伊朗核计划, 美国军方曾针对伊朗核设施实施网络战,使伊朗的关键设备(离心机组)因工作异常而停机。事后, 网络攻击中使用的“震网”病毒流入互联网, 入侵了全球数万个企业网络和大量个人电脑,造成巨大损失。

事实上, 针对关键基础设施并造成物理破坏的网络攻击不仅限于电力领域, 还涵盖应急服务、水处理、通讯网络等与民众生活息息相关的行业与领域。以追踪、分析网络攻击态势并定期发布安全报告著称的威瑞森公司曾在一份摘要中披露,距纽约不到 32 千米的一座小型水坝曾于 2013 年遭到黑客入侵,黑客一度攻陷水坝控制系统, 幸好没有引起严重后果。2015 年,一家美国自来水厂遭到黑客入侵, 水厂的流量控制和水质净化系统的阀门多次被黑客控制, 导致供水中的化学物含量异常。幸运的是,水厂很快发现异常,及时进行了修正。

网络威胁难以杜绝

2015 年 12 月, 美国国防部高级研究计划局提出“网络攻击快速侦察、隔离与鉴定”(RADICS)的研究项目,打算在 4 年内投入 7700 万美元,用于研制“网攻预警系统”,以便及时发现和处置针对电网等关键基础设施的网络攻击。美国乡村电力合作协会的毛里斯·马丁指出,按照现阶段电网系统的预警能力,从黑客发动攻击到发现电网系统异常,平均需要 205 天,这让黑客可以有足够的时间制造麻烦。RADICS 项目可以通过异常检测、工业控制系统协议分析、网络威胁快速鉴定等技术手段,快速甄别网络攻击,并在一周内完成修复, 这对与国防能力密切相关的关键设施相当重要。

E-ISAC 的报告称,作为基础设施的运营者, 必须随时准备好面对具有高度针对性的、直接的打击,包括利用企业的工业控制系统来攻击这些基础设施。美国爱达荷国家实验室的安迪·巴克曼认为,完全消除网络威胁几乎是不可能的, 只能依靠严格落实安全措施和制定完善的应对预案来减少损失, 这是一场持久战。巴克曼表示:“你无法预测黑客何时发动攻击, 你也不知道黑客会从哪个地方入手。我们可以把这些攻击想象成小偷走在街上, 随手摇晃路边住宅的门把手, 寻找犯罪机会。此外,黑客在网络攻击时还会不断清扫留下的痕迹, 这也让网络攻击变得更加隐蔽。” 张晓红

热点聚焦