

电网

不可忽视的电力基础设施网络威胁

近几年来，可以越发明显地看到对北美电力网络的大规模网络攻击代表着一种对美国国家安全的严重威胁。一段时间以来，一些美国高层官员一直把此项威胁列为美国所面临的最严重威胁之一，并警告说美国尚未采取充分措施应取这一威胁。

文 | Richard B. Andres

网络武器可以使电网瓦解的概念并不新鲜，但是却在 2010 年 6 月首次得到广泛的公众关注，当时有关一种名为 Stuxnet 病毒报道浮出水面，这种病毒攻击了控制着伊朗核离心分离机的监测、控制和数据采集 (SCADA) 系统。这次攻击当中有两个特别方面引起了电力行业的注意。第一个方面是，病毒在多年不断毁坏硬件的过程中，都处于未被检测到的状态。第二个方面是被病毒接管的西门子 SCADA 基础设施系统与控制着众多全球电力基础设施的系统都相似。

从国家安全的角度来说，北美电力基础设施已经受到用于摧毁硬件的恶意软件所感染的事实带来的非常深远的影响。在某些条件下，这类攻击有可能导致美国断电数月乃至数年。这种大面积断电的影响将是灾难性的。在全国性断电的头几分钟，实际上所有商业活动都会因为电力系统崩溃而停止；汽油泵将停止运转；政府和应急救援机构所使用的电话，都将很快不起作用；采用电力水泵的城市失去水压，下水道系统污水将倒灌进入淡水系统；燃油输送管道将

停止工作；绝大多数家庭只有 3 天食品贮量并且没有贮存饮用水；医院将在少数几天内继续运作；国民警卫队和执法机构已经在记录当中声明，他们认为员工们将在不到一个星期内就停止上班；疾病和饥饿将在几天内到来。

诸如这样一幅场景给财产和生命带来的损害程度将取决于断电的规格和持续时间。只要断电规模小至足以让受影响的人们退出受影响地区，并且来自未受影响地区的修理队伍和应急救援人员能够进入，那么生命损失可以降低至最低。但是，最近发生的 2012 年飓风桑迪过后断电事故提醒我们，受影响区域不需要特别大就会导致修理和应急救援队伍的来到被推迟。最差场景下长达数月之久涉及整个大陆的断电将夺去数以百万计的生命。但是，即使较小规格和较短期的断电，其影响也是摧毁性的。

电网崩溃最有可能的原因是主要电力事故的来源。这些状态通常是可以防止的。但不幸的是，网络武器技术的演进速度正在超过网络防御技术，现在有可能只攻击大型供电设施，未来将有可能对小型供电展开。自冷战以来美国已

经大致开展过 6 次战争，这些战争的敌手都缺乏反击的能力。但北美电网对网络攻击的脆弱性代表着一种可投放力量的廉价途径，并对大批美国潜在敌人具有不可抗拒的诱惑力。

想让电网解体的难度很大，还有许多措施可以加大这种难度。工业控制系统和 SCADA 基础设施可以得到更好的保护。电力行业可以分享有关网络攻击的更多信息，并授权联邦能源管理委员会和北美电力可靠性公司制订更严格强制性标准。本地发电系统可以增强自己孤岛式运行能力以及断电启动的能力。

就目前而言，绝大多数公司均至少从外围意识到了这个问题。但是，行业领导者似乎正在等待一场巨大事件的发生来刺激他们采取措施，而这种策略是危险的。如果真有这样的事件发生，那么这场事件至少会让人们产生这样的疑问，为什么电力行业没有保护自己客户的生命，并非非常有可能导致国会重新思考电力基础设施私有体制的问题，这样对任何人都没有利益可言，不过现在正是行动的良机。□□□