军界瞭望 周刊 B
高端·权威·独家
2013年3月28日 星期四
本报军事专刊部主编 总第236期
新民晚报 上海市拥军优属基金会 联合主办
本刊高级军事顾问：向守志上将 刘精松上将 杨怀庆上将 吴铨叙上将 隋永举上将（排名按姓氏笔画为序）
新民网:www.xinmin.cn 24小时读者热线 962288 来稿:qianw@wxjt.com.cn 信函:dzlx@wxjt.com.cn 主编 张黎明 责任编辑 钱 卫 视觉设计 竹建英

海军编队赴南海西太平洋 展开战备巡逻和远海训练

由海军南海舰队4艘军舰组成的舰艇编队近日在南海、西太平洋等海域进行战备巡逻和远海训练。执行这次任务的是两栖登陆舰井冈山舰、导弹驱逐舰兰州舰、导弹护卫舰玉林舰和衡水舰，并随舰搭载4架直升机、1艘气垫艇和1个陆战连等兵力。编队将进行指挥所开设、机动作战、海上维权、远海护航、支援作战快速反应等课目的训练。

井冈山舰是我国目前吨位最大、武器系统较先进的两栖船坞登陆舰，兰州舰和玉林舰均执行过亚丁湾、索马里海域护航任务，具有较强的防空、反导和反潜能力，衡水舰是刚服役不久的新型护卫舰。

■ 气垫艇与井冈山舰在进行协同训练 新华社 高毅 摄

遭遇黑客，新虚拟战争会降临朝鲜半岛吗？

国防大学 李大光

近日，朝鲜中央广播电台先后6次发布空袭警报，并指示朝鲜军民模拟遭到空袭进行相关的应对演练。与此同时，韩国部分电视台和金融机构遭遇黑客攻击网络瘫痪。虽然最后查明网络攻击来自韩国某银行的内部电脑，但韩国情报机构一度推定此次网络攻击是朝鲜所为。一边拉响警报、一边遭遇黑客，新虚拟战争是否降临朝鲜半岛？

■ 3月20日，韩国信息安全局的工作人员检查网络遭袭击的情况 图IC

黑客事件源于“内战”

“黑客警报！”3月20日，一场突如其来的网络攻击震惊韩国朝野。韩国新闻机构报道称，至少3家电视台和2家金融机构的网络遭到恶意代码入侵，几乎同时陷入瘫痪，并称黑客为了躲避追踪，使用了通信密码化等“高难度技术”。事件发生后，韩国和西方国家的新闻机构众口一词地指责“是朝鲜干的”。许多西方新闻机构还纷纷列举朝鲜黑客的“前科”作为证据。韩国军方随即将情报作战防卫级别上调一级，这意味着人力增加3倍以上。

3月21日上午，负责调查的韩国多部门联合应对小组声称，“经过分析，攻击韩国网络的恶意代码来源IP地址属于中国。”随后，韩国政府相关人士向媒体表示，这起事件很有可能是朝鲜网络部队通过中国网络实施的攻击。许多韩国民众对网络攻击表示担忧，韩国《中央日报》更是刊登社论将网络安全提升至关系韩国“生死存亡”的高度。一时间，网络威胁成为韩国的头号国家议题。有消息称，就连美国五角大楼也开始重新评估朝鲜的实际威胁，其中包括网络战能力。

不过，此次网络袭击事件的调查工作在3月22日有了出人意料的新进展——“韩国内战”才是真相。韩国通讯委员会宣布，国内主要电视台和金融机构先前遭遇的网络攻击来源位于韩国境内。导致网络瘫痪的恶意代码来自韩国农业协同银行的内部电脑。据介绍，韩国农业协同银行一直使用私自设立的IP地址，与中国的IP地址相同。网络分析人员先前误把这家银行的IP地址当做来自中国，产生了“误判”。

显然，这起事件与朝鲜或中国没啥关系。那么为什么事件发生后，韩美都在第一时间把矛头指向朝鲜呢？这与韩美等国的长期宣传有关。

传说朝鲜网军很厉害

“朝鲜网军很厉害”，这种观点近几年一直在美国和韩国的新闻机构中流传，并频频见诸报端。按照他们的说法，朝鲜从1986年就开始集中培养网络战士。1998年，朝鲜就组建了一支专门从事网络战的部队，代号121。自那时起朝鲜网络部队的规模和能力一直持续扩大。

美国福克斯新闻网2011年曾报道称，朝鲜网络部队的人数多达3万，其实力足以与美国中情局抗衡。韩国《东亚日报》则报道称，朝鲜从各大学中挑选成绩最优秀的学生送往“秘密学校”学习黑客技术和网络袭击战术。朝鲜利用这种方式每年可以培养100至110名职业“黑客”。韩国《朝鲜日报》还在报道中引用韩国情报机构对朝鲜网络战能力的评价——“具有致瘫美军太平洋司令部及对美国国防相关网站造成严重破坏的能力”。

不过，也有军事专家指出，炒作“朝鲜网军”只是为了给美韩等国扩充网络部队寻找理由和假想敌。3月21日，韩国国防部就表示要将韩军网络司令部所属的人员数量提升一倍。此外，负责反间谍和内部警卫的韩军机务司令部同样具备网络战能力，并拥有大量黑客。至于所谓“韩国网络被攻击事件”不乏“自己人”出手的例子。2011年9月，韩军机务司令部下属的黑客非法入侵朝鲜大学某教授的邮箱被曝光，两名相关黑客（军人）和一名军官因此被拘捕，韩军机务司令部在国内进行黑客攻击的事实浮出水面。

长期以来，美国有一些人热衷于宣扬美国有遭遇“数字珍珠港”的风险，并将其他国家树为威胁，为美军组建和扩编网络部队造势。早在2002年，美国海军就率先组建了网络部队，随后美国空军和陆军也纷纷组建自己的网络部队。2010年5月，美军更是设立网络司令部，统一协调与电脑网络有关的军事行动。今年3月12日，美军网络司令部司令透露，美国正在组建40支网络部队，其中13支专注“进攻”，另外27支负责监控、培训和后勤。对于这些部队平时在网络中干些什么，执行过哪些行动，五角大楼讳莫如深，也很少受到美国国会的监督。

“网攻”可能引发战争

纵观此次韩国网络攻击事件的调查，其过程可谓一波三折，也使人们注意到韩国和朝鲜正轮番扮演着两种新角色——“黑客和反黑客”。虚拟网络抹去了国家边界，将韩国和朝鲜拉入了更广阔的网络战场。也许网络战不如传统战争那样令人害怕，但杀伤力同样不可小觑。

更令人担忧的是，“网络战争”中的“误判”有可能引发现实世界的战争。特别是当一些国家自恃军力，将“先发制人”的进攻性策略和“有罪推定”用于军事决策。2011年5月和7月，美国先后发布《网络空间国际战略》和《网络空间行动战略》，宣称“攻击网络即战争”，美国可发起传统方式的军事回击。五角大楼将其形象地描述为“如果你关掉我们的电网，我们也许会向你的烟囱里扔枚导弹。”今年早些时候，美国有关部门还对动用网络武器的政策和程序展开法律审核。按照初步结论，奥巴马政府可能获得更大权限，只要有证据显示美国“即将”遭到别国的重大网络攻击，总统可下令发起先发制人的网络攻击。

然而，所谓的“证据”如何取得、又有多少可信度值得怀疑。十年前，美国政府言之凿凿地说有“证据”显示伊拉克拥有大规模杀伤性武器，并因此发动了伊拉克战争。时至今日，事实证明所谓“伊拉克拥有大规模杀伤性武器”纯属无稽之谈。再以此次韩国网络攻击事件为例，3月21日，韩国联合应对小组在记者会上公布了攻击者的IP地址，并称该地址属于中国，还介绍了部分攻击细节。看起来也是“证据充分”，可是事实如何已见分晓。

无论是为了在网络空间拥有更多“不对称优势”，还是仅仅为了自保，各国纷纷组建网络安全部队已是不争的事实，具有跨国破坏性的网络武器有不断扩散的趋势，一些国家或国家集团有意无意地“误判”引发网络战争，甚至进一步引发传统战争的危险正变得越来越大。

热点聚焦