

新民晚报社
上海市国防教育协会
联合主办

军界瞭望

23
点燃十月革命的
“克伦斯基攻势”

本报时政新闻中心主编 | 第 447 期 | 2017 年 7 月 24 日 星期一 责编:吴 健 视觉:竹建英 编辑邮箱:wujian@xmwb.com.cn

防范“数字炸弹”，俄军自建“专用网”

近来,受“网络干预大选”、“特朗普通俄门”等事件影响,美俄摩擦不断,美国国会和媒体屡屡指责俄罗斯大搞“网络入侵”。殊不知,俄罗斯也高度警惕美国对其实施“网络战争”,担心“数字炸弹”会危及国家安全。

沉默的“特洛伊木马”

7 月中旬,多家俄罗斯媒体援引美国《华盛顿邮报》的报道,称美国前总统奥巴马在任期间,曾批准在俄关键网络系统中植入数字武器的计划,这种武器相当于“数字炸弹”,能在美俄关系尖锐化的危急关头发挥作用,破坏具有战略意义的俄基础设施网络。美国国家安全局、中情局以及网络司令部都参与该计划。

据悉,“数字炸弹”是个长期行动,不仅需要数月来定位植入代码,后续也需要维护投入。其中,“攻击代码”由美国国家安全局开发,可以远程触发,实现攻击电网或干扰俄未来总统竞选等。《华盛顿邮报》称,“数字炸弹”计划在特朗普当选总统后有所放缓,美国官员关注的焦点是特朗普是否废止前任的政策。知情人士称,关于“数字炸弹”计划的实施,美国情报机构不需要特朗普的进一步批准,如需终止该计划,特朗普必须签署一份取消命令。一位匿名的美国官员表示,他们还没有看到特朗普会这么做的迹象。

完全隔离的“网”

关于“数字炸弹”计划的真实性,俄国内尚存争议,但对于利用互联网进行“信息进攻”的危害性,俄罗斯人早有提防。前不久,勒索病毒软件波及俄罗斯银行,罪犯或许不需要炸弹和冲锋枪,就能用篡改软



▲ 俄军高度重视内网安全
► 俄军对网络高效安全运行予以重点关注



件逼迫对方就范。如果这些科技用到军事领域,破坏力就更难想象了。

为了防患于未然,俄国防部新近宣布,军队已完成了封闭式军用网络的建设。俄罗斯《消息报》透露,该网络称为“模块化封闭式数字传输系统”(SSPD),正常情况下,所有终端、线路和单个设备都不与互联网连通,实现完全隔离。系统允许加密信息进行快速和安全的传输,针对可疑的登录和连接,能进行自动监控并快速定位与追溯。

其实,SSPD 的工程建设早在 2012 年就开始了,2016 年夏末完成,经过近一年的调试,于 2017 年 5 月达到设计工作状态,但由于不少军事单位需要持续增加服务器和用户终端,因此全面运行推迟了一段时间。尽管 SSPD 要求与互联网隔离,但网络建设不可能全靠军方力量。SSPD 建设期间,俄国防部的的主要职责是进行系统的顶层构架和

终端位置的地理规划,之后很大一部分工程交由民间承包商担负,他们都受到军方技术人员的监督。参与施工的“互联网事”公司 CEO 萨姆罗金称,SSPD 至少采用双回路通信,“一用一备”,首先完成了主用回路,然后不断提高备用线路的可靠性。

杜绝“非法连接”

俄军方透露,SSPD 全部服务器均设在军事基地内,且进行严密监视。观察俄军“西方-2017”大演习和叙利亚作战的试用情况,SSPD 的视频实施传输服务能覆盖到前沿的营连分队,未来能覆盖到每架飞机,每辆坦克和每个单兵。俄军没有公开系统的整体数据传输速度,部分专家判断 SSPD 可能达到 3G 水平。由于俄罗斯幅员辽阔,偏远地区的网速实际水平可能较差,不过 SSPD 可以重点保证克里米亚、叙利亚战略方向的快速军用通信。

SSPD 的构架,线路和使用终端,与民用设施没有根本差别,只不过能连入网络的各种终端(如电脑和手持式信息交换机)须得到国防部认证,且安装俄军用操作系统(MSVS)的特殊设备。俄总参通信总局对全部硬件接口进行了加密设置,确保任何非法设备(如打印机,扫描仪,闪盘,移动硬盘乃至投影仪)无法连接,且军用终端能对未认证的连接进行记录和自动上传。目前,俄罗斯军网有自己的网站,采用三级域名(例如 domain.mil.zs),使用 MSVS 即可登录访问,网站的发布内容、登录访问和下载记录由总参第八局(即保密局)负责定期鉴定和审计。

SSPD 有一套完善的电子邮件服务系统,允许内部邮件交流,军人所有日常文书工作和书面手续(报告、申请、名单、带照片的工作总结等)都可以经由系统交流。俄军计划逐步减少物理性的重要文书工作,

一方面消除纸质文件在流转和存储中的破损被盗风险,另一方面能全面有效监控和访问各种常规信息。

换一种思路

俄罗斯互联网技术和基础设施发展基金会主席德米特里·布尔科夫就美俄军用网络进行了对比,认为俄军网络的统一化设计比美军网络更可靠,“美国人的网络实际上漏洞百出,国防部、中情局、陆海空军各有一套系统和通信协议,系统有许多与互联网的连接点,这样一来,遭受非法入侵的危险性很高”。俄总统网络问题顾问戈尔曼·克利缅科说得更直白,“不管啥事,放到互联网上就等于公开了”。他评论说:“当年斯诺登只是为美国国家安全局‘棱镜’监控系统的某个二级分包商工作,却能访问工作范围外的高密级数据库,从而获得大量信息,要是在俄罗斯,这是被严格禁止的。”

如同所有网络服务一样,SSPD 也将进行不断的扩容,服务和软件更新虽不像手机 APP 那样高频率地进行,但势必引入更多的民间力量参与。如何在此过程中防范可能出现出现的俄罗斯“斯诺登”,杜绝失密或“数字炸弹”入侵,无疑是个崭新课题。根据目前民用网络服务和流量爆炸性增加的趋势,还有一种理论认为,干脆把军用信息伪装后与浩如烟海的民用信息一道处理,快速发送,快速处理,加密存储后快速灭失,失密概率可能比防范严密但入侵目标明确的军用网络还小。 李鹏



美国谋求核武库“减量提质”

近日,瑞典国际和平研究所(SIPRI)发布关于全球核武器的报告,称全球核弹头数量虽与 2016 年初相比有所减少,但质量却稳步提高,尤其是美国出于霸权考虑,不惜投入巨资推进核武器现代化。

数量在下降,质量在提高

报告指出,截至 2017 年初,全球 9 个有核国家共部署 4150 枚核弹头。如果把封存的、退役的以及等待拆除的核武器都算在内,那么全球就有约 14935 枚核弹头,比 2016 年的 15395 枚下降了约 3%。

核武器总量能够减少,主要是拥有全球 93%核武器的美国和俄罗斯执行削减核库存的政策,但双方这一步伐变得越来越慢,甚至出现“逆增长”。美国国务院在 2017 年 4 月发布最新评估,称美军已部署的核弹头居然比 2016 年 10 月增加 44 枚,但美国官员辩解称总量仍低于《美俄削减战略武器条约》规定的上限,并指责俄罗斯的同类武器数量虽在同期减少了 31 枚,但超出条约上限 25 枚。

不过,SIPRI 认为美国是全球核武库升级的“主要动力源”。美国计划从 2017 年到 2026 年花费



■ 美军 B-52 轰炸机发射核导弹示意图



■ 美军 B-52 轰炸机能在核常任务之间快速转换

4000 亿美元维持和更新核力量,目标是减少现有核武器的体积重量、准备时间、附带损伤和维护难度,提高打击精度、灵活性、可靠性及安全性。美国《防务新闻》称,美国空军正在研发两款新型核导弹,以替代快到寿命末期的“民兵-3”洲际导弹和空射巡航导弹(ALCM)。核专家克里斯滕森说:“美国现任政府正在延续奥巴马前总统雄心勃勃的核武器现代化计划。预计的支出增加并不令人感到意外。”

裁减只是变相存储

分析人士指出,美国所谓裁减核武器及其运载工具,并不能被完全相信,原因很简单——核裁军条约并未要求将裁减的核运载工具完全销毁,美国兰德公司研究员库珀称:“美军把相当一部分运载工具用来搭载常规弹药,等于变相将核运载工具‘储存’起来。”他指出,作为美国“三位一体”核力量支柱的 B-52 轰炸机,近年来逐渐向常规武器

平台转型,截至 2017 年 6 月,转为非核状态的 B-52H 轰炸机已达 41 架,“它们并非丧失携带核武器的能力,只要需要,任何一架都可以在短时间内挂载核导弹,这得益于核武器小型化技术进步”。

美军认为,尽管核轰炸机数量在减少,但核战能力没有削弱。美国《空军》杂志称,2017 年 4 月,美国空军全球打击司令部(GSO)成立了核指挥、控制和通信中心,简化了约 62 项不同系统的管理流程,形成唯

一的核战指挥控制节点,将轰炸机、洲际导弹发射控制中心、飞行联队指挥所、“空军一号”等作战要素集成起来,为国家领导层提供了更安全、更可靠、更灵活的核指挥手段。

“非核威慑”成目标

尽管 SIPRI 的报告认为全面废除核武器还是一件遥远的事情,但美国《空军》杂志认为,美军正试图发展一种“非核威慑”能力。库珀说:“仅靠核威慑不足以遏制各种规模的战争,核威慑虽然可畏,但没有一国敢轻易动用核武器,这就让某些疯狂的‘非国家行为体’(如极端组织)有了挑战美国红线的底气。然而一旦常规武器有了与核武器同等威力后,效果就完全不同了——没有人会在

使用常规武器应对挑战方面有所犹豫,因为这不不太可能带来核灾难。”美国总统特朗普认为,现有裁军条约对美国不利,并声称要扩展核力量,但这个想法实现起来并不容易。美国战略司令部司令海登上将说:“可行之道就是大力发展‘非核威慑’能力。例如,新型舰载常规武器不会像陆基洲际导弹那样容易被误判为核攻击,又能为美军提供‘足够的打击手段’。” 王权