新民环球

本报国际新闻部主编 | 第 602 期 | 2018 年 12 月 20 日 星期四 本版编辑:张 颖 编辑邮箱:xmhwb@xmwb.com.cn

新防卫大纲强化信息领域攻防 “一明一暗”两支力量值得警惕

日本网军:一张“藏得很深”的王牌

本报记者 **吴健** 特约撰稿人 **宋涛**

日本政府 18 日举行内阁会议，批准了新版《防卫计划大纲》，强调日本自卫队将进一步强化信息等新领域的防卫能力，重视人工智能和先进网络技术的研发。

但就在不久前，日本负责网络安全的阁僚、网络安全战略本部负责人樱田义孝刚刚闹出大笑话，面对国会议员质询，他承认从未用过电脑，而被问及 U 盘时，樱田只知道 U 盘要插入插孔，但具体细节不清楚。樱田在众议院内阁委员会辩解称:“因为手机特别方便，我一天使用好几次手机(办公)”。

这些奇葩言论在日本国内外引起热议，不由得让人怀疑，对电脑一无所知的外行掌控下的日本网络安全，还能好吗?美国《华盛顿邮报》对此嘲讽道，“(不用电脑的话)至少他不会遭到过黑客攻击”。那么，日本网络安全和网络战能力会像这位负责人那样“不靠谱”吗?

日本自卫队网络防卫队控制中心

■ 日本网络防卫队在演练中 本版图片 GJ

起步和美国差不多 明确提出“瘫痪战”

作为曾在信息技术发展中发挥重要作用的国家，日本对网络安全和网络战的重视度极高。早在 2005 至 2009 年度《中期防卫力量发展计划》中，就明确提出新作战理论“瘫痪战”，而且日本自卫队认定“网络瘫痪战”是重中之重，瘫痪对手的作战网络将令取胜事半功倍。要知道，美国国防部也不过在 2005 年才明确把网络空间与陆、海、空、太空定义为同等重要的五大决胜作战域。2011 年版日本《防卫白皮书》更对政府机关及自卫队等关键部门的网络安全现状作出分析，指出，“网络安全对国家安保有重大影响，日本今后要把提高预防黑客攻击能力作为一个重要课题”。

具体网络战建设上，早在 2008 年，日本自卫队统合幕僚监部（统幕）就成立首支网络战专业部队——指挥通信系统队，里面的网络运用队专责维护、管理与监察防卫信息通信网，并与陆上自卫队系统防护队联合应对网攻。2009 年，由于韩国和美国政府网站频遭黑客攻击，日本防卫省官网也不断收到带病毒的邮件，防卫省立即新组建“电脑空间防卫队”，负责搜集最新电脑病毒信息、研究避免病毒感染对策，同时还负责加强对防卫省和自卫队情报系统的监管。

网上“战略预备队” 随时可“由守转攻”

经过多年建设，今天的日本网络战力量包括“一明一暗、一攻一防”两大部分。明面上是 2014 年设立的日本自卫队网络防卫队（前身就是电脑空间防卫队），由防卫大臣直辖，统合幕僚长指挥，24 小时监视防卫省和自卫队网络，重点是防卫省系统与外网连接的部分及三大自卫队网络重叠部分，同时整合网络空间研究和情报搜集功能，并将分析结果告知各自卫队。此外，“网络防卫队”还负责对日本自卫队的其他部队进行技术支援、调查研究构成威胁的病毒、实施网络演习等。

网络防卫队起初才 90 余人，但根据计划将扩充至千人。日本政府反复强调成立网络防卫队就是“自卫”，但随着规模扩大，其在网络空间的行为早就“由守转攻”了。一名政府内部人士称，“网络空间作战，单纯‘专守防卫’不可能，因为这形同静候对方黑客破坏你的防火墙，如果不反击，他们迟早会成功。”事实上，网络防卫队早就在实际操作获得政府默许，当受到所谓“敌国武力攻击之网络攻击”时，“可行使自卫权应对”。换言之，网络防卫队已成为日本网络主动攻击的“战略预备队”。

除了较为人知的网络防卫队，日本还有一支隐藏极深的“网络黑暗势力”，那就是电磁波部，这是自卫队情报本部的一部分，地位与美国国家安全局(NSA)相当。据美国“拦截”网站称，电磁波部最早的任务是窃听各种通信，保密级别很高，只向首相等少数高官汇报。防卫省官员称:“很少有人知道电磁波部具体干什么，也很少有人能进他们的大楼。”而且，电磁波部的工作虽受法律约束，但不接受任何独立监督。

日本广播公司(NHK)发现，电磁波部有个未公开的互联网监视计划，瞄准电子邮件等网络通信方式。

前防卫省官员披露，电磁波部有约 1700 名员工和六处侦察监视阵地，可对通话、电子邮件和其他通信情况进行全天时监控。“拦截”网站称，电磁波部用名为 X KEY SCORE 的软件来监控网络活动，重点是筛选电子邮件、在线聊天、网络浏览历史和社交媒体活动的信息副本。它使用的另一套互联网监控程序则重点监控通过卫星传输的通信，2012 年，这个代号“MALLARD”的程序每周可收集约 20 万次互联网会话的记录，并对其进行分析，这些数据一般会保存两个月。

然而，电磁波部觉得这些监控手段还不够，比如，洋葱路由器能让用户浏览互联网时隐藏 IP 地址，进而摆脱追踪。因此，电磁波部策划组织了“匿名互联网”行动，意图通过搜集用户利用洋葱路由器等隐私工具的数据，发现各种可疑行为。这一过程中，电磁波部和网络防卫队密切合作，前者负责明确监控目标、监控既定目标和分析所获情报，后者负责分析恶意软件、制定对策措施。

不过，正因为保密级别过高，电磁波部内部信息交流和沟通也存在问题，与别国情报部门的合作更是障碍重重。电磁波部下辖的 11 个局处业务互不交叉，并且独立运行，官员间的交流也受到严格限制，办公楼内各房间都装有不同的锁，只有具有相应的安全许可、访问代码和身份证明的特定人员才能进入。而且以保密为借口，电磁波部不愿与政府其他部门分享情报。

这种过度的“安全顾虑”，甚至被延伸到日本的铁杆盟友美国身上，一位美国国家安全局高级官员就曾经表示，日本电磁波部的信号情报搜集能力“十分出色”，但保密意识过强。

美国国家安全局曾牵头秘密成立太平洋国家情报机构联盟，目的是分享涉及亚太地区安全议题的情报，澳大利亚、加拿大、英国、法国、印度、新西兰、泰国、韩国和新加坡等国的信号情报机构均参加，而“日本是唯一受邀后拒绝加入的国家”，原因是日本认为，一旦参加，该组织的情况被泄露，可能给自身带来极大的风险。

秘密获取境外情报 关注周边尤其中国

事实上，电磁波部的存在，更多是为日本获取境外情报服务。日本福冈县有个重要的基地，位于太刀洗町(隶属三井郡)和筑前町(隶属朝仓郡)之间，正式名称叫情报本部太刀洗通信所，而实际掌握者就是电磁波部。该基地有五座大孔径天线，主要开展对中国、朝鲜、韩国等周边国家的网络监视行动。

澳大利亚墨尔本大学教授、政府网络监控项目专家理查德·坦特认为，太刀洗通信所“可看到”200 多颗卫星，意味着该基地可使用监控系统，截获上述卫星通信和数据传输。坦特指出，上述 200 多颗卫星中，至少有 30 颗为中国卫星，此外，“俄罗斯、欧洲甚至美国拥有或经营的卫星”，也是基地的监控目标。此外，该基地还负责短波通信监测，主要目标仍是中朝韩等周边国家。

这一切都表明，虽然日本网络安全主管者有点“不靠谱”，但日本政府对培植网络战能力依然相当重视，值得警惕。

相关链接

美国大力支持 日本强化网战

作为日本军事力量背后的真正“老大”，美国对于日本政府强化网络战能力也给予了大力支持。按照现行《美日防卫指针》，两国将共同应对网络攻击，甚至提出对被指“网络攻击源头”的国家进一步施压。

日美两国 2013 年 5 月就举行了首次网络安全对话，协商制定网络空间的国际规则，就网络攻击威胁交换看法，并探讨重要基础设施网络的防护方法。

一名日本高级防务官员称，识别网络攻击源需要非常复杂的计算机技术，因此对美合作非常必要，例如，电磁波部使用的 XKEY SCORE 监控软件就是美国提供的。日本官员透露，日本电磁波部与美国国家安全局维持密切合作关系，双方共同开展日本周边国家通信情况监控工作，美方就对日方提供的有关朝鲜导弹发射情报非常欣赏。

除了合作监控，日本还主动为美国网络监控活动提供场所和资金支持。

据前美国国家安全局雇员斯诺登曝光的文件，该局在驻日美军三泽、横田基地和冲绳汉森兵营都安排了网络监控人员，其中三泽基地内的安全行动中心通过“情妇行动”，依托 10 余个大型监控天线，监控亚太地区 16 颗目标卫星传输的通话、传真和互联网数据;通过代号“量子插入”的黑客行动，向监控对象所用电脑植入木马病毒，盗取有用情报。横田基地内有一处工程保障设施，专门用于制造和维护美国海外情报设施使用的监控天线。日本政府不仅承担该设施的建造费用(约 660 万美元)，还为该设施的工作人员发放工资（每年约 37.5 万美元）。在汉森兵营，也有美国国家安全局的大型监听站，主要用来搜集高频通信信号，该设施的建造费用(约 5 亿美元)同样由日本政府承担。

作为“投桃报李”，美国也对日本网络战建设提供了战略意见。去年底，日本政府基于美方建议，决定在自卫队内新设统管太空、网络空间和电子战部队的指挥机构——天网电司令部，进一步强化网络战的管理和统筹。