



美国国家安全局局长、网络司令部司令保罗·中曾根

美伊网络战的虚与实

三份网络战略报告都表明，美国国防部认定伊朗仅具备相对有限的网络攻防能力，对伊朗实施网络攻击和网络威慑，体现出美国政府的精心算计。

——汪晓风

在不时升级的“美伊较量”中，“网络战”成为关键词之一。

据美国《华盛顿邮报》报道，美国总统特朗普6月22日宣布对伊朗追加制裁，不久后，批准美军网络司令部对伊朗发动报复性网络攻击，目标是伊朗控制火箭和导弹发射的电脑系统。报道称，美方网络攻

击使伊朗这一武器系统“瘫痪”。

而据伊朗法尔斯通讯社报道，不清楚美方所谓网络攻击是否达到效果。报道暗示，美国媒体“虚张声势”，“旨在影响民意和挽回白宫丧失的名声”。

美方此番行动效果究竟如何，尚未有确切说法。但可以确定的是，这是继“震网

行动”（2010年）后美国针对伊朗的又一次重大网络行动。

而伊朗也不止一次声称挫败美国网络战。早在2009年，美国一家网络安全公司就把伊朗列为世界上最强大的五个网络大国之一。2015年又有消息称，伊朗开始制定全新网络安全战略。目前伊朗网络安全

伊朗与美国及其盟友的网络攻防博弈是一个长期过程,其对地区形势和国际安全将产生长期而深远的影响。

方面的实力到底有多强? 美伊网络战玄机几何?

美伊“网斗”由来已久

多年来,美国一直在探索打击伊朗关键目标的网络手段,对伊朗的关键信息系统和重要网络系统进行渗透,伊朗也力求通过网络途径进行适当防守反击。

美国极力阻止伊朗核能力尤其是武器化能力取得进展,这是美国对伊政策的重中之重。显然,作为高度机密和最高安全等级的核活动,无论是和平利用核能的核电活动,还是具有核武器意义的铀浓缩活动,都在严密监视和严格保护之下,支持研发和生产控制的计算机系统也是独立运行的。

据外媒报道,2010年,为了破坏伊朗核设施,美国和以色列情报部门联合研制了一款名为“震网”的计算机病毒,通过非常手段植入伊朗核设施的计算机系统,致使伊朗纳坦兹铀浓缩工厂约1/5的离心机

转速异常至报废,伊朗核计划因而遭受重挫。

据称美国和以色列还联手研发了一款名为“火焰”的计算机病毒,目标直指伊朗关键行业的网络系统,这是一种主要用于窃取计算机网络系统中的信息和数据的工具,该病毒被设计成主要在中东地区传播。

2016年,该病毒被网络安全公司发现,伊朗被迫暂时切断石油部门等关键基础设施与互联网的连接。不久,伊朗计算机应急响应部门发布一款能够检测和清除“火焰”病毒的软件,随后,“火焰”病毒制造者发出指令,令该病毒自毁消失,以避免外界对其追踪溯源。

伊朗网络战部队也频繁对美国目标实施网络攻击,显示伊朗政府在网络空间与美国对抗的实力和意图。2016年3月,美国司法部起诉7名伊朗黑客,指控他们实施了针对46家机构的网络攻击,引发美国公众对伊朗对美国发动更大规模网络攻击的担忧。这些攻击可以追溯到2013年,攻击对象包括美国和以色列的关键基础设施、科研机构、银行系统以及个

伊朗总统鲁哈尼5月8日发表电视讲话,宣布伊朗中止履行伊核协议部分条款,不再对外出售重水和浓缩铀。这张拍摄于2010年10月26日的照片显示的是伊朗布什尔核电站



人网络账户,造成了程度不同的系统瘫痪和数据损毁。

三份报告

美国和伊朗在地缘政治和网络空间进行复合博弈。地缘政治上,伊朗被美国认定为其主导地区秩序的挑战者,威胁美国及盟友安全。随着网络空间发展和国家安全议题的不断融合,美国不断渲染来自伊朗的网络威胁。

2011年7月,美国国防部推出网络空间行动战略报告称,“外国行为者针对美国公共和私营部门实施系统的网络空间活动,其数量和复杂程度不断增加。”报告认为,美国的经济、社会、军事运行日益依赖互联网,对美国怀有敌意的外国政府试图对其进行攻击。

作为反击手段,该战略强调变被动防御为主动防御,以更有效地阻止、击败针对美国网络系统的入侵和其他敌对行为,这一定程度上可以作为此前对伊朗核设施进行网络攻击的注脚,因为该战略所称主动防御包含针对对手的网络能力,开发具有攻击性的网络武器。

2015年4月,美国国防部发布网络战略报告,认为伊朗等国“拥有欠发达的网络能力,但对美国及美国在网络空间的利益表现出公开的敌意。”在该战略指导下,美国网络司令部重点提升网络威慑能力,并将网络空间的作战行动与其他领域的作战行动纳入联合作战体系,重点包括攻击并切断主要对手用于指挥控制的网络基础设施,并允许以传统军事手段应对网络攻击和以网络手段应对其他攻击的作战形式,其目标也包含对伊朗的“威胁”实施全方位打击的可行性。

2018年9月,美国国防部网络战略报告进一步指出,伊朗等国正在“利用恶意网络活动,伤害美国的公民并威胁美国的国家利益”。因而该战略提出了一个“防御前

置”概念,寻求提前制止、挫败针对美国利益的恶意网络活动。

美军6月份对伊朗控制火箭和导弹发射的电脑系统发动网络攻击,即是“防御前置”网络作战理念的实践,特朗普还为此签署一项行政命令,撤销奥巴马政府对攻击性网络行动附加的严格限制。

总体上看,美国将伊朗塑造成网络威胁重要来源,既是对伊朗实施全面威慑的重要手段,也是增强自身网络攻防能力的重要途径。三份网络战略报告都表明,美国国防部认定伊朗仅具备相对有限的网络攻防能力,对伊朗实施网络攻击和网络威慑,体现出美国政府的精心算计。

伊朗网络攻防能力

网络战能力是攻击和防御能力的组合,包括入侵敌方计算机网络系统、前沿部署和实施网络打击的攻击能力,以及进行入侵检测、阻遏攻击和应急恢复,保护对己方关键信息基础设施、重要网络系统和数据信息的防御能力。鉴于伊朗政府未进行相关披露,对伊朗网络战能力的评估和分析也就莫衷一是。综合各方信息,伊朗网络战能力大致可从“三个来源”作出评判。

第一个来源是伊朗伊斯兰革命卫队的网络战分支。情报搜集是伊朗伊斯兰革命卫队的重要职能之一,与其他国家情报机构在网络领域的优势一样,伊朗伊斯兰革命卫队也掌握了从事网络战所必备的人员、技术和设施,其任务是进行网络攻击及防止对伊朗关键计算机网络系统的攻击。

2011年12月,在伊朗东北部,美国一架RQ-170无人机的指挥控制信号被接管而落入伊朗之手,据信这是伊朗伊斯兰革命卫队网络战部队的“杰作”。伊朗伊斯兰革命卫队还与网络安全与通信领域的公司发展合作,致力于构建一个不断扩大的合作网络,主要目标是抵御美国的网络攻击和攻击美国的网络信息系统。

第二个来源是黑客行动主义者群体。这是一些分散的个人黑客或黑客组织,他们得到伊朗政府默许或支持,必要时被组织起来对特定目标发动网络攻击。这些黑客参与政府网络作战的外围和支持工作,对于一些需要人海战术的攻击而言,是一支不可忽视的作战力量。

如一个名为“Ashiyaneh”的黑客组织,自称对2010年千余个美国、英国和法国的网站被黑负责。这支力量日常活跃在网络社交媒体和论坛上,开展发送虚假信息和钓鱼式攻击等活动。

第三个来源是一个名为“伊朗网络军”的神秘组织。自2005年公开活动以来,以“伊朗网络军”名义发动的网络窃密和网络攻击活动接连不断,攻击目标不仅包括美国和以色列,还涉及极端组织“伊斯兰国”和一些逊尼派组织。对于“伊朗网络军”的来源和构成也有各种说法。2010年,一名自称代表“伊朗网络军”的成员将其描述为一群黑客志愿者,然而伊朗伊斯兰革命卫队一名军官很快回应,称“伊朗网络军”是他们创建,是一支负责防御网络攻击的网络军事部队。

伊朗政府并不热衷于将自身网络作战实力示人,也刻意隐匿其网络空间的战略意图。北约卓越合作网络防御中心是网络安全和网络防御的专门研究机构,长期跟踪全球网络安全战略或网络国防战略态势,该中心网站信息显示,迄今已有80多个国家推出了国家网络安全战略,而伊朗并不在其列。

尽管2015年1月就有媒体报道称,伊朗正在制定一项新的网络安全战略,但迄今仍未见正式文本,这更为伊朗的网络战攻防能力增添了神秘色彩。无论如何,伊朗与美国及其盟友的网络攻防博弈是一个长期过程,其对地区形势和国际安全将产生长期而深远的影响。G

(作者系网络安全问题专家、复旦大学国际问题研究院副研究员)