2022年9月13日 星期二 责编:张亮 万建刚 美编:雷林燕 审读:邱立波

大讲堂

“护国隐士”与“黑客帝国”

西工大著名的“为国铸剑,隐姓埋名”雕塑。
图据西北工业大学官方微博

2022年9月5日,国家计算机病毒应急处理中心和360公司分别发布了关于西北工业大学(以下简称西工大)遭受境外网络攻击的调查报告。报告发现美国国家安全局(NSA)下属的特定入侵行动办公室(TAO)多年来对我国国内的网络目标已经实施了上万次的恶意网络攻击,控制了相关网络设备,疑似窃取了大量高价值数据。

此次网络恶意攻击中,美国国家安全局先后使用了54台跳板机和代理服务器,分布在日本、韩国、瑞典、波兰等17个国家,其中70%位于中国周边。其中,用以掩盖真实IP的跳板机都是精挑细选的,所有的IP都属于非“五眼联盟”国家。攻击手段也极其狡猾。技术团队将本次攻击活动所使用的武器类别分为四大类,包括漏洞攻击突破类武器、持久化控制类武器、嗅探窃密类武器、隐蔽消痕类武器。先后使用了41种专用网络攻击武器设备,仅后门工具“狡诈异端犯”就有14款不同版本。

美国国家安全局妄图窃取西工大的关键网络设备配置、网管数据、运维数据和核心技术数据,对西工大的持续网络攻击正是后冷战时代网络战争的缩影。在这条看不见的战线上,各国依托互联网平台,以新兴信息手段,围绕国家利益展开激烈交锋。

为什么美国对这所深居西北的高校虎视眈眈?网络攻击无所不用其极,美国究竟是何居心?让我们一起来认识一下这座位于古城西安的“护国隐士”。

主讲人
惠贞书院
孙鋆

参考资料
西北大学官网
新华社、人民网

护国隐士,为国铸剑

西北工业大学的诞生,始于卢沟桥事变。为躲避战火,以国立北平大学、国立北平师范大学、国立北洋工学院以及北平研究院为代表的一众平津高校,几经坎坷,最后转移到了陕西汉中,改名组建为“国立西北联合大学”。

1938年“西北联大”拆分出的西北工学院就是如今西北工业大学的前身。抗战胜利后,国立西北工学院保留建制;中华人民共和国成立后,国立西北工学院改名西北工学院,合并华东航空学院,正式成立“西北工业大学”。1961年,西北工业大学划归国防部国防科学技术委员会管理,被确定为国防工业院校,成为“国防七子”(又称“国防七校”,指的是工信部直属的七所工业高校、包括了北京理工大学、北京航空航天大学、南京理工大学、南京航空航天大学、哈尔滨工业大学、哈尔滨工程大学以及西北工业大学)之一。

西北工大科研实力极其强悍,材料科学、工程学、化学、计算机科学、物理学、地球科学、数学7个学科进入ESI国际学科排名前1%;而在航空、航天方面,更是一枝独秀。

2019年建国70周年阅兵仪式上,西北工业大学就骄傲地宣称:“天上飞的都被我们承包了。”这句话当之无愧。国产大型喷气式民用飞机C919、国产隐形第五代制空战斗机歼-20、新一代国产军用大型运输机运20、战略轰炸机轰20、战术通用直升机直20、ARJ21支线客机、CR929远程宽体客机,这些“大国飞机”,总设计师或常务设计师都来自西北工业大学,号称“军机三总师”。其中歼-20总设计师杨伟、运-20总设计师唐长红,以及歼-15常务副总师赵霞,同为西北工业大学空气动力学78级的同班同学,被称为“一小班三总师”。不单是飞机,新一代大涵道比涡扇发动机、可用于大型客机及运输机的涡扇15,其总设计师程荣辉也同样是西工大校友。

不仅是飞机,在导弹、火箭等领域,西北工业大学也颇有成就。在8月进行的南海实射训练中,南部战区海军航空兵先后发射了数十枚空空导弹,这种由飞机携带、攻击空中目标的导弹,是歼击机的主要武器之一。而我国空空导弹研究院的总设计师樊会涛,毕业于西北工业大学航空发动机专业。

在航天领域,西工大曾重点参与载人航天与探月、神舟系列飞船研制等航天项目,是“为中国首次载人航天飞行作出贡献单位”的两所高校之一;在航空领域,一半以上的重大型号总师、副总师是西工大校友,西工大也被社会誉为“总师摇篮”;在航海领域,同样有大批西工大校友活跃在船舶工业、水中兵器行业的重要管理岗位与核心技术岗位上……。

据不完全统计,在西工大为国防科技事业发展和国民经济建设输送的20多万名毕业生中,走出了65位共和国将军、48位两院院士,还有6位中国十大杰出青年。尤其在航空、航天、航海“三航”领域,出身西工大的工程师更是众星云集。

西工大毕业生的卓越表现被人们称为“西工大现象”。在这种现象背后,是一代又一代西工大学子公为天下、报效祖国的坚定信念:在艰苦的国防攻坚任务面前,西工大学子不退缩;在成果展现之后,为了国防事业的保密性,选择隐姓埋名,就像母校一样,深藏于古都西安的黄土之中。国之大事,在祀与戎。护国隐士,为国铸剑。

黑客帝国的“不存在局”

西北工业大学的遭遇,仅是美国对华大肆网络攻击窃密的冰山一角。长期以来,为达到美国政府情报收集目的,美国国家安全局针对全球发起大规模网络攻击,我国正是重点攻击目标之一。

美国国家安全局全名为:national security agency,隶属于美国国防部,因其特殊性质,英文世界中戏称其为不存在局(no such agency)。事实上,该局的存在直到1975年才得以披露。这个部门承担的任务是出于情报或反情报目的,对信息和数据进行全球监控收集和处理,专职“信号情报”(对应传统的“人力情报”)。在互联网时代前,该局专职无线电通讯的信号识别和拦截。现在,专职对网络空间内的信息与数据进行拦截与识别。

在大肆渲染敌对国家网络攻击的背景下,美国才是当之无愧的“黑客帝国”。“棱镜计划”“怒角计划”“星风计划”“强健计划”“上游计划”“电幕行动”……随着一件件丑闻的曝光,在引发国际舆论哗然的同时,美国维持其网络霸权的野心也暴露无遗。

2013年的“斯诺登事件”让国际社会得以一窥其伪善的真面目。NSA前外包技术员斯诺登曝光美国政府广泛进行网络监听,甚至连自己的盟国都不放过。

此外,NSA还长期“偷窥”及收集通信行业存储的大量个人信息及行业关键数据,导致全球数亿公民隐私和敏感信息无处藏身,犹如“裸奔”,其公民身份、财产、家庭住址、甚至通话录音等数据面临恶意采集、非法滥用、跨境流出的严重威胁。

当今世界,百年变局叠加世纪疫情,国际形势可谓是波诡云谲。在此背景之下,网络空间安全威胁是世界各国所面临的共同挑战,维护网络安全,保障公民人权已经成为了国际社会的共识。

9月5日,外交部发言人毛宁在例行记者会上回答有关提问时表示,美方行径严重危害中国国家安全和公民个人信息安全。中方强烈谴责,要求美方作出解释并立即停止不法行为。

网络空间安全威胁是各国面临的共同挑战,维护网络安全是国际社会的共同责任。中国坚持和平利用网络空间,愿同国际社会一道,加强对话与合作,共同反对网络霸权,共同应对各类网络攻击,维护和平、安全、开放、合作、有序的网络空间,推动建立多边、民主、透明的全球互联网治理体系,携手构建网络空间命运共同体。