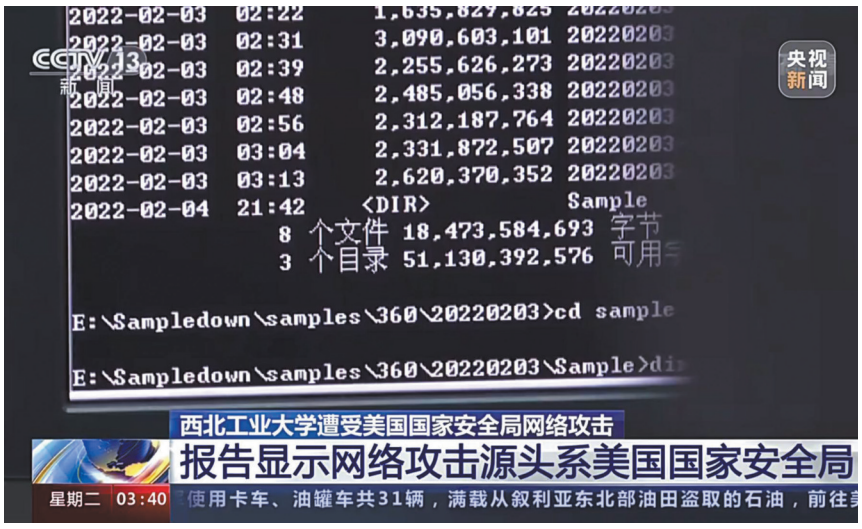
以假邮件“钓鱼”，美国使用41种网络武器攻击西北工业大学

揭开“黑客帝国”虚伪面纱

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遭受美国国家安全局网络攻击的调查报告，美国国家安全局（NSA）下属的特定入侵行动办公室（TAO）使用了40余种不同的专属网络攻击武器，持续对西北工业大学开展攻击窃密，窃取该校关键网络设备配置、网管数据、运维数据等核心技术数据。

作为拥有最强大网络技术实力的国家，美国以“国家利益”为幌子，违反国际法和国际关系基本准则，无视基本道德信义，对他国实施大规模网络窃密与监听监控，严重损害他国国家安全和公民个人信息安全。“网络霸凌”大国的种种行径，暴露了美国才是全球网络空间不安全的罪魁祸首。



调查报告披露，美国国家安全局(NSA)下属的特定入侵行动办公室(TAO)先后使用41种专用网络攻击武器，对西北工业大学发起上千次攻击，窃取了一批核心技术数据。 央视视频截图

以假邮件“钓鱼”

美国使用41种网络武器攻击西北工业大学

电子邮件，这一高校师生频繁使用的通信工具，竟被美国无底线地利用了。

今年4月，西北工业大学就电子邮件系统遭受钓鱼邮件攻击的情况报警称，发现一批以科研评审、答辩邀请和出国通知等为主题的钓鱼邮件，内含木马程序，引诱部分师生点击链接，非法获取师生电子邮箱登录权限，致使相关邮件数据出现被窃取风险。同时，部分教职工电脑也存在遭受网络攻击的痕迹。

西北工业大学位于西安，隶属于工业和信息化部，是我国从事航空、航天、航海工程教育和科学研究领域的重点大学，拥有大量国家顶级科研团队和高端人才，承担国家多个重点科研项目。接到报警后，西安市公安机关高度重视，组织警力与网络安全技术专家成立联合专案组对此案进行立案侦查。国家计算机病毒应急处理中心和360公司联合组成技术团队，全程参与了此案的技术分析工作。

技术团队先后从西北工业大学的多个信息系统和上网终端中提取到了多款木马样本，综合使用国内现有数据资源和分析手段，并得到了欧洲、南亚部分国家合作伙伴的通力支持，全面还原了相关攻击事件的总体概貌、技术特征、攻击武器、攻击路径和攻击源头。调查显示，美国国家安全局持续对西北工业大学开展攻击窃密，窃取该校关键网络设备配置、网管数据、运维数据等核心技术数据。美方先后使用了41种专用网络攻击武器装备，仅后门工具“狡诈异端犯”就有14款不同版本。

技术团队将此次攻击活动中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。

“最开始使用漏洞攻击突破类武器，突破之后投送第二类持久化控制类的武器工具。接着使用第三类嗅探窃密类武器，长期潜伏窃取我们重要的数据。当认为任务已经完成之后，开始使用第四类隐蔽消痕类武器，把现场清理干净，让被害人无法察觉。”国家计算机病毒应急处理中心高级工程师杜振华介绍。

美国国家安全局特定入侵行动办公室成立于1998年，是目前美国政府专门从事对他国实施大规模网络攻击窃密活动的战术实施单位，由2000多名军人和文职人员组成，下设10个处室。为了隐匿对西北工业大学等中国信息网络实施网络攻击的行为，美方做了长时间准备工作，并且进行了精心伪装。

调查显示，特定入侵行动办公室在针对西北工业大学的网络攻击行动中先后使用了54台跳板机和代理服务器，主要分布在日本、韩国、瑞典、波兰、乌克兰等17个国家，其中70%位于中国周边国家，如日本、韩国等。其中，用以掩盖真实IP的跳板机都是精心挑选，所有IP均归属于非“五眼联盟”国家。

技术团队通过威胁情报数据关联分析，发现针对西北工业大学攻击平台所使用的网络资源共涉及5台代理服务器，NSA通过秘密成立的杰克·史密斯咨询公司、穆勒多元系统公司这两家掩护公司向美国泰瑞马克公司购买了埃及、荷兰和哥伦比亚等地的IP地址，并租用一批服务器。

“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。”9月5日，外交部发言人毛宁表示。

为达收集情报目的

美国国家安全局针对全球发起大规模网络攻击

美国在全球实施大规模、有组织、无差别的网络窃密、监控和攻击，是名副其实的“黑客帝国”“窃密帝国”。

西北工业大学的遭遇，仅是美国对华大肆网络攻击窃密的一个缩影。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。

2月23日，北京奇安盘古实验室披露了隶属于美国国安局的黑客组织“方程式”利用顶级后门对包括中国、俄罗斯等全球45个国家和地区开展长达十几年的“电幕行动”网络攻击，涉及的机构目标包括知名高校、科研机构、通信行业、政府部门等。

3月2日，360公司发布的报告披露，美国国安局利用网络武器对中国等全球47个国家及地区的403个目标开展网络攻击，数十年不曾停歇。

此次关于西北工业大学遭受境外网络攻击的调查报告还发现，美国国家安全局还利用其控制的网络攻击武器平台、“零日漏洞”和网络设备，长期对中国的手机用户进行无差别的语音监听，非法窃取手机用户的短信内容，并对其进行无线定位。

长期以来，美国滥用其技术优势，在全球范围内实施大规模、有组织、无差别的网络窃密、监控和攻击，手段包括利用模拟手机基站信号接入手机盗取数据，操控手机应用程序、侵入云服务器，通过海底光缆进行窃密，在美国近100所驻外使领馆内安装监听设备对驻在国进行窃密等等，是名副其实的“黑客帝国”“窃密帝国”。

2013年，美国防务承包商前雇员斯诺登曝光了美国政府大规模网络监控的丑闻。美国国家安全局代号为“棱镜”的全球秘密监听项目24小时运行，对电子邮件、脸谱网消息、谷歌聊天、Skype网络通话等进行监听监控。

美国实施的是无差别监视监听，从竞争对手到盟友，无不在其监听范围之内。“维基揭秘”网站在2015年爆料，从上世纪90年代起，德国经济、财政和农业等部门就进入了美国的监听范围。2006年至2012年间，美国国家安全局对法国总统、多名部长、法国驻美国大使等政界要员进行监听，其中包括希拉克、萨科齐和奥朗德3任法国总统，以获取施政纲领、对外政策等情报。

2020年，“瑞士加密机”事件浮出水面。美国中央情报局自二战后长期控制一家瑞士全球加密机公司，该公司售往全球一百多个国家的加密设备都被CIA植入了后门程序，用来破解各国发送加密信息的代码，借此窃取多国机密。

去年，丹麦媒体曝光了美国国家安全局利用同丹麦情报部门的合作关系，监听包括德国前总理默克尔在内的欧洲国家领导人和高级官员。

除了竞争对手和盟友，监控窃听的“天罗地网”连美国国内的民众也不放过。

近日，美国乔治城大学隐私与技术法律中心公布一份名为《美国的天罗地网：21世纪数据驱动下的驱逐》的报告。报告显示，美国入境和海关执法局精心设计了一张复杂而庞大的监视网络，可以监视生活在美国的大多数人，且无需获得许可。美国国家情报总监办公室今年4月发布的年度报告显示，过去一年，美国联邦调查局在没有搜查令的情况下，对美国民众的电子数据进行了多达340万次的搜查。

“今天美国人越来越多地把监控手段应用到全球其他地区。”美国凯斯西储大学法学教授科弗警告说：“现在我们面对的是监控工业复合体。”

据中央纪委国家监委网站

我国成功发射遥感三十五号05组卫星

9月6日12时19分，我国在西昌卫星发射中心使用长征二号丁运载火箭，成功将遥感三十五号05组卫星发射升空。卫星顺利进入预定轨道，发射任务获得圆满成功。

遥感三十五号05组卫星主要用于科学试验、国土资源普查、农产品估产及防灾减灾等领域。

这次任务是长征系列运载火箭第436次飞行。 **据新华社**

教育部要求严厉打击隐形变异违规校外培训

记者6日从教育部获悉，教育部日前召开2022年全国“双减”工作秋季学期视频调度会，强调严厉打击隐形变异违规校外培训，形成警示震慑。

据了解，教育部在视频调度会上强调，各地要充分认识校外教育培训治理工作的复杂性、艰巨性和长期性，系统破解难题，构建长效机制，严厉打击隐形变异培训，让违规机构和个人无处遁形。要强化非学科类培训监管，促进其成为学校教育的有益补充。同时，要扎实做好预收费资金监管，切实做到校外培训机构全部纳入监管、资金全额纳入监管，坚决维护群众利益。要健全校外培训执法体系，加大行政执法力度，严肃查处违规行为。 **据新华社**

美国法官批准任命独立专员审查海湖庄园查获物件

美国佛罗里达南区联邦地区法院法官艾琳·坎农5日批准任命一名独立专员，审查联邦调查局人员从前总统特朗普住所海湖庄园查获的物件。

坎农在一项法庭命令中说，这名独立专员将负责审查海湖庄园查获物件中个人物品、文件，以及可能涉及律师与客户保密特权或行政特权的材料。

坎农还暂时叫停美国司法部出于调查目的审查或使用从海湖庄园查获的物件，以待该独立专员完成审查。美国司法部和特朗普律师被要求不晚于9日联合提交独立专员人选名单等。

8月8日，美国联邦调查局人员在位于佛罗里达州棕榈滩的海湖庄园执行搜查令。据近期被授权解封的信息，查获物件中有超过1.1万份政府文件和照片，其中100余份标有密级，54份为“秘密”、31份为“机密”、18份为最高级别的“绝密”。

特朗普否认有不当行为，指责联邦调查局及该机构上级美国司法部出于政治目的搜查海湖庄园，称查获物件中有一些材料受律师与客户保密特权和行政特权保护，主张任命独立专员进行审查。

美国司法部认为让独立专员介入将减缓调查进程，同时强调特朗普已无权主张行政特权。

据新华社