西北工业大学遭美国国家安全局网络攻击调查报告披露：

13名攻击者真实身份已成功查明

今年6月22日，西北工业大学发布《公开声明》称，该校遭受境外网络攻击，随后西安警方对此正式立案调查，中国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，并于9月5日发布了第一份“西北工业大学遭受美国NSA网络攻击调查报告”，调查报告指出此次网络攻击源头系美国国家安全局（NSA）下属的特定入侵行动办公室（TAO）。27日，技术团队再次发布相关网络攻击的调查报告，报告披露，特定入侵行动办公室（TAO）在对西北工业大学发起网络攻击过程中构建了对我国基础设施运营商核心数据网络远程访问的（所谓）“合法”通道，实现了对我国基础设施的渗透控制。

此次调查报告显示，美国国家安全局（NSA）下属的特定入侵行动办公室（TAO）对他国发起的网络攻击技战术针对性强，采取半自动化攻击流程，单点突破、逐步渗透、长期窃密。

研究团队经过持续攻坚，成功锁定了TAO对西北工业大学实施网络攻击的目标节点、多级跳板、主控平台、加密隧道、攻击武器和发起攻击的原始终端，发现了攻击实施者的身份线索，并成功查明了13名攻击者的真实身份。

调查报告显示，研究团队发现，攻击者武器操作失误暴露工作路径。央视视频截图

关注1
TAO攻击渗透西北工业大学有哪些流程？

调查报告显示，经过长期的精心准备，TAO使用“酸狐狸”平台对西北工业大学内部主机和服务器实施中间人劫持攻击，部署“怒火喷射”远程控制武器，控制多台关键服务器。利用木马级联控制渗透的方式，向西北工业大学内部网络深度渗透，先后控制运维网、办公网的核心网络设备、服务器及终端，并获取了部分西北工业大学内部路由器、交换机等重要网络节点设备的控制权，窃取身份验证数据，并进一步实施渗透拓展，最终达成了对西北工业大学内部网络的隐蔽控制。

TAO将作战行动掩护武器“精准外科医生”与远程控制木马NOPEN配合使用，实现进程、文件和操作行为的全面“隐身”，长期隐蔽控制西北工业大学的运维管理服务器，同时采取替换3个原系统文件和3类系统日志的方式，消痕隐身，规避溯源。TAO先后从该服务器中窃取了多份网络设备配置文件。利用窃取到的配置文件，TAO远程“合法”监控了一批网络设备和互联网用户，为后续对这些目标实施拓展渗透提供数据支持。

TAO通过窃取西北工业大学运维和技术人员远程业务管理的账号口令、操作记录以及系统日志等关键敏感数据，掌握了一批网络边界设备账号口令、业务设备访问权限、路由器等设备配置信息、FTP服务器文档资料信息。根据TAO攻击链路、渗透方式、木马样本等特征，关联发现TAO非法攻击渗透中国境内的基础设施运营商，构建了对基础设施运营商核心数据网络远程访问的“合法”通道，实现了对中国基础设施的渗透控制。

TAO通过掌握的中国基础设施运营商的思科PIX防火墙、天融信防火墙等设备的账号口令，以“合法”身份进入运营商网络，随后实施内网渗透拓展，分别控制相关运营商的服务质量监控系统和短信网关服务器，利用“魔法学校”等专门针对运营商设备的武器工具，查询了一批中国境内敏感身份人员，并将用户信息打包加密后经多级跳板回传至美国国家安全局总部。

关注2
TAO在攻击过程中是怎么暴露身份的？

TAO在网络攻击西北工业大学过程中，暴露出多项技术漏洞，多次出现操作失误，相关证据进一步证明对西北工业大学实施网络攻击窃密行动的幕后黑手即为美国国家安全局。

首先，攻击时间完全吻合美国工作作息时间规律。TAO在使用tipoff激活指令和远程控制NOPEN木马时，必须通过手动操作，从这两类工具的攻击时间可以分析出网络攻击者的实际工作时间。其次，语言行为习惯与美国密切关联，技术团队在对网络攻击者长时间追踪和反渗透过程中发现，攻击者具有以下语言特征：攻击者有使用美式英语的习惯；与攻击者相关联的上网设备均安装英文操作系统及各类英文版应用程序；攻击者使用美式键盘进行输入。第三，攻击者武器操作失误暴露工作路径。第四，大量武器与遭曝光的美国国家安全局武器基因高度同源。此次被捕获的、对西北工业大学攻击窃密中所用的41款不同的网络攻击武器工具中，有16款工具与“影子经纪人”曝光的TAO武器完全一致；有23款工具虽然与“影子经纪人”曝光的工具不完全相同，但其基因相似度高达97%，属于同一类武器，只是相关配置不相同；另有2款工具无法与“影子经纪人”曝光工具进行对应，但这2款工具需要与TAO的其他网络攻击武器工具配合使用，因此这批武器工具明显具有同源性，都归属于TAO。技术团队综合分析发现，在对中国目标实施的上万次网络攻击，特别是对西北工业大学发起的上千次网络攻击中，部分攻击过程中使用的武器攻击，在“影子经纪人”曝光NSA武器装备前便完成了木马植入。按照美国国家安全局的行为习惯，上述武器工具大概率由TAO雇员自己使用。 **据央视**

“鲲龙”AG600M飞机完成12吨投汲水试验

9月27日，由我国自主研制的“鲲龙”AG600M飞机以全新消防涂装在湖北荆门漳河机场成功完成12吨投汲水试验，接下来将全面转入适航取证阶段。

27日上午10时许，满载12吨水的AG600M飞机从漳河机场跑道陆上起飞，在投水区域前完成投水后平稳降落在漳河水库，在水面高速滑行15秒完成12吨汲水，随即腾空而起，在空中完成一系列既定试飞科目后，在投水区域再次投水后降落漳河水库。整个试验过程飞机状态良好，各系统运行稳定，投水精准度及投水量满足设计目标。

AG600飞机是为满足我国应急救援体系和国家自然灾害防治体系建设需要研制的重大航空装备，是我国首次按照民用适航标准研制的大型特种飞机。AG600M是AG600的优化机型，最大起飞重量60吨，最大载水量12吨，最小平飞速度220千米每小时，航程4500千米，具备优越的低空、低速、短距起降性能。

本次试验有效评估了飞机的投水灭火效果，是AG600M飞机服务我国应急救援体系、国家自然灾害防治体系建设的关键一步和必备环节。试验活动现场，航空工业通飞华南公司与光大金租签署了4架AG600M飞机购机协议和支持AG600飞机研制的融资协议，与河南航投签署2架意向购机协议。 **据新华社**

意大利政局“右转”会带来哪些影响？

意大利内政部26日发布了对99%选票的计票结果，焦尔吉娅·梅洛尼领导的意大利兄弟党得票率约为26%，成为议会第一大党。同时，意大利兄弟党所在的中右翼政党联盟得票率约为44%，领先其他党派或党派联盟。

分析人士指出，意大利中右翼政党联盟能否给出解决经济与民生困局的可行方案受到各方关注。同时，由于意大利兄弟党等右翼党派长期持“疑欧”立场，欧盟一些官员和学者对意大利未来政策走向感到担忧。

中右翼党派联盟主要由意大利兄弟党、前副总理萨尔维尼领导的联盟党和前总理贝卢斯科尼领导的意大利力量党组成。选举前，中右翼政党联盟达成约定，将支持得票最多政党的领导人担任总理一职。这意味着，梅洛尼可能出任总理。

根据意大利宪法，政府总理人选须由总统提名，而后需要在议会通过信任投票才能上任。意大利《晚邮报》报道，意总统马塔雷拉将于10月24日会见新一届议会两院主席与主要党派领导人，这个过程将持续两至三天，之后宣布其提名的总理人选。此后，各党派将通过谈判来推举内阁部长人选，这一过程最长可能耗时数月。

鉴于意大利右翼政党长期持“疑欧”立场，其未来上台后有可能带来的政策变化引发欧盟官员和学者担忧。此前，梅洛尼曾批评欧盟的官僚主义作风，认为欧盟不允许成员国捍卫自身利益，意大利应在欧盟与北约等组织中保持相对独立地位。

分析人士指出，欧洲右翼势力的抬头并不只是出现在意大利，在本月早些时候的瑞典议会选举中，右翼政党民主党成为第二大党。在新冠疫情、乌克兰危机升级等多重因素冲击下，欧洲的能源危机、通胀难题与民生困境不断加剧，并正在对一些国家的政治生态产生越来越大的影响。如果这一趋势延续下去，欧洲的稳定与欧盟的团结都将经受严峻考验。 **据新华社**

白杰品股

收复失地

问：周二沪指高开，盘中震荡走高，收盘上涨，你怎么看？

答：受央行利好消息提振，市场小幅高开，随后持续震荡走高，沪指结束4连跌，创业板指表现最好，收涨2.23%。盘面上，大消费、医药板块全面回暖，北上资金净买入约33亿元。截至收盘，两市涨停70只，跌停1只。技术上看，沪深股指均收复5日均线，两市合计成交6662亿元环比略减；60分钟图显示，各股指均收复5小时均线，60分钟MACD指标均呈现出金叉状态；从形态来看，虽然沪指本周连续两日刷新本轮调整低点，但最终如预期反包收复失地，这也不影响其他股指在上周五这个时间窗口出现了趋势转折。短期来看，缩量上涨反映出市场惜售心态，后市仍有继续上攻动能，若创业板指能快速收复60小时均线，则后市反弹能看高一线。期指市场，各期指合约累计成交、持仓均减少，各合约负溢价水平整体有所增加。综合来看，连板个股数量萎缩至极致数年来罕见，受益于利好组合拳不断，短期市场风险偏好有所修复，后市成交的恢复仍需连阳的刺激。

资产：周二按计划持股。目前持有华创阳安（600155）99万股，五粮液（000858）3.5万股，康芝药业（300086）83万股，新希望（000876）24万股，康达新材（002669）28万股。资金余额4800163.39元，总净值28956713.39元，盈利14378.36%。

周三操作计划：五粮液、康达新材、新希望、康芝药业、华创阳安拟持股待涨。 **胡佳杰**