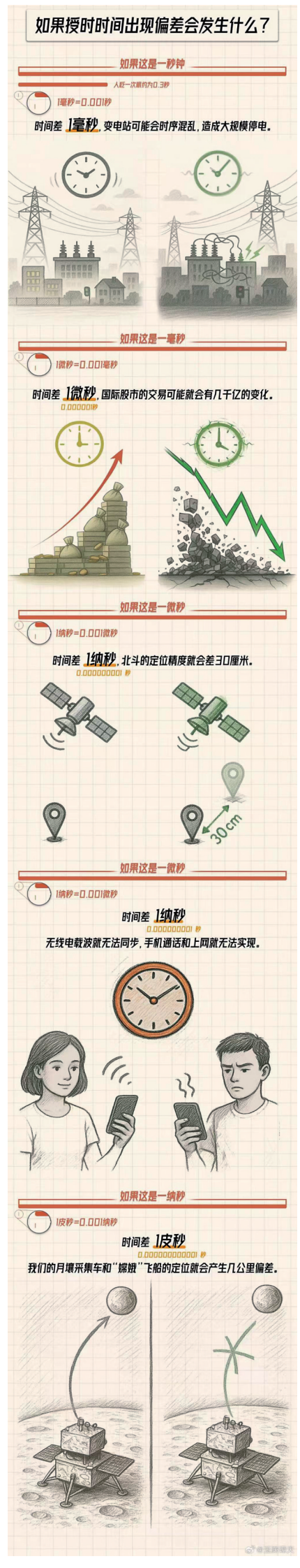
近期，国家安全机关破获一起美国重大网络攻击案，掌握美国国家安全局网络攻击入侵中国国家授时中心的铁证，粉碎美方网攻窃密和渗透破坏的图谋，全力守护“北京时间”安全。

○利用某境外品牌手机短信服务漏洞，秘密网攻控制工作人员手机终端
○窃取手机内存储的敏感资料
○利用窃取的登录凭证，入侵国家授时中心计算机

美国安局42款武器 网攻国家授时中心 妄图瘫痪“北京时间”



国之重器 不容有失

被美国情报机关长期网络攻击入侵的国家授时中心都有哪些职能？在国际上的地位和作用如何？

据专家介绍，中国科学院国家授时中心原名陕西天文台，位于陕西省西安市，成立于1966年，承担着国家标准时间，也就是“北京时间”的产生、保持和发播任务。为国家通信、金融、电力、交通、测绘、国防等行业领域提供高精度授时服务，还为测算国际标准时间提供重要数据支撑。高精度的国家标准时间是现代社会运行的基础，没有哪个物理量能像时间这样既维系着经济社会的精密运转，又支撑着亿万人的协同生活，还保障着科学研究的顺利进行。

国家授时中心自主研发了世界领先的时间自主测量系统，还建设有国家重大科技基础设施——高精度地基授时系统，相关设施一旦遭受网攻破坏，将影响“北京时间”的安全稳定运行，引发网络通信故障、金融系统紊乱、电力供应中断、交通运输瘫痪、空天发射失败等严重后果，甚至可能导致国际时间陷入混乱，危害损失难以估量。

中国科学院国家授时中心综合办公室副主任魏栋表示，时间差一毫秒，变电站就会时序混乱，造成大面积的停电。时间差一微秒，国际股市的交易就可能会有几千亿的变化。时间差一纳秒，也就是10亿分之一秒，北斗的定位精度就会差30厘米，同时也会影响到人们日常通信，无线电载波无法同步，手机通话和上网无法实现。时间差一皮秒，也就是10万亿分之一秒，月壤采集车和嫦娥飞船的定位就会产生几公里的偏差，可能造成“嫦娥”无法成功返回。

国际标准时间是综合各国时间后得出的。国家授时中心产生和保持的国家标准时间准确度长期位居世界前列。从2024年1月到现在，我国的准确度排名世界第一。从2021年起，我国自主研制的各类原子钟相继被国际权度局测试认可，用于国际标准时间的产生。

魏栋介绍，我国在国际标准时间计算中的权重也稳步提高，从2021年的5.66%提升到了目前的19.51%，达到了世界第二。

目前国家授时中心正在建设国家重大科技基础设施，高精度地基授时系统，以提高我国授时系统的安全性、可靠性和授时精度，更好地服务于国民经济和国家发展。

机关算尽 原形毕露

国家安全机关介绍，经调查，美方针对国家授时中心的网络攻击活动长期蛰伏、高度隐匿，甚至动用了国家级网络间谍武器，呈现递进式、体系化特点。这种刺探和入侵，从一开始就被国家安全机关察觉和掌握。

2022年3月25日起，美国安局利用某境外品牌手机短信服务漏洞，秘密网攻控制国家授时中心多名工作人员的手机终端，窃取手机内存储的敏感资料。

2023年4月18日起，美国安局多次利用窃取的登录凭证，入侵国家授时中心计算机，刺探该中心网络系统建设情况。

上海交通大学信息内容分析技术国家工程中心主任李建华介绍，美国安局窃取了多名工作人员的手机的一些资料，同时通过远控也获取了多名工作人员合法登录的权限，渗透到我们国家授时中心的内网。第二个阶段通过了利用高强度的武器平台，组合了大量的恶意代码、间谍软件等等网络攻击武器，对于国家授时中心的专网信息系统，实施高强度的渗透和攻击，对于国家授时中心的重要信息系统的资料，包括信息和数据实施了窃取。

2023年8月至2024年6月，美国安局专门部署新型网络作战平台，启用42款特种网攻武器，对国家授时中心多个内部网络系统实施高烈度网攻，并企图横向渗透至高精度地基授时系统，预置瘫痪破坏能力。

见招拆招 斩断链路

国家安全机关见招拆招，固定美方网攻证据，指导国家授时中心开展清查处置，斩断攻击链路，升级防范措施，消除危害隐患。

国家安全机关分析发现，美方网攻活动大多发生在北京时间深夜至凌晨，利用美国本土、欧洲、亚洲等地的虚拟服务器作为“跳板”，以此隐藏攻击源头，还使用了高强度的加密算法擦除攻击痕迹。

国家安全机关长期跟踪，多次阻断美方攻击链路，固定了美方网攻证据，并指导国家授时中心开展清查处置，升级防范措施。

李建华介绍，美方采用的“跳板”技术，也就是说作为美国情报机构，它在欧洲、在亚洲甚至在非洲，在我们周边的很多国家都部署了大量称为跳板的主机服务器。在它的攻击渗透过程当中，还大量地采用“零日漏洞”，包括“横向提权”和“跨网渗透”等技术，突破重要信息系统的入侵检测系统。

专家介绍，美方实施的网络攻击是一种典型的国家级网络攻击，国际上将这一行为简称APT，也就是高级持续性威胁攻击。

李建华表示，目前的网络攻击呈现APT化的特点，它的目标和任务是监控其他一些国家的重要基础设施，包括关键的重要信息系统，这样一种监控和远程的渗透乃至干扰、摧毁和破坏。这个是对国际上面任何一个国家来讲，在经济全球化这样一个大时代面前都是一个巨大的威胁。

军地创新服务专业委员会专家组副组长金飞指出，美国的攻击是系统性的战略行为，其目的是延缓中国的和平崛起，为中国的经济建设和社会发展制造更大的障碍，维持其在国际上的霸权。

专家介绍，一些国家实施的高级持续性网络威胁攻击，严重危害全球网络空间安全，对网络空间互信机制造成破坏，国际社会应有效约束这种“数字霸权”行为。

贼喊捉贼 霸权嘴脸

近年来，美国强推网络霸权，一再践踏国际网络空间规则。以美国安局为首的间谍情报机关任性妄为，持续针对中国、东南亚、欧洲及南美洲等地实施网攻活动，入侵控制关键基础设施，窃取重要情报，监听重点人员，肆意侵犯他国网络主权和个人隐私，严重危害全球网络空间安全。

美方还惯于利用其在菲律宾、日本以及中国台湾省等地的技术阵地发动网攻，从而达到隐藏自身、嫁祸他人的目的，可谓损招用尽。

同时，美方还贼喊捉贼，屡屡渲染“中国网络威胁论”，胁迫他国炒作所谓“中国黑客攻击事件”，制裁中国企业，起诉中国公民，妄图混淆视听，颠倒黑白。铁的事实证明，美国才是真正的“黑客帝国”，是网络空间的最大乱源。

相关提醒

国家安全机关提示

国家安全机关依法防范打击网络间谍活动，对国内机关、团体、企业事业组织和其他社会组织开展反间谍安全防范指导和检查。关键基础设施运营者要履行本单位反间谍安全防范工作主体责任，定期对从业人员开展网络安全教育、培训，采取反间谍技术安全防范措施，防范、制止境外网络攻击、入侵、窃密等间谍行为。

公民和组织应当支持配合国家安全机关开展网络反间谍工作，针对发现的疑似网络间谍行为，及时通过12339国家安全机关举报受理电话、网络举报平台(www.12339.gov.cn)、国家安全部微信公众号举报受理渠道，或直接向当地国家安全机关进行举报。

据国家安全部、央视