武汉市地震监测中心遭受网络攻击

“黑手”疑来自美国

2022年6月，西北工业大学曾遭受境外黑客攻击。

昨天，武汉市应急管理局发布声明称，该局所属武汉市地震监测中心遭受境外组织的网络攻击。这是继2022年6月份西北工业大学遭受境外网络攻击后又一具体案例。国家计算机病毒应急处理中心和360公司组成的专家组发现，此次网络攻击行为由境外具有政府背景的黑客组织和不法分子发起，初步证据显示对武汉市地震监测中心实施网络攻击来自美国。

武汉市应急管理局在声明中称，经国家计算机病毒应急处理中心和360公司监测发现，其所属武汉市地震监测中心部分地震速报数据前端台站采集点网络设备遭受境外组织的网络攻击。

声明表示，为进一步查明事实，依法处理相关幕后黑客组织和不法分子的网络攻击行为，武汉市地震监测中心第一时间封存相关网络设备，并将遭受网络攻击的情况向辖区公安机关报案，我单位将保留进一步追诉的权利。

武汉市公安局江汉分局随即发布警情通报，证实在武汉市地震监测中心发现了源于境外的木马程序，该木马程序能非法控制并窃取地震速报前端台站采集的地震烈度数据。该行为对国家安全构成严重威胁。江汉分局已对此案立案侦查，并对提取到的木马样本进一步开展技术分析。“初步判定，此事件为境外黑客组织和不法分子发起的网络攻击行为。”

武汉市地震监测中心是继去年6月西北工业大学遭受境外黑客组织网络攻击之后的又一国家单位。西北工业大学受到攻击后，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对此案进行全面技术分析工作，最终确定了此次案件的“真凶”是美国国家安全局（NSA）特定入侵行动办公室（TAO）。

记者获悉，当前中国国家计算机病毒应急处理中心和360公司组成的专家已赴武汉开展取证工作，初步证据显示对武汉市地震监测中心实施网络攻击来自美国。

众所周知，美国在世界范围展开网络攻击、实施窃密行为，最臭名昭著的两大机构分别是NSA和CIA（中央情报局）。

根据360公司的监测结果，NSA对至少上百个中国国内的重要信息系统实施网络攻击，其中一款名为“验证器”的木马程序被发现在一些部门的信息系统中运行，向NSA总部传送情报。而且，结论显示，不仅在中国，其他国家的重要信息基础设施中，也正在运行大批的“验证器”木马程序，并且数量远超中国。

此外，据国家计算机病毒应急处理中心的研究发现，CIA针对全球发起的网络攻击行为早已呈现出自动化、体系化和智能化的特征，其网络武器使用了极其严格的间谍技术规范，各种攻击手法前后呼应、环环相扣，现已覆盖全球几乎所有互联网和物联网资产，可以随时随地控制别国网络，盗取别国重要、敏感数据。

美国在变本加厉对全球目标实施攻击窃密的同时，还不遗余力地“贼喊捉贼”，纠集其所谓盟友国家，大肆宣扬“中国网络威胁论”，诋毁污蔑我国网络安全政策。 据环球网

联合国安理会举行会议 图源新华社

外交部回应

将采取必要措施维护中国的网络安全

据新华社电 针对有外国政府背景的黑客组织对武汉市地震监测中心实施网络攻击一事，外交部发言人毛宁26日表示，中方谴责上述不负责任的行为，将采取必要措施维护中国的网络安全。

当日例行记者会上，有记者问：7月26日，武汉市应急管理局和公安局分别发布公开声明和警情通报称，经国家计算机病毒应急处理中心和360公司监测发现，武汉市地震监测中心遭受网络攻击。另据报道，初步证据显示网络攻击来自美国。请问发言人对此有何评论？

毛宁表示，根据中方相关机构发布的通报，有外国政府背景的黑客组织对武汉市地震监测中心实施了网络攻击，严重威胁中国国家安全。“我们谴责上述不负责任的行为，中方将采取必要措施维护中国的网络安全。”

有记者追问称：一段时间以来，美国总统国家安全事务助理、国务卿、商务部长、白宫国家安全委员会发言人等官员接连就所谓“中国对美国发动网络攻击”事件发表评论，美国国家安全局官员甚至表示“间谍活动是民族国家都会做的事”。中国相关机构此时发布声明，是否是对美方言论的回应？

毛宁表示，中方有关声明客观专业，陈述的是基本事实，同美方对华攻击抹黑有着本质区别。美国政府一方面对包括中国在内的全球各国从事恶意网络活动，另一方面却反复炒作“中国黑客攻击论”，是典型的双重标准和政治操弄。

毛宁说，网络安全是各国面临的共同挑战。美方把网络安全问题政治化、武器化的做法，严重干扰了国际社会通过对话合作共同应对挑战的努力，严重损害了国家间的互信。美方应立即停止有关错误做法，与国际社会一道，通过对话合作制定并遵守共同的规则，以建设性和务实态度维护网络空间的和平、安全与稳定。

新闻多一点

美国背后隐藏着啥居心？

境外势力为何要窃取我国地震检测中心数据？黑客木马程序可能怎样危害我国的国家安全？该如何进行防御和反制？记者专访了时事观察员、军事技术专家宋忠平。

可能被用来诱发人为地震

“我们一般描述一场地震，除了震级，接着就要说烈度。烈度也是一个重要的技术指标，对一个地区造成的伤害，烈度比震级更能说明问题。所以，各国在进行地震研究时，都要针对烈度来做相关的技术分析，来研讨如何防范地震所造成的巨大损失。”宋忠平认为，如果证实了是美国的网络黑客对中国的地震监测中心实施攻击，那么这本身不仅是不人道的，而且几乎等同于恐怖袭击行为。

为什么这么说？“一方面，他可以了解之前的一些数据，对中国相关地区的地震分布情况有所了解。”宋忠平说，如果全面掌握了一个国家地震带的分布，以及地震常态化的震级和烈度的话，就可以人为地来诱发地震。比如使用核弹打击板块中的某一个点，有可能就会造成这个板块发生位移，导致新的地震。

在国产科幻大片《流浪地球II》中有个桥段，就是全球3000多枚核弹以相控阵形式排列在月球表面一个关键区域，同时引爆诱发月球核心的聚变，从而炸毁月球。而这些核弹的总当量，只有直接炸毁月球所需总能量的上亿分之一。

“如果境外势力拿到了中国地震监测中心的数据，然后又了解了整个地球和我国国土以及周边地质板块的具体结构，还有地震的详细规律，那么在理论上是可以利用核打击手段来诱发地震的。”宋忠平透露，这也是美国军方一直在研究的一个领域。

“另一方面，境外势力也可能使用黑客手段，误导我们的地震预警，甚至发出错误的报警信号，也就是虚警，这将可能造成社会的紊乱。”宋忠平强调，境外势力可能采取的这种借助地震的攻击手段，所针对的并不只是中国政府，而是中国的普通老百姓，这种恐怖行为也是国际社会、国际法所坚决谴责的。

宋忠平特别强调，“我们必须明白一点，美国对中国的博弈是全方位的，其中科技博弈是美国极端重视的。因为美国全球霸权的一大根基便是科技霸权，他们担心中国科技能力的不断飞跃。”

宋忠平认为，通过各种手段对中国进行打压，美国现在采取的手段已经让人无法接受了，几乎达到了无所不用其极的地步。

努力做到“魔高一尺，道高一丈”

那么，该怎样防范境外势力对我国无孔不入的网络攻击呢？

宋忠平说：“第一，我们需要把重要的网络系统尽快实现国产化，无论是操作系统、中间件、数据库等都尽可能完全实现国产化覆盖。因为采用国外进口软件，尤其是基础应用软件，可能本身就存在着‘后门’、木马程序。实现国产化，能将安全系数增到最大，将危险系数降到最低。”

第二，建立起比较强大的软硬件相结合的防火墙和防水墙。“确保外部黑客攻不进来，也要确保内部人员没有办法对外泄密，既要有防火墙，还要有防水墙，两者兼而有之。”

对此，宋忠平解释说，我们需要做好全方位对网络攻击的监控，还要不断地研究对方网络攻击新手段，做到“魔高一尺，道高一丈”，确保能做到防患于未然。

“还有一点，要对人员加强保密意识教育。各类网络设备、机器都是由人来控制，由人来操作。对于相关人员，关键还是要做到应管尽管，并做好必要的保护工作。”宋忠平提醒道。

争取建立网络安全国际统一战线

如何反制，宋忠平提出了建议，“我们可以通过发表一系列关于网络攻击的报告，把美国对中国的各种网络攻击行为林林总总地描述出来，向国际社会广而告之，让193个联合国成员都了解美国的卑鄙勾当。同时，也可以考虑在联合国安理会层面发起相关的会议，把我们的证据提交出来，让安理会来评评理。”

虽然西方舆论基本上被美国控制，但还有广大的发展中国家和新兴国家，大家缺乏的是团结。“国际舆论的制高点，如果我们不去占领，就会被美西方长期占据。”宋忠平说，“我们需要争取建立关于网络安全的统一战线，可以广泛组织论坛、会议，也可以借助现有平台，形成常态化机制，来针对这些事情进行多方面、全方位的揭露。”

据潮新闻