哈尔滨市公安局通缉3名美国特工，背后藏着什么深意？

20250418 卢克文工作室 嘉宾老纪678

2025年4月15日，哈尔滨市公安局发布《悬赏通告》，悬赏通缉隶属于美国国家安全局(NSA)的犯罪嫌疑人凯瑟琳·威尔逊、罗伯特·思内尔、斯蒂芬·约翰逊。

通缉理由是，这3个家伙针对中国实施网络攻击活动，哈尔滨市公安局还具体列出了攻击目标：第九届亚冬会的赛事信息系统，我国关键信息基础设施，以及华为公司等企业。

详细列出攻击目标，相当于直接骂了一句“不要脸”。为啥？因为这些都是民生民用设施，你美国国家安全局没事攻击民用设施，是不是不要脸？

这么“直白”的悬赏通缉，咱们官方还是第一次。不过，通缉外国特工，这事自带戏剧性，有人就提出质疑，“反正又抓不到，搞这形式干吗？”

其实，这事不能这么看，悬赏通缉不是为了抓到他们，而是另有深意。

01

整件事在新华社通稿里讲得清清楚楚，咱们先解读一下，通稿主要有六个部分。

第一部分就是指名道姓，美国国家安全局3名特工是犯罪嫌疑人，悬赏大家提供线索或协助抓捕。

第二部分是概括整个事件：亚冬会被网络攻击后,及时报案，哈尔滨市公安局追查到3名特工和两所美国高校参与实施了攻击活动。

这部分有个亮点，“在相关国家支持下”，意思是哈尔滨市公安局在相关国家支持下破的案。

这个相关国家，虽然没有指明，但大家都知道是俄罗斯。

通稿里加上这句话有二层意思：第一层是，我有证人，你的网络攻击行为，我们有第三者可以验证，稳固证据链。第二层是，我有帮手，并且在网络安全上合作程度很深。

第三部分是直接指出幕后真凶，美国国家安全局(NSA)。

这部分非常有玩味，居然把美国国家安全局四级架构列了出来，首先是NSA，然后是所属的信息情报部（代号S），再是所属的数据侦察局（代号S3)，最

后是下属的特定入侵行动办公室（代号S32）。

并且还指出，依托所属多家掩护机构，匿名租用位于欧洲、亚洲等国家和地区的网络服务器。

外行看热闹，内行看门道。如果略知情报工作的话，就会知道这种提法是多么侮辱人。

美国公开的情报机构有18家，分为行政、军队和独立三种，比较有代表性的有：中央情报局(CIA)属于独立情报机构，负责人力情报；联邦调查局(FBI)属于司法部，负责反间谍；国家安全局(NSA)属于国防部，主要负责通信监控和网络攻防。

通俗地讲，中央情报局是策反间谍；联邦调查局是抓间谍；而国家安全局则是搞专业技术，精通黑客、监听、网侦，能攻能守。

在所有情报机构里，国家安全局最为神秘，代号“查无此局”。

其人员，主要由现役军人以及特招的网络高手组成，保密非常严格，组织架构和人员信息是绝密，知道的人极少。

而这份通稿里，直接翻了个底朝天，把人员信息和组织架构抖得一干二净，啪啪打脸。

这相当于直接喊话：别说真实的人，连虚假的人、匿名的人，都给你整得明明白白，就问你服不服，认不认吧。

第四部分是讲攻击过程，是陈述事实。

有三个事实：

其一，赛前攻击亚冬会注册系统、抵离管理系统、竞赛报名系统，意图窃取隐私数据。

其二，赛中重点攻击赛事信息发布系统，妄图影响亚冬会赛事的正常运行。

其三，还攻击黑龙江省内能源、交通、水利、通信、国防科研院校等重要行业，意图引发社会秩序混乱。

这部分意思很通俗，就是犯罪事实清楚，可以依法审判。

第五部分是讲攻击方式和手段，这段最为关键。

整个段落又分为两个层次，第一个层次讲攻击手法多样，涵盖了数百类已知和未知手段，并且还“表扬”了美国国家安全局，“攻击方式超前”。

为啥要表扬呢？

这是人类首次利用AI智能体发起的网络攻击，攻击代码由人工智能动态生成，自动规划工具方案、探测漏洞，并实时调整攻击策略和攻击范围，速度和规模远超传统黑客。

这么牛B的攻击被防住了，当然要表扬一下。

第二层次更有意思，说在网络攻击中，他们向基于微软Windows操作系统的特定设备发送未知加密字节，疑为唤醒、激活提前预留的特定后门。

这是吓死人的节奏，微软必须要站起来走几步了。

这句话意味着实锤微软有后门，看来“微软要退出中国市场”的传言，并非空穴来风，无论退不退，国内大规模系统替换恐怕是要启动了。

第六部分是指证其他参与对象，分别是加利福尼亚大学和弗吉尼亚理工大学。

这段先是讲这3名特工是惯犯，曾参与对华为公司的网络攻击活动。然后讲美国加利福尼亚大学、弗吉尼亚理工大学也参与了本次网络攻击。

加利福尼亚大学是网络教育中心，负责培训教育人员。弗吉尼亚理工大学是美国6所高级军事院校之一,负责网络攻防演练。

这部分相当于在舆论战场引爆一颗“深水炸弹”,学术机构沦为情报工具，“科技无国界”的口号以后怎么喊?

02

了解了这件事的来龙去脉，咱们就分析一下，为啥要发这个通缉令，究竟有什么战略意图。

首先，得搞清楚为啥是哈尔滨市公安局担任“破局者”？

这是国家的“不对称策略”，用低级别的行政机关应对外国国家级部门，是举重若轻，看似随意，实则表达“杀鸡焉用牛刀”。

上次通缉缅北电诈时，发布通缉令的是温州市公安局，很多人也不理解，各种猜测都有，除开温州市公安局反电诈侦察能力强外，这个也是主要原因。

此次通缉由哈尔滨市公安局主导，从明面上讲，哈尔滨是亚冬会举办地公安机关，承担赛事网络安全保障任务，侦察缉拿理所当然。

从暗面上讲，一个地区级公安部门能在指导帮助下，72小时内完成初步溯源，锁定NSA的TAO部门，这种国家级网络攻防能力，放眼全球已经是“大砍刀”,何必再动用国家级的“青龙偃月刀”。

说到这，必须简单聊聊美国网络攻击的厉害之处,通缉令里虽然有“表扬”，还远远不够，NSA确实有过人之处。

NSA这次攻击，用上全部压箱宝，有量子攻击系统、酸狐狸平台和AI智能体攻击。

这3件宝物是美国独门绝技，相当于如何接近、怎么放毒和直接打杀。

量子攻击系统，担任“如何接近”，2004年研发,投入超千亿美元，拥有20年实战经验，原理很简单,相当于是个中间人，只要看到你，就直接劫持到他那里。

比如你在看小黄站时，量子服务器比真实服务器更快响应，直接把你连接至NSA控制的服务器。

这次在亚冬会攻击中，NSA利用量子系统，劫持赛事信息发布系统，植入后门程序篡改比赛数据。

酸狐狸平台，相当于“怎么放毒”，擅长精准投递恶意代码，有智能过滤机制，能够定向攻击高价值目标。

该平台在2010年，利用“震网”病毒攻击伊朗核设施，远程操控离心机超速运转，让伊朗损毁了五分之一的离心机。

AI智能体攻击，相当于“直接打杀”，首次将大语言模型与智能体结合，实现攻击链的全自动规划。

这套系统非常牛B，能够动态生成代码，为目标量身定做，还可以多目标协同，

同时操控500+数字黑客,对亚冬会票务、抵离系统实施交叉渗透。

根据技术团队披露，这种攻击已远远超越传统黑客手段，是真正的“数字幽灵”，还可无限复制。

面对这么厉害的对手，咱们不仅搞定，而且还发布通缉令，其意图就三点：震慑、替代、夺权。

第一，战略威慑。

说白了，中国此次高调通缉，就是对美国网络霸权发起挑战。

长期以来，美国有技术心理优势，在硬件软件上也是领先，在网络上更是说一不二的霸主。

这次反制，通过穿透式溯源，锁定3名特工，并关联到加州大学、弗吉尼亚理工等高校，证明中国已掌握“逆向网络战”核心技术，能够将匿名攻击转化为“阳光下的追凶”。

另外，360集团的“AI红客”智能体在此次事件中首次实战应用，通过模拟攻击者行为模式，实时阻断定向攻击。这种“以AI治AI”的策略，标志着中国在智能防御领域已与美国形成均势。

通缉令发布后，美国网络攻击频率明显下降，从“全面渗透”转向“低频试探”，证明此举对美方形成技术震慑。

除了技术震慑外，还要打破美国的“贼喊捉贼”叙事策略。

美国长期以“网络安全卫士”自居，却通过《外国情报监视法》702条款胁迫科技公司配合窃密。

这次公开攻击证据，就是要国际社会看看，美国这样做合不合法，特别是攻击国际赛事、窃取运动员隐私，算不算“数字恐怖主义”？

第二，加速国产化替代。

近年来，国内核心部门已经在逐步更换计算机等设备，通缉令发布后，国家网信办将出台《关键信息基础设施国产化比例要求》，明确能源、交通、金融等领域2025年国产化率需达70%以上。

例如，电力系统将全面替换思科设备，金融核心系统转向华为高斯数据库911。

微软Windows系统因存在后门风险，将被排除在政务采购清单之外，鸿蒙系统装机量已经突破5亿台(2025年Q1数据)，操作系统国产化步伐将加快。

另外，芯片也将迎来新一波暴发，目前华为昇腾910B芯片在AI训练场景性能超越英伟达A100，长江存储128层3DNAND量产打破三星垄断。

第三，争夺网络治理话语权。

中国通过此次事件，要完成从“规则接受者”到“标准制定者”的转变。

首次将境外情报机构人员纳入刑事追责范围，此举直接回应美国《云法案》对境外数据的单边管辖，就是要“管辖权对等”。

中国向联合国提交《网络攻击溯源技术指南》，提出“行为-意图-结果”三位一体的证据认定标准，这是咱们定的新规矩。

还创新反制工具，建立“不可靠实体清单”，对参与网络攻击的外企实施出口管制、投资限制等制裁。

同时，加强多边合作，构建“去西方中心化”治理网络，与36国签署《数据安全合作备忘录》，发布《全球网络权力指数报告》，将美国列为“网络霸权国”，中国排名跃升至第二位。

总之，这次悬赏通缉是一场“非对称威慑”的战略试验，超越了单一案件追责，本质是对美国网络霸权的一次系统性反制。

其深意在于：短期，震慑境外势力，维护国内网络安全；中期，推动国产化替代与网络安全立法；长期，争夺全球网络治理规则主导权，塑造“数字中国”安全范式。

这一策略若成功，将为中国在AI时代的网络空间博弈提供重要支点。