耸人听闻的“假旗行动”

燕梳楼

作者丨燕梳楼

在这份报告里，列举了美国利用海底光缆和科技公司等优势地位，对全球实施大规模、无差别的监听和窃密。
不仅如此，他们还通过技术手段虚构出中国背景的“伏特台风”网络攻击组织，以此嫁祸和抹黑中国，也就是所谓的“假旗行动”。
为了满足情况需要，美国国家安全局下属的“特定入侵行动办公室”在全球范围内植入特定目标的间谍程序超过5万个。令人震惊的是，中国境内主要城市无一幸免。
美国的网络攻击和间谍程序，导致大量中国网络资产和敏感数据面临严重威胁，其中西北工业大学和武汉市地震监测中心成为重灾区。由此可见，网络安全已成为中美博弈的新战场。
我们先来理解一下什么是“假旗行动”。所谓的假旗从字面上理解就是通过优势技术和高科技企业合谋，通过插入中文等其他语种的字符串，刻意误导溯源分析，嫁祸他国。调查显示，微软、谷歌等网络巨头均涉其中。
早在2017年“维基揭秘”就曝光了来自美国中央情报局（CIA）网络情报中心的“大理石”软件框架。2023年初，德国网络安全专家弗里德里希团队发现一段来自中国黑客的陌生代码，背后竟然是一个鲜为人知的美国黑客组织。
由此，美国网络监控背后的“假旗行动”露出冰山一角。为了彻底撕开美国监听全世界的无耻行径，弗里德里希团队继续秘密研究，终于找到美国网络攻击的秘密工具——“大理石”软件包。
“大理石”软件的厉害之处在于，能够模拟中文、俄文等多种语言特征，从而故意制造误导性信息，让他国认为攻击来自中国、俄罗斯情报机构及关联企业的错觉。此举不仅可以让美国CIA洗脱嫌疑，还能在国际上离间和孤立中俄。

当然，你要认为美国只是针对“敌对国家”你就低估了他们的无耻。包括他们的盟友德国、日本、法国等国的重要政治人物、外交官和商业领袖，都在他们的监控窃听之下，包括他们的每一封邮件，每一句话。
美国的这种无差别监听和窃密，意味着美国全球互联网早已在其掌控之中。其不仅用过“假旗行动”来嫁祸中国，国会每年还花16亿美元通过舆论操控来抹黑中国。其实凶手恰恰是自己的 “盟友”。
除了“假旗行动”，美国还有一个无比庞大的全球监听网络。主要分两块来说。一个是先天掌握的垄断优势。大西洋海底光缆和太平洋海底光缆均在美国掌控中，美国建立了7个截流中心，窃取这些光缆传输信号。
获得这些数据后，美国和其它“五眼联盟”国家合作，将窃取的数据实时转化成可阅读、可检索的情报信息，美国CIA实施了两个项目，这即是臭名昭著的“上游”和“棱镜”， 对相关数据进行提取、汇聚、还原、解码和分析。
另一个就是技术优势。除了“大理石”软件外，他们还有一个代号为“水蝮蛇”的装备，看起来和普通的USB接口一样，只要插入任何特定物理隔离网络，就能把窃取的数据通过信号方式发送出来，甚至实现远程控制。
报告显示，亚洲、东欧、非洲、中东和南美等目标国家和地区，已被植入超过5万个NSA间谍程序。当然这种操作相对比较困难，需要通过“供应链”攻击的方式，也就是说要在大型互联网企业或设备供应商的配合下，才能有效完成。
比如预留后门，或者对出口设备进行拆解改装，或者故意在技术上设置漏洞，无声无息地潜入我们自认为相对安全的物理网络或通信工具。美国微软、雅虎、谷歌、脸书、苹果等各大互联网企业均涉其中。
由此，你还觉得网络安全和我们没有关系吗？要知道，美国是可以通过“棱镜”计划直接从这些互联网企业巨头的服务器上调取数据的，我们通话记录、财产信息、人物关系都在他们的窃取之中。
只是我们普通人的信息没有价值吧，但对一些重要的政治、经济人物，一些机密文件和核心数据，就很危险了。这也是我们逐步替换

使用国产系统和软件的原因，对某些手机和车辆也禁止的。

所以说，网络安全已经成为中美博弈的新战场。对国家而言严重危害国防安全和经济发展，对企业而言则会造成信息误判竞争被动，而对我们个人而言，则会导致密码和身份信息被盗用。

我们必须要支持和配合国家的信息和网络安全建设，抵制美国构建的覆盖全球的“监控帝国”。不要再天真的以为科学无国界，他们的每一个产品都是射向我们的子弹。

当一个国家，一个企业，一个个人完全透明时，这仗还怎么打？生意还怎么做？安全感从哪里来？

所以，任何时候我们都只能相信自己的国家，支持自己的国货。