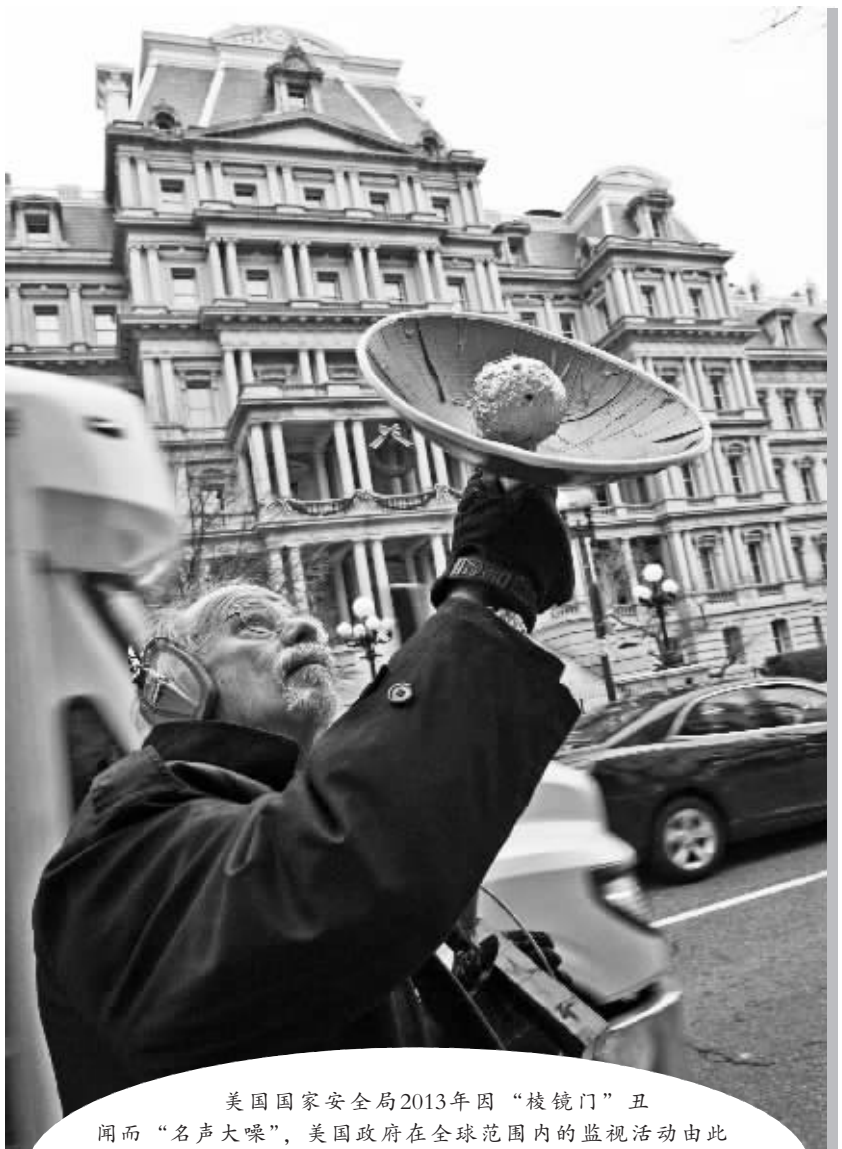
美国安局间谍设备大起底

——一些监视设备为苹果、惠普等产品量身打造



美国国家安全局2013年因“棱镜门”丑闻而“名声大噪”，美国政府在全球范围内的监视活动由此成为媒体追问热点。德国《明镜》周刊披露，除黑客团队外，美国国安局内部还有一个秘密团队，专门制作各类间谍设备，为美政府的情报活动提供想象力丰富的技术支持。

间谍设备花样繁多

《明镜》周刊2013年12月30日报道，美国国安局这个下设团队内部代号为ANT，是英文“高级网络技术”的简称，研发的设备主要用于网络设备渗透、手机和计算机监控等。

这家周刊获得一份近50页的内部名录，详细罗列ANT研发的产品、用途及价格。

比如，名录介绍一条经过技术处理的显示器连接线，称可以帮助国安局黑客团队“看到目标显示器上所展示的东西”，每条售价33美元；

一个特制“短信基站”售价4万美元，可以帮助情报人员模拟目标网络手机信号塔，进而监听目标手机；

名录中有一种看似普通移动存储装置的计算机监视设备，可以利用无线电信号发送或接收目标计算机的数据，售价为每个2万美元。

《明镜》周刊报道，这份名录的时间为2008年，其中不少设备可以应用的服务器系统或手机已经退市，因而可以推断名录并不完全。结合当年情况，外界仍可以据此看出美国国安局手中掌握的丰富“谍战”资源。

根据知名企业产品量身定制

这份名录还显示，美国国安局将不少知名信息技术企业为对象，量身打造监视设备，以确保情报获取范围扩展到尽可能广的用户群。这些企业包括美国思科、戴尔、惠普和中国华为等，ANT团队研发的部分产品针对前者生产的服务器、计算器或者手机设备。

《明镜》周刊提到，尽管名录对应的2008年还没有迎来智能手机的全球普及潮，但美国国安局针对手机的间谍设备已经出现。其中，名录还介绍一款研发中的木马病毒，目标就是美国苹果公司的智能手机iPhone。

接受《明镜》周刊采访时，不少企业表示对美国国安局根据自己产品定制间谍设备不知情。思科公司在一份回复中说，公司对“任何可能损害我们顾客网络或产品完整性的行为感到深切担忧”。

监视范围覆盖敌友

《明镜》周刊报道，美国国安局研发的各类间谍设备用途不仅是追踪潜在恐怖分子。从2013年“棱镜门”丑闻的发展来看，美国的不少盟友已经“中招”。

比如，德国总理安格拉·默克尔的手机遭窃听，显然受到了特制“短信基站”的监视；一种代号为DROPMIRE的雷达系统也被用于监视盟友，包括欧盟常驻美国首都华盛顿的代表。

除针对个人外，美国国安局的间谍设备还被用于监视国际通信企业，如比利时电信公司以及手机支付运营商MACH。

2013年9月，比利时电信公司检查内部计算机系统时发现“入侵痕迹”，当地媒体把矛头直指美国国安局。比利时政府还发表声明谴责“他国”入侵比利时主要电信运营商的计算机系统。

上图：2013年12月16日，在美国华盛顿，示威者打扮成间谍在美国贸易代表办公室外集会，嘲讽并抗议美国对国外商业代表实施监控。

走近美国安局黑客团队

“棱镜门”丑闻让美国秘密监视项目大白于天下，也让美国国家安全局成为焦点。德国《明镜》周刊聚焦国安局负责监视项目的核心黑客团队，以秘密文件为来源详细介绍这个部门的秘密任务。

入侵全球通信网络

美国国安局下设的这个黑客部门名为“定制入口行动办公室”（TAO，简称“行动办公室”）。用国安局的话说，这个部门的任务就是“获得无法获得的东西”。“行动办公室”1997年设立。当时，互联网处于萌芽阶段，全球只有不到2%的人口能接触互联网。

设立之初，“行动办公室”就与国安局其他部门完全隔离，而且任务明确：夜以继日地找办法入侵全球通信网络。《明镜》周刊报道，一份有关职责描述的内部文件明确将网络攻击行为列入“行动办公室”的任务范畴。换句话说，美国政府授权这些人员去“黑”全世界的通信网络。秘密文件显示，2010年，“行动办公室”在全球范围内实施了279次网络入侵行动。

招募人才不拘一格

为组建最优秀团队，美国国安局在招募人才方面不拘一格，甚至主动邀请在网络世界呼风唤雨的天才黑客加盟。

国安局局长基思·亚历山大近年来多次出现在美国的大型黑客大会上，有时着军队制服，有时则穿T恤和牛仔裤，以期通过形象认同博取潜在黑客雇员的好感。

久而久之，不少黑客摇身一变，成为政府公务员。而在国安局内部，“行动办公室”是人员平均年龄最低的部门。尽管“资历浅”，但这些“黑客公务员”实力不可小觑。在一些跨部门的情报协作行动中，他们往往成为破解网络通信“密码”的关键。

《明镜》周刊报道，如果有必要，美国联邦调查局甚至可能出动自有专机将“行动办公室”技术人员及时送至目标地点，实地获取情报。在最短半小时内，这些人员可以完成任务，然后随专机“消失”而不会在事后被查寻到行踪。

“寄生”微软视窗操作系统

监视任务需要创造性思维，“行动办公室”也不例外，例证之一是“躺枪”的美国微软公司“视窗”操作系统。

《明镜》周刊报道，“视窗”操作系统用户经常遇到这样的问题：一旦检测到内部故障，系统会主动弹出窗口提示，并要求用户将故障信息报告生产商或者重启程序。在黑客眼中，这种故障就是可乘之机。

根据美国国安局开发的一款“钓鱼”软件，当一台计算机已经成为国安局目标、配有特定身份识别码后，“行动办公室”技术人员就可以在“视窗”操作系统提示故障时得到实时提醒。

这种监视手段虽然“被动”，最初只能让技术人员获得计算机主人发送出来的信息，但“筛选”效果显著，而且故障报告本身意味着计算机出现潜在漏洞，为技术人员今后利用这些漏洞进一步植入间谍软件提供机会。

包括“被动”和“主动”方式在内，“行动办公室”所渗透的电脑遍及全球。美国政府公开的2013年度情报财政预算显示，2013年年底前，美国国安局预计在全球8.5万台目标计算机中植入间谍软件。这些行动大部分由“行动办公室”通过互联网实现。

已成功监视到海底光缆

除了针对具体目标外，国安局的监视对象还包括通信信息交流的“主管道”。

《明镜》周刊援引一份标注为“绝密”和“仅限本国人员”的秘密文件报道，“行动办公室”已经成功监视到代号为“Sea-Me-We 4”的大型海底光缆系统。这一系统连接欧洲与北非、欧洲与海湾国家，途经印度和巴基斯坦，延伸至马来西亚和泰国。

这份标注时间为2013年2月13日的文件称，“行动办公室”成功搜集到“Sea-Me-We 4”的网络管理信息。经过一系列“网站化妆行动”，技术人员获得了海底光缆控股集团的管理网站接入方式，搜集到显示光缆系统布局等方面的更进一步信息。文件称：“今后计划展开更多行动，搜集有关这一海底光缆和其他光缆系统的更多信息。”

美国大使馆楼顶的白盒子，疑为监听设备。

本版文字均据新华社 CFP供图