卖设备偷情报，美国窃听逾120国？

美国媒体日前披露，美国和原联邦德国（西德）的情报部门从20世纪70年代开始秘密操控瑞士加密设备供应商克里普托AG公司以获取别国机密情报，两德统一不久后德国方面退出，而美国直至2018年才停止这一情报窃取行动。

分析人士指出，美国素来以“网络安全卫士”自居，频频指责他国发起网络攻击，却无视自身的斑斑劣迹。此次曝出的通过瑞士公司设备窃取他国情报事件，再次凸显出美国贼喊捉贼的网络霸凌思维。

“屡立战功”

德国媒体早在1996年就怀疑德美两国机构在克里普托AG公司的设备上“做手脚”，但当时克里普托AG公司回应称报道毫无依据。美国《华盛顿邮报》11日刊登长篇报道再次聚焦这一问题，披露了该报和德国电视二台联合调查获取的与此相关的美国中央情报局机密文件。

报道称，1970年左右，美国中情局和西德情报机构联手秘密收购并实际控制了克里普托AG公司。该公司多年来将加密设备出售至超过120个国家，包括伊朗、印度、巴基斯坦以及一些拉美国家，而美德通过在设备上开的“后门”获得他国机密信息。“外国政府给美国和西德付了大价钱，却让这两个国家（可能最多五六个国家）阅读自己最机密的通信信息”。

这套情报窃取手法一度“屡立战功”。报道称，通过克里普托AG公司的设备，美国与西德情报人员曾在1979年美国驻伊朗大使馆人质危机期间监视伊朗宗教领袖的言行，在1982年马岛战争中向英国提供阿根廷军方的情报，在1986年柏林舞厅爆炸案后掌握利比亚领导人的相关情报。

报道称，1990年两德统一之后，德国情报机构认为上述情报窃取行动暴露风险太大，不久便退出。美国中情局随即买下了德方持有的股权并继续执行该行动直到2018年。

劣迹斑斑

美媒披露的上述行动只是美国网络恶行的一个例子，这样的例子还有很多。

依据美国防务承包商前雇员爱德华·斯诺登的爆料，早在2009年初，美国国家安全局就曾侵入中国公司系统窃取源代码，读取客户名单和内部邮件。

2017年4月，媒体爆料与美国国家安全局相关的黑客组织攻击转账结算系统SWIFT在中东地区最大的金融服务提供商EastNets，窃取了大量主机信息、登录凭证等。

去年6月，美国情报部门被曝对伊朗部分计算机系统发起攻击，使伊朗的火箭发射系统瘫痪；向俄罗斯电力系统植入恶意程序代码，以便刺探情报或对俄电力系统发动网络攻击。

而在体制和战略方面，美国政府2017年将美军网络司令部正式升级为美军第十个联合作战司令部，地位与美国中央司令部等主要作战司令部持平；2018年发布网络战略报告，强调要在网络空间里“先发制人”。有分析认为，种种动向表明，美国正紧锣密鼓地为网络战加强准备。

舆论指出，实施监控、窃取信息、暗中破坏，美国在网络安全领域的劣行层出不穷，却还不断指责他国破坏网络安全，可谓贼喊捉贼、倒打一耙。这种双标行为凸显了美国唯我独尊的霸权思维。

德瑞不安

上述情报窃取行动曝光后，与这一行动相关的德国和瑞士出现了要求调查和表达担忧的声音。

在德国，多名联邦议院议员要求政府调查这一事件。德国自由民主党议员斯特凡·托梅表示，“这种行为无法容忍”。他说，联邦政府不能保持沉默，应立即启动“毫无保留的全面调查”。左翼党议员安德烈·黑恩则称这一情报窃取行动是“德国联邦情报局最大的历史丑闻”。

在瑞士，有媒体认为这起事件恐将影响这个永久中立国今后在国际事件中的“中立性”。

《新苏黎世报》说，瑞士向来以在国际事务中保持中立而著名，瑞士科技公司也依赖国家的中立地位发展业务。“斯诺登事件”以来，美国供应商被贴上了不安全的标签，瑞士公司则在国际市场上取得领先。如果直到两年前克里普托AG公司实际上还是美国中情局监听网络的一部分，这会影响瑞士整个行业的声誉，从而损害竞争优势。　据新华社

延伸阅读

近年来美国发动的网络攻击

事实上，美国一直在加强对网络武器的研发和实战运用，以下是近年来源于美国的重大网络攻击事件。

美国《纽约时报》2019年6月报道，美情报人员正加大力度向俄电力系统植入恶意程序代码，以便刺探情报或对俄电力系统发动网络攻击。

2019年5月，特朗普在接受采访时，公开承认曾于2018年中期选举时，允许相关部门对俄罗斯发动网络攻击，以阻止所谓的俄罗斯对美国中期选举的干涉。

中国国家计算机网络应急技术处理协调中心发布的《2018年我国互联网网络安全态势综述》显示，来自美国的网络攻击数量最多，且呈愈演愈烈之势。2018年位于美国的3325个IP地址向中国境内3607个网站植入木马，向中国境内网站植入木马的美国IP地址数量较2017年增长43%。

2017年4月，媒体爆料美国国家安全局下属的“方程式”组织攻击转账结算系统SWIFT在中东地区最大的金融服务提供商EastNets，窃取了大量主机信息、登录凭证等。

2015年，美国媒体披露，美英情报机构监听多国网络安全厂商，获取病毒样本以削弱反病毒产品。

《纽约时报》2017年报道，2014年美国时任总统贝拉克·奥巴马下令，用网络战和电子战手段破坏朝鲜试射弹道导弹。

2014年，美国“截击”网站报道，美国网络安全公司赛门铁克公司发现一个先进复杂、可以隐形的计算机恶意软件“雷金”，这正是美英情报部门多年来对欧盟计算机系统进行网络攻击所用的技术。

2012年，美国《华盛顿邮报》报道，美国和以色列联手研发“火焰”病毒。这种用于窃取信息的病毒一度在中东地区传播，甚至迫使伊朗短暂切断石油部门和相关设施的互联网连接。

2010年，伊朗纳坦兹核设施电脑网络遭名为“震网”的病毒攻击，1000台铀浓缩离心机瘫痪。有媒体披露，这种网络病毒由美国和以色列开发，用以打击伊朗核计划。

德国《明镜》周刊网站2014年援引美国防务承包商前雇员爱德华·斯诺登披露的资料说，早在2009年初，美国国家安全局就侵入中国华为公司系统窃取源代码并读取华为客户名单和内部邮件。　据新华社

相关链接

美国中央情报局

美国中央情报局（英语：Central Intelligence Agency），总部位于美国弗吉尼亚州的兰利。与苏联国家安全委员会（克格勃）、英国军情六处和以色列摩萨德，并称为“世界四大情报机构”。

其主要任务是公开和秘密地收集和分析关于国外政府、公司、恐怖组织、个人、政治、文化、科技等方面的情报，协调其他国内情报机构的活动，并把这些情报报告到美国政府各个部门的工作。

它也负责维持大量军事设备，这些设备在冷战期间用于推翻外国政府做准备，例如苏联、危地马拉的阿本斯、智利的阿连德等对美国利益构成威胁的反对者。美国中央情报局总部设在弗吉尼亚州的兰利。

美国中央情报局分为四个主要组成部分：情报处、管理处、行动处、科技处。情报技术人员多具有较高学历，或是某些领域的专家。该机构的组织、人员、经费和活动严格保密，即使国会也不能过问。

斯诺登事件

2013年6月，前中情局职员爱德华·斯诺登将两份绝密资料交给英国《卫报》和美国《华盛顿邮报》。6月5日，英国《卫报》先扔出第一颗舆论炸弹：美国国家安全局有一项代号为“棱镜”的秘密项目，要求电信巨头威瑞森公司必须每天上交数百万用户的通话记录。6月6日，美国《华盛顿邮报》披露称，过去6年间，美国国家安全局和联邦调查局通过进入微软、谷歌、苹果、雅虎等网络巨头的服务器，监控美国公民的电子邮件、聊天记录、视频及照片等秘密资料。美国舆论随之哗然，保护公民隐私组织予以强烈谴责，表示不管政府如何以反恐之名进行申辩，不管多少国会议员或政府部门支持监视民众，这些项目都侵犯了公民基本权利。

这是一起美国有史以来最大的监控事件，其侵犯的人群之广、程度之深让人咋舌。

维基解密事件

2010年7月25日，维基解密网站 通过英国《卫报》、德国《明镜》和美国《纽约时报》公布了92000份美军有关阿富汗战争的军事机密文件。

机密文件中，最具破坏性的消息是北约联军在阿富汗杀死平民的事件。文件声称，驻阿富汗美军有些不愿公之于众的“秘密”，其中包括数百名阿富汗平民遭到误杀、误伤。许多人是无辜的摩托车手或者司机，他们因被怀疑是自杀式炸弹袭击者而遭到射杀。文件还披露了驻阿英军部队在喀布尔射杀平民的事件。文件披露，2000名阿富汗平民被塔利班路边炸弹炸死。许多误杀平民事件此前并未得到披露。

此外，泄密文档还透露，北约联军有一支特种部队——“373特遣部队”，该部队负责“击毙或者俘获”塔利班头目，他们在实施行动时不需要对塔利班头目进行审判。而为了顺利完成追杀任务，“373特遣部队”有时候不惜杀害阿富汗平民，包括妇女和儿童，只要“373特遣部队”认为有必要，阿富汗警务人员也难遭幸免。　晚综