美以“黑客帝国”攻陷伊朗核设施

伊朗两成离心机报废 三五年内难造出原子弹

近来，美国和以色列官员相继表态称西方对伊朗的制裁正在发挥作用，伊朗的核能力明显受到打击，没有三五年根本不可能制造出原子弹。而此前，西方官员一直坚称伊朗很快就会制造出原子弹。是什么导致西方官员的看法发生变化？

《纽约时报》最新刊登的文章给出了答案：美国和以色列的科学家对伊朗的核设施发动了一次网络战，他们散布的病毒堪称“网络超级弹”，成功攻陷了伊朗核设施的电脑控制系统，导致两成离心机失效。

伊朗核设施

图中人：以色列摩萨德前首脑达甘

周悟空 制图

病毒重挫伊朗核计划

最近，以色列已退休的摩萨德首脑达甘和美国国务卿希拉里先后表示，伊朗的核能力遭到极大削弱。希拉里引述的理由是西方的制裁取得效果。达甘则说伊朗核计划遇到重大技术障碍，2015年前不会取得突破性进展。而此前，以色列一直坚称，伊朗核计划即将取得成功。

显然，美以两国的看法逆转有更深层的原因，最大的可能因素就是Stuxnet电脑病毒。

在以色列内盖夫沙漠里，隐藏着该国从未公开承认过的一座核武库——迪莫纳基地。

专家称，在迪莫纳基地高高的铁丝网背后，美以科学家使用和伊朗纳坦兹基地几乎完全相同的离心机进行Stuxnet电脑病毒攻击实验。2009年中到年底，Stuxnet电脑病毒肆虐全世界，伊朗损失最为惨重，纳坦兹核工厂近1/5的离心机遭到破坏，从而大大延迟了伊朗的核计划。

西门子卷入其中

德国汉堡独立计算机安全专家拉夫尔·兰纳是最早发现Stuxnet病毒的人之一，他和5名雇员破解了Stuxnet病毒，结果发现，这种病毒只有在侦测到一种特定型号的自动化控制系统时才会爆发，而这种系统恰恰被用于伊朗的核工厂。

仔细研究该病毒演变轨迹，专家们发现了众多熟悉的名字。其中之一就是西门子。2008年初，德国西门子和美国爱达荷州国家实验室（它也是负责核武器的美国能源部的下属机构）合作，研究其计算机自动控制系统中的漏洞。美国情报系统称，伊朗核工厂也运用了西门子的系统。

西门子解释说，该项目只是公司为确保产品免遭网络攻击的常规工作之一。

据专家分析，Stuxnet病毒主要由两部分组成：第一部分让伊朗的离心机失控；第二部分的作用更像是来自间谍电影：电脑程序会秘密录下伊朗核工厂离心机正常运转时的状况，当离心机失控后，程序会自动播放录像带，从而给监控人员留下离心机运作正常的印象。但实际上离心机早已瘫痪。

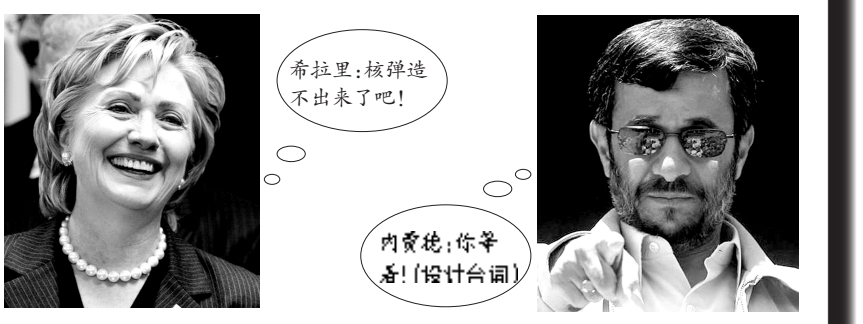
测试离心机来自黑市？

一名美国核武专家表示，“Stuxnet病毒之所以能取得成功是因为以色列此前已在和伊朗类似的离心机上做过实验。”

以色列用于测试Stuxnet病毒的离心机的来源也很离奇。上世纪70年代，荷兰设计出一台用于提纯铀的离心机。一名叫凯德·可汗的巴基斯坦籍科学家当时参与了这一工作，他盗窃了离心机的设计图纸，并于1976年逃回巴基斯坦。不久，巴基斯坦生产出了名为P—1的第一代离心机。凯德·可汗后来通过地下黑市将P—1卖给了伊朗、利比亚等国家。

尚不清楚以色列如何得到P—1离心机，但专家相信，以色列迪莫纳基地里运转着大量P—1离心机。

核专家称，迪莫纳基地里的这些P—1离心机在测试Stuxnet病毒的有效性方面发挥了重要作用。



美以笑得合不拢嘴

当然，美国和以色列官方从未公开提过Stuxnet病毒，更别提两国在其中的角色。但美国和以色列官员私下里对其成功笑得合不拢嘴。在最近一次关于伊朗的会议上，奥巴马总统首席核武顾问萨默尔对Stuxnet病毒的问题避而不答，只是笑眯眯地说：“我很高兴地听说他们（伊朗）在离心机方面遇到了麻烦。”

内贾德承认遭到攻击

2009年11月，伊朗总统内贾德打破沉默，称该国核工厂遭到网络病毒攻击，但只对离心机造成“很小影响”。然而，2010年12月，美国科学与国际安全组织发布了一份关于Stuxnet病毒的长篇报告，称伊朗核工厂的P—1离心机在2009年遭到网络病毒的攻击，导致984台离心机报废。

“网战超级弹”这样炸响

最初感染

Stuxnet病毒通过U盘等可移动设备感染装有Window操作系统的电脑，并藏身其中。

升级和扩散

如果感染病毒的电脑连接了互联网，Stuxnet会自动升级为最新版本，然后通过感染其他联网电脑或可移动设备而不断扩散。

最终目标

Stuxnet病毒自动搜寻安装了西门子“进程控制系统7”的应用软件的电脑，并通过移动设备将其控制器感染。几天后，病毒开始扩散，导致离心机的叶轮运转缓慢，直至机器瘫痪。同时，病毒还会对外发出机器运转正常信号，蒙蔽控制人员。

网战案例

●早在1991年的海湾战争中，美军就对伊拉克实施了网络战。开战前，美国中央情报局派特工到伊拉克，将其从法国购买的防空系统使用的打印机芯片换上了含有计算机病毒的芯片。在战略空袭前，又用遥控手段激活了病毒，致使伊防空指挥中心主计算机系统程序错乱，防空C3I系统失灵。

●2008年8月的俄格冲突中，俄罗斯创造了一个网络战的经典案例。在军事行动前，俄控制了格鲁吉亚的网络系统，使格鲁吉亚的交通、通讯、媒体和金融互联网服务瘫痪，从而为自己顺利展开军事行动打开了通道。

1月17日《晶报》A24 张运贵