# 看看‘黑客帝国’做了些啥

2月10日又一个“国际互联网安全日”。自46年前互联网在美国创立、20多年前开始走向大众，“安全”一直是全世界越来越多网民的期盼，也是越发依赖互联网的各国的追求。

在网络安全领域，头号强国美国历来喜欢一面鼓吹网络自由，一面装扮成网络攻击受害者。然而，美国防务承包商前雇员斯诺登等公布的材料，让美国这个“黑客帝国”的真面目显露无遗。

## “重视”中国

在网络安全方面，美国几乎是习惯性地频频把矛头指向中国，而事实上，中国受到的网络攻击最大来源恰恰就是美国。从政府机构到企业，都是美国网络攻击对象。

根据中国国家互联网信息办公室的数据，去年3月19日至5月18日，2077个位于美国的木马或僵尸网络控制服务器，直接控制了中国境内约118万台主机。2016个位于美国的IP对中国境内1754个网站植入后门，涉及后门攻击事件约5.7万次。

美国黑客是中国网络的“老主顾”。早在5年前，中国国家互联网应急中心就指出，利用木马和僵尸程序控制中国境内计算机的境外IP地址中，来自美国的分别占到16.61%和22.34%，均排名第一。

频繁攻击中国网络，恐怕不仅仅是美国黑客的“个人爱好”。2012年10月，美国总统奥巴马签署名为《美国网络作战政策》的总统指令，要求美国国家安全和情报官员制定一份美国可以进行网络攻击的目标名单。美国国家安全局已在全球超过5万台计算机中植入恶意软件，中国是其中的主要目标之一。

不只是网络攻击，在网络监控方面美国对中国也十分“重视”。在已曝光的美国2010年“监听世界地图”中，中国是东亚地区首要监听对象，北京、上海、成都、香港及台北等城市，均在美国国家安全局重点监控目录之下。

从2009年起，美国国家安全局就开始入侵中国大陆和香港的电脑和网络系统，中国大陆和香港已有数百个目标受到监视。在香港的目标中，多数是政府官员、商人和学生。

## “放眼”世界

全球最大的网络安全公司赛门铁克在其互联网安全威胁报告中指出，网络攻击源的数量美国位居第一，占世界总量的25%；位于美国的僵尸控制服务器数量居世界首位，占33%；“钓鱼网站”有43%位于美国。

根据奥巴马签署的《美国网络作战政策》，为实现美国在全世界的国家安全目标，美国可以动用独特的和非常规的武力，在事先不进行任何警告的情况下发动攻击。其实美国的“网络战”早已在全球施展开。

美国《纽约时报》2012年6月报道说，奥巴马上任后曾下达密令，升级在小布什政府期间启动的针对伊朗的网络攻击计划。

同年5月，美国对中东地区“放火”。被称为“火焰”的电脑病毒在伊朗等国蔓延。据美国媒体披露，此病毒由美国和以色列联合研发，目的是收集情报，为对伊朗核设施发动网络攻击做准备。美以两国还利用具有破坏性的“震网”蠕虫病毒攻击伊朗的铀浓缩设备。

此外，美国一些官员私下承认，2003年美国对伊拉克通信系统发动攻击，导致与伊拉克共享手机信号和卫星电话系统的周边国家手机服务暂时中断。科索沃战争时期，美军攻击南联盟电信网络，意外影响到国际通信卫星组织的卫星信息系统，导致系统受阻数日。

《纽约时报》说，早在2010年，美国就在韩国和其他盟友的帮助下，“直接侵入了朝鲜网络”，并植入木马，试图监控朝鲜网络的内部运作。

据报道，美国国家安全局下属的“获取特定情报行动办公室”已在全球多国采取行动，除中国外，还有俄罗斯、巴西、埃及、印度、墨西哥、沙特阿拉伯及东欧部分地区。“监听世界地图”则包含了世界90个国家的监控点。

## “照看”盟友

对于“友邦国家”，美国这位“老大哥”也可谓“尽心”。中国互联网新闻研究中心去年发表的《美国全球监听行动纪录》指出，为实现其安全目标，美国通过拦截英国、挪威、日本等国的卫星数据，进行外国卫星情报收集。

“棱镜”计划曝光后，“黑客帝国”的更多劣迹为世人熟知。比如窥探德国总理默克尔手机长达十多年；每天收集全球各地近50亿条移动电话记录；秘密侵入雅虎、谷歌在各国数据中心之间的主要通信网络，窃取了数以亿计用户的信息；多年来一直监控手机应用程序，抓取个人数据。

美英两国还利用“雷金”恶意软件，攻击过欧盟计算机系统。赛门铁克公司报告说，自2008年以来，“雷金”被用来攻击多个国家的政府部门、研究机构以及私营公司的计算机网络，包括比利时、印度、墨西哥等，以获取系统中的数据。

研究人员指出，“雷金”与美国以往攻击伊朗使用的恶意软件有相像之处，此类间谍工具“几乎天下无敌”。鉴于“雷金”精密复杂以及开发设计需要大量时间和资源，“这只能是国家行为”。

[焦点科普]

## 个人上网如何保安全

这是一个网络时代。支付宝、网银、微信、电邮、QQ……每一个人的生活要想和网络脱了干系，实在不容易。网络虽便利，可陷阱也不少。

腾讯等最新发布的一份研究报告显示，中国网民最担心泄露的信息类别是网银信息(53.8%)，其次是身份信息(23.7%)，再次是网站账户、密码(16%)。

网银主要涉及民众的资金安全，所以担心程度最高，身份信息涉及民众的个人隐私，因此担心程度也较高。看来，大家需要多长几个心眼儿，确保自己的资金和隐私不受损失。

一、首先最基本的一点是，给自己的电脑以及手机安装杀毒软件，并及时更新杀毒软件。

二、在进行网银、支付宝等涉及资金的网络操作时，要确保使用安全的浏览器、登录正确的网站地址，不要单凭记忆输入网址，小心上“李鬼”的当。

三、网上购物选择正规、大型电商。淘宝购物不要随便打开旺旺中的重新支付、低价促销等链接。

如果有“密码+校验码”双重验证设置，请不要嫌麻烦，这样更安全。

四、在网站注册账号时，只填带*的必填项，尽量提供最少的信息。

五、不随意打开陌生邮件，尤其是带附件的邮件或者声称中大奖的邮件。

六、尽量别“蹭网”。手机接入未经认可的无线网络，有可能会被窃取个人移动设备信息。

七、如今在微信上测性格、测运势等链接泛滥。这些链接通常会要求你提供姓名、年龄等基本信息，后台还会直接获取你的手机号码等信息。为了一个压根不靠谱的测试结果，提供这么多重要信息，实在得不偿失。

八、不要把个人敏感照片、数据上传到云端，“因为你不知道它会飘到哪儿”。 **(据新华社)**

[述评]

## 互联网安全 共治方是正道

**互联网给人们生产生活带来前所未有的便捷，但同时互联网发展也对国家主权、安全、发展利益提出了新的挑战，迫切需要国际社会认真应对、谋求共治、实现共赢。**

**如何建设安全、有序的互联网，不少国家都在寻求良方。而值得注意的是，却有国家逆“共治”的潮流而动，图谋一家主导、一国独大，一味谋求自身的“绝对安全”。**

**作为互联网的诞生地，美国曾引领了全球互联网创新与创业浪潮，但随着互联网具有越来越多的公共属性，创建者也并不意味着拥有永久的控制权。令人遗憾的是，美国恰恰认为自身有这一权力，并不断付诸行动。**

**过去两年，随着“棱镜门”等事件曝光，越来越多的国家尝试从更广阔的视野，思考互联网治理问题：因为“棱镜门”事件，德国总理默克尔提议并与法国探讨，在欧盟内部建立一个独立的通信网络，避免欧盟各国之间的数据通信“绕道”美国；巴西也宣布构建自己的海底通信电缆，直接与欧洲相连，避免数据遭美国截取；日本、俄罗斯和印度也一直在为强化互联网安全而积极行动……**

**互联网是人类文明的一大进步，同时也是人类治理所面临的全新挑战。网络空间的高度复杂性、相关利益方的高度多元化，注定了单极思维行不通。由一个国家做“控制者”，以伪善的理由借互联网损害其他国家的利益，则会带来更大危害。**

**互联网把全世界带向“互联互通”，因而也必须“共享共治”，并为此制定规则。特别是不同的国家管理网络空间的权力，是维护网络空间安全的重要前提，它们为维护网络空间秩序和安全所实行的公共政策，理应得到尊重。网络行为规则，必然要相关国家在平等基础上协商。唯有如此，网络的共同安全才能真正得到保障。**

## “十三连跌”终止 国内汽、柴油价格迎年内首次上调

国内成品油价格“十三连跌”的漫漫“熊途”将止。9日，国家发展改革委发出通知，决定自2月10日零时起上调汽、柴油限价，每吨汽、柴油分别上调290元和280元，折算到90号汽油和0号柴油(全国平均)每升零售价格分别上调0.21元和0.24元。调整后北京的92号汽油每升为6.00元。 **(据新华社)**