肆无忌惮的网络霸权

起底美国“黑客帝国”真面目

最近,一批美军秘密文件出现在社交媒体上,内容涉及俄乌冲突等各方面情报,还暴露了美方对联合国秘书长古特雷斯以及韩国、以色列、乌克兰等盟友的窃听行动。

与此前的“棱镜门”等诸多丑闻一样,这次泄密事件再次展现了美国肆意对他国进行窃听、发动网络攻击等霸凌恶行。长期以来,这个名副其实的“黑客帝国”一直在违反国际法和国际关系基本准则,打着“维护国家安全”幌子在网络空间肆意妄为,严重损害别国主权和全球互联网用户隐私,其根本目的是利用网络霸权来维护自身在现实世界中的霸权。

窃密者　“不会接受任何地方处于其监控视野之外”

据《纽约时报》报道,韩国政府去年年底应美方请求对美出售炮弹,但强调这批武器的“最终用户”必须是美军。此次泄露的美国情报部门对韩窃听内容显示,韩国政府内部有人担心美国将这批武器转运至乌克兰,这将违反韩国不向交战国提供致命武器的政策。

窃听事件曝光后,韩国舆论一片哗然。韩国最大在野党共同民主党发表声明指责美方此举侵害韩国主权,要求美方说明真相并确保此类事件不再发生。《韩民族日报》评论说,韩美虽为同盟,但美国在敏感问题上窃取韩国内部信息会严重损害韩国国家利益。韩国广播公司指出,若窃听一事属实,美国的国际信誉将不可避免地受损。

这并非第一次出现韩国遭美国窃听丑闻。2013年,美国国家安全局泄密文件就显示,美国对包括韩国驻华盛顿大使馆在内的数十个外交机构实施窃听。韩国政府当时要求美国做出解释,美方则以“将重新评估情报行动”的说法搪塞。如今看来,美方评估的结果就是“继续窃听”。

遭美国窃听的盟友还可以列出一串名单,比如欧洲国家、以色列、乌克兰等。美国还窃听了此前古特雷斯和其他联合国工作人员关于黑海粮食运输协议的对话。

事实上,无论盟友还是“对手”,都是美国无差别窃听的对象。英国情报专家安东尼·韦尔斯在《五眼联盟》一书中指出:“历史上,在情报投资规模、全球情报资源数量以及分析方法上投入最多的国家一直是美国。”

2013年,美国前防务承包商雇员爱德华·斯诺登向媒体曝光了美方代号“棱镜”的大规模窃听项目,其对象不仅覆盖美国公民,也包括法国、德国等欧洲国家的政要和民众。前英国《卫报》记者格伦·格林沃尔德在讲述斯诺登事件的《无处藏身》一书中列举了一组数据:美国国家安全局曾在30天内远程窃取970亿封邮件和1240亿条电话数据,其中包括德国的5亿份、巴西的23亿份、印度的135亿份、法国的7000万份、西班牙的6000万份……

2015年“维基揭秘”网站爆料,美国国家安全局曾在希拉克、萨科齐和奥朗德担任法国总统期间对其实施窃听。同年,该网站曝光美方针对日本的大规模窃听项目“目标东京”,对象涉及日本内阁府、经济产业省、财务省、央行等。

2021年5月,丹麦媒体爆料,美国国家安全局通过丹麦国防情报局接入当地网络,在2012年至2014年间窃听德国、法国、挪威、瑞典等国政要的短信和电话通话,这令欧美互信再遭重创。

美国的窃听无孔不入,手段五花八门,包括利用模拟手机基站信号接入手机盗取数据,操控手机应用程序,侵入云服务器,通过海底光缆进行窃密等。

“没有可避难之地,没有可安息之所,美国政府不会接受任何地方处于其监控视野之外。”美国记者巴顿·格尔曼在《美国黑镜》一书中这样写道。

攻击者　“通过网络攻击威胁着生活各个领域”

2010年,伊朗纳坦兹核设施大量铀浓缩离心机突然瘫痪。事后调查发现,这是一种名为“震网”的计算机病毒攻击所致,“震网”事件是首个得到充分技术实证、对现实世界中的关键工业基础设施造成了与传统物理毁伤等效的网络攻击行动。

全球网络安全厂商的接力分析勾画出了这次攻击行动的真相,并将幕后黑手锁定为美国等国的情报机构。2016年,美国导演亚历克斯·吉布尼执导的纪录片《零日》上映,片中就详细描述了美国及其盟友用“震网”病毒攻击伊朗的过程。

2012年,《华盛顿邮报》报道,美国和以色列联手研发的“火焰”病毒一度在中东地区传播,迫使伊朗短暂切断石油部门和相关设施的互联网连接。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种名为“雷金”的计算机恶意软件,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使用的工具之一。

古巴外交部负责美国事务的官员约翰娜·塔夫拉达在接受新华社记者采访时指出,美国将互联网武器化,向一些网络平台投入大量资金,试图通过编造故事、传播谣言来抹黑古巴,为美国对古制裁寻找借口。

乌克兰危机升级后,俄罗斯频遭网络攻击,俄总统府、国防部等核心政府部门网站一度频繁出现页面瘫痪或无法访问的情况。美国前国务卿希拉里·克林顿在接受美国媒体采访时公开鼓动美国黑客对俄进行网络攻击。美军网络司令部司令保罗·中曾根承认,美军开展了进攻性网络行动以支持乌克兰对抗俄罗斯。

俄外交部国际信息安全司司长安德烈·克鲁茨基赫说,截至2022年5月,来自美国等国的6.5万多名黑客定期参与针对俄方关键信息基础设施的攻击。西方某些国家大肆鼓吹其“有权”发动所谓“先发制人”的网络攻击,“网络绞杀”已成为西方制裁措施的一部分。

根据黑客组织“影子经纪人”爆料,美国国家安全局针对包括俄罗斯、日本、西班牙、德国、意大利等在内的超过45个国家的287个目标进行网络攻击,持续时间长达十几年。“维基揭秘”曝光了8761份据称与美国中央情报局网络攻击活动有关的秘密文件,其中包含庞大的网络攻击装备库,覆盖了很多平台,不仅包括常见的操作系统,还包括智能电视、车载智能系统、路由器等网络节点单元和智能设备。

中国也是美国网络攻击的主要目标之一。中国国家互联网应急中心网站2021年发布的互联网网络安全态势综述报告显示,2020年中国捕获计算机恶意程序样本数量超过4200万个,其中境外恶意程序主要来自美国,占比达53.1%。2020年,控制中国境内主机的境外计算机恶意程序控制服务器数量达5.2万个,其中位于美国的控制服务器约1.9万个,高居首位。

美国不遗余力地推动网络空间军事化,大力发展进攻性网络作战力量,打造体系化的网络攻击平台和制式化的攻击装备库。2017年,美军网络司令部升级为美军第十个联合作战司令部,网络空间正式与海洋、陆地、天空和太空并列成为美军的“第五战场”。2018年美国国防部网络战略报告强调,要在网络空间“先发制人”。美国兰德公司预计,到2024年,美国拥有全方位作战能力的网络任务分队数量可能达到167支。

土耳其安全问题专家伊斯迈尔·哈科·佩金在接受新华社记者采访时说:“美国拥有强大的网络部队,有能力通过网络攻击威胁日常生活各个领域,从卫生系统到水电系统,可不费吹灰之力使各国陷入困境。”

霸凌者　“规则只有一个,那就是没有规则”

美国掌握网络霸权,可以在网络空间利用不对称优势霸凌他国。

美国拥有庞大复杂的情报体系,其情报作业遍布网络空间和物理空间各个领域,各种攻击武器完整覆盖从服务器到智能移动设备的各类使用场景,适配各类操作系统,功能上涵盖侦察、物理隔离突破、内网横向移动、持久化潜伏驻留、供应链与物流链渗透、远程控制等网络攻击各个环节。

从“棱镜”计划、“怒角”计划、“星风”计划,到“电幕行动”、“蜂巢”平台、“量子”攻击系统,众多事实证据证明,美国是名副其实的“黑客帝国”。

对于美国倚仗网络霸权霸凌世界的恶行,各国看得一清二楚。

美国的目的是维护自身霸权。伊朗政治分析人士拉扎·卡莱诺埃指出,网络战是美国“混合战争”的工具之一,与经济制裁、恐怖活动、心理战以及军事行动一样,都是其用来干涉其他国家、实现自身政治目的的手段。

美国的行动严重危害世界。美国为谋求自身绝对安全,肆意侵犯他国网络主权、破坏他国信息安全,严重阻碍国际社会在维护网络空间安全和数据安全方面的努力,严重影响网络空间的国际秩序,严重破坏全球战略稳定。俄外交部国际信息安全司司长克鲁茨基赫说,美国等西方国家将网络空间军事化,试图将这一空间变成国家间对抗的舞台,这加剧了引发直接军事对抗的风险,会带来难以预测的后果。

美国的规则是“唯我独尊”。美国在肆意破坏网络安全的同时,还经常贼喊捉贼地污蔑其他国家。克罗地亚萨格勒布大学教授赫尔沃耶·克拉希奇指出,美国一方面在不断对包括盟友在内的国家进行监听,另一方面则在大肆指责别国搞网络监控,这是典型的双重标准。俄外交部发言人玛丽亚·扎哈罗娃说,美国寻求以武力为基础在全球范围内确立其数字技术主导地位,在信息通信技术领域推行所谓“基于规则的秩序”,但华盛顿自己却不遵循“任何规则”。

最近发生的美国情报泄露事件再次证明了“维基揭秘”网站创始人朱利安·阿桑奇的论断:不要期待这个“监听超级大国”会做出让人尊重的行为。对美国而言,“规则只有一个,那就是没有规则”。

新华社北京4月17日电

2013年10月26日,数百名民众在美国首都华盛顿参加示威活动,抗议美国家安全局(NSA)针对普通美国民众的大规模监控活动。

本版图片据新华社