

“棱镜门”十周年 美国“监听瘾”越来越重

2013年6月5日,英国《卫报》率先通过美国前防务承包商雇员爱德华·斯诺登的爆料,曝光了代号“棱镜”的美国秘密监听项目。其监听对象不仅包括美国民众,也包括法国、德国等欧洲国家的政要和百姓。

十年过去了,遭到美国政府通缉的斯诺登如今居住在俄罗斯,已获得俄罗斯国籍。“棱镜门”事件引发全球对美国大规模监听活动的强烈谴责,但美国并未悔改,十年来仍不断曝出各种监听他国的丑闻,其中不少受害国家还是美国的盟友。这些事件反复证明,美国为维护自身霸权不择手段,是不折不扣的“黑客帝国”。

惊天丑闻

德国《明镜》周刊援引斯诺登提供的文件披露,美国国家安全局2009年对122名外国领导人实施监听,建有一个专门存放外国领导人信息的数据库,其中关于时任德国总理默克尔的报告就有300份。监听名单从“A”开始,按名字首字母顺序排列,第一位是时任马来西亚总理阿卜杜拉·巴达维,默克尔排在“A”区第9位,名单上最

后一位是时任乌克兰总理尤利娅·季莫申科。

斯诺登提供给《卫报》的一份文件显示,美方设于英国北约克郡的一处情报分支机构在2009年二十国集团峰会上监听时任俄罗斯总统梅德韦杰夫与俄国内的卫星通话。这次监听的时间是在梅德韦杰夫与时任美国总统奥巴马举行会谈后数小时,两人在会谈中刚

刚就建立互信达成共识。

“棱镜门”事件令美方十分尴尬和恼火,斯诺登因此被美国政府以间谍罪、盗窃罪和未经授权泄露国防及情报信息等罪名通缉。2019年,美国政府还起诉斯诺登,指控他出版的回忆录未经政府审查,违反了保密协议,要求没收其出书和参加公共活动获得的收入。斯诺登在社交媒体上嘲讽:

“很难想象还有比美国政府的一纸诉状更能证明这本书内容真实性的方式了。”

国际社会“苦美久矣”

上海国际问题研究院网络空间国际治理研究中心秘书长鲁传颖表示,面对美国政府肆无忌惮的网络监听和窃密活动,国际社会亦是“苦美久矣”,这也反映出当前国际法和全球治理机制的“失灵”,即并不能完全对逐渐综合化的网络空间安全议题做出有效的回应。

第一,美国在各种舆论压力下转嫁危机。这主要体现在:对内,迫于民众和企业压力,大幅增加监管举措,避免引发民意的指责;对盟友国家,根据不同的情况提供有限的“承诺”,缩小监控的范围,以减轻国际舆论压力;对其他国家的诉求,则置之不理,甚至通过增加预算拨款和成立新的机构加大监控力度。“棱镜门”事件爆发后,国际社会虽然在一段时间内向美国政府施加了压力,例如2014年在巴西圣保罗召开的“互联网治理的未来——全球多利益相关方会议”,商讨网络空间全球治理改革等。这些举措在美国政府的操纵下并没有对美国在大规模网络空间开展大规模监控产生实质性的改变。这反映出当前国际法和全球治理机制的“失灵”,并不能完全对网络空间安全这一新议题做出有效的回应。

第二,美国仗仗网络霸权有恃无恐监听他国。全球网络技术标准主要由美国制定,各国只能被动采纳。各国在关键网络技术、设备和产品上严重依赖美国的供给,还不时面临各种形式的技术封锁。由于其他国家的网络空间技术能力落后于美国,这就使美国可以无惧其他国家的施压和报复措施,继续在网络空间开展相关行动。大规模网络监控依托网络空间先进的技术手段,被监控者难以察觉,即便是被发现,也难以“取证”,更不用说开展起诉。从现实情况看,各国无法通过国际法和相关的网络空间全球治理机制维护自身权利。

第三,美国网络霸权行径加剧全球网络空间分裂。在网络自由主义思想的影响下,大多数国家的政府选择网络所带来的效率和便捷性,而忽视了网络空间的疆界意识,为“棱镜计划”的开展留下了可乘之机。“棱镜门”事件之后,各国政府面临保护国家网络空间安全、公民隐私、企业知识产权的巨大压力。“棱镜门”事件揭露了各国所面临的三种威胁,一是美国在他国的网络空间如入无人之境;二是美国跨国企业将本国用户数据传回美国的过程中遭到美国政府的截留;三是诸多美国互联网企业私下与美国情报机构合作,为情报部门的监控预留后门。网络空间国际行为规范的缺失,进一步迫使各国政府必须从立法和执法层面规范外部行为体在本国网络空间的行为规范。以德国为例,在“棱镜门”事件之后,时任德国总理默克尔加大了数据保护的立法和执法力度,发布《信息保护基本条例》,设立信息安全官,加大对企业跨境数据传输的监管,要求大企业在德国设立数据中心。此外,在欧盟各国的推动下,欧盟法院在裁定中指出,由于美国未能对来自欧盟的用户数据进行有效保护,欧美之间签订的《安全港协议》《隐私盾协议》先后宣告无效。

监听成瘾

“间谍行为为了一项已经嵌入美国历史、根深蒂固的习惯。”美国《时代》周刊一篇文章这样评论。

美国并未从“棱镜门”事件中汲取教训,“监听瘾”反而越来越严重,不断践踏别国主权,侵犯互联网用户隐私,严重危害国际网络安全。2015年“维基揭秘”网站爆料,美国国家安全局曾对多位法国总统进行长时间窃听;2021年丹

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;今年4月,一批美军秘密文件出现在社交媒体上,内容涉及美国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,再次暴露美国监听行动范围之广。

如今,美国的对外监听行为已走向“制度化”。美国政府打着“国家安全”和“反恐”名义,通过《涉外情报监视法》等立法,不断扩大安全机关权限,对他国进行监听。美国《涉外情报监视法》702条款将于今年年底到期,该条款允许美国情报机构在未经法院许可的情况下对“外国目标”实施监听,搜集其电话、短信及互联网通信内容。最

近,美国政府正敦促国会延长该条款有效期,白宫方面甚至直接将条款称为美国的“宝贵工具”,宣称延长该条款有效期是本届美国政府的“关键优先事项”。

“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·格尔蒙在《美国黑镜》一书中如此揭露。

手段多样

美国的窃密手段不仅五花八门,而且对网络空间的接入路径、终端设备和软件服务的妨害也日渐加深,具体包括利用模拟

手机基站信号接入手机窃取数据,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。此外,美国在近100所驻外

使领馆内也安装了监听设备,以便对驻在国进行窃密。2021年5月,法国总统马克龙和时任德国总理默克尔表示,美国国家安

全局利用丹麦情报部门对盟国领导人进行监听的做法不可接受。这再次揭露了美国监听全球

霸权工具

多年来,美国声称维护联合国作用,却在联合国掀起“监听风暴”;自诩自由、民主的所谓“捍卫者”,却利用先进技术构建“监听帝国”;标榜维护信息安全,却在全球布下“信息安全陷阱”。这些自相矛盾的举动充分表明,美方在网络

空间实施双重标准,其根本目的是维护自身霸权和私利。

厄瓜多尔拉丁美洲新闻社的评论文章指出,随着霸权开始衰落,美国为维持自身地位而变得更加暴力和危险。这时,美国的各种干预活动变本加厉,斯诺登披露的

大规模监听活动就是其中之一。

伊朗政治分析人士拉扎·卡莱诺埃认为,包括监听在内的网络战是美国“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、达到自身政治

目的的手段。

西班牙《国家报》刊文指出,世界上有许多地图,如地理地图、人口地图、经济地图、军事地图及政治地图,这些地图可以提供各类信息,但都无法像美国的“监听地图”那样呈现出关于霸权的赤裸裸现实。

黑客帝国

一段时间以来,美国政府、智库、媒体等基于意识形态偏见,一再对其他国家在互联网管理、数据安全等方面的合理做法提出无端指责。实际上,“贼喊捉贼”的美国一贯大搞“数字霸权”,破坏全球网络空间的公平基础,妨碍通信行业合作创新,是全球互联互通的最大障碍。

美国声称倡导网络透明和信息自由流通,实际上却是全球头

号“黑客帝国”,多年来投入大量资金和资源开发部署用于监控网络通信的技术,把全球互联网空间视为“自家后院”,肆意践踏本国公民乃至其他国家的数据隐私权。

美国的“数字霸权”不仅体现在其各种网络监控上,还在于其利用自身产业优势和市场地位,在涉及数据通信和互联网服务的行业中搞双重标准,打击来自新兴经济体的跨国企业,维护自身在网络空间的主导地位。

移动通信技术是支撑全球互联网进一步提升和普及的重要技术。第五代移动通信技术(5G)建设过程中,美国在毫无实质证据的

前提下,以“国家安全”为由极尽所能对其他国家施压,要求他们将中国企业排除出5G网络建设,而那些迫于压力如此照办的国家往往会付出高昂成本以及5G部署延后的代价,最终损害的还是当地企业和消费者的利益。

在下一代移动通信技术(6G)上,美国仍坚持这一思路,拉拢盟友搞研发“小圈子”,把中国排除在外,完全无视全球产业合作对通信技术创新和标准设立的关键推动作用。

美国的单边霸凌行径甚至延伸到偏向娱乐的互联网短视频平台。抖音海外版(TikTok)成为深受美国年轻人青睐的短视频平台

后,很快吸引美国政府注意,成为被无端打压的目标。这种出于政治目的对合法经营的外国互联网企业公开进行打压的行为,违背了最基本的市场公平。

互联网诞生至今,已催生大量数字技术和服务,不断融入我们生活的方方面面。同时,各国也越来越认识到数据的价值,无论是发达国家还是发展中国家,都在加强相关立法管理,推动互联网、大数据等有序和良性发展。而美国为一己私利,不但一再践踏互联网的包容性,还对其他国家的网络管理横加指责,阻挠创新交流,令全球“数字鸿沟”问题不断恶化。