法治日报
星期一
2022年9月19日

环球法治 05 专刊

主编/赵阳
见习编辑/王卫
美编/李晓军
校对/张胜利

LEGAL DAILY

编者按

9月5日，国家计算机病毒应急处理中心和360公司分别发布了关于西北工业大学遭受境外网络攻击的调查报告。调查发现，美国国家安全局（NSA）下属的特定入侵行动办公室（TAO）使用了40余种不同的专属网络攻击武器，持续对西北工业大学开展攻击窃密，窃取该校关键网络设备配置、网管数据、运维数据等核心技术数据。调查报告揭开了“黑客帝国”的真面目，也向国际社会抛出一个问题：网络攻击无所不用其极，美国究竟是何居心？

美国才是全球网络空间不安全的罪魁祸首

图为位于马里兰州米德堡的美国国家安全局（NSA）。 CFP供图

□ 际文

近日，国家计算机病毒应急处理中心和360公司分别发布了关于西北工业大学遭受境外网络攻击的调查报告，报告揭露了美国国家安全局（NSA）长期以来针对包括西北工业大学在内的中国信息网络用户和重要单位开展网络间谍活动。

作为拥有最强大网络技术实力的国家，美国以“国家利益”为幌子，违反国际法和国际关系基本准则，无视基本道德信义，对他国实施大规模网络窃密与监听监控，严重损害他国国家安全和公民个人信息安全。“网络霸凌”大国的种种行径，暴露了美国才是全球网络空间不安全的罪魁祸首。

网络窃密细节披露

国家计算机病毒应急处理中心13日公布《美国NSA网络武器“饮茶”分析报告》。报告显示在此次针对西北工业大学的攻击中，美国NSA下属特定入侵行动办公室（TAO）使用“饮茶”作为嗅探窃密工具，将其植入西北工业大学内部网络服务器，窃取了SSH、TELNET、FTP、SCP等远程管理和远程文件传输服务的登录密码，从而获得内网中其他服务器的访问权限，实现内网横向移动，并向其他高价值服务器投送其他嗅探窃密类、持久化控制类和隐蔽消痕类网络武器，造成大规模、持续性敏感数据失窃。随着调查的逐步深入，技术团队还在西北工业大学之外的其他机构网络中发现了“饮茶”的攻击痕迹，很可能是TAO利用“饮茶”对中国发动了大规模的网络攻击活动。

9月5日，外交部发言人毛宁就此事回答记者提问时表示：“美国国家安全局对中国实施网络攻击和数据窃密的证据链清晰完整，涉及在美国国内对中国直接发起网络攻击的人员13名，以及为构建网络攻击环境而与美国电信运营商签订的合同60余份、电子文件170余份。报告显示，美方先后使用41种专用网络攻击武器装备，对西北工业大学发起攻击窃密行动上千次，窃取了一批核心技术数据。美方还长期对中国的手机用户进行无差别语音监听，非法窃取手机用户的短信内容，并对其进行无线定位。”

事件曝光后，9月8日，外交部美大司司长杨涛就美国对我西北工业大学实施网络攻击窃密向美国驻华使馆提出严正交涉。

事实上，中方已经通过多个渠道要求美方对恶意网络攻击作出解释并立即停止不法行为，但是迄今还没有得到美方实质性回应。正如发言人所说，美方行径严重侵犯中国有关机构的技术秘密，严重危害中国关键基础设施安全、机构和个人信息安全。美方有关行为必须立即停止，并作出负责任的解释。

“黑客帝国”的真面目

美国政府主导的网络犯罪已成为全球网络毒瘤，中国是美国网络攻击的重要目标，但绝不是唯一目标。

长期以来，美国滥用其技术优势，在全球范围内实施大规模、有组织、无差别的网络窃密、监控和攻击，手段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，在美国近100所驻外使领馆内安装监听设备对驻在国进行窃密等，是名副其实的“黑客帝国”“窃密帝国”。

2013年的“斯诺登事件”让国际社会得以一窥美国“黑客帝国”真面目。美国前防务承包商雇员斯诺登曝光美国政府广泛进行网络监听，连自己的盟国都不放过。此后，一些西方国家媒体也纷纷揭批“盟友”美国的行径：德国《明镜》周刊报道说超过5亿条德国电话和互联网数据被美国国家安全局窃取，法国《世界报》则报道了法国境内约7000万条电话数据被美国国家安全局窃取的情况。

2015年“维基解密”公布的据称是美国中央情报局网络攻击项目的文件显示，美国国家安全局对希拉克、萨科齐和奥朗德3位法国前总统都进行过监听，以了解他们的施政纲领和对外政策。

尽管各国舆论一致谴责，但美国非但没有收手，反而变本加厉。2021年5月，丹麦广播公司曝光了美国国家安全局通过丹麦国防情报局接入丹麦互联网获取原始数据，以监听时任德国总理默克尔以及法国、瑞典、挪威等欧洲盟国领导人和高级官员。监听丑闻曝光后，法国总统马克龙以及默克尔均要求美国就此作出解释。马克龙说：“如果这一消息是准确的，这在盟国之间是不可接受的。”

对此，法国24小时新闻台在报道中称，美国网络监控的野心并不新鲜，他们想要窃听整个世界，包括他们的盟友。多年来，美国还打着“维护公共安全”的幌子，要求一些高科技公司在加密应用程序中设置“后门”，以便为其开展所谓“网络执法行动”提供便利。

不仅如此，在美国国内，民众隐私也被肆意践踏。就在今年4月，美国国家情报总监办公室发布的年度报告显示，过去一年，美国联邦调查局在没有搜查令的情况下，对美国民众的电子数据进行了多达340万次的搜查。

“今天美国越来越多地把监控手段应用到全球其他地区。”美国凯斯西储大学法学教授科弗警告说。

违反国际关系准则

美国违反国际法和国际关系基本准则，在国内外大范围监控、监听等行为，招致国际社会的普遍不满。

英国《卫报》认为，“9·11”事件的一大后遗症是，美国成了“监控无处不在”的国家，其庞大的监控基础设施数量激增，以至于没有人知道它的成本是多少，也没有人知道它雇用了多少人，“多年过去了，这个监控国家依旧在秘密地运行”。

曾供职于英国阿伯丁大学的国际法学教授托尼·卡蒂认为，《外国情报监视法》允许美国情报机构跟踪世界上任何人的电子活动，这被广泛认为是对世界各地人们人权，特别是隐私权的侵犯，是对其他国家管辖权的非法干预。

美国国会参议院情报委员会的两名议员披露，美国中央情报局有一个秘密、未公开的数据存储库，一直在美国境内实施大规模监控项目。这两名议员称，该计划涉及大量的数据收集，可以未经授权就对美国人进行“后门”搜查。美国《财富》杂志网站指出：“近10年来，美国情报机构大规模违规收集数据，这对美国来说，是最糟糕的事情。”

然而，具有讽刺意味的是，美国这样一个窃密大户，居然打着“清洁网络”的旗号，声称要维护网络安全。这充分暴露了美国维护网络安全是假，打压竞争对手是真；维护盟友安全是假，维护自身霸权是真。

正如有评论所说，对内虎视眈眈，长期以非法手段监控美国公民，对外长臂管辖，辅以多方窃密和网络攻击，美政府编造的“国家安全”种种说辞正一个接一个被世人识破，成为美国谋求霸权最显著的政治注脚。

维护网络安全是国际社会的共同责任。对此，国际社会早有共识，越来越多的国家正在致力于携手构建网络空间命运共同体。美国政府的恶劣行径终将自食恶果。

短评

网络空间安全应由世界各国共同开创

众所周知，美国为了巩固其全球霸主地位，利用技术资源优势，经常打着“国家安全”和“人权保护”的幌子，自诩为国际社会的“网络卫士”“人权卫士”。实际上，美国从未停止过对他国政府、企业、个人的无差别监听、窃密与攻击，横行网络世界，无端发起单边制裁，制造混乱。

诸多臭名昭著的监听计划，使美国网络霸权暴露无遗。尽管美国极力塑造网络自由民主的国际形象，但“棱镜计划”“怒角计划”“星风计划”“强健计划”“上游计划”“电幕行动”等监听行为相继被曝光在光天化日之下，举世哗然，使得国际社会不得不重新审视美国网络战略。

事实上众多监听丑闻仅仅是美国实施网络监听的冰山一角，即使受到国际社会的强烈谴责和声讨，美国依然未放弃全球网络监听行动，继续在网络霸权的道路上我行我素、恣意妄为。

美国这种毫无底线地干涉他国内政，肆意践踏他国公民人权的恶劣行径，给全球互联网安全带来了严峻的风险和挑战。

中国历来倡导诚实守信、健康文明的网络行为，致力于推动建立普遍适用的网络空间国际规则，呼吁构建和平、安全、开放、合作、有序的网络空间命运共同体。2022年7月，世界互联网大会国际组织在北京成立，来自6大洲近20个国家的百余家互联网机构、组织、企业及个人加入，成为初始会员。该组织的成立顺应了信息化时代的发展潮流，呼应了国际社会深化对话合作的呼声。网络空间关乎人类命运，网络空间安全应由世界各国共同开创。

“积极网络防御”拟将写入新版《国家安全保障战略》

日本又要图谋“自卫队网络防卫队”扩军

□ 本报记者 苏宁

据日本媒体报道，多名日本政府相关人士透露，日本政府正计划建立所谓“积极网络防御”体制，并拟将其作为方针写入今年底出台的新版《国家安全保障战略》。据称，“积极网络防御”体制将授权自卫队及日政府相关机构对网络空间实施常态化巡逻监控、侦测攻击症候、锁定攻击源头并先行采取反制措施。分析人士指出，这一举动是日本在网络空间“扩军”的新动向，对于日本在新兴领域突破专守防卫、发展先制作战能力的企图，外界必须保持警惕。

确立“积极网络防御”

据日本《读卖新闻》报道，为强化应对以通信、电力等重要基础设施为目标的网络攻击，日本政府计划建立所谓“积极网络防御”体制。该体制旨在通过常态化实施网络巡逻监控，第一时间掌握并应对可能危及日本安全保障的可疑网络行为。为此，日本政府将授予相关机构实施系统网络入侵、可疑网络行为解析等权限，相关机构有权采取摧毁攻击方数据及文件等反制措施。

报道认为，此前日本政府一般在网络攻击事态发生后再开展情报搜集等应对工作，如果“积极网络防御”体制得以实现，日本网络防卫能力将得到根本性强化。

据了解，“积极网络防御”体制的工作将由内阁网络安全中心（NISC）与自卫队网络防卫队共同承担，目前自卫队网络防卫队编制约540人。今后，日本政府将从经费及编制等方面进一步加强对NISC和自卫队网络防卫队的投入。

分析人士指出，“积极网络防御”的概念并非首次提出，官民合作，对网络攻击进行事前的、积极的防御是日本既定的网络安全战略，日本2018版及2021版《网络安全战略》中都有提及。但是，此次将“积极网络防御”确立为体制提出且明确相关内容尚属首次，另外，由于网络领域是日本防卫力量建设重点，因此，将“积极网络防御”体制明确写入《国家安全保障战略》的新动向十分重要，值得外界持续关注。

网络“扩军”潜滋暗长

近年来，日本积极强化常规防卫力量引起外界关注，然而，在网络等新兴领域，日本以维护网络安全为名推进网络作战力量“扩军”却不易被人察觉。

综合日媒报道，日本自2006年起，每年举行“分野横断演习”，参加人数由最初的90人扩大到2021年的4800人；2008年成立“自卫队指挥通信系统队”；2014年增设由防卫大臣直接管辖的“网络防卫队”；2022年3月进一步整编成立“自卫队网络防卫队”。根据计划，自卫队网络作战力量还将在2023年底前扩充至1000人以上规模，并建立统一的指挥体系，此次将“积极网络防御”写入安保战略文件，与此不无关系。

日本防卫省还通过开展国际合作、加强院校培训等多项措施提升网络防卫相关人员的素质。自2021年起，自卫队连续两年参加北约网络防御卓越中心（CCDCOE）举行的网络防御实战演习“锁盾”（Locked Shields）；海上自卫队的网络作战力量于2021年首次与美国海军实施了应对网络攻击的共同训练；陆上自卫队高等工科学校2021年起正式开设网络专修课程；陆上自卫队通信学校也设立了负责网络培训的网络教官室。

此外，日本防卫省面向全社会公开招募网络人才，聘请担任网络安全顾问。日本电报电话公司和另一家大型网络安全公司分别有1名网络专家通过公开招募，以“网络安全综合顾问”的身份到防卫省任职；防卫省还将一些通过选拔的网络人才发展为“预备自卫官”，这些人平时在地方企业供职，有任务时可迅速投入战斗。

图为在日本东京的防卫省总部，一名工作人员在大门旁守卫。 新华社发

谋求松绑炒作网络威胁

日本将网络、电磁、太空等新兴领域作为未来防卫力量发展重点，近年来连续组建成立网络防卫队、电子作战队和宇宙作战群。为谋求军事松绑，日本不惜罔顾事实，抹黑攻击，恶意渲染“邻国威胁”，大肆炒作网络威胁。

日本2021版《网络安全战略》首次明确称中国、俄罗斯和朝鲜构成所谓“网络威胁”，并表明同美国、澳大利亚和印度等国开展合作的方针。分析人士指出，日本在网络安全战略上刻意配合美主导的“印太战略”；日美“2+2”会谈称网络攻击适用于《日美安保条约》第5条；日美网络作战力量开展联合训练。种种迹象表明，日本肆意树立假想敌，煽动对立，选边站队，其目的就是以此掩盖其强化网络作战能力，打造网络攻防联盟，实现在网络领域军事松绑的真实企图。

有分析指出，在和平宪法尚存背景下，日本可能以网络安全防御和太空安全保护为由，发展天基侦察监视系统，通过与美国合作开发类似“星链”的低轨卫星互联网系统，增强自卫队态势感知和通信能力。另外，网络空间军事行动的隐秘性和特殊性，将成为日本自卫队活动的“灰色地带”。可以预计，未来日本将进一步扩充军备、扩大自卫队活动范围，并变得越来越具有进攻性，值得持续关注。

环球观察

冬季临近 欧洲能源危机仍难以解决

□ 本报见习记者 王卫
□ 本报记者 吴琼

在出台多轮对俄罗斯制裁措施后，欧洲能源和生活物品价格大幅攀升，民生日益艰难。近日，欧盟委员会在法国斯特拉斯堡发布年度“盟情咨文”，聚焦欧盟面临的能源危机。“盟情咨文”提出了一系列“节能降费”新提议，以应对可能在今年冬天进一步恶化的能源危机，包括强制能源公司出让利润、要求成员国减少电力和天然气的使用量等。有分析认为，这些措施力度远远不够，无法向当前陷入经济困境的普通民众提供实际支持，短期内欧洲能源危机仍难以解决。

要求企业团结捐资

据道琼斯旗下新闻网站Market Watch报道，当地时间14日，欧盟委员会主席冯德莱恩发表年度“盟情咨文”时表示，“发电公司正在获得巨额利润。在市场经济中，获得利润是可以的，但在这个时期，由于俄乌冲突引发能源危机，公司通过榨取消费者的利益而获得创纪录的收入是错误的，这样的利润必须分享，分配给最需要的人。”

冯德莱恩表示，欧盟委员会建议改革欧盟电力市场，并对电力企业设置收入上限，预计此举将获得超过1400亿欧元资金，可用于缓解消费者的生活压力。

这份“盟情咨文”没有提及相关措施的具体内容，但多家媒体此前援引欧盟内部消息称，欧盟将要求石油、天然气、煤炭以及相关精炼加工企业参与“团结捐资”，以帮助欧洲国家缓解能源危机，各企业出资额度将根据2022财政年度所得应税超额利润计算，筹得的资金将用于帮助消费者和特定行业缓冲高涨的能源价格。

分析认为，“团结捐资”实质上是一种变相的暴利税，此前德国和意大利等国曾先后推出类似政策，欧盟委员会认为，2022年石油、天然气和煤炭公司的利润将同比增长5倍，因而有理由要求它们“团结捐资”。

此外，欧盟委员会还计划要求成员国将当前的用电量减少10%，将天然气的使用量减少15%，以确保各国民众“安全过冬”。

据悉，欧盟委员会主席每年向欧洲议会全会发表一次“盟情咨文”，回顾欧盟过去一年工作，阐述欧盟工作计划，对外政策等，并接受欧洲议会议员问询。在能源价格不断飙升的背景下，欧盟委员会今年报告的一大重点无疑是能源问题。

能源价格涨幅惊人

“盟情咨文”显示，与新冠疫情之前相比，欧盟天然气价格现已上涨10倍以上，“入不敷出正成为数百万企业和家庭焦虑的根源”。

据报道，俄乌冲突爆发后，欧洲对俄罗斯的石油和煤炭出口实施了制裁，作为回应，俄罗斯减少了对欧洲的天然气供应。目前，俄罗斯已对欧盟13个成员国部分或全部切断了天然气供应，随着冬季临近，欧盟国家正面临能源危机，部分国家可能出现轮流停电、工厂关闭甚至经济严重衰退的局面。

报道称，俄罗斯2日宣布“北溪-1”天然气管道将完全停止向欧洲输气，这导致荷兰所有权转让中心（TTF）天然气10月期货5日盘中价格一度暴涨超过30%。法国官方1日发布的数据显示，从2021年第二季度到2022年第二季度，法国家庭能源开支增长了28%。若政府没有采取天然气价格管制、零售电价涨幅设限之类的措施，能源开支涨幅将是现在的两倍。

能源价格飙涨也给欧洲工业带来沉重打击。据欧洲有色金属协会统计，受能源价格等因素影响，欧盟锌、铝产能已下降近半。欧洲化肥协会日前也宣布，在欧洲天然气价格比美国高出8到10倍的情况下，欧洲关键化肥原料氨的产能已萎缩38%。德国基尔世界经济研究所副所长斯特凡·科茨警告说：“从经济发展趋势上看，一场雪崩正在到来。”

德国《南德意志报》评论指出，随着乌克兰危机的持续，欧洲社会的团结正在瓦解。因为，每过一天，人们对供暖成本高企和物价上升的担忧都在加剧。

解决危机十分困难

当地时间14日，联合国秘书长古特雷斯在记者发布会上表示，当前欧洲能源危机仍难以解决。古特雷斯认为，在欧洲能源问题上，各方的利益交织在一起，有欧盟成员国的利益，也有能源公司的利益，这让解决欧洲能源危机十分困难。

欧盟委员会方面此前曾提议，通过限制俄罗斯天然气价格来达到降低能源价格的目的，但这一提议遭到不少成员国反对，因此限制俄罗斯天然气价格并没有出现在这份“盟情咨文”中。很显然，欧盟内部对于如何应对能源危机，仍然存在分歧。

古特雷斯表示，他14日与俄罗斯总统普京进行了通话，就续签和扩大黑海粮食出口协议进行了讨论。古特雷斯称，2023年全球或将面临真正的缺粮局面，出口俄罗斯化肥对于未来粮食供应安全至关重要，当前应移除俄罗斯化肥出口过程中存在的障碍。

“我们讨论了俄罗斯粮食和化肥出口中依然存在的障碍，我必须说，在化肥出口方面，全球面临一个强烈波动的局面，我们面临着化肥供应紧缩，移除俄罗斯化肥出口的障碍在当下是非常重要的。”古特雷斯说。

不过，强制能源公司出让利润以及要求减少用电量、天然气用量的做法，是否会遭到相关企业的反对、是否会对经济发展造成影响，目前仍是未知数。

英国《泰晤士报》网站报道说，在“长期和痛苦的经济压力下”，英国今年冬天有可能出现大规模的骚乱。

分析人士称，2022年以来，欧洲的能源危机问题持续发酵，许多国家的天然气价格屡创新高，导致生活成本飙升，在这期间，欧洲对进口能源高度依赖的脆弱性暴露无遗，各国政府和居民纷纷表示难以招架。可以预见的是，短期内，欧盟难以走出能源困境，欧盟各方围绕如何解决能源问题的博弈，仍将持续较长时间。