实施窃听窃密 蓄意嫁祸他国

——揭秘美国政府机构实施的网络间谍和虚假信息行动

今年以来,中国国家计算机病毒应急处理中心等机构先后发布专题报告,全面揭露美国政府机构对全球电信和互联网用户实施无差别监听,并为背后相关利益集团攫取更大的政治利益和经济利益,虚构子虚乌有的中国网络攻击威胁,合谋欺诈美国国会议员和纳税人的事实。

近日,相关机构再次发布专题报告,进一步公开美国联邦政府、情报机构和"五眼联盟"国家针对中国和其他国家及全球互联网用户联合实施网络间谍窃听窃密活动,并通过误导溯源归因分析的隐身"工具包"实施"假旗"行动掩盖恶意网络攻击行为、嫁祸他国的铁证,彻底揭穿"伏特台风"这场由美国联邦政府自编自导自演的政治闹剧真相。

网络空间的"变色龙"

此前,中国国家计算机病毒应急处理中心已经连续公开披露多款美国国家安全局(NSA)、中央情报局(CIA)开发的网络武器,详细分析了相关美国情报机构在对外网络攻击中所用的多款网络武器的功能,以及采用的高隐蔽性攻击技战术,但这些显然只是美国"黑客帝国"庞大网络武器库的"冰山一角"。

长期以来,美国在网络空间积极推行"防御前置"战略并实施"前出狩猎"战术行动,也就是在对手国家周边地区部署网络战部队,对这些国家的网上目标进行抵近侦察和网络渗透。为适应这种战术需要,美国情报机构专门研发用于掩盖自身恶意网络攻击行为、嫁祸他国并误导溯源归因分析的隐身"工具包",代号"大理石"(Marble)。该工具包是一个工具框架,可以与其他网络武器开发项目集成,辅助网络武器开发者对程序代码中各种可识别特征进行"混淆",有效"擦除"网络武器开发者的"指纹",使调查人员无法从技术角度追溯武器的真实来源。

该框架还有一个更加"无耻"的功能,就是可以随意插入中文、俄文、朝鲜文、波斯文、阿拉伯文等其他语种的字符串,这显然是为了误导调查人员,并栽赃陷害中国、俄罗斯、朝鲜、伊朗以及众多的阿拉伯国家。

"大理石"工具包框架充分暴露了美国情报机构在全世界开展的无差别、无底线网络间谍活动,并实施"假旗"(False Flag)行动,以误导调查人员和研究人员,实现栽赃"对手国家"的阴谋。

这种"假旗"行动并不仅限于代码特征层面,通过巧妙模仿网络犯罪团伙的攻击技战术,美国情报机构还可以虚构出各类完美的"口袋"组织。因此,美国网络战部队和情报机构的黑客就如同变色龙一般在网络空间中任意变换身份、变更形象,"代表"其他国家在全球实施网络攻击窃密活动,并将脏水泼向美国的非"盟友"国家。"伏特台风"行动就是一个典型的、精心设计的、符合美国资本集团利益的虚假信息行动。

网络空间的"窥探者"

美国国家安全局的资料显示,美国依托其在互联网布局建设中先天掌握的技术优势和地理位置优势,牢牢把持全球最重要的大西洋海底光缆和太平洋海底光缆等互联网"咽喉要道",先后建立7个国家级的全流量监听站,与美国联邦调查局(FBI)和英国国家网络安全中心(NCSC)紧密合作,对光缆中传输的全量数据深度开展协议解析和数据窃取,实现对全球互联网用户的无差别监听。

这些互联网数据监听的受益者众多,除了美国联邦政府情报机构和军事机构外,还有大量美国联邦政府行政部门,包括白宫、内阁官员、美国驻外大使馆、美国贸易代表办公室、美国国会,以及美国国务院、农业部、司法部、财政部、能源部、商务部、国土安全部等。"伏特台风"计划的参与者不仅仅限于美国情报机构,而是为了服务所谓美国资本的共同利益,很多美国政府机构都在其中起到了推波助澜作用。

情报监听的输出结果必然是各种可读的信息和数据,因此把海底光缆中的传输流量实时转化、翻译成可阅读、可检索的情报信息是美国国家安全局的另一项重要工作。为解决这个问题,美国国家安全局实施了两个重点工程项目:一是"上游"(UpStream)项目,主要功能是将前述监听站拦截的海底光缆原始通信数据进行全量留存,形成规模庞大的数据"水库"。二是"棱镜"(Prism)项目,其主要功能一方面是将"上游"项目中的原始通信数据按照互联网应用进行分类,并对通信内容进行还原分析;另一方面,为有效解决"上游"项目中的加密数据破解和网络通信流量路径覆盖不全等突出问题,美国政府强制规定"棱镜"项目直接从美国各大互联网企业的服务器上获取用户数据。

从美国国家安全局的文件中可以看到,隶属于美国国家安全局的"特定入侵行动办公室"(TAO)在全球范围内发动无差别的网络秘密入侵行动,并植入了超过5万个间谍程序(Implants),受害目标主要集中在亚洲地区、东欧地区、非洲地区、中东地区和南美地区。从美国国家安全局的内部文件中可以清楚看到,中国境内的主要城市几乎都在其网络秘密入侵行动范围内,大量的互联网资产已经遭到入侵。上述间谍软件程序的命令控制中心很多都位于美国本土之外的军事基地。

事出反常必有妖

在第二份关于"伏特台风"调查报告发布后,虽然美国官方机构与其主流媒体仍然保持沉默,但一些前任和现任美国政府机构官员以及部分美国网络安全公司通过社交媒体平台、美国的网络安全行业媒体和独立新闻媒体表达了对我方调查报告的观点与看法,其中不乏一些负面声音,声称我方报告"歪曲""滥用"了美国相关公司的研究成果,这些美国公司也争先恐后地发声"撇清关系"。

"威胁盟"公司的改口行为特别耐人寻味。该公司在接受媒体采访时声称,由于其在后续研究中发现了前期涉"伏特台风"报告中提供的感染指标存在错误才修改了原报告,这种"敷衍"的解释更加令人怀疑。"威胁盟"这种异常举动,只能说明其对原报告的篡改过程是在强大外部压力下被动而匆忙完成的。最新报告中的证据充分表明,美国情报机构对中国、俄罗斯、伊朗和阿拉伯国家实施的网络间谍活动,以及针对美国国会和纳税人实施的虚假信息行动是铁一般的事实。

微软公司威胁情报战略总监德格里波(Sherrod DeGrippo)在2024年度黑帽大会(BlackHat)期间表示所谓的"伏特台风"组织仍在活跃,且没有停止的迹象,却仍然没有给出任何能够说明该组织具有所谓"中国政府支持背景"的确凿证据。

多年来,美国联邦政府机构出于自身一己私利,不断将网络攻击溯源问题政治化,一些像微软和CrowdStrike这样的公司则为了迎合美国政客、政府机构和情报机构,出于提高自身商业利益考虑,在缺乏足够证据和严谨技术分析的情况下,热衷于用各种各样稀奇古怪且带有明显地缘政治色彩的名字对黑客组织进行命名,如"台风""熊猫"和"龙"等。

中国一向反对政治操弄网络安全事件的技术调查,反对将网络攻击溯源归因问题政治化。而美国联邦政府机构则不断在幕后教唆纵容,在通过编造子虚乌有的网络攻击威胁骗取了大量国会预算后,野心越来越大,终有一天将会"搬起石头砸自己的脚"。克里斯托弗·雷等美国无良政客为谋取不正当利益,频繁登场操弄"伏特台风"虚假叙事欺骗美国国会和民众,也必将遭到美国人民对其的正义审判。 (新华社北京10月14日电)

朝方指责韩军方系无人机侵朝领空事件"主犯"

新华社首尔10月14日电 朝中社14日报道,朝鲜劳动党中央委员会副部长金与正当天发表谈话说,朝方清楚知道韩国军方系无人机侵犯朝鲜领空事件的"主犯"。

据朝中社此前报道,朝鲜外务省11日晚间发表声明,谴责韩国无人机侵犯朝鲜领空,称此系严重犯罪行为。据韩联社11日报道,韩国国防部长官金龙显当天表示,韩军方没有向朝鲜发射无人机。

据朝中社13日报道,朝鲜国防省发言人说,朝鲜人民军总参谋部已指示朝韩边境的部队进入射击准备态势。

联合国秘书长:

联黎部队将继续坚守阵地

新华社联合国10月13日电 联合国秘书长古特雷斯13日表示,尽管联合国驻黎巴嫩临时部队(联黎部队)在过去几天内遭到多起袭击,但联黎部队仍将继续坚守在所有阵地。

古特雷斯当天发表声明说,以色列国防军坦克破坏联黎部队驻地大门强行进入的行为令人深感担忧。声明强调,联合国的"不可侵犯性"必须在任何时候得到无条件尊重,联合国机构人员及其财产的安全必须得到保障。

古特雷斯说,对维和人员的袭击违反了包括国际人道主义法在内的国际法,这些行为可能构成战争罪。他呼吁包括以军在内的各方不要采取任何危及维和人员的行动,停止敌对行动并全面执行联合国安理会第1701号决议。

古特雷斯表示,联黎部队正在采取一切可能措施,保证维和人员安全。他对联黎部队维和人员致以敬意。

连日来,以军频频袭击联黎部队。10日,以军一辆坦克向联黎部队位于纳古拉地区司令部的一座哨塔开火,造成两名维和部队人员受伤;11日,以军袭击又造成两名维和部队士兵受伤;12日,联黎部队一名维和人员遭附近军事活动的枪弹击伤;13日,两辆以军坦克强行进入联黎部队驻地。以方行为受到国际社会广泛谴责。12日,参与向联黎部队派遣维和人员的40个国家发表联合声明,强烈谴责针对维和人员的袭击。

13日早些时候,以色列总理内塔尼亚胡在视频声明中说,黎真主党将联黎部队用作"人盾",以军曾多次提出联黎部队撤出战区的要求,但屡遭拒绝。他声称,拒绝撤离将危及联黎部队士兵及以军士兵的生命安全。

10月2日,一名男子游览摩洛哥东南部拉希迪耶附近暴雨过后的沙漠。

撒哈拉沙漠部分地区近日遇到罕见降雨,雨量之大为数十年来少见,导致一些地方出现水从沙丘中冒出的奇景,有些干旱地区甚至遭遇暴雨引发的洪水。

新华社/美联

美国向以色列提供"萨德"反导系统说明什么

美国国防部13日说,美国将向以色列提供一套"萨德"反导系统并派遣相关美军人员,以帮助以方提高防空能力。在以色列对黎巴嫩军事行动日益升级且誓言报复打击伊朗的背景下,美国这一举动被认为给中东紧张局势火上浇油。伊朗方面已回应说,"在保护伊朗人民和捍卫国家利益方面,伊朗没有红线"。

对以色列有何意义

"萨德"是"末段高空区域防御"的音译,是一种先进的地对空导弹防御系统,能够拦截短程、中程和远程弹道导弹。据美国媒体报道,美军共有7套"萨德"反导系统。一套"萨德"系统需要约100名士兵才能操作,由至少6个用卡车搭载的发射器组成。

美国总统拜登13日在被问及向以色列提供"萨德"系统的原因时说,这是为了"捍卫以色列",随后没有回应媒体的后续追问。五角大楼表示,在伊朗于4月13日和10月1日两次对以色列发动导弹袭击的背景下,部署一套"萨德"系统将帮助以方增强防空能力。

近年来,以色列着力构建多层次反导体系,包括主要防御远程导弹威胁的"箭"式反导系统、主要用于拦截短程火箭弹和导弹袭击的"铁穹"防御系统以及"铁穹"的海军版本"C-穹顶"等。10月1日晚,伊朗向以色列发射约200枚弹道导弹。伊朗媒体报道说,伊朗导弹击中以空军基地,摧毁数十架F-35战机。

美国在中东地区部署"萨德"系统已有先例。去年10月7日新一轮巴以冲突爆发后,拜登指示美军向中东地区部署一套"萨德"系统。2019年,美国曾以军事训练为目的向以色列提供一套"萨德"系统,用于所谓"整合防空演习"。

是同意报复伊朗吗

《纽约时报》报道13日援引一名美国高级军事官员的话说,向以色列部署"萨德"系统和相关必要人员,将需至少一周时间。

美国国防情报局前分析师哈里森·曼认为,美国提供的"萨德"系统一旦部署到位,以色列将无所顾虑地打击伊朗的敏感目标。《华盛顿邮报》报道援引美国卡内基国际和平基金会高级研究员、美国国务院前巴以问题顾问阿伦·米勒的话称,此举表明,美国判断以色列对伊朗的报复行动将是大规模的,足以迫使伊朗方面作出回击。

此前,美国方面已表示反对以方打击伊朗核设施,同时暗示不支持以方打击伊朗产油设施。美国最新举动是否意味着拜登政府态度发生某种转变,目前还不得而知。

事实上,过去一段时间,美国一边在口头上呼吁中东各方停火,另一边在行动上不断为以色列提供军事支持。在10月9日美国国务院例行记者会上,就有记者质疑,以色列对黎巴嫩发起地面军事行动,中东局势持续升级。在这种情况下,美国表达对以方支持,同时又声称希望通过外交途径寻求冲突解决方案,"你们在支持(冲突)升级的同时认为这能实现外交解决方案,如何能自圆其说?"

对美国有何影响

最近一段时间,美西方媒体一直在渲染,拜登政府已逐渐失去对以色列军事决策的约束力,如以军空袭炸死黎巴嫩真主党领导人纳斯鲁拉据说事先并未通知白宫。

米勒在社交媒体上写道,眼下距离美国大选投票日仅有三周时间,拜登政府选择此时为以色列提供"萨德"系统是国内政治需要使然,而无关美国对以色列的信任。拜登政府不想在伊朗面前显得软弱,同时借此提振民主党总统候选人哈里斯的选情。

美国马里兰大学国际和安全研究中心研究员克莱·拉姆齐对记者说,在11月美国大选前这一段时间,以色列政府将有可能把提前告知美国以方军事行动计划视为没必要,因为大选最后的冲刺阶段,拜登政府无法承受以色列军事行动给民主党选情带来的负面影响。

美国战略与国际问题研究中心中东项目主任乔恩·阿尔特曼日前撰文认为,美国对通过外交途径实现中东局势降温持续无能为力,这将"削弱美国对中东地区乃至全世界的影响力",白宫"必须为此感到担忧"。以色列总理内塔尼亚胡认为得到了美国的保证,即在任何情况下美国都站在以色列一边,这会助长以色列在军事行动中采取更加冒险的举措。

(新华社华盛顿10月13日电)

出口遍及200多个国家和地区

我国"新三样"丰富全球供给

新华社北京10月14日电 回应质疑,数据说话。针对部分国家对我国"新三样"产品加征关税,海关总署14日发布的数据显示,我国"新三样"出口市场遍及200多个国家和地区,在全球受到广泛欢迎。

在当天国新办举行的新闻发布会上,海关总署统计分析司司长吕大良介绍说,据海关统计,今年前三季度,我国出口电动汽车、锂电池和光伏产品7578.3亿元,占我国出口总值的4.1%。

吕大良表示,当前,全球新能源产业仍处于快速发展阶段,我国出口的"新三样"等绿色低碳产品不仅丰富了全球供给,缓解了全球通胀压力,也为全球应对气候变化和绿色转型作出了巨大贡献。

"确实有部分国家对我国'新三样'产品加征关税,我们认为这是不公平、不合规、不合理的贸易保护主义做法,最终也会影响到全球绿色低碳转型进程。"吕大良表示,希望有关国家能够放弃错误做法,在共同发展中寻求自身合理利益,为全球经济增长开辟新的动力源,共同应对气候变化全球性挑战。

美"星舰"第五次试飞"筷子"成功回收助推器

10月13日,"星舰"从位于美国得克萨斯州博卡奇卡的基地发射升空。美国太空探索技术公司新一代重型运载火箭"星舰"13日实施第五次试飞。火箭助推器在降落时由发射塔上被称作"筷子"的机械臂"夹住",首次实现在半空中捕获回收;飞船溅落在印度洋。 新华社/法新

2024宁夏青少年禁毒知识竞赛总决赛在银川举办

10月13日,由自治区禁毒办、教育厅、团委、宁夏广播电视台联合举办的2024宁夏青少年禁毒知识竞赛总决赛在银川举办。本次大赛对巩固学校毒品预防教育成果,增强宁夏青少年学生抵御毒品侵害能力,促进青少年健康成长、家庭和睦和社会发展,具有重要意义,这也是对宁夏校园禁毒教育工作成效的一次检验,同时为全国青少年禁毒知识竞赛选拔优秀参赛选手。

本次大赛以"防范青少年药物滥用"为主题。经过层层选拔,全区14支代表队、共计42名选手参加现场总决赛。竞赛内容涵盖我国禁毒方针政策、禁毒法律法规、禁毒历史、毒品知识、毒品危害、毒品防范、药物滥用、毒情形势等,也是宁夏按照全国禁毒知识竞赛的赛制和比赛方式组织开展的竞赛活动。

比赛现场紧张有序,参赛队员阳光自信、沉着冷静的表现赢得了现场观众的阵阵掌声。经过激烈角逐,最终大武口区代表队获得一等奖,沙坡头区代表队和盐池县代表队获得二等奖,青铜峡市代表队、同心县代表队、兴庆区代表队获得三等奖。本次总决赛中的优秀选手将参加全国大赛。

宁夏青少年禁毒知识竞赛经过多年运行,已成为宁夏禁毒预防宣传教育的一项品牌赛事,持续开展并巩固了"学生不吸毒、校园无毒品"的成果,面向青少年的毒品预防针对性宣传和面向全民的普及性宣传,达到"教育一个孩子,影响一个家庭,带动整个社会"的良好效果,在全社会形成"健康人生、绿色无毒"的浓厚氛围。

自治区公安厅禁毒总队相关负责人表示,青少年是祖国的未来,民族的希望,做好青少年毒品预防安全教育工作责任重大、使命光荣。呼吁全社会共同努力,积极支持宁夏禁毒事业,以全民参与、众志成城的崭新姿态,为宁夏打赢新时代禁毒人民战争、奋力创建全域禁毒示范省区作出新的更大贡献。

(胡 俊)

惠州市仲恺高新区与中卫市开展劳务协作

近日,广东省惠州市仲恺高新区管委会、社会事务管理局等相关部门工作人员及茂佳科技(广东)公司、锐成实业有限公司、TCL王牌电器(惠州)公司企业代表赴中卫市开展劳务对接工作,签订劳务合作协议,并就中卫市零工市场建设运营进行了交流。

仲恺高新区作为广东省惠州市的创新高地和产业集聚地,拥有先进的技术和丰富的产业资源,可为中卫市的劳动者提供广阔的就业空间和良好的职业发展机会。此次来访的企业都是各领域的佼佼者,他们精心筛选了500多个岗位,无论是技术工种还是普通劳动力岗位,都为不同层次的求职者提供了多种选择。中卫市也将积极组织劳动力资源,努力为企业输送优秀人才。中卫市人社部门负责同志向仲恺高新区及来访企业介绍了中卫市零工市场的建设和运营情况,双方就零工市场的管理、服务、信息化建设等方面进行了交流和探讨,并提出许多建设性意见。

下一步,中卫市将以此次劳务对接工作为契机,进一步加强与惠州市仲恺高新区的合作,建立健全劳务输出服务体系,不断拓展劳务输出渠道,提高劳务输出质量,根据用工需求,将有针对性地开展技能培训,并及时解决劳务合作中出现的问题,确保劳务输出工作顺利进行。

(夏 蒙)