操弄网络攻击溯源 栽赃陷害中国

——揭开“伏特台风”真相

2024年2月1日，美国国会众议院“中国问题特别委员会”举行了“中国对美国国土和国家安全的网络威胁”听证会。会议围绕2023年5月被美国微软公司披露的名为“伏特台风”（Volt Typhoon）且所谓“具有中国政府支持背景的黑客组织”展开讨论，称其对美国关键基础设施发动了网络攻击并试图进一步实施破坏，给美国国家安全造成严重威胁。“伏特台风”是何方神圣？其与中国政府的关联证据何在？既然去年5月就已经披露了攻击活动，美国政客为何时隔8个月旧事重提，再次向中国发难？

何为“伏特台风”？

2023年5月24日，“五眼联盟”国家（美国、英国、加拿大、澳大利亚、新西兰）的网络安全主管部门联合发布了名为《中华人民共和国国家支持背景的黑客正在使用逃避检测技术》的预警通报。预警通报称名为“伏特台风”的黑客组织针对美国关键基础设施单位实施了网络间谍活动。

该预警通报直接引用了微软公司于同日发布的《“伏特台风”组织利用逃避检测技术针对美国关键基础设施发动攻击》的技术分析报告和溯源分析结果。微软公司技术分析报告中将攻击者按照微软公司的内部规则命名为“伏特台风”，并直接指出该组织是所谓“总部位于中国且由国家政府支持的网络攻击行为主体”。

虽然“五眼联盟”的预警通报和微软公司的技术报告详细介绍了攻击者的技战术特征和感染指标等，但没有给出具体的溯源分析过程，而是直接给“伏特台风”打上了“具有中国政府支持背景的黑客组织”标签。

该预警通报一经发布就被路透社、华尔街日报、纽约时报等新闻媒体大量转载，纽约时报还报道称美国情报机构在2023年2月发现关岛和美国部分地区的电信网络遭到入侵，并将上述攻击与相关预警通报联系起来。

不难看出，关于“伏特台风”组织以及该组织的归属，美国政府、网络安全企业和新闻媒体的最主要参考依据就是微软公司的技术分析报告和“五眼联盟”发布的联合预警通报。

“伏特台风”真的具有国家支持背景吗？

一直以来，网络攻击活动的归因分析都是国际性难题。“伏特台风”这一名称和归因都源自美国微软公司的技术分析报告和“五眼联盟”发布的联合预警通报，但微软公司并没有给出详细的归因分析过程和根据，且报告中也提及，黑客使用逃避检测技术为取证和溯源工作带来较大困难。

中国国家计算机病毒应急处理中心和计算机病毒防治技术国家工程实验室联合360数字安全集团通过对报告给出的相关攻击活动技术特征进行溯源分析，发现能够被查找到的13个恶意程序样本关联多个IP地址。这些IP地址与很多的网络攻击事件相关，并且也存在多个IP地址与同一攻击事件或网络安全风险存在关联的现象，其中与13个恶意程序样本关联程度最高的有5个IP地址。

而与这5个IP地址都有关联的网络攻击事件报告是美国威胁盟公司于2023年4月11日发布的《关于“暗黑力量”勒索病毒团伙研究报告》。报告显示，“暗黑力量”首次被发现攻击活动时间为2023年1月，仅2023年3月全球范围内就至少有10个机构遭到该组织攻击并被勒索。受害机构所在国家包括阿尔及利亚、埃及、捷克、土耳其、以色列、秘鲁、法国、美国等。

另外，通过对美国流明科技公司2023年12月发布报告中包含的恶意程序样本和IP地址等技术特征进行检索，并未找到其与微软公司和“五眼联盟”预警通报中所述技术特征之间的关联关系。

技术团队判定，来自“伏特台风”的恶意程序样本并未表现出明确的国家背景黑客组织行为特征，而是与“暗黑力量”勒索病毒等网络犯罪团伙的关联程度明显。在此情况下，微软公司及“五眼联盟”国家仅凭受害单位和攻击者的攻击技战术这些模糊的归因因素就将“伏特台风”扣上所谓“中国政府黑客”的帽子未免过于牵强。

“伏特台风”的真相

2024年1月31日对于美国国会、美国政府网络安全主管部门和美国网络安全企业来说是一个重要的时间节点。在同一天，美国国会、美国司法部、美国国土安全部共同针对“伏特台风”打出了一套“组合拳”。

首先，参加听证会的美国国会议员以及美国国家安全局、美国网络安全与基础设施安全局、美国联邦调查局和美国国家网络总监办公室的一把手们大肆鼓吹“中国威胁论”，要求国会在网络安全方面进一步加大人、财、物投入。其次，2024年美国总统大选，共和、民主两党自然都不想在中国问题上“丢选票”，通过公开“讨伐”中国，国会议员们还可以提高自身曝光率，收获不错的政治资本。

美国网络安全企业当然希望美国联邦政府的钱包越鼓越好，而且“中国威胁论”也成为这些企业开拓欧美市场最好的营销广告。最终，在2024年3月11日，拜登政府公布的2025财年预算申请文件中，联邦政府在民事行政部门和机构的网络安全预算达到了创纪录的130亿美元，较2024财年又提高了10%。

就在微软公司发布报告的前两个月，也就是2023年3月24日，微软公司获得了美国国防部联合作战云项目的第一批任务订单。在美国流明科技公司发布有关KV僵尸网络与“伏特台风”存在关联的分析报告的前一个月，2023年11月7日，美国流明科技公司刚刚赢得了美国国防信息系统局价值1.1亿美元的五年期合同订单。

美国政客、高官和企业家因“伏特台风”虚假叙事赚得盆满钵满，而且也达到在国际社会抹黑中国形象、离间中国与他国关系、遏制中国经济发展的目的。

美国政府搞小圈子、小院高墙，甚至操弄微软等公司开展虚假叙事，把网络攻击溯源当成政治游戏、当成打压中国的工具、当成攫取资本为自身谋利的抓手，彻底暴露了美“歇斯底里”和“无底线”的对华政策，以及美国政客、高官和企业家勾连腐败真相，这样只会破坏国际公共网络空间的正常秩序，破坏中美关系，影响美国政府在全球的声誉。

近年来，中国公安机关侦破西北工业大学、武汉市地震监测中心等多个机构被美国家安全局、中央情报局网络攻击案件表明，美国才是真正的“黑客帝国”“窃密帝国”。

（新华社北京4月15日电）

俄罗斯举办火箭模型发射活动庆祝宇航日

4月14日，在俄罗斯圣彼得堡，青少年为发射火箭模型做准备。

当日，俄罗斯圣彼得堡举办火箭模型发射活动，庆祝俄罗斯宇航日。1961年4月12日，苏联宇航员加加林完成世界上首次载人航天飞行，这一天后来被确定为俄罗斯宇航日。

新华社发

武装冲突满一年！苏丹或陷入“全球最大饥饿危机”

4月15日，苏丹武装冲突满一年。目前，交战双方苏丹武装部队与苏丹快速支援部队仍无停火迹象。冲突已造成苏丹约1.4万人丧生，超过810万人流离失所，约1800万人粮食供应得不到保障。联合国世界粮食计划署敲响警钟：苏丹正经历着世界最大的流离失所者危机，并可能急剧恶化为全球规模最大的饥饿危机。

冲突现状如何

苏丹快速支援部队领导人达加洛曾和苏丹主权委员会主席兼武装部队总司令布尔汉一起推翻巴希尔政权。之后，双方陷入激烈的权力争夺。苏丹武装部队致力于建立对全国军队的掌控权，而快速支援部队则捍卫其独立性。由于缺乏一个能够有效调和双方分歧的政治机构，去年4月15日，双方在首都喀土穆大打出手，冲突骤起。

战火延宕一年之后，冲突双方目前在喀土穆、达尔富尔、科尔多凡等地持续交火，很难判断哪一方占据上风。其中，围绕喀土穆的争夺最受瞩目，目前快速支援部队称控制着喀土穆和北喀土穆90%以上的区域，而苏丹武装部队则在喀土穆附近的恩图曼市取得了一些进展，重新控制了国家广播电视台总部和瓦德·巴希尔大桥等重要战略要地。

一年来，持续冲突将苏丹本就脆弱的经济推向崩溃边缘。

苏丹经济严重依赖农业，约65%的人口从事农业。2023年，苏丹谷物产量几乎减半，贸易中断、物价上涨、人道主义援助物资进入受阻等因素导致粮食供给缺口进一步扩大。

苏丹目前有180多万人越境进入南苏丹、乍得等国。世界粮食计划署东非地区主管迈克尔·邓福德2月就曾警告，苏丹面临着世界最大的流离失所者危机。雪上加霜的是，苏丹约1800万人面临严重食物短缺。世界粮食计划署执行干事辛迪·麦凯恩3月再发警告，苏丹持续近一年的武装冲突可能使这个国家陷入“全球最大饥饿危机”。

总部位于英国的慈善机构救助儿童会近日警告说，苏丹有380多万儿童严重营养不良，未来几个月近23万儿童和孕产妇“很可能将死于饥饿”。

外溢影响多大

当前，苏丹武装冲突已演化为消耗战，外溢效应明显。苏丹地处非洲东北部、红海沿岸，毗邻七国，隶属萨赫勒地区和非洲之角，由于该地区各国冲突相互关联，武装叛乱频发，军火走私问题严重，战火延宕可能加剧地区不稳定状态和邻国人道主义危机。

苏丹大量难民越境进入南苏丹、乍得、中非、埃及、埃塞俄比亚和乌干达等国，如此大规模难民涌入导致资源压力骤升，让本就面临严峻安全和发展挑战的周边邻国状况雪上加霜。乍得政府已于2月宣布全国进入粮食和营养紧急状态。南苏丹第一副总统里克·马沙尔近日警告，苏丹冲突已对该国安全“构成重大威胁”。

亟需更多关注

苏丹武装冲突爆发以来，周边国家及地区和国际组织纷纷出面调停，呼吁停火止战，通过对话解决危机。然而，由于冲突双方分歧严重，虽经多方斡旋，冲突双方数次达成停火协议，但并未得到落实。有分析认为原因有三：一是冲突双方实力相当；二是冲突双方不愿妥协；三是国际社会疲于应对乌克兰危机和新一轮巴以冲突，对稳定苏丹局势分身乏术。

苏丹政治活动家海德尔·赛义德指出，冲突持续时间越长，和平希望就越渺茫，因为更多武装团体将脱离中央控制，部落间的冲突将加剧，种族主义和仇恨言论将不断抬头，基于身份和政治派别的杀戮将蔓延，这一趋势难以遏制。

与此同时，苏丹正迫切期待国际社会的关注和援助。苏丹代理外交部长阿里·萨迪克表示，乌克兰危机及新一轮巴以冲突受到国际社会广泛关注，掩盖了苏丹因持续冲突而日益严峻的人道主义危机。他说，尽管国际社会也向苏丹提供了一些援助，但支持的力度还远远不够。联合国2月曾发出为苏丹提供27亿美元人道主义援助的呼吁，但迄今仅筹集到1.55亿美元，可谓杯水车薪。

（据新华社开罗4月15日电）

新闻速读

七国集团领导人举行会议 协调对伊朗措施

新华社罗马4月14日电 七国集团领导人14日举行视频会议，协调对伊朗袭击以色列的外交回应措施，呼吁各方保持克制并采取行动降低紧张局势。

这次会议由七国集团轮值主席国意大利总理梅洛尼召集。七国集团领导人在会后发表的联合声明中说，七国领导人将继续努力稳定形势，避免局势进一步升级，“我们随时准备采取新一轮措施，对破坏该地区稳定的新行动作出反应”。

声明说，与会方强烈谴责伊朗对以色列的袭击，向以色列及其人民表示支持，并重申对以色列的安全承诺。

七国领导人承诺加强合作以结束加沙危机，其中包括立即实现可持续的停火、释放被扣押人员，以及向巴勒斯坦人提供更多人道主义援助。

美国政府一名高级官员14日在美国国家安全委员会举行的媒体吹风会上说，七国集团领导人就如何回应伊朗的袭击进行了“详细而有启发性的”讨论，协调一致对伊朗进行制裁是讨论的一部分。该官员表示，各方在某些对伊措施上仍存在尚未克服的障碍。

意大利外长塔亚尼说，七国集团外长将于4月17日至19日在意大利卡普里岛举行会议，讨论中东地区局势。

阿根廷今年已报告超25.2万例登革热确诊病例

当地时间4月14日，阿根廷卫生部发布最新报告称，2024年1月1日至4月14日，该国已报告252566例登革热确诊病例。报告称，与往年相比，此次登革热疫情更严重、规模更大。

报告称，阿根廷全国24个省份中，19个省份已存在登革热病毒本土传播现象。截至目前，累计发病率为每10万人573例。从去年7月底至今，因登革热死亡人数为197人。所有年龄段均出现登革热死亡病例，其中死亡率最高的是80岁以上人群。

登革热是由登革病毒引发的急性传染病，主要通过蚊媒传播，多在热带和亚热带地区流行，典型症状包括持续发热、头痛、肌肉痛、关节痛等，严重时可致死亡。

（据央视新闻客户端）

加沙停火谈判暂无进展 冲突双方立场并无改变

最近两天，加沙地带的停火谈判仍在艰难进行，双方立场并无改变，谈判并未取得进展。

以色列方面4月14日表示，哈马斯拒绝了谈判调解人最新向其提交的被扣押人员交换协议大纲。此前一天，以总理办公室发表声明称，哈马斯至今仍拒绝任何妥协性建议，坚持要求彻底结束冲突、以军从加沙地带完全撤出。以政府和安全部队一致反对“这些毫无根据的要求”。目前达成停火、释放被扣押人员的“唯一障碍在哈马斯”，而不是以色列方面。

哈马斯发表声明称，已向埃及和卡塔尔递交了针对以色列提议的回应。哈马斯在声明中重申其在停火谈判中的诉求，即实现永久停火、以军全部撤出加沙地带、允许流离失所者重返家园、加快救援物资进入加沙地带以及开始重建工作。

（据环球网）

巴布亚新几内亚发生6.5级地震

新华社悉尼4月15日电 莫尔兹比港消息：南太平洋岛国巴布亚新几内亚15日发生6.5级地震。目前暂无人员伤亡和财产损失报告。

据美国地质调查局地震信息网消息，地震发生于当地时间6时56分（北京时间4时56分），震中位于西新不列颠省金贝东南偏东110公里处，震源深度49公里。

太平洋海啸预警中心未针对此次地震发布海啸预警。

巴布亚新几内亚地处大陆板块交界处，位于环太平洋火山带，地震频发。

保障奥运期间食品安全 法国将对相关场所完成10万次检查

为避免巴黎奥运期间发生食物中毒事件，法国政府正加快推进对当地食品安全的管控。

据法国电视新闻网报道，法国农业部长费诺当天前往奥运主办区域塞纳-圣但尼省进行卫生检查时表示，法国为保障食品安全已投入3800万欧元。

法国政府预计，整个奥运期间将提供1300万份餐食，其中220万份提供给运动员、500万份供应给观众，350万份供应给志愿者。费诺称，“所有餐饮供应都将接受卫生检查，并且这一行动会辐射到奥运周边的餐饮场所”。

今年1月起，法国农业部已在巴黎进行1500次检查，涉及区域包括餐厅、超市、食品卡车等。法国农业部统计数据显示，2024年，法国预计将对与食品相关的场所完成10万次检查，这一数字比2023年多了一倍。费诺表示，巴黎奥运临近，法国将尽力维护在食品安全方面的国际声誉。

（据《环球时报》）

4月14日，在奥地利维也纳，小朋友参加自行车节趣味骑行活动。

4月13日至14日，奥地利首都维也纳举办一年一度的自行车节。自行车节上不仅举行自行车骑行、特技表演等活动，还展示最新的自行车及相关用品。

新华社发