

武器平台“网络化” 攻击他国“常态化”

美国政府网络“黑手”祸害世界

本报记者 张红

热点对话

中国国家计算机病毒应急处理中心近日就美国政府对各国开展网络攻击发出预警并发布相关报告,曝光了美国政府专用的“轻量化”网络武器,以及美国在全球范围部署网络攻击平台,并在法国、德国、加拿大、土耳其、马来西亚等设置多层跳板服务器和VPN通道。此前,360集团公司连续发布美国国家安全局(NSA)对全球以及中国进行网络攻击的相关报告,揭露美国网络攻击活动常态化,潜在威胁越来越大。美国在网络安全领域的霸权给全球网络安全带来了什么危害?本报邀请3位专家进行深度解读。



■ 复旦大学网络空间国际治理研究基地主任 沈逸



■ 对外经贸大学国际学院教授 陈须隆



■ 华中科技大学国家治理研究院特聘研究员 王鹏

美国在网络安全领域追求怎样的地位?

中国国家计算机病毒应急处理中心的报告指出,全球互联网和世界各地的重要信息基础设施已经成为美国情报部门的“情报站”。现有互联网的骨干网设备和世界各地的重要信息基础设施,只要包含美国互联网公司提供的硬件、操作系统和应用软件,就极有可能包含零日漏洞或后门程序,并成为美国情报机构的攻击窃密目标,全球互联网上的全部活动、存储的全部数据都会“如实”展现在美国情报机构面前,成为其对全球目标实施攻击破坏的“把柄”“素材”和机会。

沈逸:美国是典型的网络霸权国家。其核心特征是在全球网络空间谋求建立以美国为中心,以保障美国绝对安全为目标,以其他国家的绝对安全为代价,让美国及其核心盟友享受非对称行动自由的网络空间行动秩序。这种目标对全球网络空间的安全、稳定以及良性秩序的发展,构成了最为直接和最为严峻的挑战与威胁。

陈须隆:美国寻求网络安全领域的绝对优势地位,把网络安全作为美国国家安全战略的重要组成部分,从法理层面、技术层面和资源层面抢占全球网络空间的制高点。美国还着力打造网络安全国际盟友体系,堪称网络安全领域的霸主。美国是世界公认的“黑客帝国”和“窃密大户”。值得关注的是,美国把网络安全领域作为大国竞争的重要舞台和前沿阵地,具有进攻性。美国网络武器丰富,“弹药”充足,而且随着智能化水平的提升而花样翻新。凭借这些防不胜防的网络武器,美国情报机构得以对全球范围的高价值目标实施无差别攻击、控制和间谍窃密,使互联网在某种程度上变成美国的监控网、窃密网和攻击网。

王鹏:在网络空间,美国处于霸权地位,努力维系着一个霸权体系。在涉及网络空间的话语中,美国长期在“网络霸权”与“网络安全”两者之间蓄意切换、偷换概念。网络霸权是一种权力,具有排他性、单边性、进攻性;网络安全则属于权利范畴,是每个国家捍卫自身主权与国家安全、人民安全的正当要求。美国凭借其在网络领域长期积累下来的技术、资金和人才优势,对其他国家进行降维打击。国际社会,有实力反制美国并对其网络安全构成实质性威胁的大国屈指可数。因此,美国得以在本国网络总体较为安全的前提下,利用自身在“硬技术”层面的优势,肆意侵入他国网络,远程控制、窃取数据、破坏设施,以此谋求政治、军事、外交、经济上的优势;同时又利用“软技术”的优势,譬如脸书、推特等社交媒体,来影响目标国的舆论、选情,甚至煽动民意、颠覆政权,实现对自身全球物

理空间和网络空间的双重护持;与此同时,还经常栽赃、嫁祸于人,“贼喊捉贼”地指责他国“网络盗窃”“践踏网络秩序”等。

美国的网络攻击行为呈现怎样的特点?

中国国家计算机病毒应急处理中心的报告指出,美国中央情报局的黑客攻击和网络间谍活动目标,涉及俄罗斯、伊朗、中国、日本、韩国等世界各国政府、政党、非政府组织、国际组织和重要军事目标,各国政要、公众人物、社会名人和技术专家,教育、科研、通讯、医疗机构,大量窃取受害国的秘密信息,大量获取受害国重要信息基础设施的控制权,大量掌握世界各国的公民个人隐私,服务于美国霸权。

陈须隆:从不断曝光的信息看,美国的网络攻击行为呈现如下特点:一是国家行为,有目的、有计划、有重点、有建制地开展,其攻击规模、深度、强度都是无可匹敌的;二是常态化,随着其“防御前沿”战略的实施,网络空间攻击行动更加主动、频繁;三是多样化,美国网络攻击的对象、目标和手段都是多种多样的;四是体系化,美国打造了体系化的网络攻击平台和制式化的攻击装备库,重点在网络空间安全主动防御体系、网络空间攻击支撑体系、网络空间攻击装备体系三大体系上进行技术与装备的变革和发展,构筑了完整的网络战武器系统;五是军事化,美国组建了网络司令部,美国陆海空三军都有网络部队,还组建了一支“网络特种部队”。据悉,美国目前共有133支网络作战部队,规模大约6200人,2020年已经具备了作战能力;六是阵线化,美国依托其盟友体系,与盟友签订“网络威慑倡议”等,相互支持各自对重大网络攻击的响应。

王鹏:美国的网络攻击有很明显的特点:规模化,能够同时对大片商用或军用终端、设备进行大规模高强度打击;隐秘化,在“平时”(与战时相对),采用“小伎俩”“轻量化”手段加强渗透和破坏,让人习焉不察,隐秘性更高;定向化,除了大规模实施攻击外,美国也具备技术条件,对特定国家或组织的网络空间目标实施精准打击,实现点面结合。以此次曝光的“蜂巢”平台为例,它属于“轻量化”网络武器,其战术目的是在目标网络中建立隐蔽立足点,秘密定向投放恶意代码程序,利用该平台对多种恶意代码程序进行后台控制,为后续持续投放“重型”武器进行网络攻击创造条件。美国中央情报局运用该武器平台,根据攻击目标特征,定制适配多种操作系统的恶意代码程序,对受害单位信息系统的边界路由器和内部主机实施攻击、入侵,植入各类木马、后门,从而实现远程控制,可对全球范围内的信息系统实施无

差别网络攻击。沈逸:用美国自己的分类来说,美国在网络空间的行动包括网络攻击、网络防御、网络利用。对网络空间的监听,属于网络利用,用网络手段搜集情报;网络攻击行动比较经典和典型的,是对伊朗浓缩铀项目的工业控制系统实施的“震网”攻击,这种攻击可以从物理上对目标进行毁伤。美国在从事网络利用和网络攻击时,没有边界,没有底线,甚至不遵循他自己倡导的一些行为规范,让整个世界,包括其部分盟友,比如德国等,都暴露在美国网络攻击的威胁之下。

美国为何不断把“脏水”泼向中国?

近日,美国联邦调查局局长克里斯托弗·雷在接受《60分钟》主持人采访时,老调重弹,声称目前来自中国的间谍活动和网络安全威胁的规模“史无前例”。在网络安全方面抹黑中国、渲染“中国威胁”,已是美国的惯常操作。2月1日,美联社曾报道,克里斯托弗·雷在里根总统图书馆的一次演讲中声称,中国对西方的威胁比以往任何时候都“更加肆无忌惮”“更具破坏性”。4月8日,美国政府及公司公开散布关于中国黑客攻击的虚假信息。

沈逸:长期以来,美国在网络空间追求绝对安全,采取具有显著双重标准特点的行动。美国本身是全球最主要的网络攻击策源地之一,却不断对中国进行莫须有的指责,这就是最典型的“双标”。美国政客希望通过所谓“点名羞辱”的方式,构建对中国的负面认知,掩盖美国威胁全球网络安全的事实。同时,对美国政客来说,指责和批评中国,已经成为掩盖其工作无能和谋求个人政治资本的一种最简单选项。

陈须隆:美国常年对中国实施网络攻击,窃取海量个人数据,侵犯中国公民权益,严重危害中国国家安全、关键基础设施安全以及商业和技术秘密,违背了联合国达成的网络空间国际规则,抛弃了中美2015年达成的网络安全双边共识,严重影响了中美在网络空间的互信。同时,出于打压“头号战略竞争对手”的考量,美国在国际上大肆炒作形形色色的“中国威胁论”,其中包括“中国网络威胁论”,主要目的有三:一是树立“强敌”,以便集中抹黑和打压;二是凝聚国内力量,以便增强自身网络实力;三是拉拢盟友,以便对中国进行“围剿”。

王鹏:美国这种做法是典型的“贼喊捉贼”。美国不断侵犯他人他国合法权益,却指责中国“威胁”,是典型的“只许州官放火,不许百姓点灯”。比如,中国加强网络防范,美国就攻击中国在破坏网络空间的所谓“秩序”,指责中国政府侵犯人民的信息权、知情

如何应对美国对世界网络安全造成的严重威胁?

2004年,联合国大会首次成立联合国信息安全政府专家组(UNGGE),旨在以主权国家为基础,推动构建国际网络规范。2013年,UNGGE的报告明确指出,国际法、《联合国宪章》和《世界人权宣言》等现有国际规范适用于数字领域,国家主权、人权、国家间交往等概念适用于网络空间。2018年,联合国大会还通过决议,建立一个开放式工作组(OEWG),就网络信息安全问题进行深入探讨。当前,OEWG与UNGGE并列为联合国主持下的网络空间治理独立协商机制。

王鹏:网络空间是全球公器,不是美国的自留地、殖民地。国际社会有权要求合理、合法且安全地使用网络空间。美国的霸权不仅在政治和道德层面不正义,而且在事实上降低了全球网络科技与经济发展的效率。应对美国威胁,各国需要在以下方面发力:强化信息安全顶层设计,提倡网络空间共同安全,反对网络霸权;争取实现核心技术突破,中国和广大新兴国家的资金短板已经得到极大弥补,在市场上更有后发优势,唯独在技术层面和美国仍存一定差距;加强网络空间的国际合作与“反霸权统一战线”。所有新兴国家、发展中国家,包括不愿意继续被盟友监听和人才流失、技术交流、信息互通、市场整合,形成合力,共同作用,打破美国对互联网关键技术和领域的垄断,推动国际网络空间的民主化进程。

沈逸:一个持续不断追求巩固和扩展网络霸权的美国,对全球除美国及其核心盟友之外国家的网络安全构成了必须共同面对的威胁和挑战。从应对美国的威胁和挑战的角度来说,各个国家首先需要持续不断强化自身的网络安全能力和网络威慑能力;其次要展开产业和技术领域的良性竞争,实现良性发展,提升技术实力;第三要依托以联合国为核心的真正的多边主义平台。中国和负责任的新兴大国、广大发展中国家应协同推进全球网络空间治理秩序的良性变革,从而实现对网络霸权的有效对冲与制衡。

陈须隆:事实一再证明,美国才是全球网络攻击的最大黑手与全球网络安全的最大威胁。各国要坚定地反对网络霸权主义,共同揭露和抵制美国危害全球网络安全、破坏国际规则的行径。各国要不断增强自身维护网络安全的综合实力,加强双边、多边和全球治理合作,维护各国网络主权和网络公地的公平正义,以共商共建共享原则,制定各国普遍接受的网络空间国际规则,推进全球网络安全治理。

世界不能任由网络霸权横行

李嘉宝

近日,美国网络司令部司令兼国家安全局局长保罗·中曾根公开承认,俄乌冲突爆发后,美国网络司令部开展了额外的“前出狩猎”行动,帮助乌克兰“强化网络防御”。

“前出狩猎”是美国提出的“网络战”概念之一,于2018年开始部署。它是指通过向海外派遣网络战精锐力量,采取主动追捕形式,发现并识别对手的网络行动,进行主动攻击。俄乌冲突爆发后,美国的网络“黑手”一直在翻云覆雨。中国国家互联网应急中心检测发现,2月下旬以来,境外组织通过攻击、控制中国境内计算机,进而对俄罗斯、乌克兰、白俄罗斯进行网络攻击。这些攻击地址主要来自美国。

俄乌冲突爆发之初,美国前国务卿希拉里·克林顿就呼吁美国黑客对俄罗斯发动网络攻击,还公然声称,“我们在‘阿拉伯之春’期间就是这么做的,应该竭尽全力再干一次”。这道出一个事实:美国长期凭借网络霸权横行世界、制造混乱。

一直以来,美国都是世界公认的“黑客帝国”。美国政府和有关企业违反国际法和国际关系准则,对外国政府企业或个人,实时大规模、有组织、无差别的网络窃密、监控和攻击,直接危害各国公共安全,连美国的盟友和伙伴也难逃其害。从“维基解密”到斯诺登事件,从“方程式组织”到“梯队系统”,美国是一系列跨国网络安全事件背后的“黑手”,这一点早已人尽皆知。此外,美国还拉拢盟友,使用包括网络攻击在内的手段,在多国实施渗透和破坏行动。近年来,美国主导的北约更是明确将网络空间视为“新战场”,不断推进网络军事部署,对世界和平安全构成严重威胁。

美国热衷于搞网络攻击,是其霸权思维使然。在安全问题上,美国一贯秉持追求绝对安全的逻辑,不断损害别国安全,在网络空间亦是如此。美国试图凭借技术优势,谋求对他国信息领域的“单向透明”,将网络攻击视为打压遏制“战略对手”的霸权工具。

近几年,在美国极力渲染“大国竞争”的背景下,中国成为美国发动网络攻击的主要受害者。数据显示,2020年,中国相关机构捕获超过4200万个恶意程序样本。在境外来源的恶意程序样本中,有53%来自美国。近期中国网络安全企业发现,中国公民使用的账号密码、办公文档、私人文件、电子邮件、QQ等社交软件,都已成为美国国家安全局的网络攻击目标。

极其讽刺的是,美国一边对外频频发动网络攻击,一边却自诩为“网络安全卫士”,动辄给别国扣上“网络安全威胁”的帽子,还试图主导网络安全国际议程。从鼓吹所谓“清洁网络”,到发起“打击勒索软件倡议”、酝酿成立所谓“未来互联网联盟”,再到极力鼓动中国周边国家与美国开展所谓“网络安全合作”,甚至实施网络军事力量所谓“前沿部署”……美国在网络安全领域颠倒黑白、拉“小圈子”、大搞对抗的一系列操演,暴露了其虚伪、自私、双标的真面目。

网络空间是人类共同家园,网络攻击是全球面临的共同威胁,世界不能任由网络霸权横行。从提出网络空间命运共同体的理念,到发起《全球数据安全倡议》,中国倡导构建和平、安全、开放、合作、有序的网络空间治理规则,获得许多国家的积极响应。国际社会应旗帜鲜明地反对网络霸权,推动尽快建立普遍适用的网络空间国际规则,共同维护全球网络空间的安全、繁荣与发展。

美国与沙特渐行渐远?

本报记者 高乔

美国《国家利益》双月刊网站刊文称,沙特阿拉伯和阿联酋联合酋长国在近日“欧佩克+”会议上决定,拒绝使用它们大量的闲置原油产能来弥补广泛预期的原油供应减少。近来,国际原油价格始终保持高位震荡,美国和西方国家希望沙特增加石油产量以稳定油价。然而,作为石油输出国组织欧佩克中有重要影响力的成员国,沙特坚持遵循与俄罗斯等主要产油国先前达成的产量协定,并断然拒绝将俄罗斯驱逐出石油生产联盟。专家分析指出,美国与沙特关系日渐疏离,与多方面因素有关。随着两国外交战略调整,美国与沙特的结构性矛盾将进一步凸显。

关系降至最低点

据《华尔街日报》报道,美国众议院外交事务委员会和情报委员会的领导人以及其他20多位民主党议员计划向拜登政府施压,要求其向沙特采取更强硬立场,理由是沙特政府在俄乌冲突和一系列人权问题上拒绝与美国合作。此前,美国总统拜登试图致电沙特阿拉伯王储穆罕默德·萨勒曼,讨论有关石油出口的问题,

但通话要求遭到拒绝。报道称,“长期以来,美沙关系一直以‘石油换安全’为基础,但这种关系似乎已达到几十年来的最低点”。

复旦大学中东研究中心主任、研究员孙德刚接受本报记者采访时指出,拜登执政以来,美国与沙特关系的恶化表现在多个方面。其一,美国政府认定沙特王储穆罕默德·萨勒曼是记者卡舒吉遇害的背后主谋,故在人权问题上对沙特大加指责;其二,尽管美国一直敦促阿拉伯盟友与以色列建立外交关系,但是沙特一直拒绝;其三,拜登政府召开“全球民主峰会”,邀请了伊拉克,却拒绝邀请所有阿拉伯君主制国家;其四,美国拒绝向沙特提供高尖端武器,甚至还撤走了部署在沙特的“爱国者”导弹防御系统;其

五,美国指责沙特等国在也门的军事行动造成了人道主义灾难,却对也门胡塞武装袭击沙特石油设施未采取反制措施;其六,去年美国不顾沙特等国的担忧,匆忙从阿富汗撤军;其七,美国寻求重返伊朗核协议,而沙特担心伊朗核计划将不断推进。

沙特不愿选边站

《华尔街日报》刊文指出,拜登对沙特人权记录的言论、美国对胡塞武装模棱两可的态度以及美国可能重返伊朗核协议等一系列事件,都加剧了美国和沙特之间的矛盾。俄乌冲突爆发后,美国敦促沙特增加石油产量,稳定油价,但被沙特拒绝,两国的政治

分歧愈加加深。

孙德刚分析,美国与沙特关系的恶化,深层次原因是美国把沙特视为“棋子”和“二等公民”,要求沙特政府配合美国的全球战略,却忽视沙特的安全利益与核心关切。当前,美国一直在逼迫中东盟友与美国和西方一道制裁俄罗斯。为提高制裁俄罗斯的效果,美国要求沙特石油增产以抑制全球油价快速上涨,防止俄罗斯从高价中获益。然而,沙特出口主要靠石油,油价上涨有助于沙特增加出口创汇、缓解财政紧张,因此不愿意增产石油。此外,近年来,沙特增强了外交自主性,希望在东西方之间保持一种战略平衡,不愿意对美国亦步亦趋,也不愿意在俄罗斯与美国之间选边站。

结构性矛盾凸显

美国《国家利益》双月刊网站刊文称,长期以来,“石油换安全”的观点一直支撑着美国与中东国家的伙伴关系。就美国利益来看,这种观点或许已经过时了,现在,中东国家在能源危机中“靠不住”,可能导致它们的关系沦为“不远不近”。这反映出美国与沙特利益交汇减少。

孙德刚指出,在拜登政府看来,与沙特相比,阿联酋更加积极主动地与美国合作,包括率先与以色列建交。随着俄乌局势、美国战略重心转向亚太地区等新变化,美国越来越重视阿联酋的作用,甚至将阿联酋打造成海湾地区新的战略基石。一方面,美国与以色列、阿联酋、约旦和埃及等国建立合作机制,形成美国、以色列、阿拉伯盟国三边合作平台;另一方面,美国建立了与印度、阿联酋、以色列合作的中东版“四方机制”,配合北约和美日印澳“四方机制”,避免在战略上受制于沙特。随着美国重视阿联酋和轻视沙特,美国与沙特的结构性矛盾将进一步凸显。