



美国国家安全局位于马里兰州米德堡的总部大楼

世界头号情报合作组织的新算计

“五眼联盟”近期频频出现在公众视野中，可视作该情报联盟在迅速变化的国际形势下，寻求重新定位和发展目标的一种反应，这一方面是情报联盟战略目标重大转向所致，另一方面则是因为情报来源和获取方式发生了重大变化。

——汪晓风

世界头号情报合作组织“五眼联盟”近期动作频频，从美国出面要求该组织成员和其他国家不要与中国华为公司合作 5G 项目，到联盟峰会要求社交媒体平台为其获取信息提供便利，再到热议已久的建立覆盖面更广的情报网络扩容计划，等等。这些举动背后，“五眼联盟”有何盘算？

“联盟”分工

“五眼联盟”的历史可追溯到二战期间。1943 年 5 月，英国和美国签署“英美通信情报协议”，以促进美国战争部和英国代码及密码部门间形成更密切的反法西斯合作。

二战结束后的 1946 年 3 月，该协议被

正式确定为《英美通信协定》，旨在加强美国国家安全局与英国政府通信总部之间的信号情报合作；1948-1956 年，加拿大、挪威、丹麦、西德、澳大利亚、新西兰等国陆续作为第三方加入；1955 年，修订版的《英美通信协定》正式确定，加拿大、澳大利亚、新西兰三个英联邦国家为正式合作成员，“五眼

一旦下一代移动通信基础设施由中国企业部署实施,美国及其情报联盟或将在目标国家失去获取网络情报的便利,这才是美国真正担忧的。

联盟”由此成型。

2014年丹麦《哥本哈根邮报》报道了丹麦、法国、荷兰和挪威加入该联盟的扩容计划,即构成所谓的“九眼联盟”。

此外,新加坡、日本和韩国与“五眼联盟”都有着情报共享方面的合作。近期也有报道称,德国、法国、以色列、日本、韩国、新加坡等成为该联盟新扩容方案的候选对象。不过,迄今“五眼联盟”仍维持了以五个成员国主要情报机构为核心的稳固架构。

目前“五眼联盟”的成员国构成,利于其针对全球范围的情报搜集活动开展分工协作,各成员国的情报机构按照地理分布,对信号情报、外交及安全情报的获取进行职责划分。其中,英国负责欧洲和俄罗斯西部,美国负责加勒比地区、中国、俄罗斯、中东和非洲,澳大利亚负责南亚和东亚,新西兰负责南太平洋和东南亚,加拿大则负责监听俄罗斯和中国,兼顾拉美、北大西洋和北太平洋地区。

成员国在全球分布的地理优势,使得“五眼联



2013年10月26日,在美国首都华盛顿,一名男子手举有“感谢斯诺登”的标语牌参加抗议“棱镜式”监控的集会



盟”能够对海洋、陆地和天空的无线和有线信号进行全方位和实时的监控。如拦截海底电缆数据是“五眼联盟”全球监听的重要活动,通过在美国西海岸、夏威夷和关岛设立搭线和拦截设施,窃听太平洋海底及连接澳大利亚和日本的电缆,可以无遗漏地获取跨太平洋的全部通信信息,成员国之间的情报分享也有助于各国得到与自身密切相关的外交和安全信息。

“梯队”合作

为了达到全球监控的目的,“五眼联盟”开发了各种合作项目,比如“梯队”。“梯队”是一个美国主导、“五眼联盟”成员国合作的全球情报收集和分析网络项目。“梯队”曾在许多公开资料中被提及,但美国政府一直未确认该项目的存在。

2000年,欧洲议会成立了一个委员会,以调查“梯队”的情报能力和政治意涵。2001年该委员会公布调查报告,认为“梯队”在全球范围拦截公众交换电话网络、卫星及微波通信所传送的电话、传真、电子邮件等数字和数据信息,监控和分析其中的内容。欧



2013年10月26日,人们在美国首都华盛顿抗议对国内及全球民众实施秘密监控

洲议会批评参与国实行非法情报收集,如侵犯大众的隐私权或进行国家性质的商业间谍活动。

据悉,“梯队”庞大的数据和信号采集网络遍及世界,能够监听全球90%的通信,每天收集30亿条通信和网络信息,不仅监控和获取有关外交和国家安全的情报,也参与监视商业机构和获取商业活动通信,其中最有名的是对沙特阿拉伯60亿美元客机采购案的介入。多年前,欧洲空中客车公司给沙特官员回扣的通信记录被“梯队”截获,美国国家安全局公布了一些涉及贿赂的对话记录,导致空客公司投标失败。

“梯队”截获的信息被送往位于美国马里兰州的国家安全局和英国伦敦的政府通信总部,这两个情报分析中心利用其超级计算机,对数据信息进行分析和综合,生成标准格式的情报,再分发给各个情报分析机构。

该项目监控范围非常广泛,一定程度

上覆盖了大部分国际通信和网络传输,其紧接着的“挑战”是数据存储和数据挖掘能力,即如何将截取和监听到的庞大信号数据、数字数据转化为可用的情报。

互不监听和交叉监控

互不监听是“五眼联盟”的重要规则,成员国签署“无间谍协议”,承诺相互间不进行情报收集和监控活动,同时以充分的情报共享确保每个成员国都能及时获得与本国外交与安全相关的情报。

据报道,2009年美国曾邀请法国加入“五眼联盟”,时任法国总统萨科齐希望拥有其他成员国同等地位,包括加入“无间谍协议”,当时的美国国家安全局局长表示同意,但中央情报局局长和时任总统奥巴马未置可否,而仅由美国国家安全局出面并不能令法国解除担忧,入盟提议就此作罢。

2010年,美国外国情报监视法庭签署一份文件,授权美国国安局收集各国政府及国际机构的情报,但“五眼联盟”成员不在目标之列。2013年6月,美国国安局前雇员斯诺登揭秘“棱镜”等情报计划,根据披露的内容,德国总理、罗马教皇等人均在被监听之列,德国政府愤而要求与美国及“五眼联盟”签署“无间谍协议”,但遭到奥巴马政府的拒绝。

交叉监控是“五眼联盟”的惯常做法,即由其他成员国情报机构实施监视本国目标的活动,以突破本国国内法律的各种限制。斯诺登就将“五眼联盟”描述为一个超国家的情报机构,即其行动可不遵守本国现行法律规定。

互不监听是为了令联盟成员消除戒心,更好地整合各国地理、技术和资源优势,而交叉监控则是为了消除监控和情报收集死角。一致承诺和特殊安排之间似乎存在矛盾,而这正是“五眼联盟”目标追求的体现,即尽其所能获取一切可能的情报,这种基于能力的情报文化与基于需求的情

报文化的切换,贯穿在美国及其主导的情报联盟发展演变的各个历史阶段。

当国际安全局势面临复杂状况时,情报工作更受决策者倚重,情报联盟就能获得更大行动自由度。而当出现诸如“斯诺登揭秘”这种引发社会指责的事件后,情报机构就可能回归本职,大体遵从法定权责。

而尽管“斯诺登揭秘”对情报联盟产生了冲击,但无论是全球公众的关注还是他国政府的愤怒,都难以影响到“五眼联盟”的运行,原因就在于情报在西方主要国家外交和安全中的重要地位。

定位调整

“五眼联盟”近期频频出现在公众视野中,可视作该情报联盟在迅速变化的国际形势下,寻求重新定位和发展目标的一种反应,这一方面是情报联盟战略目标重大转向所致,另一方面则是因为情报来源和获取方式发生了重大变化。

“五眼联盟”的使命随着国际局势的变化而调整,从二战期间主要针对德、日军事目标,到冷战期间针对苏联和社会主义国家,至冷战后一度陷入失去主要对手的茫然。“9·11”事件后,防止和应对恐怖主义成为美国首要战略目标,“五眼联盟”也很快将情报重点转向恐怖主义。

近年来,美国政府的国家安全战略关注重新转向地缘政治,特朗普政府提出所谓“印太战略”,增加在太平洋的军力投入,并将安全范围向西扩展到印度洋。“五眼联盟”的职能目标因此也面临调整,由此产生信号监控和情报收集能力的缺口,需要扩展新的合作伙伴加以弥补。

这可视作“五眼联盟”扩容的一个主要动因。从这一逻辑看,在印太区域具有战略利益、总体认同美国所谓“印太战略”、与美国保持密切盟友或伙伴关系的国家,有可能被吸纳为新的成员国。

20世纪90年代以来,互联网发展成为

“幽灵协议”一提出即引起舆论哗然,众多高科技公司、公民权益组织和技术社群强烈反对,理由是只有更强的加密才能更好地保护用户数据。

重要的信号传输和数据运行平台,“五眼联盟”加强了网络情报合作。互联网的信息传输主要依据传输控制协议和路由协议来确定路线,一封邮件通过互联网传输时,其拆分的数据包可能由路由协议分配至不同的路线到达目的地,情报联盟能够将各条光缆上获得的数据进行重新整合,避免单个国家网络监控的地域限制而遗漏重要信息。

美国及其情报伙伴拥有国际电信和互联网的技术和资源优势,这是“五眼联盟”可以有效进行全球监控的重要基础。对于联盟以外国家和企业运行的电信和互联网基础设施,美国则采取打压、渗透和阻挠等手段,以避免出现失去控制的局面。

2019年2月以来,即下一代移动网络技术5G开始部署应用之际,美国密集对欧洲、日本、拉美地区的盟友和伙伴展开游说,要求他们不要在5G建设中与华为公司合作,妄称在电信基础设施中使用华为设备“十分危险”。

实际上,这种逻辑并不为“五眼联盟”其他成员国认同,这些国家也都没有把与华为合作的大门关死。显然,华为并非电信运营商,其提供的是优质的5G电信设备和施工服务,并不会接触或控制用户数据。

对于“华为在电信设备中设置后门”一说,英国政府2010年专门成立了“华为网络安全评估中心”进行跟踪分析。2019年3月,该中心监管理事会发布报告称华为产品“没有后门”。所以,有分析人士指出,真正的问题并不在于产品是否安全,而在于情报联盟将会被挡道。

2019年5月,美国国务卿蓬佩奥在伦敦发表演讲,称如果英国邀请中国企业加入5G网络建设,将有损英美情报联盟,安全性不足将削弱美国在值得信赖的网络内共享情报的能力。

蓬佩奥曾任美国中情局局长,非常清楚电信基础设施对于获取通话和网络数据的重要性,一旦下一代移动通信基础设施由中国企业部署实施,美国及其情报联盟或将在目标国家失去获取网络情报的便利,这才是美国真正担忧的。

“幽灵协议”的争议

此外,拥有大规模用户群体的应用软件及其中的海量数据,也成为“五眼联盟”眼里不可不拿下的

关键目标。据斯诺登揭秘,“棱镜”计划监控的电邮、即时通信、视频、照片、存储数据、语音聊天、文件传输、视频会议、登录时间和社交网络资料等数据,主要是从谷歌、微软、苹果、脸书、雅虎等8家互联网企业获得的。

斯诺登揭秘后,主要互联网企业一方面刻意与情报部门保持距离,另一方面出于获取公众信任和提高市场占有率的目的,推出各种加密强度高、破解难度大的算法和应用。2015年,英国议会讨论一项《侦察权法草案》时,时任首相特雷莎·梅曾感慨道,“执法部门、安全部门和情报部门在数字时代显得非常吃力。”其显然很清楚关键信息基础设施对于获取网络情报的重要性。

2019年7月底“五眼联盟”年会在伦敦举行,英国政府通信总部提出可与互联网公司签订一项“幽灵协议”,由拥有高强度加密应用的公司开发一种技术,在用户私聊或群聊中添加一名隐形的警官或情报人员。

英国内政大臣帕特尔7月31日在一份官方声明中表示,“五方观点一致认为,科技公司不应在他们的系统和服务中加入包括端到端的加密方式,这种方式会让犯罪分子更有能力,也会让弱势群体处于危险之中。”

“幽灵协议”一提出即引起舆论哗然,众多高科技公司、公民权益组织和技术社群强烈反对,理由是只有更强的加密才能更好地保护用户数据。个人隐私和公共安全孰轻孰重很难给出一致答案,更可能的结果是在两者之间达成平衡,逐渐形成各方认可接受的新规则。

在新的大变革时代,技术、地缘和政治密切相关、频繁互动,正在重构既有规则和秩序。美国情报部门一向自诩站在国家安全的最前沿,能最早感受到这些变化,因此也最希望将“五眼联盟”纳入新的战略轨道。

然而,历经二战、冷战、“反恐战争”等重大变迁,“五眼联盟”如今要面对“美国优先”而非“休戚与共”的未来,其会否再次甘愿服务于美国主导的战略目标,完成扩容与扩能的任务?具体答案有待进一步观察。而目前来看,其前景更有可能是比较黯淡的。G

(作者系网络安全问题专家、复旦大学美国研究中心副研究员)