

# 美国这场黑人种族屠杀事件百年惊痛

美国总统拜登5月31日发表公告,宣布当天为“1921年塔尔萨种族屠杀100周年纪念”,呼吁美国民众“反思我们国家种族恐怖的深刻根源”。拜登6月1日前往中西部俄克拉何马州塔尔萨参加塔尔萨种族屠杀百年纪念活动并发表演讲,称塔尔萨的历史就是种族主义肆虐美国的证据。



5月31日,在美国纽约,一名参加纪念塔尔萨种族屠杀一百周年活动的妇女额头上贴有“塔尔萨”字样的装饰。新华社发(郭克摄)

## 百年惊痛

20世纪初,俄克拉何马州塔尔萨因附近发现石油迅速致富,人们蜂拥而至,包括许多黑人。在种族隔离制度下,这座城市只有寥寥几处区域允许黑人购买土地和经营生意,北部格林伍德社区即其中之一。经过黑人企业家十几年苦心经营,它成为当时全美最繁荣的黑人经济和文化中心之一,有“黑色华尔街”之称。这里不少黑人的生活水平超过很多当地白人,这引来了白人种族主义者的怨恨,成为引发种族屠杀事件的重要因素。

1921年5月30日,一名19岁的黑人擦鞋匠因涉嫌在电梯里“侵犯”一名17岁的白人女孩被捕,次日出版的当地白人报纸对此进行了添油加醋却无实据的报道。5月31日至6月1

日,白人暴徒袭击了格林伍德黑人社区。他们纵火、抢劫、开枪,甚至动用飞机从空中投掷自制燃烧弹。熊熊大火中,逾1200栋住宅和商铺被烧成瓦砾,约300名黑人遇害,约一万名黑人居民流离失所。

现年107岁的幸存者维奥拉·弗莱彻今年5月中旬在国会作证时说:“我一辈子不会忘记我们离开家时白人暴徒的暴力。我们的国家可能会忘记这段历史,但我不能。”

由于白人女孩始终否认被侵犯,被捕黑人青年数月后被无罪释放。但屠杀事件中的暴徒没人被起诉,也没有幸存者得到合理赔偿,格林伍德社区多数黑人被迫移居到城市更偏北的区域。当今的塔尔萨南富北贫,北

部黑人居民与同城白人在就业、健康和经济状况等方面差距显著。政府数据显示,白人家庭收入中位数比黑人家庭高出约两万美元;2019年生活在贫困线以下的居民中,近三分之一是黑人,仅12%是白人。

拜登在纪念公告中承认,美国联邦政府在这起事件中扮演了不光彩的角色。公告说,屠杀事件发生后,当地通过法令实施新的建筑标准,建房成本之高令多数黑人家庭无法重建家园;联邦政府把格林伍德社区列为“危险”区域,令黑人房主无法以同等条件获得住房贷款。其后几十年里,联邦政府的投资,包括穿过格林伍德的联邦高速公路建设,使社区遭到拆除和切断。

## 连锁伤害

上世纪初叶的美国,塔尔萨种族屠杀事件绝非孤例。堪萨斯大学退休美国史教授小威廉·塔特尔的研究显示,1917年至1923年间,美国各地众多有色人种社区遭遇各种形式和程度的暴力破坏,1100多名美国人在这类事件中丧生。

塔尔萨种族屠杀及类似事件的一大后果,在于剥夺了黑人代际财富的积累机会。有美国学者指出,美国白人和黑人之间财富差距巨大,部分原因在于历史上黑人城镇、房屋和企业屡遭破坏,阻碍了他们积累、继承财富和使后世子孙获得良好教育的能力。2013年的一份研究报告发现,美国白人继承遗产的可能性是黑人的5倍,而在继承遗产的家庭中,白

人继承者所获遗产是黑人的10倍。

威斯康星大学普拉特维尔分校历史学教授戴维·克鲁格勒指出,这些种族暴力事件给非洲裔美国人留下深深的心理创伤,也是导致他们与警察关系紧张的重要原因。塔尔萨种族屠杀百年纪念委员会成员拜登·奥尔当说,环视当下的美国,人们仍会看到百年前种族屠杀事件的连锁效应。

在20世纪大部分时间里,塔尔萨种族屠杀事件被忽视和遗忘。直到1997年,俄克拉何马州才成立委员会调查屠杀事件并在4年后发布详细报告。这一事件于本世纪初被列入该州公立学校课程,数年前被载入美国历史教科书。美国主流

媒体直至百年纪念日来临,才对塔尔萨种族屠杀事件进行了广泛报道。

但就在纪念日来临前,俄克拉何马州立法禁止在该州公立中小学教授因种族或性别而给学生带来“不适、内疚、痛苦或心理压力”的课程。这一举动立即引发争议,被认为将限制学校关于种族平等课题的教学和课堂讨论。

对塔尔萨种族屠杀事件的纪念以及相关的经济补偿问题,已成为美国两党严重对立的“文化战争”话题之一。从两党的分歧和愈演愈烈的“文化战争”来看,美国实现种族平等和种族正义的道路仍然漫长。

(新华社华盛顿5月31日电)

## 美国如何打造“黑客帝国”

在美国总统拜登即将访问欧洲之际,美国被曝曾在丹麦帮助下监听包括德国总理默克尔在内的欧洲政要,这是其作为全球头号“黑客帝国”的又一最新明证。

分析人士指出,美国国家安全和中央情报局等机构将传统情报手段和网络攻击深度结合,长期在全世界范围内实施无孔不入的监听。而正是这样一个“窃密惯犯”却自我标榜为“网络安全卫士”,在网络安全领域屡屡对其他国家抹黑攻击。

### “弹道无痕”

近年来,美国各种监听项目陆续被曝光,这类项目多由美国国安局负责实施。2012年7月至2013年9月,就在美国国安局利用丹麦互联网设施监听欧洲国家的同时,被认为与美国国安局有密切关联的网络犯罪组织“方程式组织”悄悄攻破总部设在迪拜的金融服务提供商East-Nets的网络,而这家公司是环球银行间金融通信协会(SWIFT)在中东地区最大的支付系统服务供应商。

根据黑客组织“影子经纪人”2017年曝光的文件,“方程式组织”首先利用日本、德国等地6台被入侵的服务器作为跳板,借助身份认证漏洞攻破East-Nets网络防火墙,获取了其感兴趣的资金流动轨迹等交易信息。专家指出,以“方程式组织”为代表的美国情报机构网络攻击团队高度追求作业过程的隐蔽性、反溯源性,其行迹很难被察觉。

2015年,迫于美国国内舆论压力,美国国会通过法案,决定结束只针对美国国内的监听项目。但此后,美国情报机构继续在未获授权的情况下监听美国境外目标的电子邮件和短信等通信。

专家指出,美国将人力、电磁等传统情报手段和网络攻击深度结合,有时会在与互联网物理隔离的内部网络中植入长期潜伏的计算机病毒,然后在合适时间“引爆”。

### “降维打击”

除国安局外,美国还有另一大情报机构——中情局,它也拥有强大的网络攻击能力,擅长发现并利用现代科技产品的程序漏洞,侵入手机、计算机乃至智能电视等电子设备,在网络空间肆意利用不对称优势对他国发动“降维打击”。

“维基揭秘”网站2017年曝光的近9000份中情局机密文件显示,该局“网络情报中心”拥有“注册用户”逾5000人,其设计的网络攻击工具超过1000个。中情局设有海外网络攻击基地,其中一个位于美国驻德国法兰克福领事馆,负责欧洲、中东和非洲地区的网络攻击活动。此外,中情局还特别设立了一个小组,专门负责收集、管理从其他国家窃取的攻击工具,这样不仅能丰富中情局的网络攻击手段,还能用虚假的“网络指纹”让被攻击方误以为遭到其他国家的攻击。

从曝光文件看,中情局网络攻击团队可以入侵智能电视,让其“假关机”变成窃听器;可以入侵智能车辆控制系统以执行暗杀等活动;开发了针对智能手机的攻击工具;可以入侵各种计算机操作系统以及网络路由器等。

专家表示,美国拥有庞大而复杂的情报体系,其情报活动遍布网络空间和物理空间各领域,其网络攻击武器完整覆盖服务器、云端、智能移动设备等各类场景,适配各类操作系统,功能涵盖侦察、物理隔离突破、内网横向移动、持久化潜伏驻留、供应链与物流链渗透、远程控制等网络攻击各环节,其行动由美国花费数十年建设的庞大情报工程体系予以支撑。

### 中国是目标之一

尽管美国在网络领域拥有巨大优势,却一直宣扬其面临所谓“数字·9·11”和“网络珍珠港”事件威胁,并以此为借口制定先发制人的网络作战策略,并把中俄作为主要假想敌。

事实上,中国早已成为美国等国发起的网络攻击的主要目标之一。

中国国家互联网应急中心网站5月26日发布的《2020年中国互联网络安全态势综述》报告显示,2020年中国捕获计算机恶意程序样本数量超过4200万个,其中境外恶意程序主要来自美国,占比达53.1%。2020年控制中国境内主机的境外计算机恶意程序控制服务器数量达52万个,其中位于美国的控制服务器约1.9万个,高居首位。

中国一家网络安全公司去年3月发布的调查报告指出,美方攻击团队长期对中国进行网络攻击和渗透,目标涉及航空航天、科研机构、石油行业、大型互联网公司以及政府机构等。

(新华社北京6月2日电)