

日前,由国家安全部指导的国安题材电影《惊蛰无声》上映,让“三神”战线走进了千家万户的团圆时刻。作为我国首部聚焦当代国家安全题材的电影力作,影片以“于无声处听惊雷”的叙事张力,展现出新时代国安干警笃行初心使命,矢志不渝践行“坚定纯洁、让党放心、甘于奉献、能拼善赢”的铮铮誓言。



资料照片

神秘神奇神圣战线的 暗战无声

影片以最新科技涉密信息外泄为导火索,将镜头对准代号为“惊蛰”的国安专项行动小组。螺旋穹顶下无人机追踪的暗战、摩天楼群的玻璃幕墙后交织着数据攻防的较量、AI换脸、量子通信干扰等新型间谍手段的呈现,不仅还原了当代隐蔽战线斗争的科技化、隐蔽化特质,更真实复刻了国家安全面临的复杂局势。电影中那些微表情的对峙、暗巷里的静默追踪、屏幕前的毫秒攻防,恰是三神战线“料敌于无形、化险于未萌”的日常写照。

当今时代,科技革命的浪潮正

以前所未有的速度席卷全球。人工智能、大数据、物联网、大模型等前沿科技,正在深刻改变我们的生活方式、生产方式乃至国家治理体系。国家安全面临着诸多新的挑战,网络窃密、技术渗透、生物信息窃取等新型安全威胁层出不穷。特别是在网数智迭代发展的背景下,数据泄露可能瞬间让个人隐私荡然无存、让核心资产灰飞烟灭、让商业机密付诸东流,更让国家安全暴露于未知的风险之中。

面对这场危机,筑牢数据安全防线,已不仅是技术命题,更是关于未来生存与发展的根本保障。近年来,国家安全机关坚定履职,依法侦办、破获一批数据安全领域重大案件,有力打击了境外间谍情报机关渗透窃密的卑劣行径,有效消

除了数据安全领域的风险隐患,取得一系列斗争成果。

隐蔽战线无声誓言的 深刻诠释

影片中国安干警隐姓埋名、深入龙潭,在反间谍战场上察微知著、破敌于未遂,在反颠覆战场上铲除隐患、筑牢长城,这与现实中国安干警的战斗轨迹高度契合。江西省吉安市国家安全局原局长徐忠坤,带领基层局创新奋进、屡立战功,最后牺牲在工作岗位上,用生命践行了“甘于奉献为家国”的忠诚誓言。四川省攀枝花市国家安全局某特色战队的带头人陈格,始终坚持奋战在反间谍工作一线,凭借卓越的专业能力屡破要案,为维护国家安全作出重要贡献,充分

展现了新时代国安干警的铁肩担当和铁军战力。云南省迪庆州国家安全局二支队支队长洛桑扎西,长期扎根祖国西南高寒边疆,面对严峻复杂的敌情形势,始终忠诚履职、担当奉献、冲锋在前、敢斗善斗,为捍卫国家安全、维护边疆稳定作出了突出贡献。当技术专家在深夜的实验室反复推演线索,当潜伏者在敌人环伺中守护机密,当行动队员为保护战友选择牺牲,这些细腻的刻画让无名英雄的形象愈发鲜活。他们也是父母、是子女、是伴侣,却在国家利益面前选择“无名无我”,将个人安危置之度外,这种“于平凡中见伟大”的叙事,正是对隐蔽战线英雄们最崇高的致敬。

当观众在阖家欢乐的时刻走进影院,感受着隐蔽战线的惊心动魄,更能体会到“岁月静好”的背后是无数国安干警的负重前行。

影片结尾,当“惊蛰”行动成功落幕,城市恢复了往日的繁华,那些坚守岗位的国安干警却依旧隐于人群,继续守护着万家灯火,这一幕,正是对神秘、神奇、神圣的隐蔽战线最生动的注解。

全民国家安全教育 走深走实

《惊蛰无声》的价值远不止于艺术表达,更在于其深刻的现实警示意义。影片中境外反华敌对势力利用外卖信息窃密、科技公司内部泄密等情节,均源自真实案例,“谍战不是故事,是真实发生的事件”呼应了全民国家安全教育时代需求。

近年来,国家安全机关大力加强全民国家安全教育工作,创新打造国家安全部官方微信公众号,大力宣传习近平新时代中国特色社会主义思想 and 总体国家安全观,大力宣传国家安全法、反间谍法等国家安全法律法规及部门规章,大力宣传全面建成国家安全机关工作新格局的理论成果、制度成果、实践成果,大力宣传新时代国安干警良好形象,为培育和增强全民国家意识和素养,筑牢国家安全人民防线作出了重要贡献。

数据托管切莫“托而不管”

在全球性数字化浪潮中,数据已跃升为保障机构运行、驱动企业发展的基础性、战略性资源。存储好、运用好海量数据不仅可以为企业洞察市场,也能帮助企业找准未来决策方向。为实现降本增效,不少企业选择将数据存储、流转在数据托管公司这个“数字超级银行”,省心又省力。但在高效的运作模式背后,也潜藏着威胁国家安全的数据泄露风险,需要引起重视。

数据托管,能够将企业数据交由专业的第三方存储,并由托管公司监管维护数据安全,但安全风险仍应警惕。

审核失察埋下泄露隐患。部分涉密单位在选择数据托管商时,未严格审核对方保密资质与安全防护能力,为数据泄露埋下隐患。某行

业论坛出现售卖金融机构客户信息行为,源头竟是一家不具备金融数据处理资质的小型科技公司。该公司虚假宣传承接数据托管业务,其员工利用管理漏洞,私自下载客户数据并在暗网售卖,致使众多金融机构客户隐私泄露,威胁国家金融安全。

管理缺口酿成数据危机。数据托管服务商的工作人员深度参与委托方数据流转,掌握着敏感信息的访问权限。一旦委托方管理松懈,易引发严重后果。某涉密单位为图便利,将实验数据存储及运维外包,合作期间,该单位未建立有效监督机制,对出入机房、数据调取等关键环节缺乏管控。某数据托管服务商工作人员因欠下巨额债务,利用工作便利窃取多项核心研发项

目的机密数据,贩卖给境外间谍情报机关,严重威胁国家安全。

境外渗透加剧安全挑战。部分境外间谍情报机关与网络犯罪团伙瞄准数据托管服务领域,频繁发动网络攻击,企图窃取我敏感数据。境外黑客组织通过大数据分析锁定我国某电商平台数据库,植入木马程序实施“钓鱼”攻击,攻破关键权限,窃取大量用户数据信息,其中包括涉及国家关键基础设施项目采购、高端科研物资购买等敏感信息,对国家安全构成严重威胁。

国家安全机关提示

《数据安全法》规定,开展数据处理活动,应当遵守法律法规,尊重社会公德和伦理,遵守商业道德和职业道德,履行数据安全保护义务,承

担社会责任,不得危害国家安全、公共利益,不得损害个人、组织的合法权益。

数据托管委托方要切实履行数据保密管理职责,明确内部监管机制,严格审核外包服务公司资质,在合同中清晰界定双方的保密权利与义务,定期排查风险隐患。同时,委托方与服务商都要强化员工管理,定期开展保密培训,提升全员保密素养,共同守护国家数据安全。

若在数据托管中发现敏感数据泄露或遭受境外黑客组织频繁攻击等问题线索,可通过12339国家安全机关举报受理电话、网络举报受理平台(www.12339.gov.cn)、国家安全部微信公众号举报受理渠道或者直接向当地国家安全机关进行举报。

(均转自国家安全部微信公众号)