

在祖国边陲，散落着一些特殊的“老哨兵”——它们是曾经的军事阵地，如今静静地矗立在风沙雨雪之中。然而，这些旧址实则承载着不可磨灭的历史记忆与国防残留信息，恰似“沉睡的密码本”，一旦被别有用心之人窥探分析，可能危及我军事安全。

废弃≠无密，风险仍需警惕

近期，国家安全机关工作发现，某军事爱好者屡次擅自进入某废弃军事阵地，甚至开展照片拍摄、非法测绘等行为。经调查，该阵地曾为某部队训练驻地，虽废弃多年，但其地理位置、建筑布局等仍具备较高军事价值。经进一步查证，该军事爱好者受好奇心驱使进入该军事阵地，并无涉外背景。国家安全机关依法对该人员开展法律科普并进行批评教育，帮助其认清危害。

警惕“沉睡密码本”成为泄密“缺口”

军事阵地的构建并非随意，其选址、布局、结构、配置等均经过严密考量，能够体现军事意图与战略意义。而废弃阵地中的残破建筑、遗留残片，甚至墙壁上的标记，经整合分析后，仍可能暴露军事敏感信息。近年来，境外间谍情报机关千方百计对此类敏感区域进行窥探窃密，应引起广大人民群众的警惕。

以公开活动为掩护。境外间谍

情报机关常以学术研究或历史考察名义，通过实地测绘、走访打听等手段对敏感区域的建筑结构与军事用途进行推测分析，或是以探险团队或环保组织人员身份为掩护，对敏感区域及周边环境进行拍摄。

派员直接非法侵入。境外间谍情报机关可能直接派遣其工作人员潜入敏感区域或周边，以窃取敏感区域的建筑施工材料进行分析、植入监控设备长期窥测等方式开展窃密活动，或利用金钱对曾参与建设、维护和守卫的内部人员进行策反渗透，使其凭借记忆绘制详图并提供信息。

技术手段远程探测。境外间谍情报机关也可能利用高分辨率卫星或无人机进行窃密活动，通过持续监控我军事阵地及周边活动来分析部署变化，或是对未完全拆除乃至废弃残留的线路进行采集分析。

国家安全机关提示

一砖一瓦皆为国防屏障，一草一木承载军事记忆。废弃军事阵地是凝固的军事档案，其信息价值具有“长尾效应”，不是可以随意拍摄、谈论的普通景观与随意出入的“军事乐园”，请广大人民群众遵守法律法规，做到不进入、不拍摄、

守护『沉睡的密码本』

“隐秘的角落”罪恶的深渊

网络空间是亿万网民共同的精神家园，清朗安全的网络环境，直接关系到每一位群众的切身利益。在我们日常使用的互联网之外，潜藏着一个不为普通人熟知的暗网，这个被称为“网络黑洞”的神秘地带，正被境外间谍情报机关及不法分子利用，成为滋生违法犯罪、侵害群众权益的重灾区。今天，让我们一起撕开暗网的“隐身衣”，认清危害，筑牢防线。

撕开暗网的“隐身衣”

可能有网民对暗网存在误解，将其等同于“深层网络”，甚至误以为是可以随意猎奇、隐藏身份的自由空间。事实上，暗网是指互联网中经过特殊加密处理的隐藏网络，普通浏览器和搜索引擎无法直接访问，需借助特定软件或特殊配置才能进入，其网址通常以“.onion”结尾。暗网依托加密技术、匿名路由掩盖使用者身份、位置和行为，看似给人“隐身”的保护，实则成为不法分子逃避监管、实施犯罪的“遮羞布”，它脱离正常网络监管，没有合法的内容审核与秩序约束，从诞生之初就成为各类违法犯罪活动滋生的土壤，将危害直接转嫁到普通百姓身上，成为威胁人民群众安全感、幸福感，侵害个人利益和公众利益的重大隐患。

个人信息的“贩卖集市”：暗网是公民个人信息非法交易的核心渠道，身份证号、手机号、家庭住址等隐私数据，被不法分子通过黑客攻击等手段窃取后，批量在暗网低价倒卖，直接侵害公民隐私和财产安全。

不良信息的“传播温床”：暗网中充斥着暴力血腥、网络赌博、反动蛊惑等违法有害信息。境外间谍情报机关利用暗网隐匿特性，通过歪曲事实、煽动对立、制造恐慌等方式，误导群众认知、扰乱公共秩序，危害国家安全。

违禁物品的“地下通道”：暗网非法交易毒品、管制器具、窃听器照器材等违禁品，这些违法交易看似远离普通人生活，实则破坏社会管理秩序，让人民群众身处潜在危险之中。

法律红线不可触碰

可能有人误以为暗网“匿名无痕”，可以逃避法律制裁，这是极其危险的认知。接入暗网通常依赖非法跨境信道、违规工具，此行为本身已违法，在暗网从事不法活动，更涉嫌犯罪。我国始终坚持国家安全一切为了人民，严厉打击各类网络违法犯罪，暗网绝非法外之地，触碰法律红线必将付出沉重代价。

根据我国《刑法》《网络安全法》《个人信息保护法》等法律法规，利用暗网实施侵犯公民个人信息、非法交易违禁品、传播违法信息、网络诈骗、网络攻击等行为，均构成违法犯罪。即便借助加密技术手段躲避追踪，有关部门依然能够溯源追踪，法网恢恢疏而不漏，不法分子最终难逃法律严惩。

不传播，对涉及军事敏感区域的打探、兼职等保持警惕，如发现可疑人员在军事敏感区域周边及废弃军事阵地进行测绘、拆解、窥探等行为的，可通过12339国家安全机关举报电话、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举报。

谁在8000米高度“放飞自我”？

2026年1月1日起，新修订的《治安管理处罚法》正式施行，首次将无人机“黑飞”行为明确纳入“妨害公共安全的行为”范畴，依法设定处罚措施。然而，个别人员非法破解无人机禁飞限制系统，擅自改装机器硬件配置，操控改装无人机飞升至近万米高空，甚至与民航客机“抢道”，严重扰乱空域安全秩序，甚至对民航安全造成威胁。

触碰“红线”陷图圈

国家安全机关工作发现，某无人机航拍“发烧友”为实现“上帝视角”取景，利用软件非法破解无人机飞行高度和禁飞区限制系统，并擅自改装无人机机电硬件配置，多次操控无人机在民航航线范围内“黑飞”，最高记录甚至超8000米，严重威胁民航安全，涉嫌以危险方法危害公共安全。在固定相关证据后，国家安全机关会同

相关部门依法对其采取刑事强制措施，等待他的将是法律的严惩。

超高“黑飞”危害大

8000米高度已达民航客机常规巡航高度。超高空“黑飞”小型无人机目标小、速度快，民航客机雷达难以及时发现，如发生紧急情况，民航客机避让难度将大大增加。高空气象存在大风、低温、低气压的现象，都将造成无人机性能恶化、地空通信失效等情形，无人机失控侵入航路航线风险显著增大。“黑飞”无人机若撞击民航客机，无人机电池及金属构件会瞬间解体并可能被吸入客机发动机导致重大故障，酿成灾难级事故。

国家安全机关提示

《无人驾驶航空器飞行管理暂行条例》规定，对微型、轻型、小型民用无人驾驶航空器系统进行改

装的，应当符合有关强制性国家标准；未经空中交通管理部门批准，不得在管制空域内实施无人驾驶航空器飞行活动。

新修订的《治安管理处罚法》规定，违反有关法律法规关于飞行空域管理规定，飞行民用无人驾驶航空器、航空运动器材，或者升放无人驾驶自由气球、系留气球等升空物体，情节严重的，处五日以上十日以下拘留。如“黑飞”危害公众安全，还可能触犯《刑法》，构成以危险方法危害公共安全罪，尚未造成严重后果的，处三年以上十年以下有期徒刑，致人重伤、死亡或者使公私财产遭受重大损失的，处十年以上有期徒刑、无期徒刑或死刑。

无人机绝非想飞就飞，每一次“黑飞”都可能酿成无法挽回的后果。请飞手群体和无人机爱好者增强法治观念，遵守法律法规，敬畏生命，合规操作，守法飞行，共同维护空域安全和社会公共安全。

（均转自国家安全部微信公众号）