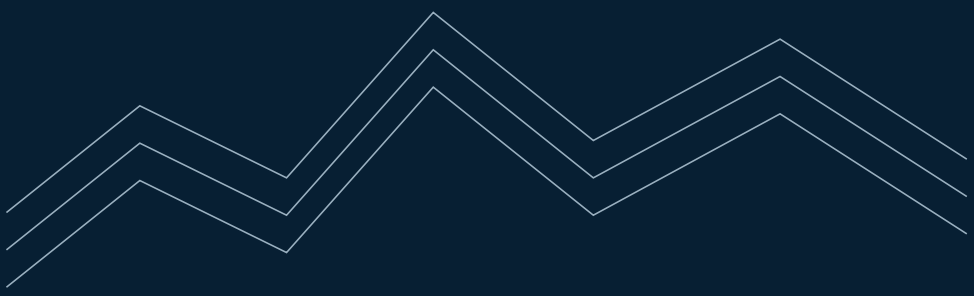
TECHNICAL SURVEILLANCE COUNTERMEASURES · DEFENSIVE TECHNICAL BRIEFING

Technical Surveillance Is a System, Not a Single Device

Illicit surveillance can combine concealed devices, location tracking, compromised accounts, radios, sensors and legitimate connected systems. A defensible TSCM response has to separate allegation, anomaly and evidence.

CARRATU INTERNATIONAL / 23 AUGUST 2026



The popular image of TSCM is a specialist walking around a boardroom looking for a radio transmitter. That threat still exists, but modern surveillance is broader. A person can be tracked through a purpose-built location device, a crowd-sourced Bluetooth tag, a compromised phone, a connected vehicle account or a cloud service. Audio and video may be captured by a concealed device, by equipment already trusted in the room, or in rarer cases by a standoff technique.

The defensive question is therefore not simply “is there a bug?” It is “what information appears to be escaping, by which technical routes could that occur, and what evidence would distinguish one explanation from another?”

Why “find the bug” is too narrow

UK NACE defines TSCM as the identification of technical security weaknesses and describes a proper inspection as including physical security, human behaviour, physical search and technical search of the electromagnetic and acoustic environment.[1] This matters because a surveillance event can exploit the space, the devices in it, the people using it, or a legitimate system that already has access.

Hidden cameras illustrate the point. UK NACE notes that commercial devices need power and a means to transmit or store video; Wi-Fi transmission and local storage are both common possibilities.[2] A detector aimed only at a continuously transmitting radio source can therefore never answer every camera or recorder scenario.

The surveillance threat surface is broader than a room search

Threat category	Information at risk	Why the risk is often misread
Concealed audio device	Conversation and ambient sound	May be wireless, wired, intermittently active or store recordings locally.
Concealed camera	Images, documents, activity and access patterns	Power source, storage, network use and physical concealment all matter.
GNSS/cellular tracker	Vehicle, vessel or object movement	A physical device may combine satellite positioning with a cellular reporting path.
Crowd-network Bluetooth tracker	Movement through nearby participating phones	Modern phones can warn about compatible trackers, but an alert is an evidential lead rather than a complete TSCM examination.
Compromised phone or tablet	Location, messages, microphone, camera and files	No separate “bug” is required if software or account control has been compromised.
Cloud or account access	Location history, backups, messages and connected-device data	Shared credentials, sessions and location-sharing settings can mimic a physical tracking problem.
Connected building equipment	Audio, video, presence and network information	Trusted cameras, conferencing systems, assistants or routers may become part of the threat model.

Threat category	Information at risk	Why the risk is often misread
Vehicle or vessel telematics	Position, journeys, diagnostics and sometimes cabin/system data	Factory or aftermarket connected services should be distinguished from a separately planted tracker.
Store-and-retrieve recorder	Audio, video or sensor data without live transmission	Absence of an RF signal does not prove absence of a recording device.
Standoff optical/acoustic technique	Conversation or activity without entering the target space	Physical control, sight lines and the acoustic environment can matter even when nothing has been planted.

Homes and offices: the environment is part of the evidence

In a home or office, the baseline is crucial. Which devices belong there? Who has had access? What changed before the concern arose? Are there new chargers, adaptors, smart devices, conferencing units or network clients? UK NACE specifically recommends physical examination for suspicious items, concealment opportunities and indications of disturbance, alongside technical examination for electromagnetic and acoustic anomalies.[1]

Where a camera is suspected, network inventory may be relevant, but it is not conclusive. UK NACE notes that some commercial cameras use Wi-Fi while others store data locally.[2] A sound conclusion must therefore combine physical, network and technical evidence rather than treat any one scan as proof.

Cars: tracking may be physical, Bluetooth-based or already built in

A vehicle can be exposed through a separately fitted GNSS/cellular tracker, a compatible Bluetooth item tracker, an account linked to built-in connected-car services, or a compromised phone travelling inside it. Apple and Google now provide cross-platform unwanted-tracker protections for compatible Bluetooth devices.[4][5]

Those alerts are useful but should not be over-interpreted. Google explains that an unknown-tracker alert is based on a tracker being detected moving with the user over time, and that the system supports compatible Find Hub tags, headphones and AirTags.[5] It does not follow that every form of vehicle tracker will advertise itself in the same way. A vehicle TSCM scope should therefore consider physical, account and device-based explanations together.

Pleasure craft: vehicle, residence and network in one platform

Pleasure craft and yachts deserve their own threat model. They may have persistent onboard power, cabins and private spaces, Wi-Fi, cellular or satellite connectivity, navigation electronics, cameras and remotely managed systems. They also move between marinas and jurisdictions and may spend long periods unattended.

A defensive examination should distinguish three categories: information intentionally or publicly broadcast by normal maritime systems; information exposed through legitimate connected services or accounts; and genuinely covert surveillance. The International Maritime Organization notes that AIS can automatically provide ship identity, type, position, course, speed, navigational status and other safety-related information to appropriately equipped recipients. Carriage requirements apply to specified SOLAS ship classes, not to every pleasure craft. [10] Publicly visible vessel-location information should therefore not be mischaracterised as evidence of a planted tracker unless the technical evidence establishes a separate device or compromised system.

Phones can become the surveillance device

The NCSC defines spyware as malware that installs without the user's consent, collects data and sends it to a third party.[7] Its 2025 BADBAZAAR and MOONSHINE advisory describes malicious apps capable of accessing microphones, cameras, messages, photos and location data. This is an important TSCM boundary: a room can be physically clean while a participant's phone remains the collection platform.

Device security therefore belongs alongside physical counter-surveillance. The NCSC recommends supported devices, managed applications, updates, logging and monitoring, and appropriate control of high-privilege applications and external interfaces.[6] In a personal case, the exact controls differ, but the analytical principle is the same: check software and account explanations before assuming every information leak requires a planted object.

Standoff collection changes the geometry of a room

Not every eavesdropping method requires a physical device inside the target space. UK NACE describes laser eavesdropping as a sophisticated standoff technique that can recover speech-related vibration from objects or windows.[3] It is a higher-end threat, but it demonstrates why technical security also considers sight lines, windows, acoustic behaviour and the wider environment.

This does not mean every overlooked office is under optical attack. Threat assessment should be proportionate to the client, information at risk, adversary capability and observed indicators. The purpose of TSCM is to narrow uncertainty, not to turn every technical possibility into an allegation.

When suspicion becomes an evidential issue

If an unwanted-tracker alert, suspicious device or other technical indicator is discovered, the fastest action is not always the best evidential action. Apple and Google both advise preserving identifying information and considering personal safety; Google notes that disabling some trackers may reset them and affect information available to law enforcement.[4][5]

UK NACE similarly advises organisations that suspect technical surveillance not to discuss the concern using the location or devices thought to be targeted and to record the reasons for suspicion before specialist investigation.[9] The appropriate response depends on personal safety, legal context and whether preserving attribution evidence matters.

What a TSCM result can and cannot prove

A positive finding may establish the presence of a device, account exposure or technical weakness. A negative finding is more limited. Some devices transmit only intermittently, some store data locally, some surveillance occurs through legitimate systems, and some software compromise leaves no separate physical object. The confidence of the conclusion should therefore reflect the scope, time window and techniques used.

Government guidance reflects the value of repeated assurance in higher-risk environments: UK guidance for working at SECRET says organisations should consider periodic TSCM sweeps of controlled office areas that frequently host SECRET meetings.[8] Periodicity matters because technical security is a condition to maintain, not a one-time certificate that a room can never be compromised.

Implications for decision-makers

• Technical surveillance risk can involve physical devices, legitimate connected systems, personal devices, accounts and the surrounding environment.

• A negative finding has to be interpreted against the scope and timing of the examination rather than treated as a permanent guarantee.

• Vehicles, vessels, homes and offices present materially different technical and evidential contexts.

• Alerts and anomalies may require separate technical, legal or forensic assessment before their significance is clear.

Real-world context: surveillance technology also creates governance risk

In February 2024 the Information Commissioner ordered Serco Leisure and associated trusts to stop using facial-recognition and fingerprint technology to monitor attendance of more than 2,000 workers across 38 facilities. The case concerned overt workplace monitoring rather than hostile surveillance, but it demonstrates a wider point: technical capability does not answer whether surveillance is necessary, proportionate or compliant. Defensive technical-security decisions require the same attention to purpose and governance.

Public source: Information Commissioner's Office, Serco Leisure enforcement action, 23 February 2024.

Sources and reading

Primary and official sources were checked for this edition on 16 August 2026. Dates below are publication or review dates where the issuing body states one; otherwise the source is identified as undated.

1. 1**UK NACE / FCDO Services.** Technical Surveillance Countermeasures (TSCM). Undated; accessed 16 August 2026.
   URL: https://www.fcdoservices.gov.uk/uk-nace/uk-nace-operations/tscm/
2. 2**UK NACE / FCDO Services.** Detecting hidden cameras at work. Published 22 December 2022; accessed 16 August 2026.
   URL: https://www.fcdoservices.gov.uk/detecting-hidden-cameras-at-work/
3. 3**UK NACE / FCDO Services.** Listening with lasers. Published 5 June 2024; accessed 16 August 2026.
   URL: https://www.fcdoservices.gov.uk/listening-with-lasers/
4. 4**Apple.** Detect unwanted trackers, Apple Personal Safety User Guide. Published February 2026; accessed 16 August 2026.
   URL: https://support.apple.com/guide/personal-safety/detect-unwanted-trackers-ips139b15fd9/web
5. 5**Google Android Help.** Find unknown trackers. Undated; accessed 16 August 2026.
   URL: https://support.google.com/android/answer/13658562?hl=en
6. 6**National Cyber Security Centre.** Device security guidance. Published 29 June 2021; reviewed 13 May 2025; accessed 16 August 2026.
   URL: https://www.ncsc.gov.uk/collection/device-security-guidance
7. 7**National Cyber Security Centre and international partners.** BADBAZAAR and MOONSHINE: Technical analysis and mitigations. Published 9 April 2025; accessed 16 August 2026.
   URL: https://www.ncsc.gov.uk/news/advisory-badbazaar-moonshine-technical-analysis-mitigations
8. 8**HM Government.** Guidance 1.2 - Working at SECRET. Updated 5 August 2024; accessed 16 August 2026.
   URL: https://www.gov.uk/government/publications/government-security-classifications/guidance-12-working-at-secret-html
9. 9**UK NACE / FCDO Services.** What to do if you suspect your organisation is being targeted by technical surveillance. Published 6 July 2021; accessed 16 August 2026.
   URL: https://www.fcdoservices.gov.uk/what-to-do-if-you-suspect-your-organisation-is-being-targeted-by-technical-surveillance/
10. 10**International Maritime Organization.** AIS transponders. Undated page; accessed 16 August 2026.
    URL: https://www.imo.org/en/ourwork/safety/pages/ais.aspx

Scope note

This publication is general defensive information, not a substitute for a site-specific technical examination, digital-forensic assessment, legal advice or emergency response. Technical examination should be undertaken by suitably competent specialists for the environment and risk involved.

PDF edition

Download the publication in a formatted edition suitable for circulation or offline reading.