GARDAWORLD
SECURITY

Case study

Protecting defense sector assets in Ukraine

Defence companies operating in Ukraine – particularly those involved in unmanned systems, advanced engineering, and logistics, are now priority intelligence targets.

Beyond cyber and human intelligence activity, there is a clear and sustained shift toward technical surveillance operations targeting offices, accommodation, and operational environments.

For organizations handling sensitive design data, supply chain information, and operational coordination, maintaining physical and technical security has become a critical requirement, not a supporting function.

Trigger event: March 2026

Recent open-source reporting highlights an attempted espionage operation targeting a Ukrainian drone manufacturer (TechEx). Devices with audio and video capability were covertly installed within the office of a senior engineer to capture sensitive information, including:

- Design and engineering data
- Supply chain and logistics routes
- Partner networks
- Operational use of systems by Ukrainian forces

> The operation appears to have been part of a broader effort to map and penetrate Ukraine's defense-industrial base. While Ukrainian counter-intelligence successfully disrupted the activity, the incident underscores a key reality: even well-protected organizations remain vulnerable to state-level technical surveillance.

What this means for operators

This case is not isolated. It reflects a wider pattern of targeting across:

- Defense manufacturers and drone developers
- Government and command environments
- Executive leadership locations and travel
- Facilities supporting international partners

> Internal security measures, while necessary, are not designed to detect or counter covert technical surveillance deployed by capable state actors. The gap between standard corporate security and specialist counter-surveillance capability is now operationally significant.

Our approach

Our in-country Technical Surveillance Countermeasures (TSCM) teams in Ukraine provide discreet, technically advanced counter-surveillance support aligned to the realities of the operating environment.

Services include:

Workspaces and technical facilities

- Full-spectrum sweeps of offices, R&D environments, and meeting spaces
- Detection of RF, GSM, Wi-Fi, Bluetooth, and hard-wired devices
- Physical search for passive (non-RF emission) devices using techniques such as Non-linear junction detection and thermal inspection for concealed electronics

Accommodation

- Pre-occupancy and in-stay sweeps of hotels and temporary housing
- Inspection of fixtures, power systems, communications infrastructure, and furnishings

Vehicles

- Inspection of executive and operational vehicles
- Identification and removal of tracking or audio-enabled devices

All activity is fully licensed under Ukrainian law and conducted with minimal disruption, supported by documented findings and, where required, forensic-grade reporting. Sweep schedules can be structured as one-off, periodic, or continuous monitoring depending on threat exposure.

Case study:
Protecting defence sector assets in Ukraine

GARDAWORLD SECURITY

Outcome

Clients operating in similar environments benefit from:

- Early detection and removal of covert surveillance devices
- Protection of sensitive intellectual property and operational information
- Reduced exposure across supply chains, partner networks, and field operations
- Increased confidence in the integrity of workspaces and communications

This capability provides a specialist layer of assurance that internal resources alone are not designed to deliver.

Why it matters

Technical surveillance is now a routine component of intelligence activity targeting Ukraine's defense sector. The focus is not limited to systems or infrastructure, but extends to people, environments, and decision-making spaces.

For organizations supporting defense operations—directly or indirectly—maintaining control over information is fundamental to both commercial and operational continuity.

Advisory

Where organizations maintain a presence in Ukraine, whether permanent or periodic, TSCM should be considered a planned and recurring security measure, not a reactive response.

Assessments can be aligned to:

- New facility setup or expansion
- Sensitive project phases or partner engagements
- Executive travel or site visits
- Changes in threat posture or operating environment

Confidential consultations are available to determine appropriate coverage based on operational footprint and risk exposure.