Securitas

Risk Intelligence

Decision Advantage in the Gray Zone

Safeguarding Aerospace & Defense through Risk Intelligence

intelligence@securitas.com

Contents

As Sophie Cairney, Lead Risk Intelligence Consultant, Securitas Risk Intelligence Center, puts it: “The aerospace and defense industry is caught more in the crossfire of ‘convergence’ than ever before. This includes how geopolitical and conflict related threats can directly and indirectly impact private sector organizations, and the security requirements to safeguard against these. But not every threat starts with a ‘bang’ – and organizations using intelligence-led security strategies to identify, assess, and take action to safeguard their interests will define the future of security.”

Introduction

Sophie Cairney
Lead Risk Intelligence Consultant

The aerospace and defense sector (A&D) in 2026 and beyond faces a volatile, uncertain, complex and ambiguous (VUCA) threat landscape shaped by geopolitical tensions, societal polarization, and the expanding use of gray zone tactics by both state and non state actors. As conflicts persist and strategic competition intensifies, A&D organizations are increasingly exposed to converging physical, digital, and reputational risks that challenge traditional security models and demand more agile, intelligence led decision making.

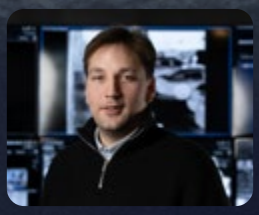
This is the central premise of the *Decision Advantage in the Gray Zone report*. Its objective is to provide a high level view of the threats shaping the industry and highlight the key risks that aerospace and defense organizations should prepare for in the year ahead. These threats may originate within the business and its operations, or emerge from an increasingly unpredictable external environment.

This condensed report summarizes the key findings of the full *‘Aerospace & Defense Industry – Top Threats 2026’* analysis, offering leaders a focused, actionable overview of the most pressing issues defining the year.

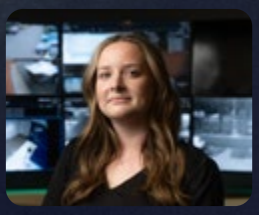
Please contact Securitas Risk Intelligence to access the full report or use the QR on the back cover of this report.

Team Members

Anastasia Jobard
Junior Protective Intelligence Analyst *(Aerospace & Defense)*



Freddie Venables
Junior Protective Intelligence Analyst *(Aerospace & Defense)*



Sophie Cairney
Lead Risk Intelligence Consultant

Our Intelligence Toolkit

Awareness

Regular scheduled & ad-hoc reporting on the global security and threat landscape. Including Intelligence reports (INTREPs) and situation reports (SITREPs)

- Daily Global Intelligence Reports
- Weekly Global Intelligence Outlooks
- Monthly Threat Forecasts
- Monthly Intelligence Summaries (INTSUMs)
- Situation Reports (SITREPs) and Intelligence Reports (INTREPs) for significant developments

Alerting

Geo-targeted email-based alerts for security and threat events nearby. Fully customizable based on severity, proximity, and frequency with incident types:

- Criminality
- Civil unrest
- Terrorism
- Weather
- Travel and transportation

Advisory

An **all-in-one** Protective, Threat, and Risk Intelligence solution for your organization, operations, and brand. Includes:

- Monitoring for your specific requirements
- Daily Monitoring intelligence summaries
- Immediate briefs for warnings intelligence
- Threat, Protective & Risk Intelligence solution
- Access to the on-demand ad-hoc reporting service

Safeguard your organization with industry-leading intelligence. Securitas Risk Intelligence goes beyond identifying what is happening. It also explains why it matters, what could happen next, and, most importantly, what actions can be taken. With four levels of premium services, we offer digital tools, managed services, and embedded expertise, all combined to create a tailored solution that meets your unique needs. In addition we offer Ad-hoc Intelligence and consultancy to meet our clients specific needs.

Analyst

Dedicated intelligence resources complete with Securitas' Global Intelligence Community expertise.

Equipped with all the tools and training to support your intelligence requirements and protect your organization.

Ad-hoc Intelligence

Subject matter expertise and consultancy for any dynamic specific intelligence requirements.
Common report types include but are not limited to:

- Travel & traveler security report: in-depth analysis of travel safety and security threats.
- Executive protection & defensive screening: information vulnerability assessment of a target principal (i.e. an executive).
- Event security assessments & screening: due diligence & live monitoring.

This report has been developed by Securitas' Risk Intelligence Center (RIC), our dedicated unit for global risk analysis and strategic insight. The RIC continuously monitors geopolitical developments, emerging threats, and industry-specific risk patterns, transforming complex information into clear, evidence-based intelligence. Its work provides the analytical foundation for Securitas Intelligence assessments and services.

Methodology

Approach

The RIC utilizes all-source intelligence, combining open-source intelligence (OSINT) and closed sources such as human intelligence (HUMINT), to provide finished intelligence. All-source intelligence uses all available and appropriate sources of intelligence based on the Customer Critical Intelligence Requirements (CCIRs).

Threats

The potential threats considered in context of this intelligence report include threats that could reasonably be anticipated based on existing intelligence, such as (but not limited to):

- Petty and opportunistic crime and organized criminal activity.
- Targeted and untargeted violent attacks, both criminal and terrorist in nature.
- Protest activity, both targeted and untargeted.
- Corporate security, including insider threats, corporate espionage, and sensitive business operations.

Inclusion in this report is not a statement that any of these threats will occur, but that the potential exists for the threat to manifest and that the threat should be considered when performing security and safety reviews and risk assessments.

Similarly, while all reasonable efforts are made to assess every potential threat vector for organizations, the security and threat landscape is dynamic and ever-changing, and new threats are constantly emerging. It is important that this report is used as a single tool as part of a wider security strategy rather than a standalone document that is expected to capture and outline all potential threats to the industry.

Language of probability

This report uses the RIC's language of probability to provide an assessment of the likelihood of a threat manifesting, based on probability, using a percentage, fraction, or ratio as a baseline. This helps to provide context and clarity, and helps promote a standardized understanding of assessment and terms used.

Term	Probability
Remote	0-5%
Highly unlikely	10-20%
Unlikely	25-35%
Realistic possibility	40-50%
Likely/Probable	55-75%
Highly likely	80-90%
Almost certain	95-99%

Threat levels

This report uses the RIC's threat level system to score threats on a 1-5 scale based on the assessed likelihood and severity, and / or intent and capability.

5 - EXTREME	*Very high / extreme threat.* Review and respond if required.
4 - HIGH	*High / major threat.* Consider taking appropriate action.
3 - MODERATE	*Moderate threat.* Maintain awareness, consider precautions.
2 - LOW	*Low / limited threat.* Be advised.
1 - VERY LOW	*Very low / insignificant threat.* For awareness.

Intelligence cut off date (ICOD)

1700hrs UTC 05 December 2025

Aerospace & Defense
Top Threats 2026

Summary

Escalating Anti War Activism and Targeting of A&D Organizations

Anti-war activism will continue to be a growing concern for the A&D industry, particularly as the Gaza–Israel conflict persists, driving overlapping motivations among activist groups toward more disruptive and sometimes violent direct action. Organizations with identifiable or perceived links to Israel and Israeli defense companies remain significant targets. These groups are expected to escalate coordinated campaigns that include physical disruptions, digital harassment, and targeted actions against senior executives and key facilities.

Geopolitical Drivers of Protest, Unrest, and Criminal Activity

Geopolitical tensions will continue to drive protest, unrest, and activism against A&D organizations, fueled by ongoing conflicts, environmental concerns, and economic competition. Criminal threats are forecasted to rise, particularly from state-backed or tolerated organized crime groups seeking to steal intellectual property, materials, and components, as well as conducting sabotage. Concurrently, corporate security threats, including espionage and sabotage, are expected to increase, requiring enhanced vigilance across the sector.

Rising Gray Zone Warfare and Sabotage Risks

Gray zone warfare (GZW) and sabotage are increasingly likely to cause significant disruption in 2026, including potential mass casualty events, supply chain interruptions, and IT or communications outages affecting critical national infrastructure and private aerospace assets. State and non-state actors will likely continue to employ these tactics to undermine, influence, and disrupt Western A&D interests, necessitating robust resilience and crisis management measures.

Increasing Targeting of Executives and VIPs

Executives and VIPs in A&D remain elevated targets for criminals and activists alike, driven by ideological extremism, criminal opportunism, and geopolitical tensions. The increased use of doxxing, synthetic media, and coordinated harassment campaigns has lowered barriers to personal targeting. Organizations should prioritize measures to protect executive personal information, monitor for impersonation, and integrate physical and cyber protections.

Persistent and Evolving Insider Threat Risks

Insider threats continue to pose a significant risk, with individuals motivated by a wide range of factors exploiting vulnerabilities to cause disruption, data loss, and reputational damage. Threat actors may include employees, contractors, activists, criminals, and hostile nation states acting either maliciously or negligently. This underscores the critical need for effective insider threat programs, access controls, and continuous security monitoring in 2026.

The overall threat outlook for the A&D industry in 2026 is moderate, driven by a combination of high level protest and unrest risks and elevated corporate security threats, while exposure to crime and terrorism remains moderate but persistent. Threat actors and global security incidents will likely impact operations, personnel safety, and brand reputation, with effects varying by geographic and industry exposure. Looking ahead, the next industry-level crisis within A&D is most likely to stem from geopolitical flashpoints or renewed conflicts, amid ongoing pressures such as climate change and political polarization that create additional vulnerabilities. Organizations that invest in early warning, resilience, and integrated cross-domain security are better positioned to maintain decision advantage in this increasingly contested environment.

Key threat areas

Protest & Unrest

Assessed threat level: 4

Crime & Security

Assessed threat level: 3

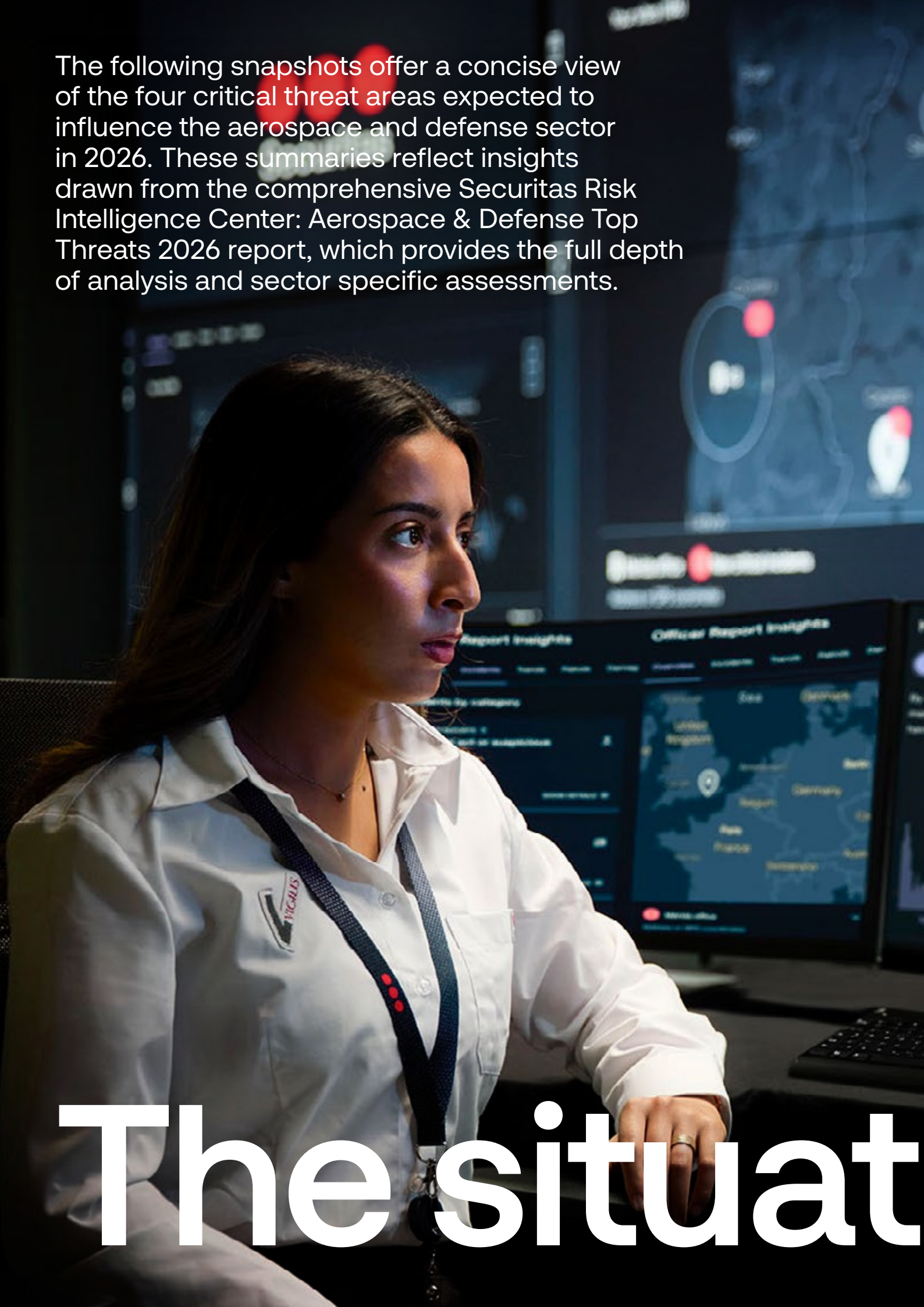
Corporate Security

Assessed threat level: 4

Terrorism & Extremism

Assessed threat level: 3

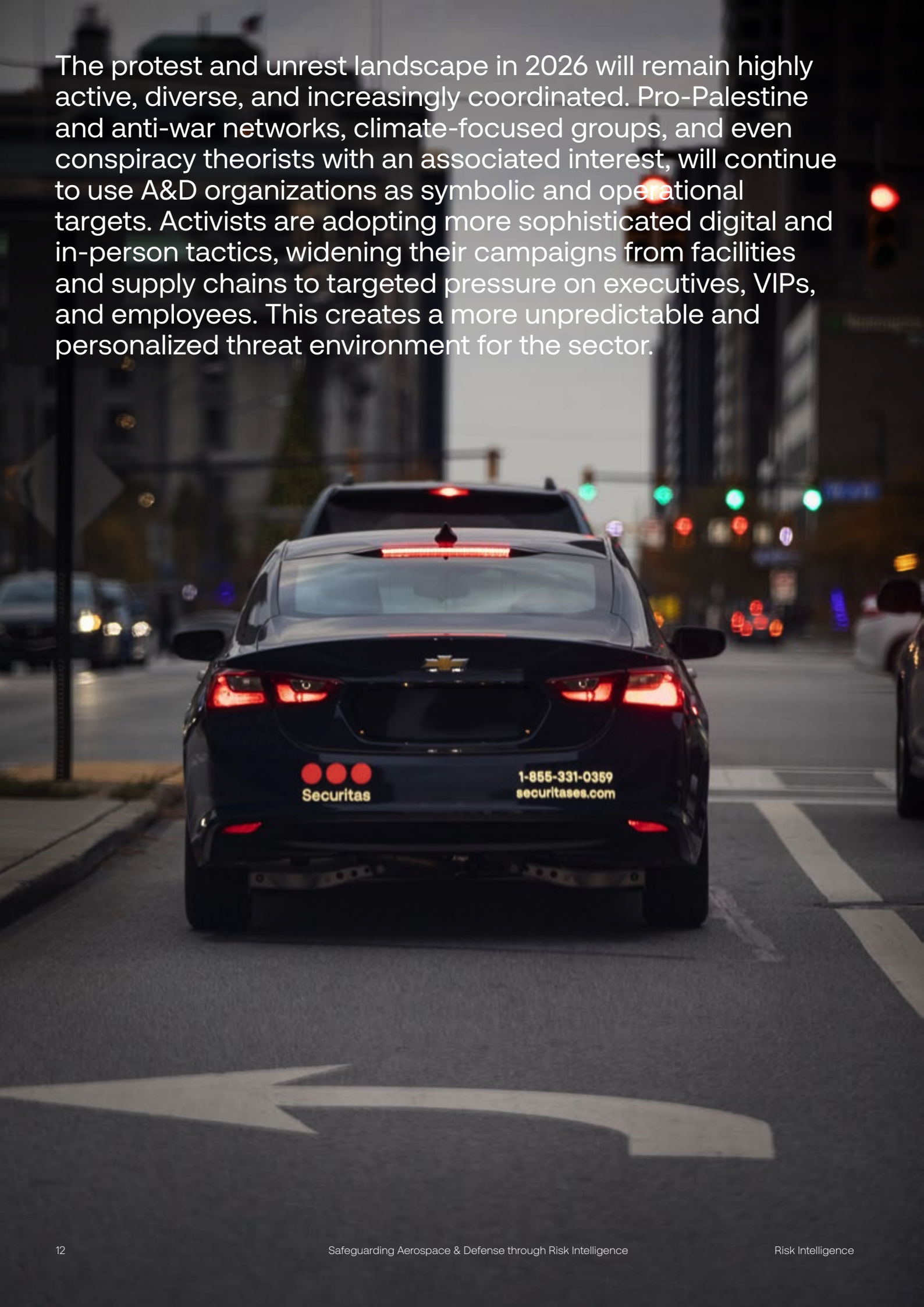
The following snapshots offer a concise view of the four critical threat areas expected to influence the aerospace and defense sector in 2026. These summaries reflect insights drawn from the comprehensive Securitas Risk Intelligence Center: Aerospace & Defense Top Threats 2026 report, which provides the full depth of analysis and sector specific assessments.



The situat


Intelligence briefs
ion

The protest and unrest landscape in 2026 will remain highly active, diverse, and increasingly coordinated. Pro-Palestine and anti-war networks, climate-focused groups, and even conspiracy theorists with an associated interest, will continue to use A&D organizations as symbolic and operational targets. Activists are adopting more sophisticated digital and in-person tactics, widening their campaigns from facilities and supply chains to targeted pressure on executives, VIPs, and employees. This creates a more unpredictable and personalized threat environment for the sector.



Protest & Unrest Snapshot

Protest & Unrest Snapshot

Threat Assessment

Most likely (MLCOA) vs Most dangerous course of action (MDCOA)

MLCOA: Activists maintain frequent protests, online mobilization, and targeted disruptions against A&D organizations, expanding pressure to include executives, board members, and employees. Visibility around homes, events, and campuses increases, with most interactions remaining non violent but disruptive.

MDCOA: Coordinated multi site direct action campaigns cause major operational disruption, with targeted harassment escalating to aggressive confrontations at private residences or workplaces. Isolated risks of violence, criminal coercion, or high impact sabotage cannot be ruled out.

Key Dynamics

1 Anti-War / Pro-Palestine Mobilization

- Gaza–Israel remains the primary driver of disruptive activism against A&D organizations.
- Activist networks target firms and suppliers perceived to be linked to defense programs, often coordinating cross border actions.
- Tactics include site blockades, supply chain disruptions, major event interference, and coordinated digital pressure campaigns.
- New activist groups adopt increasingly disruptive tactics, techniques and procedures (TTPs) despite restrictions imposed by authorities on these groups.

2 Targeting of Executives, VIPs & Employees

- Executives and senior leaders are increasingly targeted through doxxing, hostile communications, synthetic media, open letters, and social media campaigns.
- Residential targeting rises as activists use publicly available information to map home addresses and personal routines.
- Employees at site entrances are filmed, named, and shamed online, creating reputational and personal safety concerns.
- Activists also use "**relational targeting**," leveraging an executive's board roles, university affiliations, or partnerships to exert pressure.

3 Student Activism & University Pressure

- Student groups continue protests targeting university ties with A&D firms, disrupting recruitment events and research partnerships.
- Encampments, banner drops, and coordinated campus actions persist, pressuring universities to reconsider collaboration with defense organizations.

4 Environmental Activism Converging with Anti-War Narratives

- Aerospace and defense organizations remain high profile climate activism targets.
- Groups such as Extinction Rebellion (XR) and A22 affiliates focus on air shows, high visibility events, and assets associated with emissions or environmental impact.
- Increasing convergence between climate activism, anti-war, and anti-corporate narratives amplifies threat levels and broadens potential targets.

Priority Actions

- **Reduce discoverability of executive and employee information** across open sources, ensuring proactive monitoring for doxxing, impersonation, and hostile reconnaissance.
- **Prepare for cross movement mobilization** around key industry events, geopolitical flashpoints, and procurement cycles that may act as catalysts for protests or targeted campaigns.
- **Strengthen scenario-based response plans** for peaceful protest, targeted harassment, supply chain disruptions, and multi site coordinated actions—integrating physical security, HR, communications, and legal teams.

Crime will remain a persistent threat to A&D organizations throughout 2026, driven by geopolitical tensions, economic pressures, and continued strain on global supply chains. The high value of industry products, sensitive materials, and proprietary information increases exposure to theft, sabotage, illicit procurement, and criminal facilitation. Organized criminal groups (OCGs) and state-aligned actors will continue exploiting gaps in supplier verification and logistics networks, trafficking critical components through gray and black markets. As production pressures intensify, organizations face rising risks of counterfeit or stolen parts infiltrating legitimate supply chains.

Cyber threats will also escalate, with state-backed and financially motivated actors refining espionage, data exfiltration, and AI-enabled impersonation operations. Executive exposure, synthetic media manipulation, and hybrid digital/physical targeting will continue expanding the attack surface, underscoring the need for integrated cyber/physical security.

Crime & Security Snapshot

Crime & Security Snapshot

Threat Assessment

Most likely (MLCOA) vs Most dangerous course of action (MDCOA)

MLCOA: Criminal actors continue targeting A&D supply chains with recurring theft of minor materials, parts, and components. Stolen or repurposed items surface on illicit markets, increasing the risk of contaminated supply chains. Cyber criminals maintain consistent pressure for financial gain and data theft.

MDCOA: A large-scale criminal campaign — potentially backed by adversarial states — targets the A&D supply chain with theft, sabotage, and illicit procurement. Disruption forces reliance on unauthorized suppliers, introducing dangerous components into production processes and impacting safety and output.

Key Dynamics

1 Illicit Procurement & Supply Chain Vulnerabilities

- OCGs remain the primary facilitators of component theft, diversion, and covert procurement for sanctioned states including Russia, Iran, and China.
- Stolen avionics, sensors, circuit boards, and precision components are trafficked through gray and black markets at inflated prices.
- Supply shortages and production bottlenecks increase incentives to source unverified components, heightening contamination risks.
- Weak points in freight forwarding, supplier verification, and cross border compliance continue to be exploited.

2 OCG-State Collaboration Deepening

- Sanctions and export controls accelerate collaboration between adversarial states and OCGs seeking restricted parts.
- Criminal groups leverage established smuggling corridors, shell companies, and logistics intermediaries refined during recent geopolitical disruptions.
- With large assemblies remaining difficult to steal, focus increases on smaller, high value components and other more lucrative and accessible targets.

3 Escalating Cyber Espionage & AI Enabled Intrusion

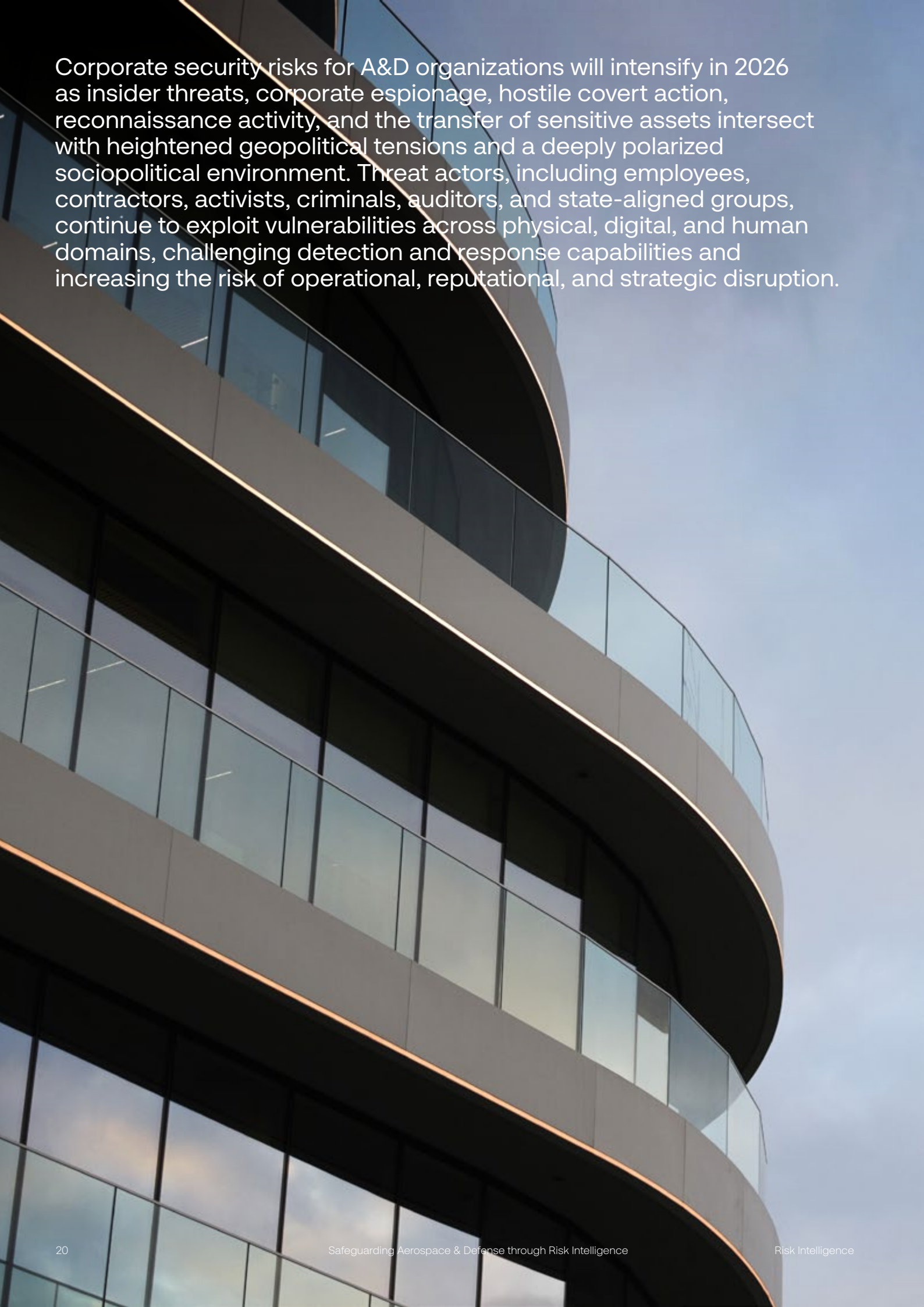
- State-backed and criminal cyber actors refine espionage, credential theft, and data exfiltration operations against A&D networks.
- AI enabled impersonation, synthetic audio/video, and deepfake documents increase deception and reduce detection barriers.
- Incidents in 2025 saw multiple sustained campaigns, including cyber attacks on major Israeli A&D firms and ongoing espionage by Russian backed actors.
- Phishing and compromise via smaller vendors or service providers remain key pathways into high-value programs.

4 Rising Targeting of Executives & Sensitive Individuals

- Personal information exposure fuels doxxing, intimidation, and hybrid digital physical pressure.
- Public databases and PII leaks lower barriers for adversaries to identify and track executives.
- 2025 saw an escalation in the severity of actions targeting executives, from online threats to attempted abductions, property sabotage, and state-linked assassination plots.
- Synthetic media, manipulated narratives, and personalized cyber impersonation intensify reputational and safety risks.

Priority Actions

- **Strengthen supplier verification and vetting** across all tiers, prioritizing controls that prevent counterfeit, stolen, or illicit components from entering the supply chain.
- **Implement integrated cyber/physical security** strategies addressing espionage, sabotage, synthetic impersonation, executive exposure, and hybrid threat pathways.
- **Conduct targeted assessments of likely threat actors** (OCGs, state-aligned networks, disgruntled insiders) to identify vulnerabilities across logistics, personnel, and digital systems.
- **Develop, test, and regularly update incident response plans**—including cyber intrusions, supply chain compromise, and executive focused targeting—supported by cross functional exercises.



Corporate security risks for A&D organizations will intensify in 2026 as insider threats, corporate espionage, hostile covert action, reconnaissance activity, and the transfer of sensitive assets intersect with heightened geopolitical tensions and a deeply polarized sociopolitical environment. Threat actors, including employees, contractors, activists, criminals, auditors, and state-aligned groups, continue to exploit vulnerabilities across physical, digital, and human domains, challenging detection and response capabilities and increasing the risk of operational, reputational, and strategic disruption.

Corporate Security Snapshot

Corporate Security Snapshot

Threat Assessment

Most likely (MLCOA) vs Most dangerous course of action (MDCOA)

MLCOA: Organizations face continued accidental or malicious disclosure of sensitive information, low level insider misuse, opportunistic reconnaissance, and sustained espionage attempts via social engineering, credential theft, drone activity, and in person infiltration. Increased ideological polarization contributes to more grievance driven insider risks, and routine hostile activity tests security posture across corporate facilities and supply chains.

MDCOA: State-sponsored and hybrid actors escalate coordinated campaigns involving insider recruitment, sabotage, complex espionage, drone-enabled reconnaissance, and exploitation of third party relationships to access or divert sensitive assets. Malicious insiders exfiltrate valuable data or enable follow-on attacks, while sophisticated adversaries leverage reconnaissance and covert action to disrupt operations, compromise supply chains, or inflict reputational and legal harm.

Key Dynamics

1 Insider Threats Rising

- Insider threats span employees, contractors, visitors, and third-party partners, acting maliciously or negligently across physical and digital environments.
- Motivations include financial pressure, ideological grievances, personal circumstances, coercion, notoriety, or exploitation by hostile actors.
- Sensitive information leaks — including internal documents, emails, or PII — via AI tools or social media create operational, legal, and reputational exposure.
- Notable 2025 cases highlight state-backed recruitment of individuals with privileged access, including trade secret theft and exfiltration for foreign intelligence programs.
- Indicators of malicious activity include repeated security violations, unexplained access attempts, unusual hours, file transfers to personal devices, and early resignation patterns.

2 Expanding Corporate Espionage Exposure

- Rising geopolitical competition increases espionage targeting proprietary designs, R&D data, IP, and dual use technologies.
- State-backed actors exploit cyber intrusions, social engineering, foreign dignitary visits, and insider access to obtain confidential information.
- Organizations involved in procurement programs, sensitive research, or government contracts face heightened targeting.
- 2025 events — from espionage arrests in Latvia, Türkiye, and Ukraine, to leaked footage of prototype aircraft — underscore the breadth of adversary tactics.
- Espionage campaigns support follow on operations including information manipulation, ransomware, or coordinated gray zone activity.

3 Sabotage & Hostile Covert Action Increasing in Frequency

- State and non state actors conduct covert activity below escalation thresholds, testing detection and response capabilities.
- Threats include arson, drone reconnaissance, parcel bombs, tampering with subsea cables, electronic warfare, and hoax bomb threats.
- Hybrid tactics target military sites, transportation hubs, logistics infrastructure, assembly facilities, and dual-use locations.
- Numerous 2024–2025 incidents across Europe highlight drones flying over nuclear facilities, ammunition trains, naval installations, and dual-use infrastructure.
- Outsourcing of covert action to criminal or extremist proxies increases plausible deniability but also elevates unpredictability and escalation risks.

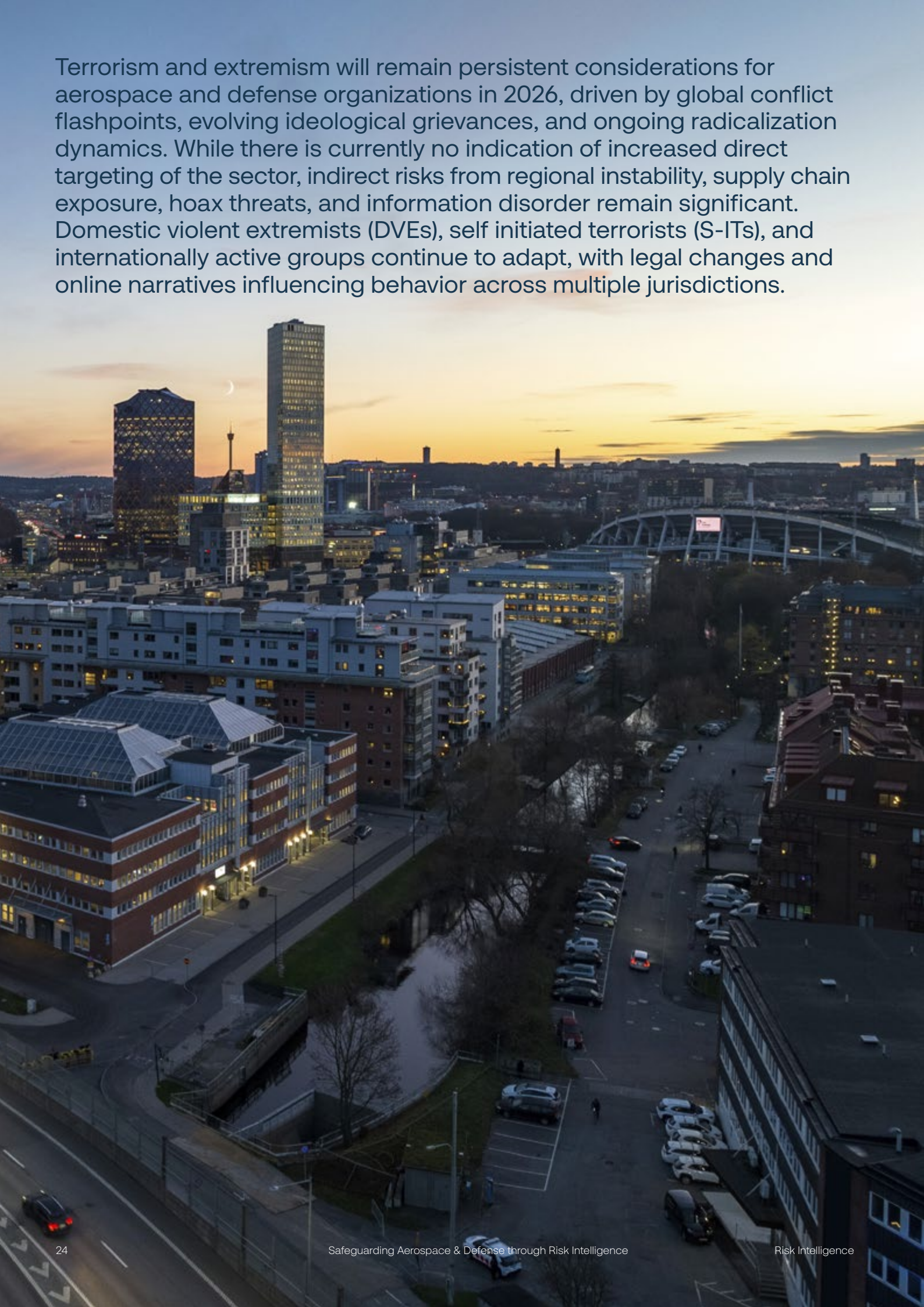
4 Hostile Reconnaissance & Security Auditing Challenges

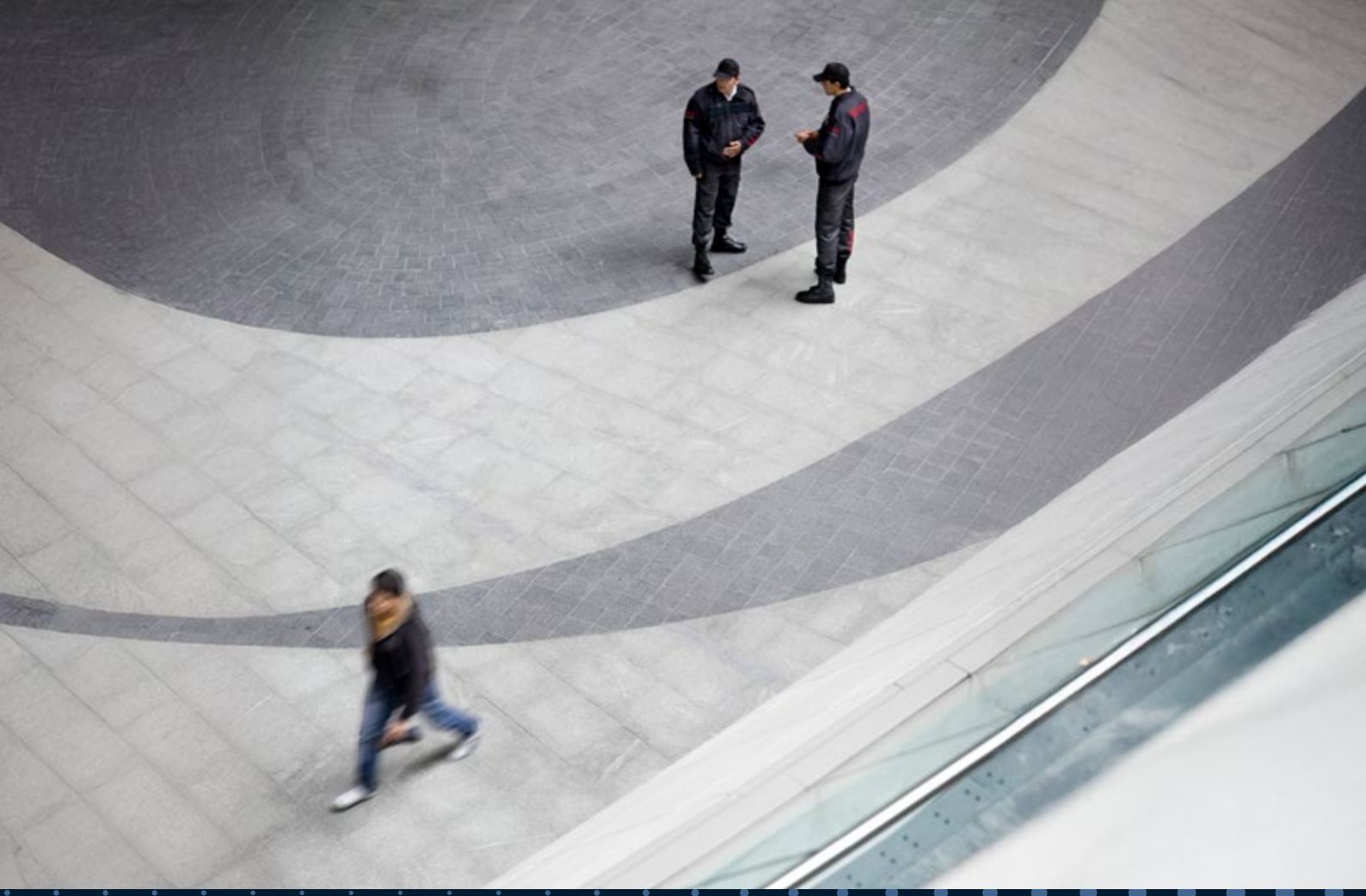
- Security auditors continue to film facilities overtly for online engagement, revealing critical information and indicators (access points, CCTV coverage, codes, employee details).
- Covert reconnaissance via drones, disguised devices, or repeated site visits provides second hand intelligence for activists, criminals, and state-backed actors.
- Auditors will continue to exploit public land rights, creating reputational risks to target organizations from mishandling of interactions with security staff.
- Drone-enabled reconnaissance at sensitive sites — including research centers and defense facilities — continues rising, frequently linked to foreign intelligence interests.

Priority Actions

- Strengthen insider threat programs using behavioral indicators, open source monitoring, and integration across HR, cyber, and physical security.
- Enhance controls on sensitive information handling, offboarding processes, and privileged access across employees, contractors, and partners.
- Expand anti-espionage and OPSEC training, especially for teams involved in R&D, procurement, sensitive projects, and foreign delegations.
- Update crisis and incident response plans to include sabotage, covert action, drone incursions, insider-enabled breaches, and reconnaissance events.
- Improve supply chain transparency, sanctions compliance, and monitoring of third party partners — including due diligence and asset tracing.
- Train frontline staff and security teams to appropriately manage auditors and hostile reconnaissance, avoiding escalation while protecting sensitive information.
- Develop counter drone readiness, engage public sector partners, and test response procedures through tabletop and multi-agency exercises.

Terrorism and extremism will remain persistent considerations for aerospace and defense organizations in 2026, driven by global conflict flashpoints, evolving ideological grievances, and ongoing radicalization dynamics. While there is currently no indication of increased direct targeting of the sector, indirect risks from regional instability, supply chain exposure, hoax threats, and information disorder remain significant. Domestic violent extremists (DVEs), self initiated terrorists (S-ITs), and internationally active groups continue to adapt, with legal changes and online narratives influencing behavior across multiple jurisdictions.





Terrorism & Extremism Snapshot

Terrorism & Extremism Snapshot

Threat Assessment

Most likely (MLCOA) vs Most dangerous course of action (MDCOA)

MLCOA: No clear signs of increased direct targeting of A&D organizations. However, terrorist incidents affecting supply chains, particularly in high risk regions with active conflict or geopolitical tension, remain a realistic possibility.

MDCOA: Perceptions of A&D involvement in global conflicts generate targeted attacks against firms, facilities, or supply chains. Information disorder, criticism of the sector, and geopolitical flashpoints converge with personal grievances, fueling radicalization among domestic violent extremists (DVEs), self-initiated terrorists (S-ITs), and established terrorist groups.

Key Dynamics

1 Evolving DVE/S-IT Motivations

- Extremist motivations include far right, far left, racial/ethnic, anti-authority, and anti-technology ideologies.
- Personal grievances increasingly intersect with geopolitical narratives amplified on social media.
- Radicalization cycles accelerate via online platforms despite increased proscription of extremist networks.

2 Legal Designations Shaping Extremist Behaviour

- New designations of groups previously considered activist or criminal networks deters some activity.
- Restrictions on and targeting of groups will cause more dedicated elements to move 'underground', enhancing operational security (OPSEC) and/or rebranding or relocating in order to avoid targeting.
- Negative public response to perceived 'heavy-handed' measures toward activist groups presents the potential for unintended increases in public support for the group and its causes.

3 Targeting via Hoaxes & Disruption

- A&D firms remain vulnerable to malicious communications, hoax bomb threats, and disruptive false alarms.
- These actions are often intended to provoke response, test security, or extract operational insights.
- Hoax activities are increasingly used to test responses and to enable reconnaissance against target sites.

4 Indirect Threats from Global Conflict Zones

- Terrorist incidents in regions with heightened geopolitical tension pose indirect risks to supply chains, logistics, and personnel.
- Western governments continue to warn that terrorist attacks remain likely in the near term, even if not specifically directed at the A&D sector.

Priority Actions

- Conduct site specific TVRAs and proximity threat assessments, focusing on facilities located near geopolitical flashpoints or key logistical hubs.
- Strengthen business continuity and crisis management plans, ensuring alignment with national counterterrorism guidance and employee awareness programs.

Read the Complete Industry Report

Contact

intelligence@securitas.com