Securitas

Risk Intelligence

Entscheidungs-vorteil in der Grauzone

Schutz für Aerospace & Defence durch Risikobewertungen

intelligence@securitas.com

Inhalt

Sophie Cairney, Lead Risk Intelligence Consultant, Securitas Risk Intelligence Center, dazu: „Die Branchen Aerospace & Defence stehen mehr denn je im Kreuzfeuer der ‚Konvergenz'. Dazu gehört auch, wie sich geopolitische und konfliktbezogene Bedrohungen direkt und indirekt auf Unternehmen im privaten Sektor auswirken können und welche Sicherheitsanforderungen zu deren Schutz bestehen. Aber nicht jede Bedrohung beginnt mit einem großen ‚Knall' – und Unternehmen, die durch Informationen gestützte Sicherheitsstrategien verfolgen, um ihre Interessen zu erkennen, zu bewerten und Maßnahmen zu deren Schutz zu ergreifen, sind die Zukunft der Sicherheit."

Sophie Cairney
Lead Risk Intelligence Consultant

Einführung

Die Aerospace & Defence stehen 2026 und darüber hinaus vor einer volatilen, unsicheren, komplexen und mehrdeutigen Bedrohungslage, die von geopolitischen Spannungen, gesellschaftlicher Polarisierung und dem zunehmenden Einsatz von Taktiken in der Grauzone durch staatliche und nichtstaatliche Akteure geprägt ist. Angesichts der anhaltenden Konflikte und der Verschärfung des strategischen Wettbewerbs sind Unternehmen aus diesen Branchen in zunehmendem Maße einer Verflechtung aus physischen, digitalen und Reputationsrisiken ausgesetzt. Das stellt herkömmliche Sicherheitsmodelle in Frage und erfordert eine agilere, informationsgestützte Entscheidungsfindung.

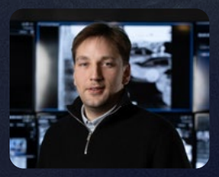
Das ist die zentrale Prämisse des *Berichts Entscheidungsvorteil in der Grauzone.* Ziel ist es, einen umfassenden Überblick über die Bedrohungen der Branche zu geben und die wichtigsten Risiken hervorzuheben, auf die sich Unternehmen zum Thema Aerospace & Defence im kommenden Jahr vorbereiten sollten. Dabei können diese Bedrohungen ihren Ursprung im Unternehmen und seinen Abläufen selbst haben oder von einem zunehmend unberechenbaren externen Umfeld ausgehen.

Dieser Kurzbericht fasst die wichtigsten Erkenntnisse der vollständigen Analyse *‚Aerospace & Defence – Top-Bedrohungen 2026'* zusammen und bietet Führungskräften einen konzentrierten, umsetzbaren Überblick über die dringendsten Probleme, die das Jahr bestimmen werden.

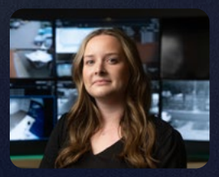
Bitte wenden Sie sich an Securitas Risk Intelligence, um den vollständigen Bericht zu erhalten, oder scannen Sie den QR-Code auf der Rückseite dieses Berichts.

Das Team

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



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



Sophie Cairney
Lead Risk Intelligence Consultant

Unser Intelligence Toolkit

Schützen Sie Ihr Unternehmen mit branchenführenden Informationen. Securitas Risk Intelligence ermittelt dabei nicht nur, was gerade passiert. Es wird darüber hinaus erläutert, warum das Geschehen wichtig ist, was als Nächstes passieren könnte und – am wichtigsten –, welche Maßnahmen ergriffen werden sollten. Mit Premium-Services auf vier Stufen stellen wir digitale Tools, verwaltete Dienste und eingebettetes Fachwissen bereit, die zu einer maßgeschneiderten Lösung kombiniert werden, die Ihre individuellen Anforderungen erfüllt. Darüber hinaus bieten wir fallbezogene Informationen und Beratungsleistungen für die konkreten Bedürfnisse unserer Kunden.

Bewusstseins-bildung

Regelmäßige geplante und fallbezogene Berichterstattung über die globale Sicherheits- und Bedrohungslage. Dies schließt Informationsberichte (INTREPs) und Lageberichte (SITREPs) ein.

- Tägliche globale Informationsberichte
- Wöchentliche globale Informationsausblicke
- Monatliche Bedrohungsprognosen
- Monatliche Informationszusammen-fassungen (INTSUMs)
- Lageberichte (SITREPs) und Informationsberichte (INTREPs) zu wichtigen Entwicklungen

Warnmeldungen

Standortspezifische E-Mail-Warnungen zu Sicherheits- und Bedrohungsereignissen in der Nähe. Diese können auf Grundlage von Schweregrad, Nähe und Häufigkeit nach Vorfallsarten angepasst werden:

- Kriminalität
- Zivile Unruhen
- Terrorismus
- Wetterereignisse
- Reisen und Beförderung

Handlungs-empfehlungen

Eine **umfassende** Schutz-, Bedrohungs- und Risikoanalyse für Ihr Unternehmen, Ihr Geschäft und Ihre Marke. Dies umfasst:

- Überwachung für Ihre konkreten Anforderungen
- Zusammenfassungen der täglichen Überwachungs-berichte
- Unverzügliche Informationen zu Warnmeldungen
- Lösung für Bedrohungs-, Schutz- und Risikoinformationen
- Zugriff auf die fallbezogene Berichterstattung

Analyst

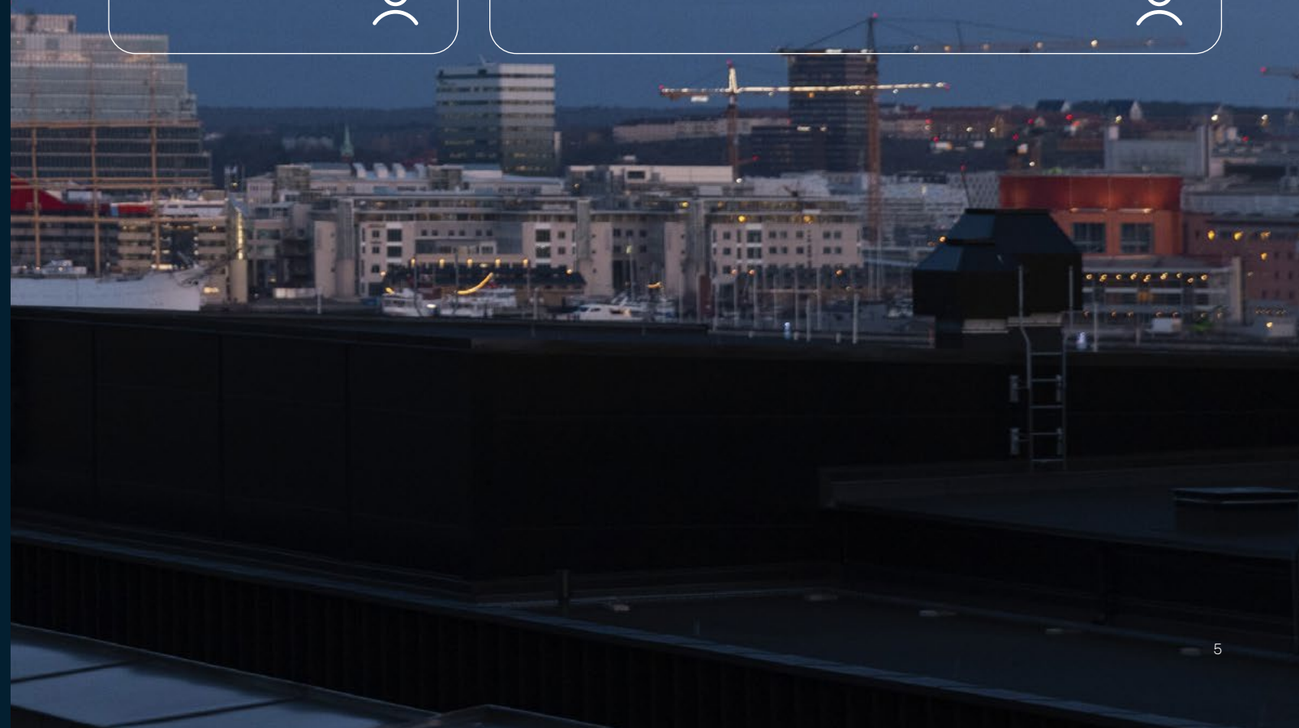
Eigens erstellte Informationsressourcen, die auf das Fachwissen der Global Intelligence Community von Securitas zurückgreifen.

Ausgestattet mit allen Tools und Schulungen zur Deckung Ihres Informationsbedarfs, um Ihr Unternehmen zu schützen.

Fallbezogene Informationen

Fachwissen und Beratung für alle dynamischen, konkreten Informationsanforderungen. Gängige Berichtstypen sind unter anderem:

- Reise- und Sicherheitsbericht für Reisende: Tiefgreifende Analyse von Gefahren für die Reisesicherheit.
- Personenschutz und Abwehrinformationen: Bewertung von Schwachstellen einer Zielperson anhand von Informationen (z. B. Führungskraft).
- Sicherheitsprüfung und -überwachung von Veranstaltungen: Sorgfältige Prüfung und Live-Überwachung.



Dieser Bericht wurde vom Securitas Risk Intelligence Center (RIC) erstellt, unserer Spezialabteilung für globale Risikoanalysen und strategische Erkenntnisse. Das RIC überwacht ständig geopolitische Entwicklungen, aufkommende Bedrohungen und branchenspezifische Risikomuster und verwandelt komplexe Informationen in eindeutige, evidenzbasierte Informationen. Diese Arbeit bildet die analytische Grundlage für die Bewertungen und Services von Securitas Intelligence.

Methodik

Ansatz

RIC nutzt Informationen aus allen Quellen und kombiniert Open-Source-Intelligence (OSINT) mit geschlossenen Quellen wie Human-Intelligence (HUMINT), um aufbereitete Informationen bereitstellen zu können. Informationen aus allen Quellen nutzen alle verfügbaren und geeigneten Informationsquellen auf Grundlage der kundenkritischen Informationsanforderungen.

Bedrohungen

Die potenziellen Bedrohungen, die im Rahmen dieses Intelligence-Berichts berücksichtigt werden, umfassen Bedrohungen, die auf Grundlage vorhandener Erkenntnisse vernünftigerweise erwartet werden können, darunter z. B.:

- Bagatell- und Gelegenheitsdelikte sowie organisierte Kriminalität.
- Gezielte und wahllose gewalttätige Angriffe, sowohl krimineller als auch terroristischer Natur.
- Gezielte und wahllose Protestaktionen.
- Unternehmenssicherheit, einschließlich Insider-Bedrohungen, Unternehmensspionage und sensible Geschäftstätigkeiten.

Die Aufnahme in diesen Bericht bedeutet nicht, dass eine dieser Bedrohungen eintreten wird. Es besteht jedoch die Möglichkeit, dass die Bedrohung auftreten kann, sodass sie bei der Durchführung von Sicherheitsüberprüfungen und Risikobewertungen berücksichtigt werden sollte.

Auch wenn alle angemessenen Anstrengungen unternommen werden, um alle möglichen Bedrohungsfaktoren für Unternehmen zu bewerten, ist die Sicherheits- und Bedrohungslage dynamisch und ständigen Veränderungen unterworfen. Zusätzlich tauchen auch immer neue Bedrohungen auf. Daher ist es wichtig, dass dieser Bericht als ergänzendes Instrument im Rahmen einer umfassenderen Sicherheitsstrategie verwendet wird. Er sollte nicht als alleiniges Dokument gelesen werden, das alle potenziellen Bedrohungen für die Branche erfasst und umreißt.

Terminologie der Eintrittswahrscheinlichkeit

Dieser Bericht stützt sich auf die Terminologie der Eintrittswahrscheinlichkeit des RIC, um die Eintrittswahrscheinlichkeit einer Bedrohung auf Grundlage der Wahrscheinlichkeit unter Verwendung von Prozentsätzen, Anteilen oder Verhältnissen als Ausgangswert einzuschätzen. Dies schafft Kontext und Klarheit und ein einheitliches Verständnis der Bewertung und der verwendeten Terminologie.

Begriff	Wahrscheinlichkeit
Fernliegend	0–5 %
Sehr unwahrscheinlich	10–20 %
Unwahrscheinlich	25–35 %
Realistische Möglichkeit	40–50 %
Wahrscheinlich	55–75 %
Sehr wahrscheinlich	80–90 %
Nahezu sicher	95–99 %

Bedrohungsstufen

In diesem Bericht werden die Bedrohungsstufen des RIC verwendet, um Bedrohungen auf einer Skala von 1 bis 5 zu bewerten. Diese Bewertung beruht auf der Einschätzung der Eintrittswahrscheinlichkeit und des Schweregrads bzw. der Absicht und Möglichkeit.

5 – EXTREM — *Sehr hohe/extreme Bedrohung.* Prüfen und wenn nötig reagieren.

4 – HOCH — *Hohe/große Bedrohung.* Geeignete Maßnahmen in Erwägung ziehen.

3 – MODERAT — *Moderate Bedrohung.* Achtsam bleiben, Vorsichtsmaßnahmen in Betracht ziehen.

2 – GERING — *Geringe/eingeschränkte Bedrohung.* Beratung in Anspruch nehmen.

1 – SEHR GERING — *Sehr geringe/vernachlässigbare Bedrohung.* Zur Bewusstseinsbildung.

Stichtag für Informationseingang

17:00 UTC, 5. Dezember 2025

Aerospace & Defence –
Top-Bedrohungen 2026

Zusammen-fassung

Die allgemeinen Bedrohungsaussichten für die LRV-Branche 2026 sind moderat. Dies ist auf eine Kombination aus hohen Risiken von Protesten und Unruhen sowie erhöhten Bedrohungen der Unternehmenssicherheit zurückzuführen. Die Gefährdung durch Kriminalität und Terrorismus bleibt moderat, aber anhaltend. Bedrohungsakteure und globale Sicherheitsvorfälle werden wahrscheinlich den Betrieb, die Sicherheit des Personals und den Ruf der Marke beeinträchtigen, wobei die Auswirkungen je nach geografischer Lage und Branche variieren. Mit Blick auf die Zukunft wird die nächste Krise in der LRV-Branche höchstwahrscheinlich von geopolitischen Krisenherden oder erneuten Konflikten ausgehen, während der Druck durch Klimawandel und politische Polarisierung steigt und zu zusätzlichen Schwachstellen führt. Unternehmen, die in Frühwarnsysteme, Widerstandsfähigkeit und integrierte bereichsübergreifende Sicherheit investieren, werden besser in der Lage sein, in diesem zunehmend umkämpften Umfeld einen Entscheidungsvorteil aufrechtzuerhalten.

Eskalierende Antikriegsbewegungen und Angriffe auf LRV-Unternehmen

Für die LRV-Branche werden Antikriegsbewegungen auch weiterhin ein wachsendes Problem sein, insbesondere da der Konflikt zwischen Gaza und Israel anhält und sich überschneidende Motivationen unter Aktivistengruppen zu härteren und manchmal gewalttätigen direkten Aktionen führen. Unternehmen mit erkennbaren oder vermeintlichen Verbindungen zu Israel und israelischen Rüstungsunternehmen bleiben wichtige Ziele. Es wird erwartet, dass diese Gruppen ihre koordinierten Kampagnen ausweiten werden, die physische Störungen, digitale Belästigung und gezielte Aktionen gegen leitende Angestellte und wichtige Einrichtungen umfassen.

Geopolitische Katalysatoren für Proteste, Unruhen und kriminelle Aktivitäten

Geopolitische Spannungen werden weiterhin zu Protesten, Unruhen und Aktivismus gegen LRV-Unternehmen führen, angeheizt durch anhaltende Konflikte, Umweltprobleme und wirtschaftlichen Wettbewerb. Es wird prognostiziert, dass kriminelle Bedrohungen zunehmen werden, insbesondere durch staatlich unterstützte oder geduldete Gruppen des organisierten Verbrechens, die versuchen, geistiges Eigentum, Material und Komponenten zu stehlen und Sabotageakte zu begehen. Gleichzeitig wird erwartet, dass die Bedrohungen für die Unternehmenssicherheit, einschließlich Spionage und Sabotage, zunehmen werden, was eine erhöhte Wachsamkeit in der gesamten Branche erfordert.

Verstärkte Kriegsführung in der Grauzone und Sabotagerisiken

Die Kriegsführung in der Grauzone und Sabotage werden 2026 sehr wahrscheinlich zu erheblichen Störungen führen, darunter potentielle Vorfälle mit vielen Opfern, Unterbrechungen der Versorgungskette und IT- oder Kommunikationsausfälle, die kritische nationale Infrastrukturen und private Luft- und Raumfahrtanlagen beeinträchtigen. Staatliche und nichtstaatliche Akteure werden diese Taktiken wahrscheinlich weiterhin anwenden, um die Interessen westlicher LRV-Unternehmen zu untergraben, zu beeinflussen und zu stören. Dies macht robuste Maßnahmen hinsichtlich der Widerstandsfähigkeit und des Krisenmanagements erforderlich.

Führungskräfte und Prominente verstärkt im Visier

Führungskräfte und prominente Persönlichkeiten der LRV-Branche sind nach wie vor ein beliebtes Ziel für Kriminelle und Aktivisten, die durch ideologischen Extremismus, kriminellen Opportunismus und geopolitische Spannungen motiviert werden. Der verstärkte Einsatz von Doxxing, künstlichen Medien und koordinierten Belästigungskampagnen hat die Hürden für persönliche Angriffe gesenkt. Unternehmen sollten verstärkt Maßnahmen zum Schutz der persönlichen Daten von Führungskräften, zur Überwachung von Identitätsmissbrauch und zur Integration von physischen und elektronischen Schutzmaßnahmen umsetzen.

Anhaltende und sich weiterentwickelnde Risiken durch Insider-Bedrohungen

Insider-Bedrohungen stellen nach wie vor ein erhebliches Risiko dar, da Personen mit den unterschiedlichsten Motiven Schwachstellen ausnutzen, um Störungen, Datenverluste und Rufschädigungen zu verursachen. Zu den Bedrohungsakteuren können Angestellte, Auftragnehmer, Aktivisten, Kriminelle und feindliche Staaten gehören, die entweder böswillig oder fahrlässig handeln. Dies unterstreicht, wie wichtig wirksame Maßnahmen gegen Insider-Bedrohungen, Zugangskontrollen und eine kontinuierliche Sicherheitsüberwachung auch 2026 sind.

Wichtige Bedrohungsbereiche

Proteste und Unruhen
Mögliche Bedrohungsstufe: 4

Kriminalität und Sicherheit
Mögliche Bedrohungsstufe: 3

Unternehmenssicherheit
Mögliche Bedrohungsstufe: 4

Terrorismus und Extremismus
Mögliche Bedrohungsstufe: 3

Die folgenden Zusammenfassungen geben einen kurzgefassten Überblick über die vier wichtigsten Bedrohungsbereiche, die die die Branche Aerospace & Defence 2026 beeinflussen werden. Diese Zusammenfassungen spiegeln Erkenntnisse aus dem umfassenden Bericht zu Aerospace & Defence – Top-Bedrohungen 2026 des Securitas Risk Intelligence Center wider, der eine umfassende Analyse sowie branchenspezifische Bewertungen enthält.

Ausgangslage

Proteste und Unruhen werden auch 2026 sehr aktiv, vielfältig und zunehmend koordiniert durchgeführt werden. Propalästinensische und Antikriegsnetzwerke, Klimagruppen und sogar Verschwörungstheoretiker mit einem entsprechenden Interesse werden LRV-Unternehmen weiterhin als symbolische und operative Ziele sehen. Aktivisten wenden dabei immer ausgeklügeltere digitale und persönliche Taktiken an und weiten ihre Kampagnen von Anlagen und Lieferketten auf gezielten Druck auf Führungskräfte, Prominente und Mitarbeiter aus. Dadurch entsteht ein unvorhersehbareres und individuelleres Bedrohungsumfeld für den Sektor.

Proteste und Unruhen – Zusammenfassung

Proteste und Unruhen – Zusammenfassung

Einstufung der Bedrohung

Wahrscheinlichste (MLCOA) und gefährlichste Vorgehensweise (MDCOA)

MLCOA: Aktivisten setzen häufige Proteste, Online-Mobilisierungen und gezielte Störungen gegen LRV-Unternehmen fort und weiten den Druck auch auf Führungskräfte, Vorstandsmitglieder und Mitarbeiter aus. Die Sichtbarkeit nahe Privathäusern, Veranstaltungen und Hochschulgeländen nimmt zu, wobei die meisten Aktionen gewaltfrei bleiben, aber dennoch für Störungen sorgen.

MDCOA: Koordinierte direkte Aktionen an mehreren Standorten führen zu erheblichen Betriebsstörungen, wobei gezielte Belästigungen bis hin zu aggressiven Konfrontationen vor Privathäusern oder am Arbeitsplatz eskalieren. Vereinzelte Risiken von Gewalt, Nötigung oder Sabotage mit weitgehenden Auswirkungen können dabei nicht ausgeschlossen werden.

Mögliche Bedrohungsstufe 4

Wichtige Dynamiken

1 Antikriegs-/propalästinensische Mobilisierung

- Der Gaza-Israel-Konflikt ist nach wie vor der wichtigste Faktor für Störmaßnahmen gegen LRV-Unternehmen.
- Netzwerke von Aktivisten zielen auf Firmen und Zulieferer ab, von denen angenommen wird, dass sie mit Verteidigungsprogrammen in Verbindung stehen. Dabei werden häufig auch grenzüberschreitende Aktionen koordiniert.
- Zu den Taktiken gehören Standortblockaden, Unterbrechungen der Lieferkette, Störungen von Großveranstaltungen und koordinierte digitale Kampagnen, die Druck ausüben.
- Neue Aktivistengruppen wenden zunehmend störende Taktiken, Techniken und Verfahren an, obwohl die Behörden diesen Gruppen Beschränkungen auferlegen.

2 Führungskräfte, Prominente und Mitarbeiter im Visier

- Führungskräfte und leitende Angestellte werden zunehmend durch Doxxing, feindliche Mitteilungen, künstliche Medien, offene Briefe und Kampagnen in den sozialen Medien ins Visier genommen.
- Auch Privatadressen werden zum Ziel, da Aktivisten öffentlich verfügbare Informationen nutzen, um Wohnadressen und persönliche Gewohnheiten zu ermitteln.
- Mitarbeiter an Standortzugängen werden gefilmt, namentlich genannt und im Internet beschimpft. Dadurch entstehen Rufschädigung und Probleme bezüglich der persönlichen Sicherheit.
- Aktivisten zielen auch auf **persönliche Verbindungen** ab und nutzen die Funktion von Führungskräften in Aufsichtsräten, die Zugehörigkeit zu einer Universität oder Partnerschaften, um Druck auszuüben.

3 Studentischer Aktivismus und Druck auf Universitäten

- Studentengruppen setzen ihre Proteste fort, die sich gegen Beziehungen von Universitäten zu LRV-Unternehmen richten, und stören Rekrutierungsveranstaltungen und Forschungspartnerschaften.
- Es kommt immer wieder zu Belagerungen, Bannern und koordinierten Aktionen auf den Geländen, um Universitäten unter Druck zu setzen, die Zusammenarbeit mit Verteidigungsunternehmen zu überdenken.

4 Umweltaktivismus verschmilzt mit Antikriegsnarrativen

- Unternehmen der Luft- und Raumfahrt sowie der Verteidigung sind nach wie vor wichtige Zielscheiben für Klimaaktivisten.
- Gruppen wie Extinction Rebellion (XR) und Mitglieder des A22-Netzwerks konzentrieren sich auf Flugshows, Veranstaltungen mit großer Öffentlichkeitswirkung und Anlagen, die mit Emissionen oder Umweltauswirkungen verbunden sind.
- Die zunehmende Verschmelzung von Klimaaktivismus, Antikriegs- und Antiwirtschaftsnarrativen verstärkt die Bedrohungslage und erweitert die potenziellen Ziele.

Vorrangige Maßnahmen

- **Verringern Sie die Auffindbarkeit von Informationen über Führungskräfte und Mitarbeiter** über offene Quellen und sorgen Sie für eine proaktive Überwachung mit Schwerpunkt auf Doxxing, Identitätsmissbrauch und feindlicher Spionage.
- **Bereiten Sie sich auf eine bewegungsübergreifende Mobilisierung** im Zusammenhang mit wichtigen Branchenveranstaltungen, geopolitischen Krisenherden und Beschaffungszyklen vor, die als Katalysator für Proteste oder gezielte Kampagnen dienen können.
- **Stärken Sie szenariobasierte Notfallpläne** für friedliche Proteste, gezielte Belästigungen, Unterbrechungen der Lieferkette und koordinierte Aktionen an mehreren Standorten unter Einbeziehung von Teams für physische Sicherheit, Personalwesen, Kommunikation und Recht.

Kriminalität wird auch 2026 eine ständige Bedrohung für LRV-Unternehmen bleiben, bedingt durch geopolitische Spannungen, wirtschaftlichen Druck und die anhaltende Belastung der globalen Lieferketten. Der hohe Wert der Branchenprodukte, sensibler Materialien und vertraulicher Informationen erhöht das Risiko von Diebstahl, Sabotage, illegaler Beschaffung und krimineller Beihilfe. Die organisierte Kriminalität und staatlich organisierte Akteure werden weiterhin Lücken in der Lieferantenüberprüfung und den Logistiknetzwerken ausnutzen, um wichtige Komponenten über den Grau- und Schwarzmarkt zu handeln. Mit dem zunehmenden Produktionsdruck steigt auch das Risiko, dass gefälschte oder gestohlene Komponenten in die legitimen Lieferketten gelangen.

Auch Cyberbedrohungen werden eskalieren, da staatlich unterstützte und finanziell motivierte Akteure Spionage, Datenexfiltration und KI-gestützte Operationen zum Identitätsmissbrauch verfeinern. Die Bloßstellung von Führungskräften, die Manipulation durch künstliche Medien und hybride digitale/physische Ziele werden die Angriffsfläche weiter vergrößern, was den Bedarf an integrierter Cyber- und physischer Sicherheit unterstreicht.

Kriminalität und Sicherheit – Zusammenfassung

Einstufung der Bedrohung

Wahrscheinlichste (MLCOA) und gefährlichste Vorgehensweise (MDCOA)

MLCOA: Kriminelle Akteure zielen weiterhin auf die LRV-Lieferketten ab und stehlen immer wieder kleineres Material, Teile und Komponenten. Gestohlene oder umfunktionierte Gegenstände tauchen auf illegalen Märkten auf, was das Risiko einer kontaminierten Lieferkette erhöht. Cyberkriminelle üben ständig Druck aus, um finanzielle Gewinne zu erzielen und Daten zu stehlen.

Mögliche Bedrohungsstufe 3

MDCOA: Groß angelegte kriminelle Kampagnen – möglicherweise unterstützt von gegnerischen Staaten – zielen durch Diebstahl, Sabotage und illegale Beschaffung auf LRV-Lieferketten ab. Störungen zwingen dazu, auf nicht zugelassene Zulieferer zurückzugreifen, wodurch gefährliche Komponenten in die Produktionsprozesse gelangen und die Sicherheit und Produktion beeinträchtigt werden.

Wichtige Dynamiken

1 Illegale Beschaffung und Schwachstellen in der Lieferkette

- Kriminelle Gruppen sind nach wie vor die wichtigsten Akteure beim Diebstahl von Komponenten, der Abzweigung und geheimen Beschaffung für Sanktionen unterliegenden Staaten wie Russland, Iran und China.
- Gestohlene Luftfahrtelektronik, Sensoren, Platinen und Präzisionskomponenten werden zu überhöhten Preisen auf dem Grau- und Schwarzmarkt gehandelt.
- Liefer- und Produktionsengpässe erhöhen den Anreiz, ungeprüfte Komponenten zu beziehen, was das Kontaminationsrisiko erhöht.
- Schwachstellen im Frachtverkehr, bei der Überprüfung von Lieferanten und der Einhaltung grenzüberschreitender Vorschriften werden weiterhin ausgenutzt.

2 Verstärkte Zusammenarbeit zwischen organisierter Kriminalität und Staat

- Sanktionen und Ausfuhrkontrollen fördern die Zusammenarbeit zwischen gegnerischen Staaten und der organisierten Kriminalität, die sanktionierte Komponenten erwerben will.
- Kriminelle Gruppen nutzen Methoden wie etablierte Schmuggelrouten, Briefkastenfirmen und Logistikvermittler, die während der jüngsten geopolitischen Zerrüttungen ausgefeilt wurden.
- Da große Baugruppen schwer zu stehlen sind, konzentriert man sich zunehmend auf kleinere, hochwertige Komponenten und andere ukrativere und leichter zugängliche Ziele.

3 Verstärkte Cyberspionage und KI-gestützte Eingriffe

- Staatlich unterstützte und kriminelle Cyberakteure entwickeln die Spionage, den Diebstahl von Zugangsdaten und die Datenexfiltration gegen LRV-Netzwerke immer weiter.
- KI-gestützter Identitätsmissbrauch, künstliche Audio-/Videodateien und Deepfake-Dokumente erhöhen die Täuschung und verringern die Entdeckung.
- Vorfälle 2025 umfassten mehrere laufende Kampagnen, darunter Cyberangriffe auf große israelische LRV-Firmen und anhaltende Spionage durch von Russland unterstützte Akteure.
- Phishing und Umwege über kleinere Anbieter oder Dienstleister sind nach wie vor wichtige Methoden, um in hochwertige Programme einzudringen.

4 Zunehmende Angriffe auf Führungskräfte und als sensibel eingestufte Personen

- Die Veröffentlichung persönlicher Daten fördert Doxxing, Einschüchterung und hybriden digitalen/physischen Druck.
- Öffentliche Datenbanken und das Durchsickern von personenbezogenen Daten senken die Hürden für Angreifer, Führungskräfte zu identifizieren und zu verfolgen.
- 2025 kam es zu einer Eskalation der Schwere der gegen Führungskräfte gerichteten Aktionen. Diese reichten von Online-Bedrohungen bis hin zu versuchten Entführungen, Sabotageakten und staatlich gelenkten Attentatsplänen.
- Künstliche Medien, manipulierte Narrative und personalisierter Cyber-Identitätsmissbrauch verstärken die Reputations- und Sicherheitsrisiken.

Vorrangige Maßnahmen

- **Verstärken Sie die Lieferantenüberprüfung und -kontrolle** auf allen Ebenen und räumen Sie Kontrollen Vorrang ein, die verhindern, dass gefälschte, gestohlene oder illegale Komponenten in die Lieferkette gelangen.
- **Setzen Sie integrierte Cyber-/physische Sicherheitsstrategien** zur Bekämpfung von Spionage, Sabotage, künstlichem Identitätsmissbrauch, Bloßstellung von Führungskräften und hybriden Bedrohungswegen um.
- **Führen Sie gezielte Bewertungen möglicher Bedrohungsakteure** (organisierte Kriminalität, staatlich organisierte Netzwerke, verärgerte Insider) zur Ermittlung von Schwachstellen in Logistik, Personal und digitalen Systemen durch.
- **Entwickeln, testen und aktualisieren Sie Notfallpläne regelmäßig** – einschließlich der Pläne für Cyberangriffe, Kompromittierung der Lieferketten und gezielte Angriffe auf Führungskräfte –, unterstützt durch funktionsübergreifende Übungen.

Die Risiken für die Sicherheit von LRV-Unternehmen werden sich 2026 verschärfen, da Insiderbedrohungen, Unternehmensspionage, feindliche geheime Aktionen, Aufklärungsaktivitäten und die Weitergabe sensibler Vermögenswerte mit zunehmenden geopolitischen Spannungen und einem stark polarisierten gesellschaftspolitischen Umfeld zusammentreffen. Bedrohungsakteure, darunter Angestellte, Auftragnehmer, Aktivisten, Kriminelle, Wirtschaftsprüfer und staatlich organisierte Gruppen, nutzen weiterhin Schwachstellen in physischen, digitalen und menschlichen Bereichen aus, was die Erkennungs- und Reaktionsfähigkeit vor Herausforderungen stellt und das Risiko von Betriebs-, Reputations- und strategischen Störungen erhöht.

Unternehmenssicherheit – Zusammenfassung

Unternehmenssicherheit – Zusammenfassung

Einstufung der Bedrohung

Wahrscheinlichste (MLCOA) und gefährlichste Vorgehensweise (MDCOA)

MLCOA: Unternehmen sind ständig mit der versehentlichen oder böswilligen Offenlegung sensibler Informationen, dem Missbrauch durch Insider auf niedriger Ebene, opportunistischer Aufklärung und anhaltenden Spionageversuchen durch Social Engineering, Diebstahl von Zugangsdaten, Drohnenaktivitäten und persönlicher Infiltration konfrontiert. Die zunehmende ideologische Polarisierung trägt zu mehr Insider-Risiken bei, die auf Unzufriedenheit zurückzuführen sind, und routinemäßige feindselige Aktivitäten testen die Sicherheitslage in Unternehmenseinrichtungen und Lieferketten.

Mögliche Bedrohungsstufe 4

MDCOA: Staatlich geförderte und hybride Akteure weiten koordinierte Kampagnen, z. B. zur Rekrutierung von Insidern, Sabotage, komplexer Spionage, drohnengestützter Aufklärung und der Ausnutzung von Beziehungen zu Dritten, aus, um auf sensible Vermögenswerte zuzugreifen oder diese umzuleiten. Insider mit böswilligen Absichten schleusen wertvolle Daten aus oder ermöglichen Folgeangriffe, während Angreifer mit raffinierten Methoden Aufklärungsmaßnahmen und geheime Aktionen nutzen, um den Betrieb zu stören, die Lieferketten zu gefährden oder Ruf- oder rechtliche Schäden herbeizuführen.

Wichtige Dynamiken

1 Insider-Bedrohungen nehmen zu

- Insider-Bedrohungen betreffen Mitarbeiter, Auftragnehmer, Besucher und externe Partner, die in physischen und digitalen Umgebungen böswillig oder fahrlässig handeln.
- Zu den Motiven gehören finanzieller Druck, ideologische Unvereinbarkeiten, persönliche Umstände, Zwang, schlechter Ruf oder die Ausnutzung durch feindliche Akteure.
- Die Weitergabe sensibler Informationen – einschließlich interner Dokumente, E-Mails oder personenbezogener Daten – über KI-Tools oder soziale Medien führt zu betrieblichen, rechtlichen und rufschädigenden Risiken.
- Bemerkenswerte Fälle 2025 zeigen die staatlich unterstützte Anwerbung von Personen mit privilegiertem Zugang, einschließlich des Diebstahls von Geschäftsgeheimnissen und Exfiltration für ausländische Geheimdienste.
- Hinweise auf bösartige Aktivitäten können wiederholte Sicherheitsverletzungen, unerklärliche Zugriffsversuche, ungewöhnliche Arbeitszeiten, Dateiübertragungen auf persönliche Geräte und Mustern folgendes frühzeitiges Ausscheiden sein.

2 Ausweitung der Spionagetätigkeit von Unternehmen

- Der zunehmende geopolitische Wettbewerb verstärkt die Spionage, die sich gegen geschützte Muster, Forschungs- und Entwicklungsdaten, geistiges Eigentum und Technologien mit doppeltem Verwendungszweck richtet.
- Staatlich unterstützte Akteure nutzen Cyberangriffe, Social Engineering, Besuche ausländischer Würdenträger und den Zugang von Insidern, um an vertrauliche Informationen zu gelangen.
- Unternehmen, die an Beschaffungsprogrammen, sensibler Forschung oder Regierungsverträgen beteiligt sind, stehen verstärkt im Visier.
- Ereignisse 2025 – von Verhaftungen wegen Spionage in Lettland, der Türkei und der Ukraine bis hin zu durchgesickertem Filmmaterial von Flugzeugprototypen – unterstreichen die Bandbreite der gegnerischen Taktiken.
- Spionagekampagnen unterstützen Folgeoperationen wie die Manipulation von Informationen, Ransomware oder koordinierte Aktivitäten in der Grauzone.

3 Sabotage und geheime feindliche Aktionen immer häufiger

- Staatliche und nichtstaatliche Akteure führen geheime Aktivitäten unterhalb der Eskalationsschwellen durch und testen so die Aufdeckungs- und Reaktionsmöglichkeiten.
- Zu den Bedrohungen gehören Brandstiftung, Drohnenaufklärung, Paketbomben, Manipulation an Unterseekabeln, elektronische Kriegsführung und gefälschte Bombendrohungen.
- Hybride Taktiken zielen auf militärische Standorte, Verkehrsknotenpunkte, logistische Infrastrukturen, Produktionsstätten und Standorte mit doppeltem Verwendungszweck ab.
- Zahlreiche Vorfälle in Europa von 2024–2025 zeigen, dass Drohnen über Kernkraftanlagen, Munitionszügen, Marineeinrichtungen und Infrastrukturen mit doppeltem Verwendungszweck fliegen.
- Die Auslagerung geheimer Aktionen an kriminelle oder extremistische Erfüllungsgehilfen erhöht die glaubhafte Bestreitbarkeit, aber auch die Unvorhersehbarkeit und das Eskalationsrisiko.

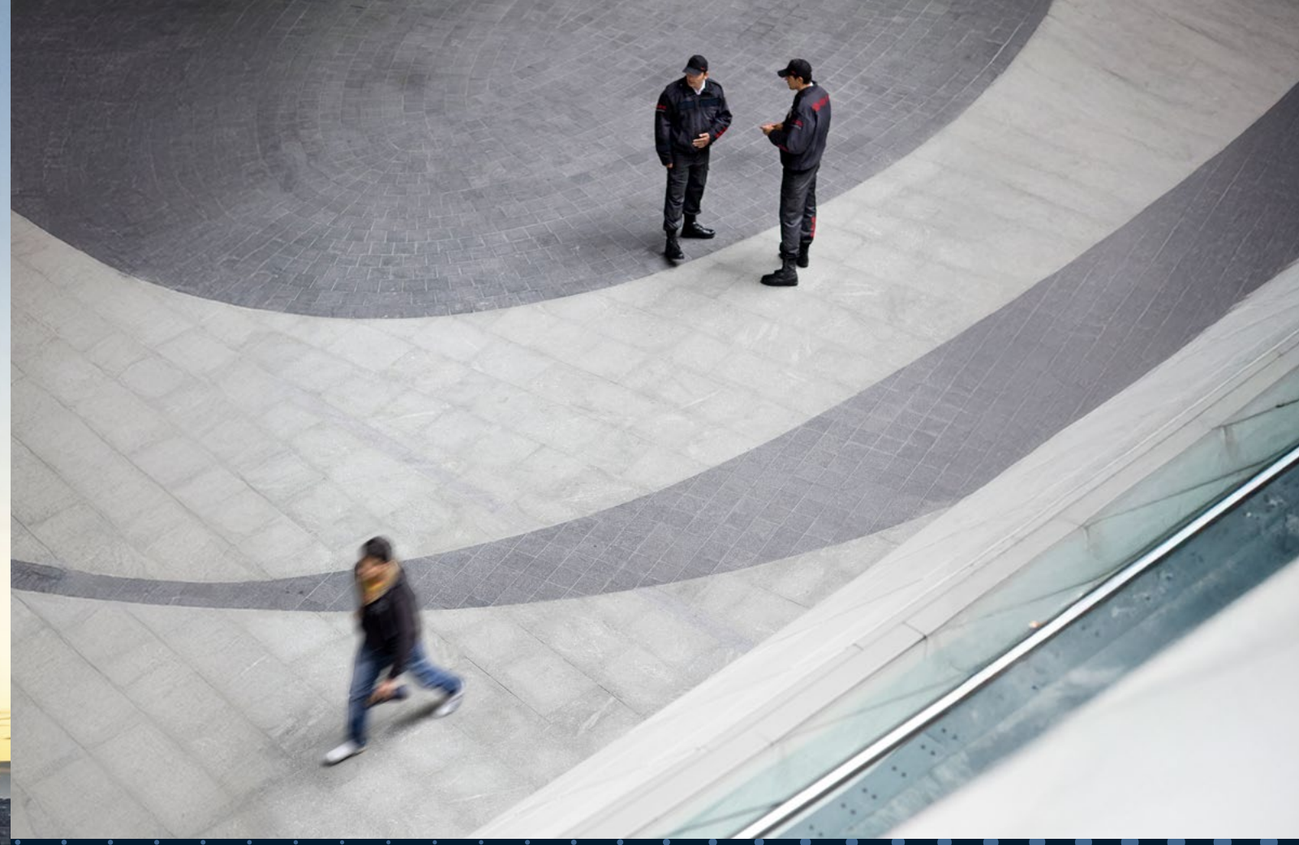
4 Feindliche Aufklärung und Herausforderungen bei der Sicherheitsüberprüfung

- Sicherheitsprüfer filmen auch weiterhin Einrichtungen zur Online-Interaktion und geben dabei wichtige Informationen und Hinweise preis (Zugangspunkte, Abdeckung von Überwachungskameras, Codes, Mitarbeiterdaten).
- Geheime Aufklärung durch Drohnen, getarnte Geräte oder wiederholte Ortsbesichtigungen liefern Aktivisten, Kriminellen und staatlich unterstützten Akteuren Informationen aus zweiter Hand.
- Prüfer werden weiterhin die Rechte an öffentlichem Grund und Boden ausnutzen und den Ruf der Zielunternehmen aufgrund des unsachgemäßen Umgangs mit Sicherheitspersonal schädigen.
- Die drohnengestützte Aufklärung an sensiblen Standorten – einschließlich Forschungszentren und Verteidigungseinrichtungen – nimmt weiter zu, häufig im Zusammenhang mit ausländischen Geheimdienstinteressen.

Vorrangige Maßnahmen

- Stärken Sie die Bekämpfung von Insider-Bedrohungen durch Verhaltenshinweise, Open-Source-Überwachung und Integration der Personal-, Cyber- und Sicherheitsabteilungen.
- Verbessern Sie die Kontrollen für den Umgang mit sensiblen Informationen, Offboarding-Prozesse und privilegierten Zugang für Mitarbeitende, Auftragnehmer und Partner.
- Weiten Sie Schulungen zur Spionageabwehr und operativen Sicherheit aus, insbesondere für Teams, die in den Bereichen Forschung und Entwicklung, Beschaffung, sensible Projekte und ausländische Delegationen tätig sind.
- Aktualisieren Sie die Krisen- und Notfallpläne, damit auch Sabotage, geheime Aktionen, Drohnenangriffe, durch Insider ermöglichte Einbrüche und Aufklärungsmaßnahmen erfasst werden.
- Verbessern Sie die Transparenz der Lieferkette, die Einhaltung von Sanktionen und die Überwachung von externen Partnern – einschließlich Due-Diligence-Prüfungen und Rückverfolgung von Vermögenswerten.
- Schulen Sie die Mitarbeitende an vorderster Front und Sicherheitsteams im angemessenen Umgang mit Prüfern und feindlicher Aufklärung, um eine Eskalation zu vermeiden und gleichzeitig sensible Informationen zu schützen.
- Fördern Sie die Bereitschaft zur Drohnenabwehr, Einbindung von Partnern aus dem öffentlichen Sektor und Erprobung von Notfallplänen im Rahmen von Tabletop- und behördenübergreifenden Übungen.

Terrorismus und Extremismus werden auch 2026 ein ständiges Thema für die Unternehmen von Aerospace & Defence sein, bedingt durch globale Konfliktherde, neue ideologische Reibungspunkte und eine anhaltende Radikalisierungsdynamik. Zwar gibt es derzeit keine Anzeichen dafür, dass der Sektor stärker ins Visier genommen wird, doch die indirekten Risiken, die sich aus regionaler Instabilität, Gefährdung der Lieferkette, gefälschten Drohungen und Störungen bei der Informationsversorgung ergeben, sind weiterhin erheblich. Gewaltbereite inländische Extremisten, Einzeltäter und international tätige Gruppen passen sich weiterhin an, wobei rechtliche Änderungen und Online-Narrative das Verhalten in verschiedenen Ländern beeinflussen.



Terrorismus und Extremismus – Zusammenfassung

Einstufung der Bedrohung

Wahrscheinlichste (MLCOA) und gefährlichste Vorgehensweise (MDCOA)

MLCOA: Es gibt keine eindeutigen Anzeichen für verstärkte direkte Angriffe auf LRV-Unternehmen. Terroranschläge auf Lieferketten, insbesondere in Hochrisikoregionen mit aktiven Konflikten oder geopolitischen Spannungen, bleiben jedoch eine realistische Möglichkeit.

MDCOA: Die Vermutung, dass LRV-Unternehmen in globale Konflikte verwickelt sind, führt zu gezielten Angriffen auf Unternehmen, Einrichtungen oder Lieferketten. Störungen bei der Informationsversorgung, Kritik an der Branche und geopolitische Krisenherde verschmelzen mit persönlicher Missgunst und fördern die Radikalisierung von gewaltbereiten inländischen Extremisten, Einzeltätern und etablierten terroristischen Gruppen.

Wichtige Dynamiken

1 **Entwicklung der Beweggründe von gewaltbereiten inländischen Extremisten und Einzeltätern**

- Zu den extremistischen Beweggründen gehören rechtsextreme, linksextreme, rassistische/ethnische, antiautoritäre und technikfeindliche Ideologien.
- Persönliche Missgunst überschneidet sich zunehmend mit geopolitischen Narrativen, die in den sozialen Medien verstärkt werden.
- Radikalisierungszyklen werden über Online-Plattformen trotz verschärfter Verbote extremistischer Netzwerke weiter beschleunigt.

2 **Rechtliche Bezeichnungen prägen extremistisches Verhalten**

- Neue Bezeichnungen für Gruppen, die zuvor als Aktivisten oder kriminelle Netze galten, verhindern einige Aktivitäten ab.
- Beschränkungen und gezielte Angriffe auf Gruppen werden dazu führen, dass engagiertere Aktivisten in den „Untergrund“ gehen, sodass die Anforderungen an die operative Sicherheit steigen bzw. Gruppen sich umbenennen oder umziehen, um einer gezielten Bekämpfung zu entgehen.
- Negative Reaktionen der Öffentlichkeit auf vermeintlich „harte“ Maßnahmen gegenüber Aktivistengruppen können zu einem unbeabsichtigten Anstieg der öffentlichen Unterstützung für die Gruppen und ihre Anliegen führen.

3 **Angriffe über Fälschungen und Störungen**

- LRV-Unternehmen sind nach wie vor anfällig für böswillige Kommunikation, gefälschte Bombendrohungen und störende Fehlalarme.
- Diese Aktionen dienen oft dazu, Reaktionen zu provozieren, die Sicherheit zu testen oder operative Erkenntnisse zu gewinnen.
- Gefälschte Aktivitäten werden zunehmend eingesetzt, um Reaktionen zu testen und die Aufklärung von Zielen zu ermöglichen.

4 **Indirekte Bedrohungen aus globalen Konfliktzonen**

- Terroristische Vorfälle in Regionen mit erhöhten geopolitischen Spannungen stellen indirekte Risiken für Lieferketten, Logistik und Personal dar.
- Westliche Regierungen warnen weiterhin davor, dass terroristische Anschläge in naher Zukunft wahrscheinlich sind, auch wenn sie sich nicht speziell gegen die LRV-Branche richten.

Vorrangige Maßnahmen

- Führen Sie standortspezifische Bewertungen der Bedrohungen, Schwachstellen und Risiken sowie räumliche Bedrohungsanalysen durch und konzentrieren Sie sich dabei auf Einrichtungen in der Nähe geopolitischer Brennpunkte oder wichtiger logistischer Knotenpunkte.
- Stärken Sie die Pläne zur Geschäftskontinuität und zum Krisenmanagement unter Berücksichtigung der nationalen Leitlinien zur Terrorismusbekämpfung und der Maßnahmen zur Sensibilisierung der Mitarbeitenden.

Kontakt

intelligence@securitas.com