Bundesministerium
Inneres

Bericht Cybersicherheit für das Jahr 2025

Bericht Cybersicherheit für das Jahr 2025

Wien, 2026

Bundeskanzleramt

Bundesministerium
Inneres

Bundesministerium
Landesverteidigung

Bundesministerium
Europäische und internationale
Angelegenheiten

Bundesministerium
Finanzen

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundesministerium für Inneres
Herrengasse 7, 1010 Wien

Grafische Gestaltung: Bundesministerium für Inneres
Druck: Digitalprintcenter des BMI

Wien, 2026

Der Bericht Cybersicherheit

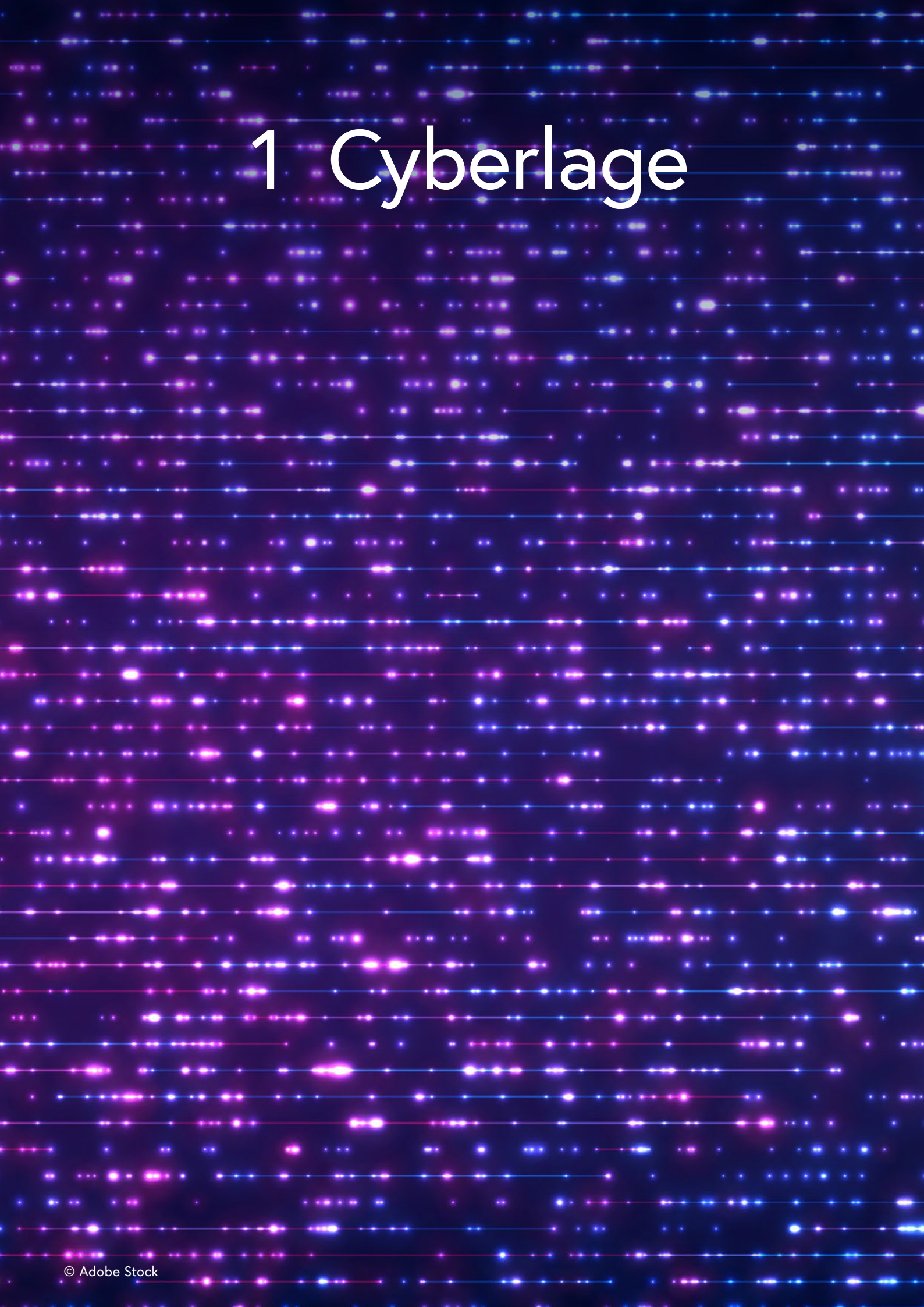
Die Österreichische Strategie für Cybersicherheit (ÖSCS) legt fest, dass durch die Cyber Sicherheit Steuerungsgruppe (CSS) ein jährlicher Bericht zur Cybersicherheit in Österreich erstellt wird. Der letzte Bericht wurde im Dezember 2025 vorgelegt.

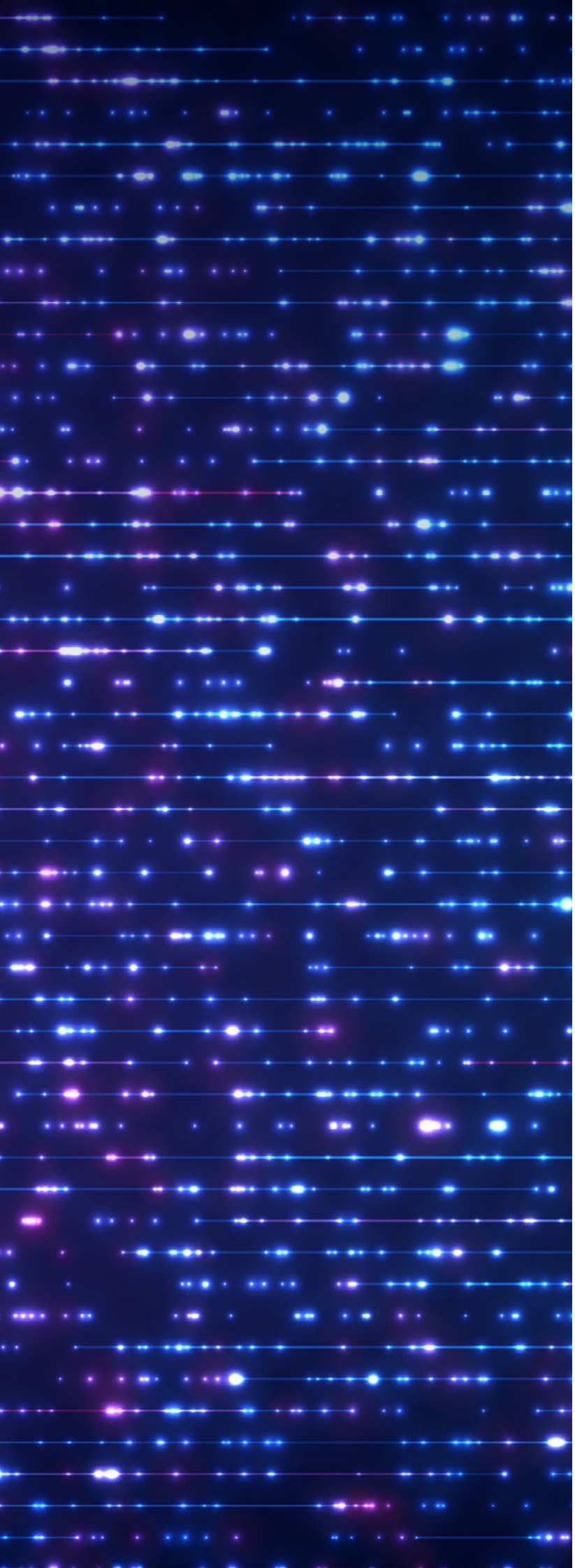
Der aktuelle Bericht Cybersicherheit für das Jahr 2025 (Beobachtungszeitraum 1. Jänner 2025 bis 31. Dezember 2025) baut auf den Inhalten des letztjährigen Berichts auf und ergänzt diesen um aktuelle Entwicklungen mit Schwerpunkten in den Bereichen internationale und operationelle Entwicklungen. Beobachtungszeitraum ist das Jahr 2025, einzelne aktuelle Entwicklungen im Jahr 2026 haben Eingang gefunden.

Zielsetzung des Berichtes ist eine zusammenfassende Darstellung der Cyberbedrohungen und wesentlicher nationaler und internationaler Entwicklungen. Grundlage dazu sind ressortspezifische Berichte zur Thematik.

Inhalt

1 Cyberlage





1.1 Lage Cybersicherheit – operative Ebene

1.1.1 Ransomware im Jahr 2025

Ransomware stellte auch im Jahr 2025 eine der zentralen Cyberbedrohungen weltweit dar, wobei insbesondere Unternehmen im Fokus standen. Ähnlich zum Vorjahr waren organisierte Gruppen, wie etwa LockBit, auch in Österreich weiter aktiv und zeigten ihre Resilienz mit neuen (Ransomware-)Kampagnen. Kennzeichnend sind vor allem die weiterentwickelten Angriffsmethoden; Cybergruppierungen arbeiten verstärkt mittels automatisierter Prozesse sowie Technologien wie künstlicher Intelligenz (KI), um Phishing-Kampagnen authentischer und wirksamer zu gestalten. Diese dienen oftmals als Einfallstor für Ransomware-Angriffe. Mit dem Einsatz unauffälliger Tools (z. B. Cloud-Dienste) kann in das jeweilige System eingedrungen, Schadsoftware platziert und (sensible) Daten exfiltriert werden. Die gestohlenen Daten dienen besonders dazu, den Druck zu erhöhen und folglich Lösegeldforderungen verlangen zu können. Diese sogenannte „Double Extortion"-Strategie hat sich mittlerweile als Standard etabliert.

Einen weiteren Trend bildet „Ransomware-as-a-service" (RaaS), ein Geschäftsmodell, bei dem spezialisierte Gruppen anderen Kriminellen, die keine Kenntnisse besitzen, ihre Schadsoftware zur Verfügung stellen. Dadurch sinkt die Einstiegshürde erheblich, während die Qualität der Angriffe steigt. Besonders die Gruppe „LockBit" dominiert weiterhin diese Szene und ist mittlerweile auch in Österreich stark relevant.

Datendiebstahl bei Software-Anbieter Infoniqa

Ein bedeutender Vorfall in Österreich im August 2025 betraf den externen Gehaltsdienstleister Infoniqa. Das Unternehmen bestätigte einen gezielten Cyberangriff, bei dem IT-Systeme vorübergehend offline genommen wurden. Die russische Ransomware-Gruppe „Warlock" reklamierte den Angriff für sich und gab an, sie habe eine Schwachstelle von Microsoft Sharepoint ausgenutzt, um in das Infoniqa-System einzudringen und rund 165 Gigabyte sensibler Daten, darunter Finanzdaten, zu entwenden. Es sollen ungefähr 300 Unternehmen betroffen gewesen sein. Die spätere Veröffentlichung der Daten bestätigt den erpresserischen Charakter des Angriffs und entspricht dem typischen Muster der „Double Extorsion".

1.1.2 Ransomwareangriffe durch „Scattered Lapsus$ Hunters"

Autobauer Jaguar Land Rover

Jaguar Land Rover (JLR) war am 31. August 2025 Ziel einer Cyberattacke geworden, der die Produktion in mehreren Ländern für fast sechs Wochen lahmgelegt hatte und sich durch sehr hohe wirtschaftliche Schäden, eine massive Produktions- und Lieferketten-unterbrechung und breite Betroffenheit auszeichnete.

Die Werke in Großbritannien, China, Indien und der Slowakei waren betroffen, was zu erheblichen Verzögerungen in der Fahrzeugproduktion führte. Der Produktionsstopp des Konzerns in großen britischen Fabriken wirkte sich sofort auf Zulieferer weltweit aus, von denen viele ihren Betrieb einschränken oder pausieren mussten, weil sie keinen Zugang zu wichtigen Bestell-, Bestands- und Logistiksystemen hatten. Berichten zufolge wurden aufgrund des Shutdowns auch Tausende von zusätzlichen Mitarbeiterinnen und Mitarbeitern in Supply-Chain-Unternehmen vorübergehend entlassen. Unter normalen Umständen produziert das Unternehmen etwa 1.000 Fahrzeuge pro Tag; Analystinnen und Analysten schätzten den wöchentlichen Verlust auf rund 50 Millionen Pfund. JLR ist einer der bedeutendsten Hersteller der britischen Wirtschaft und machte im Jahr 2024 rund vier Prozent aller Warenexporte aus. Expertinnen und Experten bewerten den Cyberangriff auf Jaguar Land Rover mit geschätzten Einbußen von 1,9 Milliarden Pfund als den wirtschaftlich folgenschwersten in der britischen Geschichte. Damit gilt er als bislang teuerster Cybervorfall im Vereinigten Königreich.

Anfang September 2025 übernahm eine Gruppe englischsprachiger Hackerinnen und Hacker über eine Telegram-Plattform namens „Scattered Lapsus$ Hunters“, einem Zusammenschluss der Namen der Hackergruppen „Scattered Spider“, „Lapsus$“ und „ShinyHunters“, die Verantwortung für den Cyberangriff. „Scattered Spider“, eine lose Gruppe junger Hackerinnen und Hacker, steckte auch hinter den Angriffen von Co-Op, Harrods und Marks & Spencer (M&S).

Angriffe auf die größten Einzelhändler Großbritanniens

2025 wurden die größten Einzelhändler Großbritanniens Opfer von koordinierten Cyberangriffen, davon waren jene gegen die Kaufhausketten Marks & Spencer und Harrods am gravierendsten.

Der britische multinationale Einzelhändler **Marks & Spencer (M&S)** bestätigte im April 2025 einen Ransomware-Vorfall, der die Computersysteme traf und erhebliche Störungen im gesamten Unternehmen verursachte. M&S pausierte alle Online-Bestellungen auf seiner Webseite und mobilen App für etwa sechs Wochen, um den Datenverlust einzudämmen, wodurch Kundinnen und Kunden nicht mehr einkaufen konnte – was einen erheblichen finanziellen Rückschlag mit sich brachte, da etwa ein Drittel der britischen Bekleidungs- und Wohnverkäufe des Händlers normalerweise online erfolgen. Der Vorfall hatte hohe geschäftliche Auswirkungen mit einem finanziellen Verlust von etwa 300 Millionen Pfund.

Das Londoner Kaufhaus **Harrods** bestätigte Anfang Mai 2025 ebenfalls, Ziel eines Cyberangriffs gewesen zu sein. Das Unternehmen gab an, dass es unbefugte Zugriffsversuche auf seine IT-Systeme gab. Der Angriff war Teil einer größeren Welle von Cyberattacken auf britische Einzelhändler. Der Geschäftsbetrieb konnte zwar aufrechterhalten werden,

der Internetzugang wurde eingeschränkt. Ende September 2025 folgte die Bekanntgabe eines weiteren – nicht mit jenem im Mai 2025 zusammenhängenden – Cybersicherheitsvorfall, nachdem Hackerinnen und Hacker einen Drittanbieter kompromittiert und 430.000 Datensätze mit sensiblen E-Commerce-Kundeninformationen gestohlen haben. Harrods teilte mit, dass es „betroffene E-Commerce-Kunden am Freitag proaktiv informiert" habe, dass ihre Namen und Kontaktdaten nach einem Verstoß bei einem Drittanbieter kompromittiert wurden. Das Unternehmen gab den Namen des kompromittierten Unternehmens nicht bekannt.

Expertinnen und Experten sehen im späteren Vorfall von Harrods ein weiteres Beispiel für die anhaltende Anfälligkeit externer IT-Dienstleister. Diese gelten als die „größte Schwachstelle" im Sicherheitsgefüge vieler Handelsunternehmen.

1.1.3 Geopolitische Konflikte, nachrichtendienstliche und hacktivistische Aktionen

Der Israel-Palästina-Konflikt hat ein weiteres Konfliktfeld im Cyberbereich geöffnet, in dem staatliche Akteure, hacktivistische Tätergruppierungen und cyberkriminelle Netzwerke agieren. Besonders im Jahr 2025 kam es zu einem erhöhten Aufkommen von Denial-of-Service-Angriffen und Hack-and-Leak-Aktivitäten. Bei letzterem handelt es sich um die Erbeutung nicht-öffentlicher Daten oder Dokumente, die anschließend – teils in verfälschter Form – veröffentlicht werden. Diese Datenlecks zielen insbesondere auf Regierungsstellen oder andere öffentliche Institutionen ab und haben bereits zur Offenlegung personenbezogener Daten öffentlicher Amtsträger oder anderen Regierungsangestellten geführt. Parallel dazu kam es zu deutlich komplexeren Operationen, die staatsnahen Akteuren zugeschrieben werden:

Angriff auf Irans Bank Sepah: Besonders hervorzuheben ist eine Kampagne der proisraelischen Gruppierung „Predatory Sparrow", die behauptet, hinter mehreren Angriffen gegen die iranische Infrastruktur zu stehen, darunter Irans Bank Sepah. Der Cyberangriff auf die Staatsbank hatte zur Folge, dass Zugriffe auf Konten sowie Zahlungsabwicklungen nicht mehr möglich waren. Zuvor hatte die Gruppierung behauptet, Angriffe auf Stahlwerke, das Eisenbahnnetz und Tankstellenzahlungssysteme im Iran angegriffen zu haben.

Cyberattacke auf Nobitex: Einen Tag nach dem Angriff auf die Bank Sepah wurde die größte iranische Kryptobörse Nobitex Ziel eines weitreichenden Hackerangriffs, bei dem fast 90 Millionen US-Dollar in Kryptowährungen gestohlen wurde, darunter unter anderem Bitcoin, Ethereum und Dogecoin. Auch zu diesem Angriff bekannte sich die Hackergruppe „Predatory Sparrow".

Mehrschichtiger DDoS-Angriff auf Plattform X: Der Angriff der pro-palästinensischen Gruppierung „DarkStorm Team“ verursachte einen weltweiten Ausfall für mehrere Stunden, bei dem mehr als 40.000 Nutzende betroffen waren. „DarkStorm Team“ gilt als eine der disruptivsten aktiven Hackergruppen. Das hacktivistische Kollektiv konzentriert sich überwiegend auf DDoS-Angriffe; ihre Strategie zielt eher auf Störung als auf destruktive Kompromittierung ab.

Cyberangriff auf die israelische Polizei: Die pro-palästinensische Hackergruppe „Handala“ behauptete in einem Telegram-Update, in die Datensysteme der israelischen Polizei eingedrungen zu sein und 2,1 Terabyte sensibler Information gestohlen zu haben, darunter 350.000 Dokumente mit persönlichen Akten.

Bedrohungsakteurinnen und -akteure neigen dazu, sich schnell zu Cyberangriffen zu bekennen oder im Hinblick auf den Auswirkungsgrad zu übertreiben; dies mit der strategischen Absicht, die Glaubwürdigkeit und das Ansehen des mutmaßlichen Ziels zu delegitimieren. Aufgrund der schwer fassbaren Kommunikationsmethoden von Cyberbedrohungsakteurinnen und -akteuren sind diese Behauptungen für Strafverfolgungsbehörden, Sicherheitsforscherinnen und -forscher oder andere Bedrohungsakteurinnen und -akteure oft schwer zu überprüfen.

1.2 Lage Cybersicherheit – Unternehmen und Sicherheitsdienstleister

Für den Bericht Cybersicherheit wurden auch 2025 wieder Unternehmen der kritischen Infrastruktur und verfassungsmäßige Einrichtungen sowie führende private Unternehmen der Cybersicherheitsbranche eingeladen, Informationen zum Berichtsjahr zu sammeln und auf Basis eines Fragebogens zu teilen. Mithilfe ihrer Expertise soll die Cybersicherheitslage Österreichs vollständig aufgezeigt werden. Der Fokus liegt nicht auf einzelnen Vorfällen, sondern auf Trends und Entwicklungen im Sinne einer Überblicksdarstellung.

1.2.1 Befragung von Unternehmen der Kritischen Infrastruktur

Im Berichtsjahr 2025 investierte erneut die Mehrheit der befragten österreichischen Unternehmen aus dem Bereich der kritischen Infrastruktur in Maßnahmen zur Cybersicherheit. Lediglich rund vier Prozent der befragten Organisationen reduzierten ihr Budget für IT-Sicherheit im Vergleich zum Vorjahr. Insgesamt bestätigt sich damit der anhaltende Trend, die Ausgaben für Cybersicherheit auf einem konstant hohen Niveau zu halten. Die gezielten Investitionen dürften dazu beigetragen haben, potenziell schwerwiegende IT-Sicherheitsvorfälle zu verhindern oder zumindest deren Auswirkungen zu reduzieren.

Die im Beobachtungszeitraum umgesetzten Maßnahmen umfassten sowohl technische als auch organisatorische Initiativen zur Stärkung der Informationssicherheit sowie zur

Verbesserung der Transparenz in der IT- und Infrastrukturumgebung. Zu den zentralen Maßnahmen zählten insbesondere der Einsatz beziehungsweise die Weiterentwicklung von Security-Information-and-Event-Management-(SIEM)-Lösungen und Security Operations Centers (SOC) zur kontinuierlichen Überwachung sicherheitsrelevanter Ereignisse. Darüber hinaus wurden Maßnahmen zum Schutz vor Distributed-Denial-of-Service-(DDoS)-Angriffen implementiert oder ausgebaut. Ein weiterer Schwerpunkt lag auf der Einführung beziehungsweise Weiterentwicklung von Informationssicherheits-Managementsystemen (ISMS), um Sicherheitsprozesse systematisch zu strukturieren und zu steuern. Ergänzend dazu wurde verstärkt in die Sensibilisierung und Schulung der Mitarbeitenden investiert, um das Sicherheitsbewusstsein innerhalb der Organisationen zu erhöhen. Technisch wurden zudem Endpoint-Detection-and-Response-(EDR)-Lösungen weiter ausgebaut sowie zentrale Log-Management-Systeme etabliert oder erweitert, um sicherheitsrelevante Ereignisse effizienter zu erfassen, auszuwerten und frühzeitig auf potenzielle Bedrohungen reagieren zu können. Die Sicherheitsstrategie vieler Organisationen orientierte sich weiterhin an einem mehrschichtigen „Defense-in-Depth“-Ansatz. Dieser wurde unter anderem durch den Einsatz von Privileged Access Management (PAM) zur kontrollierten Verwaltung administrativer Berechtigungen sowie durch regelmäßige Vulnerability-Scans zur frühzeitigen Identifikation und Behebung von Schwachstellen unterstützt. Ebenso wurden Maßnahmen zur Absicherung von Operational-Technology-Systemen weiter ausgebaut.

Infobox: Operational-Technology-Systeme (OT-Systeme)
OT-Systeme sind Hard- und Softwarelösungen zur Überwachung und Steuerung physischer Prozesse, etwa in Industrieanlagen, Energieversorgung oder Verkehrssystemen. Sie erfassen Daten aus der realen Welt und greifen direkt in Abläufe ein, um Maschinen, Produktionslinien oder Infrastrukturen sicher und effizient zu betreiben.

Als wesentliche „Lessons Learned“ erwiesen sich im Jahr 2025 insbesondere drei Aspekte: der verstärkte Einsatz von Cyber-Threat-Intelligence, eine kontinuierliche Sensibilisierung der Mitarbeitenden durch Awareness-Maßnahmen sowie regelmäßige Sicherheitsüberprüfungen, einschließlich Pentests. Diese Maßnahmen trugen wesentlich dazu bei, Bedrohungen frühzeitig zu erkennen, Angriffsflächen zu reduzieren und organisatorische Sicherheitskulturen nachhaltig zu stärken.

Ein prägender Trend der IT-Security-Branche im Jahr 2025 war der verstärkte Einsatz von künstlicher Intelligenz (KI). KI-basierte Technologien unterstützten Unternehmen insbesondere im Bereich der Verteidigung, etwa durch verbesserte Log-Analysen, automatisierte Auswertung großer Datenmengen und eine frühzeitigere Erkennung potenzieller Bedrohungen. Gleichzeitig zeigte sich jedoch auch, dass Angreiferinnen und

Angreifer zunehmend KI einsetzen, um Angriffe zu automatisieren, Phishing-Kampagnen zu professionalisieren oder Sicherheitsmechanismen gezielter zu umgehen. Künstliche Intelligenz stellt damit sowohl ein Risiko als auch eine Chance dar: Während Angriffe komplexer und effizienter werden können, erleichtert KI auf der anderen Seite die Automatisierung und Erkennung von Sicherheitsvorfällen.

Die Analyse der Vorfallsursachen zeigt ähnliche Ergebnisse zu jenen im Vorjahr. Die Bedrohungen gehen überwiegend von externen Akteurinnen und Akteuren aus. An zweiter Stelle stehen externe Abhängigkeiten, etwa von Lieferantinnen und Lieferanten oder Dienstleisterinnen und Dienstleistern, die ebenfalls Auswirkungen auf den sicheren Betrieb von Organisationen haben können. Innentäterinnen bzw. Innentäter werden hingegen von den meisten Organisationen weiterhin überwiegend als kein oder lediglich als geringes Risiko eingeschätzt.

Wurden in Ihrem Unternehmen 2025 neue IT-Security-Maßnahmen implementiert, welche die Erkennbarkeit von IT-Sicherheitsvorfällen erhöhen können?

→ Ja: 88,7 Prozent, Nein: 7,0 Prozent, Keine Angabe: 4,3 Prozent

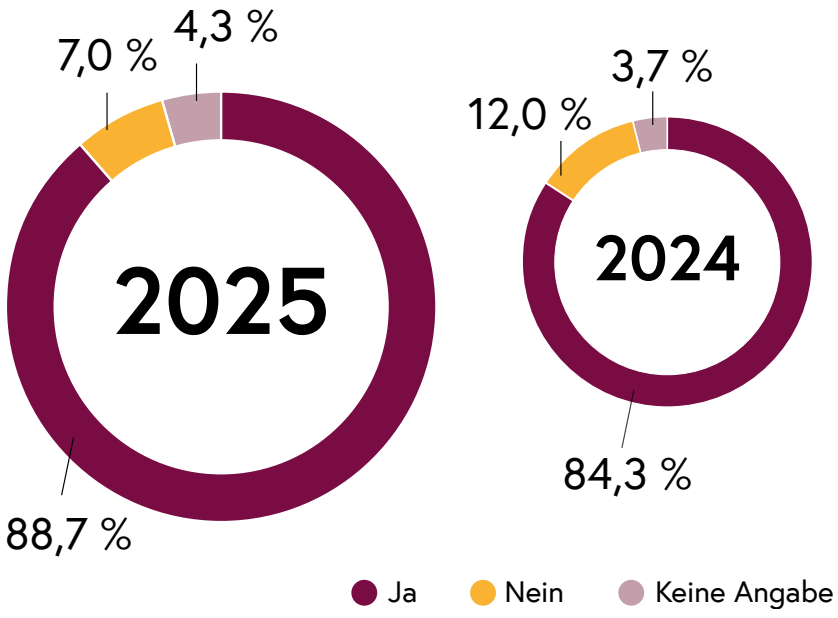


Abbildung 1: Wurden in Ihrem Unternehmen 2025 neue IT-Security-Maßnahmen implementiert, welche die Erkennbarkeit von IT-Sicherheitsvorfällen erhöhen können?

Wie hat sich in Ihrem Unternehmen im Jahr 2025 das für IT-Security zur Verfügung stehende Budget gegenüber dem Jahr 2024 verändert?

→ Gestiegen: 59,1 Prozent, Gleich: 30,4 Prozent, Gesunken: 2,6 Prozent, Keine Angabe: 7,8 Prozent

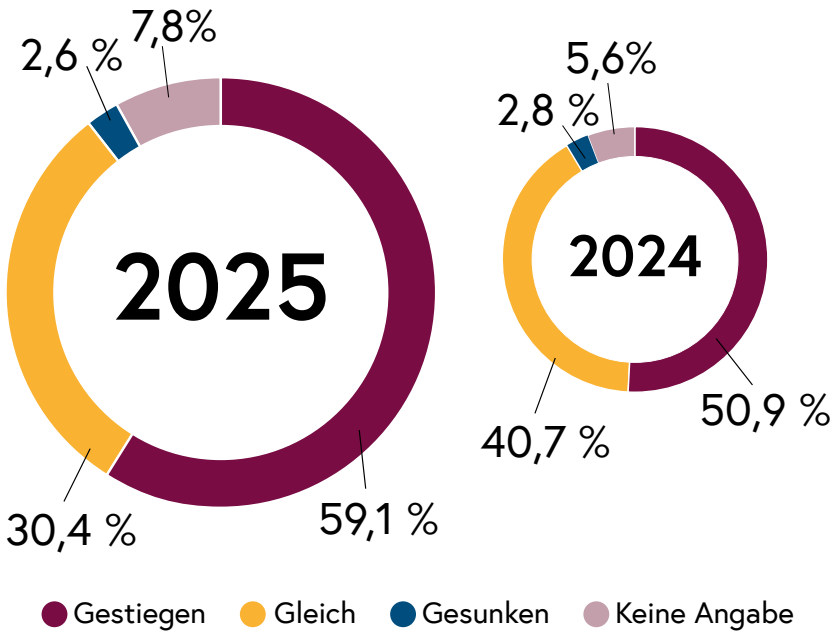


Abbildung 2: Wie hat sich in Ihrem Unternehmen im Jahr 2025 das für IT-Security zur Verfügung stehende Budget gegenüber dem Jahr 2024 verändert?

Wie beurteilen Sie die Vorfallsursache „Außentäterinnen und Außentäter“ für das Jahr 2025?

→ Großes Problem: 31,3 Prozent, Mittleres Problem: 37,4 Prozent, Kleines Problem: 23,5 Prozent, Kein Problem: 7,8 Prozent

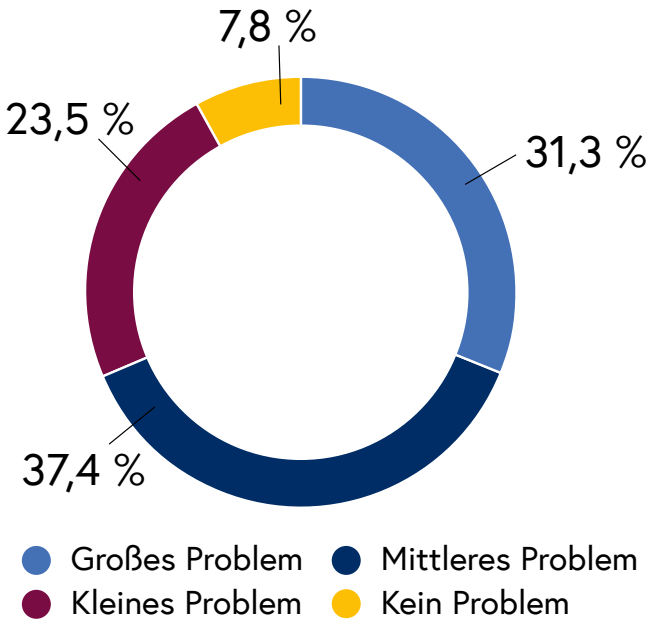


Abbildung 3: Wie beurteilen Sie die Vorfallsursache „Außentäterinnen und Außentäter“ für das Jahr 2025?

Wie beurteilen Sie die Vorfallsursache „Innentäterinnen und Innentäter“ für das Jahr 2025?

→ Großes Problem: 4,3 Prozent, Mittleres Problem: 24,3 Prozent, Kleines Problem: 40,9 Prozent, Kein Problem: 30,4 Prozent

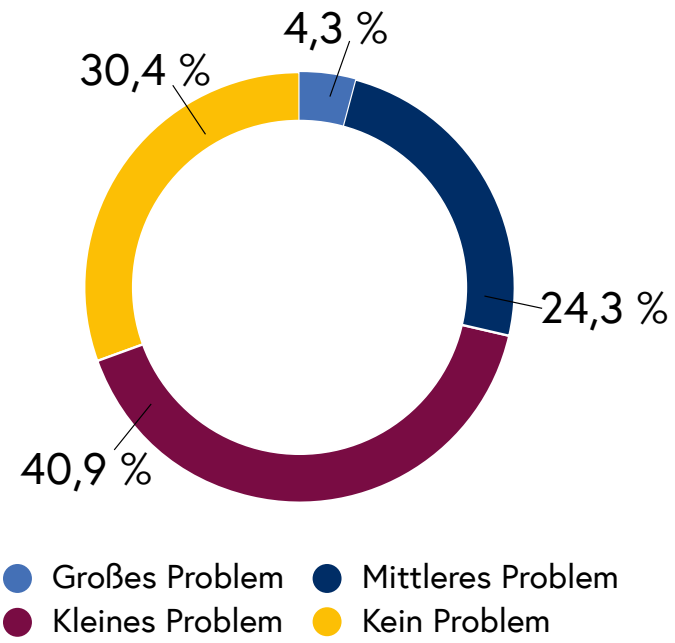


Abbildung 4: Wie beurteilen Sie die Vorfallsursache „Innentäterinnen und Innentäter“ für das Jahr 2025?

Wie beurteilen Sie die Vorfallsursache „Technische Gebrechen“ für das Jahr 2025?

→ Großes Problem: 9,6 Prozent, Mittleres Problem: 32,2 Prozent, Kleines Problem: 44,3 Prozent, Kein Problem: 13,9 Prozent

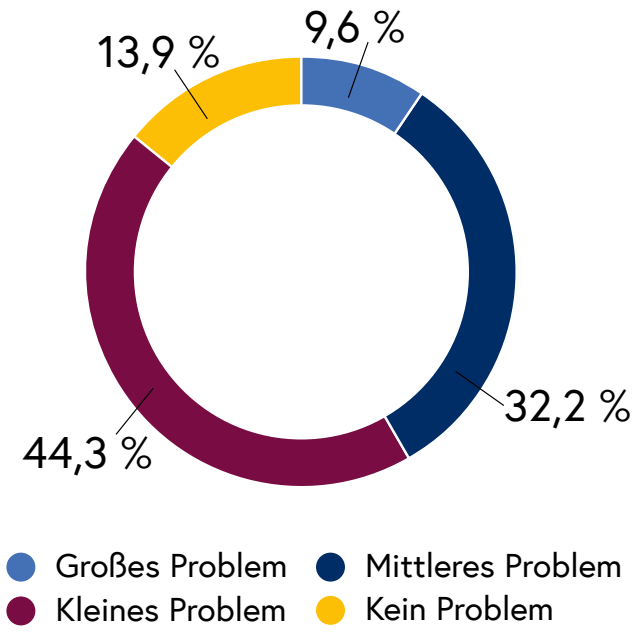


Abbildung 5: Wie beurteilen Sie die Vorfallsursache „Technische Gebrechen“ für das Jahr 2025?

Wie beurteilen Sie die Vorfallsursache „Externe Abhängigkeiten - Supply Chain“ für das Jahr 2025?

→ Großes Problem: 27,0 Prozent, Mittleres Problem: 40,0 Prozent, Kleines Problem: 21,7 Prozent, Kein Problem: 11,3 Prozent

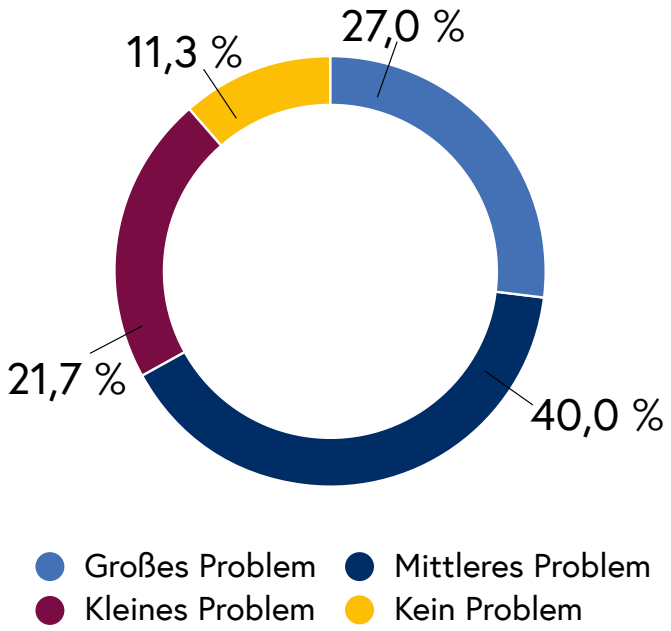


Abbildung 6: Wie beurteilen Sie die Vorfallsursache „Externe Abhängigkeiten - Supply Chain“ für das Jahr 2025?

Welche Trends konnten Sie 2025 zu den genannten Vorfallsursachen gegenüber 2024 beobachten?

Außentäterinnen und Außentäter

→ Zunahme: 34,8 Prozent, Unverändert: 55,7 Prozent, Abnahme: 0,9 Prozent, Keine Angabe: 8,7 Prozent

Innentäterinnen und Innentäter

→ Zunahme: 3,5 Prozent, Unverändert: 87,0 Prozent, Abnahme: 0,9 Prozent, Keine Angabe: 8,7 Prozent

Technische Gebrechen

→ Zunahme: 13,9 Prozent, Unverändert: 67,8 Prozent, Abnahme: 8,7 Prozent, Keine Angabe: 9,6 Prozent

Externe Abhängigkeiten - Supply Chain

→ Zunahme: 53,0 Prozent, Unverändert: 33,9 Prozent, Abnahme: 5,2 Prozent, Keine Angabe: 7,8 Prozent

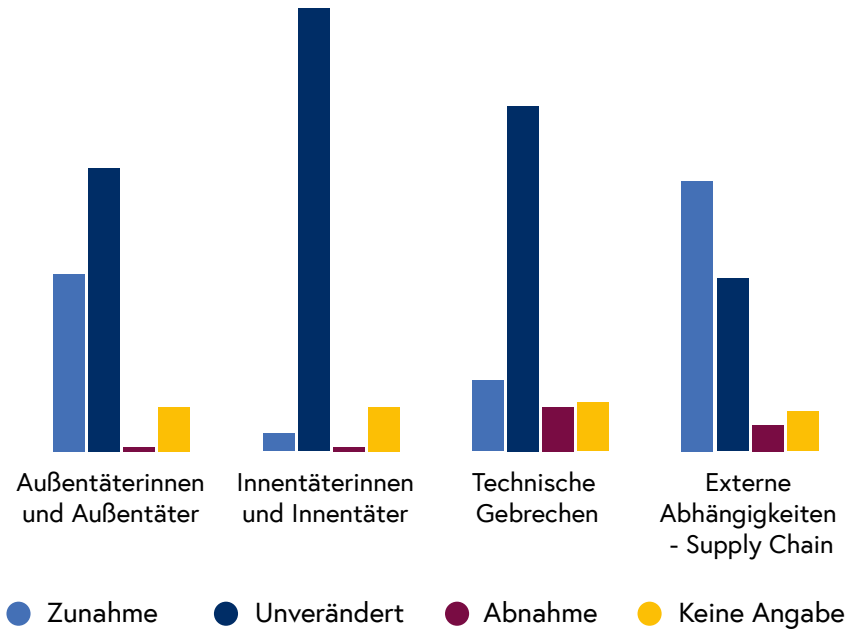


Abbildung 7: Welche Trends konnten Sie 2025 zu den genannten Vorfallsursachen gegenüber 2024 beobachten?

1.2.2 Führende private Unternehmen aus der Cybersicherheits-branche

Aus den eingegangenen Antworten der Befragung von führenden privaten Unternehmen aus dem Bereich der Sicherheitsdienstleistenden für das Jahr 2025 lassen sich nachfolgend aufgeführte Trends und gewonnene Erkenntnisse ableiten. Die Rücklaufquote der Beantwortung für das Jahr 2025 ist im Vergleich zum Vorjahr gesunken.

	SD 1	SD 2	SD 3	SD 4	SD 5	SD 6	SD 7
DDoS	=	k. A.	+	=	-	-	=
Ransomware	=	+	=	=	=	=	=
Phishing	=	+	+	+	+	=	+
CEO-Fraud/Fake Invoice/SCAM	=	=	=	-	+	=	+
Targeted Attack/APT	+	=	k. A.	=	+	+	k. A.
Innentäterinnen bzw. -täter	=	=	-	=	+	k. A.	=

Abbildung 8: Trends zu Vorfallsarten 2025 (gegenüber 2024)

Anhand der im Fragebogen ausgewerteten Ergebnisse konnten die verschiedenen Angriffskategorien, die bei den Sicherheitsdienstleistern identifiziert wurden, analysiert werden. Dabei werden die relevanten Akteure und die gewonnenen Erkenntnisse aus den Angriffen dargestellt. Ziel ist es, Handlungsempfehlungen für zukünftige Cybersicherheitsmaßnahmen abzuleiten. Als weitere Vorfallsarten wurden die Kompromittierung von Benutzerkonten sowie Cyberangriffe auf Lieferketten genannt.

DDoS: DDoS-Angriffe sind als Vorfallsursache im Jahr 2025 bei fast allen Sicherheitsdienstleistern in ihrer Häufigkeit weitgehend unverändert geblieben. Aus den bisherigen Erfahrungen lässt sich ableiten, dass präventive Maßnahmen (unter anderem etwa eine ordnungsgemäße und sorgfältige Systemkonfiguration) wesentlich dazu beitragen können, entsprechende Ausfälle zu reduzieren.

Ransomware: Die Kategorie Ransomware-Angriffe weist bei etwa der Hälfte der Sicherheitsdienstleister einen steigenden Trend auf; bei der anderen Hälfte ist sie in ihrer Häufigkeit etwa gleichgeblieben. Einer der befragten Dienstleister konnte ein unzureichend gepatchtes Testsystem als Problem identifizieren, während bei den übrigen Dienstleistern der Initial Attack Vector unklar ist. Ein zentrales „Lesson Learned" besteht darin, regelmäßige Pentests durchzuführen, um Schwachstellen frühzeitig zu erkennen und entsprechende Maßnahmen zur Risikominimierung sowie Erkennung und Abwehr einzuleiten.

Phishing: Phishing bleibt auch 2025 eine der häufigsten Angriffsmethoden und zeigt sich bei den meisten Sicherheitsdienstleistern in diesem Jahr als wachsendes Szenario. In den meisten Fällen handelt es sich hierbei um Betrüger-E-Mails oder Social-Engineering-Methoden, um Zugangsdaten der Opfer oder vertrauliche Informationen zu erlangen. Um dagegen vorzugehen, ist eine kontinuierliche Sensibilisierung der Mitarbeitenden durch Schulungen oder simulierte Angriffe ratsam, um das Bewusstsein zu stärken und die Erkennungsrate solcher Angriffe zu erhöhen.

CEO-Fraud: CEO-Fraud ist weiterhin eine ernstzunehmende Bedrohung und zeigt sich bei manchen Unternehmen als steigender Trend. CEO-Fraud kann im schlimmsten Fall zu einem hohen finanziellen Schaden führen, weshalb nicht nur Maßnahmen durch die Mitarbeitenden essenziell sind, sondern auch durch das Unternehmen selbst, zum Beispiel in Form von internen Regeln und einheitlichen Strukturen.

APT: Advanced Persistent Threats (APT) nutzen gezielte Angriffsvektoren wie Spear-Phishing, fehlende Multi-Faktor-Authentifizierung (MFA) oder auch „MFA-Fatigue", den Missbrauch gültiger Zugangsdaten, Firewall-Exploits und die Ausnutzung ungepatchter Schwachstellen. Die Umfrage zeigt, dass APT als Bedrohungsszenario auch 2025 nicht zurückgegangen ist, sondern weiterhin als ernstzunehmend einzustufen ist. Um sich gegen diese hochentwickelten Bedrohungen zu schützen, sind konsequente Sicherheitsmaßnahmen sowie in weiterer Folge die Optimierung von Pentests unerlässlich.

Infobox: MFA-Fatigue

MFA-Fatigue (Multi-Faktor-Authentifizierungs-Müdigkeit) bezeichnet eine Angriffsmethode, bei der Nutzerinnen und Nutzer mit vielen Authentifizierungsanfragen überflutet werden. Ziel ist, dass sie aus Frust oder Versehen eine Anfrage bestätigen. Angreiferinnen und Angreifer nutzen dies, um Sicherheitsmechanismen zu umgehen und unbefugt Zugriff auf Konten oder Systeme zu erhalten.

Innentäterinnen und Innentäter: Nach dem Austritt von IT-Mitarbeiterinnen und -Mitarbeitern ist ein sofortiger Passwort-Wechsel essenziell, um unbefugten Zugriff zu verhindern. Zudem wird empfohlen, regemäßige Mitarbeiterinnen- und Mitarbeiterschulungen sowie Awareness-Trainings durchzuführen, um gegen Innentäterinnen und Innentäter präventiv vorzugehen.

1.3 Lage Cybercrime

Die Betrachtung der polizeilichen Kriminalstatistik lässt mit 63.459 angezeigten Delikten im Jahr 2025 eine Steigerung von 1,8 Prozent gegenüber dem Jahr 2024 erkennen. Die genauen Deliktszahlen werden jährlich im Frühjahr mit der kriminalpolizeilichen Anzeigenstatistik veröffentlicht. Eine tiefergehende Analyse und Beschreibung der kriminalpolizeilichen Phänomene erfolgen mit dem jährlichen Cybercrime-Report des Bundeskriminalamts.

Der Begriff Cybercrime umfasst:

- Cybercrime im engeren Sinn,
- Internetbetrug und
- sonstige Kriminalität im Internet.

1.3.1 Cybercrime im engeren Sinn

Darunter fallen Straftaten, bei denen Angriffe auf Daten- oder Computersysteme unter Ausnutzung der Informations- und Kommunikationstechnik begangen werden. Beispiele dafür sind der widerrechtliche Zugriff auf ein Computersystem, die Datenbeschädigung oder der betrügerische Datenverarbeitungsmissbrauch.

Die Zahl der Fälle von Cybercrime im engeren Sinne ist 2025 im Vergleich zu 2024 um 8,6 Prozent auf 21.988 Anzeigen gestiegen. Dies lässt sich vor allem auf vermehrte Anzeigen im Bereich des § 148a StGB (Betrügerischer Datenverarbeitungsmissbrauch) und § 225a StGB (Datenfälschung) zurückführen.

Ransomware-Angriffe richteten sich beispielsweise gegen die unterschiedlichsten Branchen und Zielgruppen. Cyberkriminelle führen ihre Angriffe gegen Opfer aus, die als finanziell lukrativ angesehen werden oder die durch einen Ausfall besonders stark beeinträchtigt sein könnten. Die Motivation der Angreiferinnen und Angreifer reicht von finanziellen Forderungen bis hin zu ideologischen Gründen oder Sabotageakten. Im Cybercrime Competence Center (C4) des Bundeskriminalamts werden die angezeigten Ransomware-Fälle zentral erfasst und auf Gemeinsamkeiten analysiert. Ausgenommen sind jene Fälle, die aufgrund der Geschäftseinteilung in den Zuständigkeitsbereich anderer Behörden und Dienststellen fallen (wie z. B. der Direktion Staatsschutz und Nachrichtendienst – DSN).

So wurden im Bundesgebiet im Jahr 2025 insgesamt 111 Fälle von Ransomware-Angriffen zur Anzeige gebracht. Die Dunkelziffer ist in diesem Bereich sehr hoch. Die Angriffe richteten sich sowohl gegen Privatpersonen, Ein-Personen-Unternehmen (EPU), kleine und mittlere Unternehmen (KMU), Konzerne als auch gegen Bildungseinrichtungen, das Gesundheitswesen und Behörden. Der überwiegende Teil der Angriffe fand auf Unternehmen statt. Dabei wurden die Angriffe von 29 unterschiedlichen Tätergruppierungen durchgeführt. Es ist erkennbar, dass ein Teil der Angriffe wie bereits im Vorjahr, durch kleinere Akteurinnen und Akteure durchgeführt wurde. Etabliertere Gruppierungen wie INC (zwölf Fakten), Akira (elf Fakten) und RansomHub (fünf Fakten) verübten eine größere Zahl von Angriffen.

Bei größeren Unternehmen steigt die Gefahr, dass neben der Verschlüsselung auch mit der Veröffentlichung von Unternehmensdaten gedroht wird. Nach einem Schadensfall ist damit zu rechnen, dass es trotz vorhandener Backups zu Produktionsausfällen kommen kann. Aufgrund zunehmender Arbeitsteilung (Crimeas-a-Service) und Vernetzung der Tätergruppen wird die Strafverfolgung zunehmend erschwert.

1.3.2 Internetbetrug

Der Internetbetrug stellt zahlenmäßig den größten Faktor im Bereich der Cyberkriminalität dar. Nahezu die Hälfte der erfassten Anzeigen im Bereich Internetkriminalität fallen auf Betrugsdelikte: 2025 wurden 31.001 Fälle von Internetbetrug angezeigt, ein leichter Rückgang von 2,4 Prozent im Vergleich zum Vorjahr. Mit der fortschreitenden Digitalisierung verlagern sich Betrugsdelikte immer mehr ins Netz. Für die Täterinnen und Täter ist es ein Leichtes, aufgrund technischer Anonymisierung sowie Verschleierung der Finanzflüsse Betrugshandlungen unerkannt und damit „sicher“ durchzuführen. Zusätzlich können durch den weltweiten Online-Zugang immer mehr Menschen als potenzielle Opfer angesprochen werden. Häufige Deliktsformen sind der Bestellbetrug, der digitale Investmentbetrug, der Anrufbetrug (Stichwort: „Falsche Polizistin und falscher Polizist“) sowie alle möglichen Phishingversuche.

1.3.3 Sonstige Kriminalität im Internet

Unter sonstiger Kriminalität im Internet versteht man Straftaten, die ihren Tatort im Internet haben. Ausgenommen sind Cybercrime im engeren Sinn, Internetbetrug, bildliches sexualbezogenes Kindesmissbrauchsmaterial und bildliche sexualbezogene Darstellungen minderjähriger Personen (§ 207a StGB) und die Anbahnung von Sexualkontakten zu Unmündigen (§ 208a StGB).

Im Bereich der sonstigen Kriminalität im Internet wurde im Jahr 2025 ein deutlicher Anstieg der Delikte verzeichnet (6.682 Anzeigen, 2024: 5.370 Anzeigen). Der Grund liegt in der zunehmenden Verlagerung klassischer Strafrechtsdelikte ins Internet.

Zunahmen wurden beispielsweise bei § 105 StGB (Nötigung, 481 Anzeigen), § 107 StGB (Gefährliche Drohung, 1.714 Anzeigen) und § 27 SMG (Unerlaubter Umgang mit Suchtgiften, 1.116 Anzeigen) verzeichnet. § 3g Verbotsgesetz (Nationalsozialistische Wiederbetätigung, 1.206 Anzeigen) auf anhaltend hohem Niveau.

Gleichzeitig wurden sogenannte Crime-as-a-Service-Leistungen im Darknet angeboten. Dabei handelt es sich vorwiegend um Hacking-Tools oder Erpressungssoftware bzw. Ransomware. Durch die im Darknet angebotenen Dienste werden vor allem Erpressungen mit Ransomware begangen bzw. Massenerpressungsmails verschickt, meist begleitet von Geldforderungen in Kryptowährungen. 2025 wurden 2.380 Erpressungen im Internet angezeigt, Trend rückläufig.

Auch konnte festgestellt werden, dass Hackerinnen und Hacker künstliche Intelligenz (KI) für die Programmierung von Malware (Schadsoftware) nutzen. Da es sich bei der KI um ein lernendes System handelt, ist anzunehmen, dass in Zukunft stets komplexere Schadsoftware damit erstellt wird. Neben Malware könnte die Software beim Erstellen von Darknet-Marktplätzen oder Phishing zum Einsatz kommen.

1.4 Cyberlage Landesverteidigung

Die Cyberlage im Jahr 2025 war aus Sicht der Landesverteidigung weiterhin von hoher Volatilität geprägt. Die Entwicklungen des Vorjahres haben deutlich gezeigt, dass der Cyberraum dauerhaft als eigenständige militärische Domäne etabliert ist und in modernen Konflikten und insbesondere im Rahmen der „Hybriden Kriegsführung“ eine zentrale Rolle einnimmt. Cyberangriffe sind längst nicht mehr nur Begleiterscheinung klassischer militärischer Auseinandersetzungen, sondern werden gezielt als strategisches Instrument zur Destabilisierung von Staaten, zur Beeinflussung politischer Entscheidungsprozesse sowie zur Schwächung militärischer Führungs- und Einsatzfähigkeit eingesetzt.

Das Jahr 2025 war dementsprechend maßgeblich von der Erkenntnis geprägt, dass jede neue militärische Fähigkeit untrennbar mit einer Cyberdimension verbunden ist. Die Einführung und zunehmende Vernetzung moderner Waffensysteme sowie digitaler Führungs- und Kommunikationsmittel machten einen konsequenten Ausbau von Security-by-Design-Ansätzen, kontinuierlicher Sicherheitsüberwachung und cyberresilienten Systemarchitekturen erforderlich. Cyberverteidigung entwickelt sich damit von einem eigenständigen Fachbereich zu einer domänenübergreifenden Querschnittsaufgabe, die alle Ebenen militärischer Planung und Führung durchdringt. Gleichzeitig wurde 2025 als Wendepunkt wahrgenommen, da Cyberbedrohungen nicht mehr episodisch, sondern dauerhaft präsent waren, Angriffe deutlich gezielter und intelligenter erfolgten und Cyberoperationen klar als Instrument militärischer Einflussnahme erkennbar wurden. Wirksame Verteidigung erwies sich in diesem Umfeld nur noch durch vernetzte, internationale und proaktive Ansätze als erfolgreich.

Der Anteil an staatlich und staatsnah durchgeführten Cyberoperationen war 2025 von einem signifikanten Anstieg geprägt. Besonders betroffen waren militärische Einrichtungen, kritische Infrastrukturen, staatliche Verwaltungssysteme sowie Kommunikations- und Informationsnetzwerke. Dies zeigte sich beispielsweise bei dem Cyberangriff gegen das Außenministerium der Tschechischen Republik, der Mitte des Jahres öffentlich wurde. Neben der quantitativen Zunahme zeigte sich auch eine deutliche qualitative Weiterentwicklung der Angriffe: hochgradig koordinierte Kampagnen, der verstärkte Einsatz von automatisierten Angriffswerkzeugen, künstlicher Intelligenz sowie präzise abgestimmte Desinformations- und Einflussoperationen prägten die Bedrohungslage. Diese Entwicklungen verdeutlichen, dass Cyberoperationen zunehmend darauf abzielen, Entscheidungsprozesse auf strategischer, operativer und taktischer Ebene zu beeinflussen.

Globale Konflikte und geopolitische Spannungen haben auch im vergangenen Jahr zu einem unmittelbaren Anstieg weltweiter Cyberangriffe geführt. Der russische Angriffskrieg gegen die Ukraine sowie die anhaltenden Krisen im Nahen Osten haben erneut gezeigt, wie eng konventionelle militärische Operationen, elektronische Kampfführung, Cyberangriffe und Informationsoperationen miteinander verzahnt sind. Cyberangriffe wurden dabei sowohl zur Vorbereitung kinetischer Operationen als auch zur langfristigen Destabilisierung gesellschaftlicher und staatlicher Strukturen eingesetzt.

Vor diesem Hintergrund gewinnt Cyberverteidigung für die Landesverteidigung Österreichs weiter an Bedeutung. Für das Österreichische Bundesheer (ÖBH) steht die Stärkung robuster, widerstandsfähiger und durchhaltefähiger defensiver Cyberfähigkeiten im Mittelpunkt. Ziel bleibt der konsequente Aufbau und die Weiterentwicklung einer umfassenden Full Spectrum Cyber Defence, um Bedrohungen frühzeitig zu erkennen, wirksam abzuwehren und die Handlungsfähigkeit in allen militärischen Domänen sicherzustellen.

Im Jahr 2025 setzte das ÖBH verstärkt auf die Vertiefung internationaler Kooperationen und die enge Abstimmung mit europäischen und internationalen Partnern. Die aktive Beteiligung an multinationalen Cyberübungen, darunter EU- und NATO-geführte Großübungen, bleibt ein zentraler Bestandteil zur Weiterentwicklung der eigenen Fähigkeiten. Die im Jahr 2025 gewonnenen Erkenntnisse aus Übungen wie „Locked Shields“ fließen unmittelbar in Ausbildung, Doktrin und technische Weiterentwicklungen ein.

Neben diesen Kooperationen ist aufgrund der geopolitisch angespannten Situation die Sicherstellung der digitalen Souveränität ein wesentlicher Faktor für das ÖBH. Österreich und die EU müssen zukünftig in der Lage sein, unabhängig im digitalen Raum agieren zu können.

Die Mitarbeit im Rahmen der „Ständigen Strukturierten Zusammenarbeit“ der EU (PESCO), insbesondere im Projekt Cyber Rapid Response Team (CRRT), wird weiter intensiviert. Die Erfahrungen aus realen Einsätzen und präventiven Unterstützungsmaßnahmen haben gezeigt, wie wichtig rasch verfügbare, interoperable Cyberfähigkeiten sind.

Parallel dazu treibt das ÖBH 2025 die sichere Integration neuer Waffensysteme sowie moderner Führungs- und Kommunikationsmittel weiter voran. Die zunehmende Vernetzung militärischer Systeme erhöht die operative Leistungsfähigkeit, stellt jedoch auch wachsende Anforderungen an Cybersicherheit, Resilienz und Schutz vor hybriden Bedrohungen. Der Schutz militärischer IKT-Systeme wird daher ganzheitlich über den gesamten Lebenszyklus hinweg betrachtet.

Besonderes Augenmerk gilt weiterhin disruptiven Technologien. Die rasante Entwicklung künstlicher Intelligenz, automatisierter Entscheidungssysteme und die absehbaren Fortschritte im Bereich des Quanten-Computings eröffnen neue Möglichkeiten, bergen jedoch zugleich auch Risiken. Das ÖBH analysiert diese Technologien sowohl im Hinblick auf potenzielle Bedrohungen als auch auf ihren verantwortungsvollen und sicherheitsrelevanten Einsatz im militärischen Kontext.

Zusammenfassend lässt sich festhalten, dass Cyberverteidigung im Jahr 2025 mehr als je zuvor ein unverzichtbarer Pfeiler der österreichischen Landesverteidigung ist. Die Erfahrungen des Vorjahres haben definitiv gezeigt, dass Sicherheit im Cyberraum eine Grundvoraussetzung für militärische Einsatzfähigkeit, staatliche Resilienz und den Schutz demokratischer Strukturen darstellt. Das Bundesministerium für Landesverteidigung und das Österreichische Bundesheer werden daher auch weiterhin konsequent in Fähigkeiten, Personal, internationale Kooperationen sowie technologische Innovationen investieren, um den wachsenden Herausforderungen im Cyberraum wirksam begegnen zu können.

1.5 Verfassungsschutzrelevante Cyberlage

Im Jahr 2025 stand Österreich unverändert im Fokus fremdstaatlicher, nachrichtendienstlicher Aktivitäten. Dies hat einerseits historische Gründe, liegt andererseits aber vor allem in der geografischen Lage des Landes, seiner EU-Mitgliedschaft, im Vorhandensein von speziellem Know-how in Forschung und Technik sowie in der Funktion Österreichs als Gastgeberstaat der Vereinten Nationen und anderer internationaler Organisationen begründet.

Zahlreiche Nachrichtendienste verfügen über spezialisierte Einheiten, die im Cyberraum operieren. Diese sind primär mit der Unterstützung der Informationsbeschaffung durch Cyberspionage beauftragt. Neben Spionageaktivitäten führen diese Akteurinnen und Akteure aktive Maßnahmen geheim-/nachrichtendienstlichen Charakters, wie beispielsweise Cybersabotage oder Informationsoperationen durch. Zusätzlich zu diesen nachrichtendienstlichen Kernaufgaben gibt es Überschneidungen zu Cyberkriminellen und Hacktivistinnen und Hacktivisten. Zu den Tätigkeiten klassischer Cyberkrimineller zählen Angriffe auf Computersysteme, wie z. B. Ransomware-Angriffe. Die Entwicklungen im Bereich der Digitalisierung, die mittlerweile sämtliche Lebensbereiche betreffen, verstärken das Risiko, das von Cyberkriminellen und insbesondere von nachrichtendienstlichen Akteurinnen und Akteuren ausgeht. Die österreichischen Behörden sind folglich mit einer wachsenden Bedrohungslage konfrontiert, weshalb die kontinuierliche Erweiterung der Cyberabwehrkapazitäten unabdingbar ist. Abgesehen von der Implementierung technologischer Sicherheits- und Präventionsmaßnahmen sowie rechtlicher Absicherungen benötigt es zudem internationale Kooperationen im Bereich der Cybersicherheit und Spionageabwehr, um resilient gegenüber diesen Bedrohungen zu werden.

1.5.1 Russische nachrichtendienstliche Cyberaktivitäten

Der Schwerpunkt russischer Nachrichtendienste in Bezug auf die Unterstützung des Angriffskrieges gegen die Ukraine wird im Cyberraum primär auf zwei Arten umgesetzt: Einerseits wird Cyberspionage betrieben, um Unterstützungshandlungen des Westens für die Ukraine aufzuklären. Andererseits wird versucht, durch gezieltes Leaken ausgespähter Informationen in demokratische Wahlen oder staatliche Handlungen einzugreifen. Attraktive Ziele für Cyberspionage sind vor allem staatliche und politische Einrichtungen.

Infobox: IoT-Gerät

Ein Internet-of-Things-Gerät (IoT-Gerät) ist ein elektronisches Gerät, das mit dem Internet verbunden ist. Solche Geräte sind häufig in alltäglichen Anwendungen zu finden, etwa in Haushaltsgeräten (smarte Thermostate, Kühlschränke), Wearables (z. B. Fitnessarmbänder) oder industriellen Anwendungen (etwa Sensoren zur Überwachung von Maschinen). Sie ermöglichen Automatisierung, Datenerhebung und -analyse sowie die Fernsteuerung von Funktionen.

Im Rahmen offensiver Cyberoperationen (CNE)[1] nutzen russische Akteurinnen und Akteure auch Schwachstellen in privaten IoT-Geräten, um ihre Spuren zu verschleiern. Durch das Eindringen in unsicher konfigurierte Netzwerkgeräte (beispielsweise Router) und das Installieren von zusätzlicher Proxy-Software[2] können Cyberangriffe über diese infizierten Geräte durchgeführt werden. Für die Besitzerinnen und Besitzer kann dies zur Folge haben, dass sie durch die Vernachlässigung der eigenen IT-Sicherheitsmaßnahmen in den Fokus internationaler Spionageermittlungen geraten. Es ist daher wichtig, die eigenen internetfähigen Geräte regelmäßig zu aktualisieren und vordefinierte Standardpasswörter umgehend durch eigene, hinreichend komplexe Passwörter zu ersetzen.

Russische Akteurinnen und Akteure verschaffen sich nicht nur Zugang zu privaten Geräten, sondern auch immer wieder zu End-of-Life-Netzwerkgeräten von Organisationen in sämtlichen Sektoren und unterschiedlichen Ländern. In Kombination mit dem Einsatz spezieller Schadsoftware bleiben diese Zugriffe oftmals jahrelang unentdeckt. Derartige opportunistische Kampagnen verfolgen nicht nur Spionageabsichten, sondern können auch der Vorbereitung künftiger Cybersabotageoperationen dienen. Im Zuge von „Pre-Positioning“ wird in Systeme der kritischen Infrastruktur eingedrungen und der Zugang über einen längeren Zeitraum aufrechterhalten, um die kompromittierten Systeme bei Bedarf jederzeit und ohne viel Vorarbeit angreifen zu können.

Zu den bekanntesten russischen Cybergruppierungen zählen „APT28“, „APT29“ und „Turla“. APT28 ist mutmaßlich mit dem militärischen Nachrichtendienst GU affiliiert. Die Informationsbeschaffung zur Weiterverwendung im Rahmen von Spionage und Informationsoperationen stellt eine wesentliche Hauptaufgabe dieses Akteurs dar. Ziele sind vor allem zivile und militärische Regierungsstellen sowie die Rüstungsindustrie. APT29 wird dem zivilen Auslandsnachrichtendienst SWR zugerechnet. Der Akteur führt vorwiegend Spionageoperationen gegen Einrichtungen der EU und NATO sowie deren Mitgliedstaaten durch. Turla wird dem zivilen Inlandsnachrichtendienst FSB zugeordnet und spezialisiert sich auf Cyberspionageoperationen gegen Regierungsstellen und Forschungseinrichtungen. Zusätzlich zu den genannten Akteuren lässt sich auch eine erhöhte Aktivität des Akteurs „APT44“ feststellen, welcher ebenfalls dem GU zugeordnet wird. APT44 führt sowohl Angriffe auf kritische Infrastruktur als auch auf demokratische Wahlen durch und deckt somit ein breites Spektrum russischer Cyberoperationen ab. Die

---

1 „CNE” (Computer Network Exploitation) ist die Sammlung von Informationen und die Durchführung von Spionage über Computernetzwerke. Ziel ist es, Daten aus Zielsystemen zu extrahieren, um strategische Vorteile zu erlangen.

2 „Proxy-Software” dient als Vermittler zwischen einem Endgerät und einem anderen Netzwerk, meist dem Internet. Sie leitet Anfragen von einem Gerät weiter und maskiert dabei häufig die ursprüngliche IP-Adresse der Nutzerin/des Nutzers, wodurch ihre/seine Identität geschützt wird. Proxy-Software wird häufig für den Datenschutz, zur Überwindung von Geoblockaden oder zur Kontrolle des Datenverkehrs in Unternehmensnetzwerken eingesetzt. Akteurinnen und Akteure verwenden Proxy-Software, um während Cyberangriffen ihre eigene Identität zu verschleiern und Spuren zu verwischen.

Entdeckung des Akteurs „Laundry Bear“ ist vergleichsweise rezent, die Vorgehensweise des Akteurs ist jedoch eine Manifestation der verstärkten Zusammenarbeit staatlicher Akteure mit Cyberkriminellen, die im Hinblick auf künftige Cyberentwicklungen eine Rolle spielen wird.

1.5.2 Chinesische nachrichtendienstliche Cyberaktivitäten

In China besteht eine enge Kooperation zwischen Nachrichtendiensten und Unternehmen sowie Universitäten. Dadurch verfügen chinesische Nachrichtendienste über weitreichendes Know-how. Dieses nutzen sie beispielsweise für Vorbereitungshandlungen von Cybersabotageangriffen. Dabei versuchen chinesische Cybereinheiten, in Anlagen der kritischen Infrastruktur fremder Staaten einzudringen. Dort wird zunächst weder ein Schaden angerichtet, noch werden Informationen abgesaugt. Im Fall eines eskalierenden Konflikts können diese Zugänge jedoch rasch genutzt werden, um die Funktionsfähigkeit wichtiger Systeme zu beeinträchtigen (sogenanntes Pre-Positioning). Es gibt bisher keine Hinweise darauf, dass diese Methode in Österreich zur Anwendung gekommen ist. Nichtsdestotrotz ist der chinesische Einfluss auf Lieferketten vor dem Hintergrund des hohen Anteils an chinesischen Komponenten, die in der in Österreich genutzten Hardware verbaut sind, nicht unwesentlich.

Im europäischen Raum fokussieren sich chinesische Cyberakteurinnen und -akteure weitestgehend auf die Unterstützung von Wirtschaftsspionage. Es lässt sich jedoch auch zunehmendes Interesse an politischer Spionage beobachten. Diese richtet sich meist gegen einzelne China-kritische Akteurinnen und Akteure sowie staatliche Stellen.

Ein besonderes Merkmal chinesischer Nachrichtendienste im Cyberraum ist deren enge Verflechtung mit privaten oder halbstaatlichen Cybersicherheitsdienstleistern, die teils auch eigene finanzielle Interessen verfolgen. Cyberakteurinnen und -akteure im Dienste Chinas erfüllen oft nicht nur die klassischen politisch-nachrichtendienstlichen Kernaufgaben, wie etwa das Betreiben von Spionage, sondern verfolgen auch kriminelle Ziele. Von diesen Gruppierungen geht eine hohe Gefahr aus, da sie fortschrittliche nachrichtendienstliche Methoden anwenden, um Unternehmen nach erfolgreichem Datendiebstahl zu erpressen.

Die relevantesten chinesischen Cyberakteure sind „Salt Typhoon“, „Volt Typhoon“ und „Flax Typhoon“. Zudem gewinnt „APT41“ zunehmend an Bedeutung. Salt Typhoon führt im Auftrag des chinesischen Ministeriums für Staatssicherheit (MSS) komplexe Cyberspionageoperation durch, indem es unter anderem Schwachstellen in US-amerikanischer Infrastruktur ausnutzt und so sensible Kommunikationsdaten und -inhalte exfiltriert. APT41 wird ebenfalls dem MSS zugerechnet und betreibt Spionage gegen Telekommunikations- und Medienunternehmen sowie staatliche Einrichtungen. Volt Typhoon unterwandert im Zuge von Pre-Positioning Systeme der kritischen Infrastruktur. Flax Typhoon fokussiert

sich auf Cyberspionageoperationen in Taiwan. Dafür unterwandert der Akteur unter anderem private Netzwerkgeräte, um diese im Rahmen seiner Angriffe zu nutzen.

1.5.3 Iranische nachrichtendienstliche Cyberaktivitäten

Der Fokus der iranischen Nachrichtendienste im Cyberraum liegt auf der Absicherung des Regimes. Um dies zu erreichen, betreiben sie Cyberspionageoperationen. Gewonnene Erkenntnisse aus diesen Angriffen verwenden sie häufig auch für Desinformationskampagnen (Cyber-Enabled Information Operations). Bei den Zielen handelt es sich je nach Fokus der Informationskampagne um für den Iran relevante privatwirtschaftliche Unternehmen aus verschiedenen Bereichen. Auch iranische Dissidentinnen und Dissidenten in Österreich sind immer wieder von Spionagekampagnen betroffen.

Iranische Nachrichtendienste kooperieren häufig mit hacktivistischen Gruppierungen. Sie tun dies, um ihre Spuren zu verwischen und um internationale Unterstützung für iranische Themen zu suggerieren. Seit der Zuspitzung des Konflikts mit Israel nutzen iranische Nachrichtendienste diese Operationsform verstärkt. Zusätzlich wurden in der Vergangenheit Cybersabotageangriffe durchgeführt, die sich in der Regel primär auf den Nahen Osten, insbesondere auf Israel, konzentrieren. Dabei handelte es sich entweder um kurzfristige Vergeltungsschläge oder um längerfristige, militärische Operationen.

Zu den bedeutendsten iranischen Cyberakteuren zählen „APT35“, „Pioneer Kitten“ und „Mango Sandstorm“. APT35 wird der IRGC-IO[3] zugerechnet und fokussiert sich auf Informations- und Cyberspionageoperationen. Pioneer Kitten arbeitet ebenfalls im Auftrag der iranischen Revolutionsgarden, verfügt jedoch auch über eigene finanzielle Interessen. Mango Sandstorm führt Cyberangriffe auf staatliche sowie private Organisationen durch und wird dem iranischen Ministerium für Nachrichtenwesen (MOIS) zugerechnet.

1.5.4 Sonstige nachrichtendienstlich relevante Cyberoperationen

Aufgrund aktueller geopolitischer Konflikte gewinnt das Phänomen des „Hacktivismus“ zunehmend an Bedeutung. Ein hacktivistischer Akteur können einzelne Personen – Hacktivistinnen und Hacktivisten – oder eine Personengruppe sein, die im Cyberraum aktiv Partei für eine Sache ergreifen und dabei auch cyberkriminelle Handlungen setzen. Im Jahr 2025 kam es mehrmals zu Cyberangriffen von Hacktivistinnen und Hacktivisten auf Ziele in Österreich.

Die häufigsten Methoden im Hacktivismus sind Distributed-Denial-of-Service-Angriffe und Hack-and-Leak-Operationen. Bei DDoS-Angriffen wird eine Vielzahl von Anfragen

3 Die Islamic Revolutionary Guard Corps-Intelligence Organization (IRGC-IO) ist im Vergleich zum zivilen Nachrichtendienst VAJA/MOIS unmittelbar in die Ideologie der Islamischen Revolution iranischer Prägung eingebunden und untersteht in direkter Linie dem obersten Führer, was ihr besondere Macht und Geltung verleiht. Sie unterdrückt Dissidentinnen und Dissidenten und führt Auslandsoperationen durch, etwa Entführungen von Regimegegnerinnen und -gegnern.

an einen Server gesendet, wodurch es zu einer Überlastung kommt. Dies führt beispielsweise dazu, dass angegriffene Webseiten für einen gewissen Zeitraum nicht verfügbar sind. Bei Hack-and-Leak-Operationen handelt es sich um Angriffe, die das Ziel verfolgen, mediale Aufmerksamkeit zu erregen. Eine beliebte Umsetzung dieser Methode ist das Einbrechen in Industriesteueranlagen.

Infobox: Industriesteueranlagen (ICS)

Als Industriesteueranlagen (Industry Control System, ICS) werden jene Computer bezeichnet, die dazu dienen, beispielsweise die Maschinen einer Fabrik oder die Anlagen eines Kraftwerks zu bedienen. In vielen Fällen sind diese ICS über das Internet erreichbar. Das ist notwendig, um eine Fernwartung und eine zentrale Steuerung zu ermöglichen. Bei zahlreichen Anlagen sind die Zugänge zu diesen Steueranlagen nicht ausreichend abgesichert, wodurch auch Unbefugte mit einfachen Mitteln darauf zugreifen können. In wenigen Fällen können die Angreiferinnen und Angreifer dabei nicht nur Daten ablesen, sondern diese auch verändern und die volle Kontrolle über die Anlage übernehmen.

Meist wird hierfür vorab nach ungesicherten Zugängen gesucht. Sobald das System infiltriert ist, werden Steuerbefehle eingesetzt, um die betroffenen Anlagen zu beschädigen oder abzuschalten. Wenn es den Hacktivistinnen und Hacktivisten nicht gelingt, auf kritische Systeme zuzugreifen, wird ein aus technischer Sicht fehlgeschlagener Angriffsversuch seitens der Angreiferinnen und Angreifer dennoch häufig als erfolgreich dargestellt. Dazu werden meist Screenshots mit falschen Behauptungen gepostet oder in irreführenden Montagen präsentiert. Ziel ist es, die Auswirkungen des Angriffs schwerwiegender darzustellen als sie tatsächlich waren. Bei dieser Vorgehensweise geht es Hacktivistinnen und Hacktivisten primär darum, einen medialen Effekt zu erzielen, indem suggeriert wird, tief in das System eingedrungen zu sein.

Seit einigen Jahren befeuern geopolitische Spannungen die Annäherung bzw. Verflechtung von staatlichen Interessen und Strukturen mit hacktivistischen Akteurinnen und Akteuren und deren Aktivitäten. Aus staatlicher Sicht gibt es mehrere Vorteile, sich dieser Methoden zu bedienen, insbesondere die Möglichkeit, sich von Angriffen zu distanzieren bzw. deren Attribution zu erschweren und zusätzlich das Bild einer großen, öffentlichen Unterstützungsbewegung konstruieren zu können. Die wichtigsten hacktivistischen Gruppierungen auf russischer Seite waren in den vergangenen Jahren „z-Pentest“, „Cyber Army of Russia Reborn“ und „NoName057(16)“. Im Juli 2025 wurden in einer breit angelegten internationalen Polizeiaktion zahlreiche Führungsmitglieder der hacktivistischen Gruppierung „NoName057(16)“ identifiziert und teilweise festgenommen. In diesem Zusammenhang wurden auch mehrere russische Staatsbürgerinnen und Staats-

bürger zur Fahndung ausgeschrieben, die teilweise Verbindungen zur russischen Präsidialadministration haben. Insgesamt hatte der Schlag gegen die Gruppierung jedoch nur begrenzten Erfolg und reduzierte deren Angriffstätigkeiten nur für einige Wochen.

Im Konflikt zwischen dem Iran und Israel werden die Zusammenhänge zwischen hacktivistischen Hack-and-Leak-Angriffen und staatlichen Cyber-Enabled Information Operations deutlich. Hierbei greifen iranische Nachrichtendienste gezielt Unternehmen oder Einzelpersonen an; die dabei erbeuteten Daten werden anschließend veröffentlicht. Zur Veröffentlichung verwenden iranische Dienste sogenannte „hacktivistische Personas“[4]. Dadurch gelingt es dem Iran, die Meinungsbildung Dritter gezielt zu beeinflussen. Zum einen kann der Iran das Narrativ über das Opfer, über dessen Daten er verfügt, steuern. Zum anderen entsteht der Eindruck einer globalen Unterstützung iranischer Anliegen. Durch Verwendung hacktivistischer Personas kann der Iran beide Ziele erreichen, ohne selbst dafür direkt die Verantwortung übernehmen zu müssen. Angesichts der militärischen Überlegenheit Israels ist dies ein entscheidender Vorteil.

Infobox: Cyber-Enabled Information Operations

Als „Cyber-Enabled Information Operations“ werden Informationsoperationen in Form von Cyberangriffen verstanden, deren Ziel es ist, die Meinung des Gegenübers zu verändern. Der Cyberraum dient hierbei in erster Linie lediglich als Hilfsmittel zur Tatausführung. Zentrales Anliegen dieser Operationen ist, dass eine Verbindung zum ausführenden Staat möglichst unerkannt bleiben soll. Dazu werden unterschiedliche Methoden verwendet. Zum einen werden massenhaft angelegte Social-Media-Konten genutzt, um die Desinformation zu verbreiten. Zum anderen werden politisch motivierte Hackergruppen erfunden, um so staatliche Aktivitäten, wie Hack-and-Leak-Operationen, hinter dem Deckmantel von Anarchismus oder Rebellion zu verschleiern.

In der russischen Cyberdoktrin werden derartige Angriffe als „informationspsychologische“ Beeinflussungsoperationen bezeichnet. Hierbei geht es darum, mit gezielt gestreuten Informationen eine psychologische Reaktion bei der Zielbevölkerung hervorzurufen, um so deren Verhalten zu beeinflussen. Organisatorisch gehört diese Tätigkeit zum russischen militärischen Nachrichtendienst GU, wird jedoch in der Umsetzung teilweise an externe Firmen ausgegliedert.

4 Hacktivistische Personas sind Pseudonyme oder eigens gepflegte Benutzerkonten, mit denen Nachrichtendienste über klassische hacktivistische Kanäle (z. B. Twitter/X, Telegram) kommunizieren.

Angesichts der gegenwärtigen geopolitischen Spannungen und Konflikte wird der Hacktivismus nicht an Relevanz verlieren. Vor allem aufgrund sich verdichtender Überschneidungen und Verflechtungen zwischen staatlichen Akteurinnen und Akteuren, deren Interessen und Strukturen, und hacktivistischen Akteurinnen und Akteuren sowie deren Aktivitäten. So ist etwa eine zunehmende Konvergenz zwischen pro-russischen und pro palästinensischen hacktivistischen Akteurinnen und Akteuren zu beobachten, die sich zum einen in gegenseitiger Solidarität und überlappenden Angriffen äußert, und sich zum anderen in ein generelles anti-westliches Narrativ fügt, das Russland seit 2022 gezielt befeuert, unter anderem durch die Instrumentalisierung eines antikolonialistischen Aktivismus. Außerdem verschwimmen zusehends die Grenzen zwischen Cyber-Enabled Information Operations staatlicher Akteurinnen und Akteure und genuinen hacktivistischen Aktivitäten. Nichtsdestotrotz dürfen neben allgegenwärtigen DDoS-Angriffen auch Hack-and-Leak-Operationen gegen Industriesteueranlagen nicht außer Acht gelassen werden. Daher sind vor allem präventive Maßnahmen, wie etwa die Vorlagerung eines abgesicherten VPN-Gateways mit entsprechenden Zugriffsbeschränkungen, um keinen externen Zugriff direkt über das Internet zu erlauben, wichtig und erforderlich, um hacktivistische Kampagnen mit medialer Wirkung weitestgehend verhindern zu können.

1.5.5 Zunehmende Auslagerung von Cyberangriffen

Staatliche Cyberakteurinnen und -akteure unterscheiden sich von Cyberkriminellen in mehrfacher Hinsicht. Dazu zählen sowohl die Absichten und Angriffsziele als auch die vorhandenen Ressourcen und Fähigkeiten. Während sich die Ziele und Handlungen staatlicher Akteurinnen und Akteure oftmals durch eine facettenreiche Motivlage – wirtschaftlich, politisch, militärisch, ideologisch – auszeichnen, sind Cyberkriminelle in aller Regel lediglich finanziell motiviert. Staatliche Cyberakteurinnen und -akteure fokussieren sich auf Angriffsziele mit strategischer Relevanz, insbesondere Regierungsbehörden, militärische Einrichtungen und Bereiche der kritischen Infrastruktur. Cyberkriminelle gehen hingegen vorwiegend opportunistisch vor. Sie greifen vor allem schlecht abgesicherte Ziele an, um möglichst hohe finanzielle Gewinne zu erzielen. Immer häufiger versuchen Cyberkriminelle mit Hilfe von kurzfristig publik gewordenen Sicherheitslücken rasch eine Vielzahl an IT-Systemen zu kompromittieren, um jegliche vorliegenden Zugangsdaten exfiltrieren zu können. Diese Informationen werden zeitnah im Darknet zum Verkauf angeboten und dienen für andere kriminelle oder staatliche Akteurinnen und Akteure als Eintrittsvektor bei Folgeangriffen in diese Zielsysteme. Obwohl grundsätzlich deutliche Unterscheidungsmerkmale vorliegen, geht der Trend in Richtung einer zunehmenden Kooperation zwischen staatlichen Akteurinnen und Akteuren und der organisierten Kriminalität.

Staatliche Cyberakteurinnen und -akteure gehen diese Kooperationen in erster Linie ein, um die eigene Schlagkraft zu erhöhen. Sie können so auf größere Personalressourcen zurückgreifen und auch technisches Know how einkaufen. Ein weiterer Vorteil liegt in

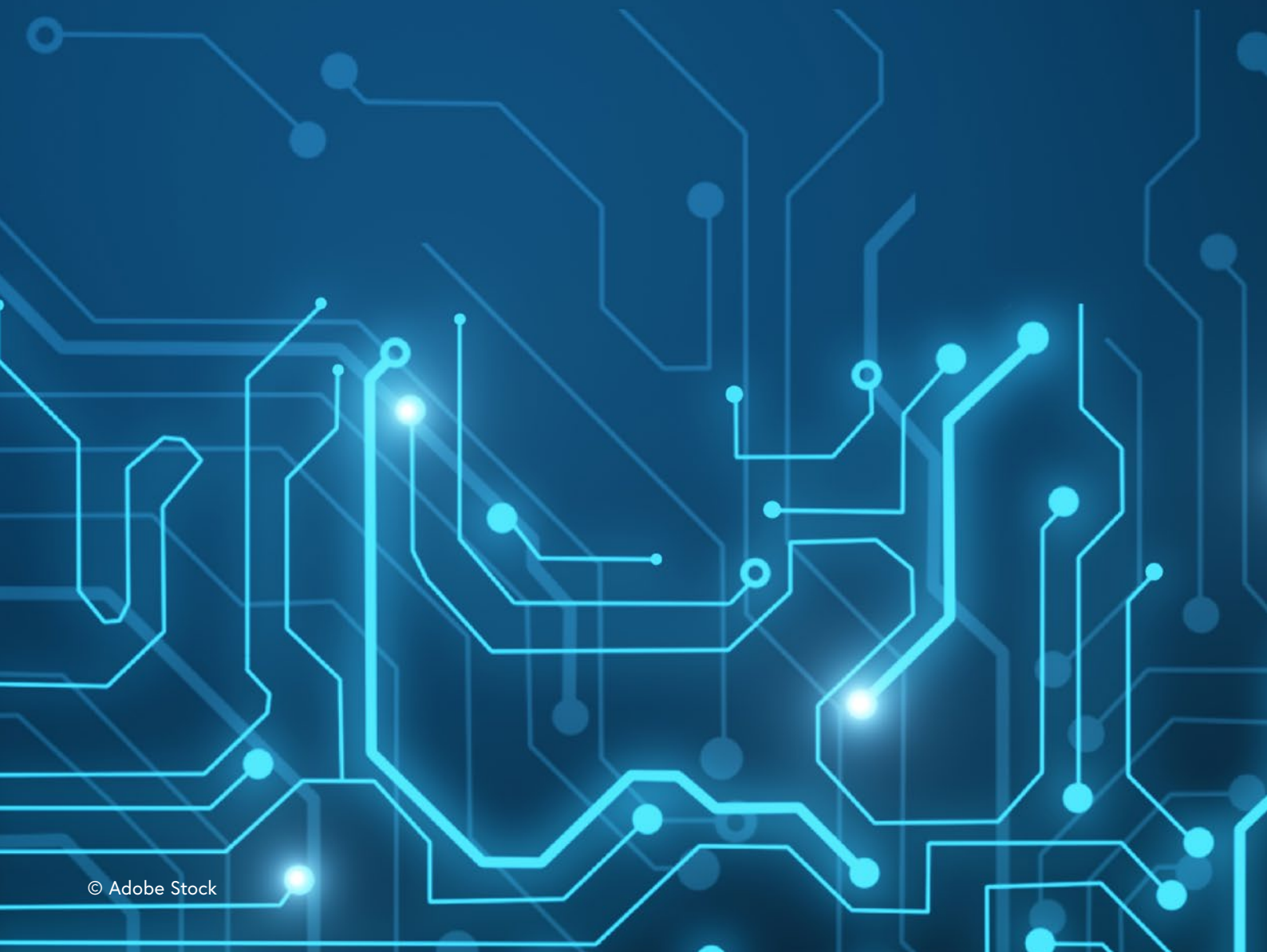
der Möglichkeit, die Verantwortung für Operationen abstreiten zu können, wenn sie an externe Stellen ausgelagert werden.

Bei der tatsächlichen Umsetzung derartiger Kooperationen gibt es unterschiedliche Ausprägungen. Während Russland stark mit Cyberkriminellen kooperiert, werden in China Cyberoperationen von Nachrichtendiensten an kommerzielle Dienstleister ausgelagert, die als mehr oder weniger private Unternehmen auftreten, in vielen Fällen jedoch eng mit dem staatlichen Sicherheitsapparat verwoben sind. Chinas Vorgehensweise, Cyberoperationen auszulagern, dürfte projektorientiert erfolgen, indem einzelne Kampagnen oder die verschiedenen Teile bzw. Phasen des Angriffs an unterschiedliche Dienstleister vergeben werden, die in der Folge als kurzlebige Akteurinnen und Akteure im Cyberraum auftreten. Die daraus resultierende Vielzahl miteinander vermischter Verfahren und Methoden hat zur Folge, dass sich Angriffe oft nur schwer einzelnen Gruppierungen zuordnen lassen. Die enge Verflechtung des kommerziellen Sektors mit dem staatlichen Sicherheitsapparat entspricht dem sogenannten „whole of society approach", bei dem sich private finanzielle und staatliche Interessen treffen.

Im Vergleich zu China besteht in Russland traditionell meist eine klare direkte Auftragsbeziehung zwischen privaten Cyberakteurinnen und -akteuren sowie Nachrichtendiensten. Dies äußert sich einerseits in der zunehmenden Auslagerung von Cyber-Enabled Information Operations an private und halbstaatliche Unternehmen. Andererseits werden Daten, die zuvor am Schwarzmarkt eingekauft wurden, immer häufiger bei Angriffen verwendet. Die nachrichtendienstliche Praxis russischer Cyberakteurinnen und -akteure nähert sich damit zusehends der chinesischen Vorgehensweise im Bereich der Cyberspionage an.

Die zunehmende Kooperation zwischen nachrichtendienstlichen Cyberakteurinnen und -akteuren und der organisierten Kriminalität bringt einige Herausforderungen mit sich. Zum einen wird die Attribution von Cyberangriffen aufgrund der kurzlebigen, projektbasierten Auslagerungen erschwert. Zum anderen findet auch ein Ressourcen- und Wissenstransfer in beide Richtungen statt. Dies wird bereits mittelfristig zu einer komplexeren Bedrohungslage im Cyberraum führen.

2 Internationale Entwicklungen



2.1 Europäische Union (EU)

Österreich setzt sich auf internationaler Ebene für ein freies, offenes und sicheres Internet ein, wobei die Einhaltung der Menschenrechte auch im virtuellen Raum gewährleistet sein muss. Dabei muss auf ein angemessenes Gleichgewicht zwischen den Interessen der Strafverfolgung und der Achtung grundlegender Menschenrechte wie dem Recht auf freie Meinungsäußerung und Informationsfreiheit sowie dem Recht auf Privatleben und Privatsphäre geachtet werden. Auch im Rahmen der Europäischen Union sind Cybersicherheit und Cyberdiplomatie in wichtiges Thema, das in einer Reihe von Gremien behandelt wird.

2.1.1 NIS-Kooperationsgruppe (inkl. Workstreams)

Die Kooperationsgruppe für Netz- und Informationssicherheit (NIS-Kooperationsgruppe) wurde durch die NIS-1-Richtlinie[5] eingesetzt und dient der Unterstützung und Erleichterung der strategischen Zusammenarbeit sowie des Informationsaustausches zwischen den Mitgliedstaaten. Sie setzt sich aus Vertreterinnen und Vertretern der Mitgliedstaaten, der Europäischen Kommission und der Agentur der Europäischen Union für Cybersicherheit (ENISA) zusammen. Der Vorsitz wird von der jeweiligen Ratspräsidentschaft gehalten.

Die NIS-Kooperationsgruppe nimmt ihre Aktivitäten auf der Grundlage von zweijährigen Arbeitsprogrammen wahr. Während das erste Arbeitsprogramm für den Zeitraum 2018 bis 2020 ein erster Schritt war, um die Arbeitsmethoden der NIS-Kooperationsgruppe zu gestalten, Vertrauen zwischen den Mitgliedstaaten aufzubauen und die dringendsten Ergebnisse im Zusammenhang mit der Umsetzung der NIS-Richtlinie zu erarbeiten, hat sich die NIS-Kooperationsgruppe mittlerweile als wichtiges Forum und Bezugspunkt für die Diskussion zur Umsetzung der Cybersicherheitspolitiken innerhalb der EU etabliert.

Das neue Arbeitsprogramm für den Zeitraum 2024 bis 2026 sieht, ähnlich wie die Vorgängerversion, die Umsetzung der NIS-2-Richtlinie[6] als oberste Priorität an und betont gleichzeitig auch die Wichtigkeit von strategischen Diskussionen über wichtige Aspekte der Cybersicherheit in der EU und Kooperation, wie beispielsweise koordinierte Risikobewertungen und die Entwicklung von gemeinsamen Instrumenten (bspw. „Toolboxen“) sowie die damit verbundene Zusammenarbeit sowohl innerhalb als auch außerhalb der EU.

Die NIS-Kooperationsgruppe traf sich im Jahr 2025 zu vier Plenarsitzungen, Work Streams hielten regelmäßige Sitzungen ab. Neben den Entwicklungen, die in diesen verschiedenen Arbeitsgruppen in Hinblick auf die Umsetzung der NIS-2-Richtlinie[7] erreicht wurden, konnte vor allem auch eine Vielzahl an Hilfsdokumenten fertiggestellt werden, so etwa

5 Richtlinie (EU) 2016/1148
6 Richtlinie (EU) 2022/2555
7 chtlinie (EU) 2022/2555

die EU-Roadmap zu Post-Quanten Kryptographie. Ein Pilot des Peer-Review-Prozesses der NIS-2-Richtlinie mit Zypern konnte ebenfalls im Rahmen des zuständigen Work Streams erfolgreich abgeschlossen werden.

Mehrere weitere Entwürfe befinden sich derzeit noch in Ausarbeitung, wie etwa eine vereinfachte Version des Referenzdokuments der Risikomanagementmaßnahmen, die ICT Supply Chain Toolbox und Risikobewertungen zu Connected Automated Vehicles und Detection Equipment.

2.1.2 Horizontal Working Party on Cyber Issues

Die Horizontale Arbeitsgruppe für Cyberangelegenheiten (Horizontal Working Party on Cyber Issues – HWP Cyber) wurde im Jahr 2016 eingerichtet. Sie ist für die Koordinierung der Arbeit des Rates der EU zu Cyberangelegenheiten, insbesondere mit Fokus auf politische und legislative Maßnahmen, zuständig. Sie legt die Cyberprioritäten und strategischen Ziele der EU als Teil eines umfassenden politischen Rahmens fest und gewährleistet eine Arbeitsplattform, die eine Harmonisierung und ein abgestimmtes Vorgehen in Fragen der Cyberpolitik ermöglicht.

Die Ratsarbeitsgruppe arbeitet eng mit anderen verwandten Arbeitsgruppen (bspw. Telekom, Data, Space) sowie der Europäischen Kommission (EK), dem Europäischen Auswärtigen Dienst (EAD), Europol, Eurojust, der European Union Agency for Fundamental Rights (FRA), der European Defence Agency (EDA), der EU-Cybersicherheitsagentur (ENISA) und dem Europäischen Kompetenzzentrum für Cybersicherheit (ECCC) zusammen. Es besteht auch eine enge Kooperation mit den weiteren EU-Stellen im Cybersicherheitsbereich, EU-CyCLONe (Europäisches Netzwerk der Verbindungsorganisationen für Cyberkrisen), dem CSIRTs-Netzwerk und der NIS-Kooperationsgruppe.

Insgesamt gab es 58 Sitzungen der HWP Cyber im Jahr 2025. Dies zeugt von der kontinuierlich hohen Arbeitsintensität zur Weiterentwicklung der europäischen Cybersicherheitspolitik. Den Vorsitz hatte im ersten Halbjahr Polen inne, bevor er im zweiten Halbjahr von Dänemark übernommen wurde. Im legislativen Bereich stand weiterhin vor allem die Umsetzung der Ende 2022 veröffentlichten NIS-2-Richtlinie, die Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union vorgibt, im Vordergrund, die primär im Zuge der NIS-Kooperationsgruppe bzw. deren Work Streams erfolgten (siehe 2.1.1).

Die relevanteste Initiative der HWP Cyber im Jahr 2025 war die Erarbeitung der Ratsempfehlung eines EU-Blueprints für das Cyberkrisenmanagement. Der Blueprint zielt darauf ab, ein Verfahren für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Cyberkrisen zu etablieren und die Rollen und Zuständigkeiten der beteiligten EU-Institutionen zu definieren. In der Empfehlung wird ein Rahmen für die Zusammenarbeit zwischen den involvierten EU-Institutionen, den Mitgliedsstaaten und anderen relevanten

Akteurinnen und Akteuren festgelegt. Dieser soll in regelmäßigen Cyberübungen getestet werden, um die Reaktionsfähigkeit der Akteurinnen und Akteure zu jedem Zeitpunkt gewährleisten zu können. Der Erstentwurf des PL-Ratsvorsitzes wurde am 24. Februar 2025 vorgestellt und anschließend intensiv diskutiert. In mehreren Feedbackschleifen wurde der Text kontinuierlich überarbeitet und den Mitgliedsstaaten die Möglichkeit gegeben, Verbesserungsvorschläge einzubringen. Nach ausführlichen Konsultationen wurde die Empfehlung schließlich am 6. Juni 2025 vom Rat der EU angenommen. Die erste Cyberübung zur Erprobung des Verfahrens auf politischer Ebene in der Praxis wurde im November im Rahmen der HWP Cyber durchgeführt. Die Ergebnisse samt extensiver Verbesserungsvorschläge und Lessons Learned wurden anschließend in einem Vorsitzbericht von DK festgehalten und in der HWP Cyber erörtert.

Ein weiterer Fokuspunkt der Arbeiten in der HWP Cyber im Jahr 2025 war der Aktionsplan für die Cybersicherheit von Krankenhäusern und Gesundheitsdienstleisterinnen und -dienstleistern (Health Care Action Plan). Er wurde am 27. Jänner 2025 in Form einer Empfehlung durch die Europäische Kommission vorgestellt. Es handelt sich dabei um ein nicht bindendes und non-legislatives Instrument. Der Aktionsplan zielt darauf ab, die Cybersicherheit und Resilienz im Gesundheitswesen zu stärken und die Abhängigkeit von externen Anbieterinnen und Anbietern in kritischen IKT-Bereichen zu reduzieren. Dafür wird ein breites Arsenal an verschiedenen Maßnahmen skizziert. Der Plan umfasst u. a. Maßnahmen zur Prävention von Cybersicherheitsvorfällen und zur Reaktion auf diese sowie zur Verbesserung des Informationsaustauschs. Die Implementierung des Aktionsplans soll in enger Kooperation mit der ENISA erfolgen. Der Aktionsplan wurde im Rahmen der HWP Cyber vor allem in der ersten Jahreshälfte viel diskutiert. Die Ergebnisse wurden in einem Bericht der PL-Präsidentschaft zusammengefasst. In der zweiten Jahreshälfte fand darüber hinaus eine öffentliche Begutachtung statt, deren Ergebnisse im Rahmen eines DK-Vorsitzberichtes in der HWP Cyber erörtert wurden.

Darüber hinaus wurden von der HWP Cyber im Jahr 2025 auch Vorbereitungsarbeiten für die Vereinfachungsinitiative der Europäischen Kommission im Rahmen des digitalen Omnibusses geleistet. In einer gemeinsamen Sitzung mit der Arbeitsgruppe Data Protection wurden die Ansichten der Mitgliedstaaten zur möglichen Einführung eines „Single-EntryPoint“ für Meldeverpflichtungen ausgetauscht. Diese wurden anschließend in einem Vorsitzbericht festgehalten und im Rahmen der HWP Cyber erörtert und diskutiert. Der gesammelte Input der Mitgliedsstaaten wurde von der Europäischen Kommission teilweise im Vorschlag zum Digital Omnibus, der im November 2025 veröffentlicht wurde, aufgegriffen.

Zu den Arbeiten der HWP Cyber im Bereich der Cyberdiplomatie darf auf Punkt 2.1.10 verwiesen werden.

2.1.3 Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats

Die Horizontale Arbeitsgruppe zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen (HWP ERCHT) wurde im Jahr 2019 eingerichtet. Der Fokus der Arbeit liegt auf der Verbesserung der Resilienz der EU und ihrer Mitgliedstaaten, dem gemeinsamen Vorgehen bei der Abwehr von hybriden Bedrohungen sowie der Bekämpfung von Desinformation. Cyber zählt zu den 13 Domänen hybrider Bedrohungen und stellt häufig ein Schlüsselelement hybrider Einflussnahme dar. Die Arbeitsgruppe dient der Koordinierung innerhalb des Rates und der Zusammenarbeit mit anderen Organen, Diensten und Agenturen der EU.

In Umsetzung des Strategischen Kompasses für Sicherheit und Verteidigung wurde 2022 ein **EU-Instrumentarium für eine koordinierte Reaktion der EU** auf gegen sie und ihre Partnerinnen und Partner gerichtete **hybride Bedrohungen („EU Hybrid Toolbox“)** entwickelt. Diesbezügliche Ratsschlussfolgerungen und Durchführungsleitlinien sehen unter anderem ein gemeinsames Lagebild, einen gemeinsamen Entscheidungsfindungsprozess sowie mögliche Antworten in Bezug auf hybride Bedrohungsakteurinnen und -akteure vor. Bei Cyberangriffen als Teil einer hybriden Kampagne wird das Vorgehen mit der HWP Cyber Issues koordiniert. Ein Beispiel für den Einsatz der Hybrid Toolbox ist das Statement der Hohen Vertreterin zur Verurteilung von Russlands persistenten hybriden Kampagnen gegen die EU, ihre Mitgliedstaaten und Partnerinnen und Partner vom 18. Juli 2025.

Um die Reaktionsfähigkeiten der EU auf hybride Bedrohungen zu verbessern, sieht der Strategische Kompass zudem die Schaffung von **EU-Schnelleinsatzteams für hybride Bedrohungen (Hybrid Rapid Response Teams - HRRT)** vor. Diese sollen sich auf einschlägige nationale und EU-interne zivile und militärische Fachexpertise, z. B. im Cybersicherheitsbereich, stützen, um EU-Mitgliedstaaten, Partnerländer sowie GSVP-Missionen und Operationen bei der Abwehr hybrider Bedrohungen zu unterstützen.

Im April/Mai 2025 fand der erste Einsatz eines HRRT zur Unterstützung von Moldau in Vorbereitung der Parlamentswahlen (28. September 2025) statt. Das Missionskonzept umfasste Unterstützung in den Bereichen Cybersicherheit (Wahlinfrastruktur), strategische Kommunikation und Bekämpfung von FIMI sowie Krisenmanagement.

Weitere thematische Schwerpunkte im Jahr 2025 umfassten die **Stärkung der demokratischen Resilienz, hybride Bedrohungen gegenüber kritischer Infrastruktur** sowie **ausländische Informationsmanipulation und Einmischung (FIMI)**. In allen diesen Schwerpunkten standen auch Cyber-Aspekte im Fokus.

2.1.4 Netz nationaler Koordinierungszentren und Europäisches Kompetenzzentrum

Das Europäische Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (European Cybersecurity Industrial, Technology and Research Competence Centre - ECCC) erlangte im Jahr 2024 nach intensiven Aufbauaktivitäten seine finanzielle Autonomie und bezog mit rund 30 Mitarbeitenden Büroräumlichkeiten in Bukarest in Rumänien. Damit ist es nun in der Lage, seinen Auftrag gemäß der Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 vollumfänglich zu erfüllen. Diese Verordnung sieht die Einrichtung des ECCC und des Netzwerks nationaler Koordinierungszentren (National Coordination Centres - NCC) vor, um den Kompetenzaufbau sowie die Steigerung der Resilienz, digitaler Souveränität und Wettbewerbsfähigkeit der EU im Bereich Cybersicherheit zu erfüllen.

Das ECCC verantwortet und implementiert das EU-Finanzierungsprogramm „Digitales Europa (DEP)“ im Bereich der Cybersicherheit und wickelt das EU-Forschungsförderungsprogramm Horizont Europa im Bereich Cybersicherheit ab. Es erstellt des Weiteren einen Rahmen für die Steigerung und Koordinierung von Investitionen in die Cybersicherheit zwischen der EU, den Mitgliedstaaten und indirekt der Industrie. In diesem Zusammenhang ist es der Auftrag des ECCC und des Netzwerks, die EU zu unterstützen. Dies erfolgt durch:

- Stärkung ihrer Führungsrolle im Bereich der Cybersicherheit, um das Vertrauen und die Sicherheit, einschließlich der Vertraulichkeit, Integrität und Zugänglichkeit von Daten, zu steigern;
- Förderung der Abwehrfähigkeit und Zuverlässigkeit der Netz- und Informationssysteme, darunter der kritischen Infrastruktur und gängiger Hard- und Software;
- Steigerung der globalen Wettbewerbsfähigkeit und der hohen Standards der Cybersicherheitsbranche der EU sowie der Verwandlung der Cybersicherheit in einen Wettbewerbsvorteil für andere Wirtschaftszweige der EU.

Das ebenfalls mit der Verordnung eingerichtete Netzwerk nationaler Koordinierungszentren unterstützt das ECCC bei seinen Aufgaben und soll sich auf nationaler Ebene für die Entwicklung neuer Cybersicherheitskapazitäten und den weiteren Kompetenzausbau einsetzen sowie die nationale Cybersicherheits-Community europäisch vernetzen. In Österreich wurde im Berichtszeitraum das Nationale Koordinierungszentrum (NCC) vom BKA in Kooperation mit der Österreichischen Forschungsförderungsgesellschaft (FFG) betrieben. Mit dem Bundesgesetz über die Zahl, den Wirkungsbereich und die Einrichtung der Bundesministerien (Bundesministeriengesetz 1986 – BMG) idF BGBl. I Nr. 10/2025 sind die Zuständigkeiten mit November 2025 dem Bundesministerium für Inneres übertragen worden.

Der Verwaltungsrat (Governing Board) des ECCC fand sich unter Teilnahme des Bundeskanzleramts und des Bundesministeriums für Inneres zusammen. Dabei erarbeitete das ECCC gemeinsam mit den Mitgliedstaaten einen Entwurf für das Arbeitsprogramm Cybersicherheit 2025 bis 2027 des EU-Förderprogrammes „Digitales Europa“ (DEP) entlang der 2023 verabschiedeten Strategischen Agenda und überführte die Arbeitsgruppen des ECCC-Verwaltungsrats in folgende neue Struktur: Es gibt nun Arbeitsgruppen zu

1. Community Building
2. Boost application process
3. International awareness
4. Strategic advice
5. Cyber Skills
6. Cyber Hubs.

Das NCC nahm an Sitzungen des NCC-Netzwerkes und von ECCC-Arbeitsgruppen aktiv teil. Diese umfassten insbesondere die ECCC-Arbeitsgruppen zu Cybersecurity Skills (Nr. 5) und zur Einrichtung der Europäischen Kompetenzgemeinschaft (Nr. 1).

Ein konkretes Beispiel sind zwei Projekte zum Aufbau von grenzüberschreitender Security Operation Center (SOC) Infrastruktur zwischen Mitgliedstaaten, wodurch zukünftig (Bedrohungs-)Informationen zu Cyberaktivitäten ausgetauscht werden können. Die an den Projekten teilnehmenden Mitgliedstaaten beschaffen gemeinsam mit dem ECCC mit DEP-Mitteln Infrastruktur. Diese Projekte sollen in weiterer Folge bei der Durchführung des Cyber Solidarity Acts unterstützen.

Im Jahr 2025 wurde durch die European Cybersecurity Competence Centre (ECCC) in enger Kooperation mit den Nationalen Koordinierungszentren (NCC) das ATLAS-Tool entwickelt und veröffentlicht. Ziel dieses Instruments ist der Ausbau und die Stärkung der NCC-Community auf europäischer Ebene. Der European Cybersecurity ATLAS ist eine gemeinschaftliche Plattform, die dazu dient, Unternehmen im Rahmen der Europäischen Kompetenzgemeinschaft für Cybersicherheit (Cybersecurity Competence Community – CCC) zu vernetzen und soll insbesondere die österreichische Cybersicherheitsgemeinschaft gezielt mit europäischen Akteurinnen und Akteuren verbinden. Darüber hinaus verfolgt das Tool das Ziel, die internationale Sichtbarkeit der beteiligten Organisationen zu erhöhen sowie den Zugang zu Informationen über neue Technologien, innovative Prozesse und potenzielle Marktchancen zu erleichtern. Auf diese Weise soll die grenzüberschreitende Zusammenarbeit gefördert und die Wettbewerbsfähigkeit im Bereich der Cybersicherheit nachhaltig gestärkt werden.

2.1.5 EU-CyCLONe

Das Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe = European Cyber Crisis Liaison Organisation Network) dient zur Unterstützung des koordinierten Managements Cybersicherheitsvorfälle großen Ausmaßes und Krisen auf operativer Ebene.

Im Jahr 2019 als informelle freiwillige Kooperation formiert, wurde EU-CyCLONe mit Inkrafttreten der NIS-2-Richtlinie am 16. Jänner 2023 offiziell eingerichtet. Ziel ist es, die Kooperation und Koordination zwischen EU-Mitgliedstaaten sowie EU-Institutionen und -Organen zu stärken und als operative Schnittstelle zwischen der technischen und der politischen Ebene zu fungieren.

Zu den Hauptaufgaben zählen eine verbesserte Vorbereitung auf die Bewältigung großflächiger Cybersicherheitsvorfälle und Krisen, die Entwicklung eines gemeinsamen europäischen Lagebildes, die Beurteilung von Folgen und Auswirkungen sowie die Erstellung von Vorschlägen für Abhilfemaßnahmen. Darüber hinaus soll die Koordinierung des Krisenmanagements und die Unterstützung der Entscheidungsfindung auf politischer Ebene gewährleistet werden.

Die Mitglieder von EU-CyCLONe nehmen regelmäßig an europaweiten (Cyber-)Krisenübungen teil, wie etwa an der jährlichen „BlueOLEx“ (nähere Informationen dazu im Kapitel „Cyberübungen“). Im Juni 2025 wurde der EU-Blueprint für Cybersicherheitskrisenmanagement (kurz Cyber Blueprint) veröffentlicht, der den EU-Rahmen für das Krisenmanagement darstellt und Leitlinien für die Reaktion der EU auf massive Cybersicherheitsvorfälle enthält. Neben der Darstellung von EU-CyCLONe hierin als ein zentraler Akteur, erhielt das Netzwerk mit dem Cyber Blueprint zusätzliche Aufgaben, u. a. die Erstellung einer gemeinsamen Taxonomie für den Schweregrad von Vorfällen, um zu einem verbesserten Informationsaustausch beizutragen.

Österreich wird im EU-CyCLONe durch das Innenministerium vertreten.

2.1.6 Computer-Security-Incident-Response-Teams-Netzwerk (CSIRTs-Netzwerk)

Das Netzwerk der Computer-Security-Incident-Response-Teams (CSIRTs-Netzwerk oder CNW) wurde durch die EU-Richtlinie 2016 / 1148 (NIS-1-Richtlinie) geschaffen, die dessen Tätigkeitsbereich festgelegt. Die EU-Richtlinie 2022 / 2555 (NIS-2-Richtlinie) hat, basierend auf den Erfahrungen der ersten Jahre, die Aufgaben des CNW etwas erweitert.

Das CSIRTs-Netzwerk setzt sich aus Vertreterinnen und Vertretern der CSIRTs der Mitgliedstaaten und dem CERT der EU-Institutionen (CERT-EU) zusammen. Die Europäische Kommission (EK) nimmt als Beobachterin am CSIRTs-Netzwerk teil. Die EU-Cybersicherheitsagentur (ENISA) führt die Sekretariatsgeschäfte und unterstützt aktiv die

Zusammenarbeit zwischen den CSIRTs. Anfang 2026 schlägt die europäische Kommission im Rahmen eines Cybersicherheitspakets vor, ENISA als vollwertiges Mitglied in das CNW aufzunehmen. Ob dieser Vorschlag zukünftig Umsetzung erfährt, wird sich weisen. Österreich ist im CSIRTs-Netzwerk durch das GovCERT Austria, dem Austrian Energy CERT (AEC), dem Austrian HealthCERT (AHC) und dem nationalen Computer-Notfallteam CERT.at vertreten.

Das Netzwerk arbeitet primär online, die vertretenen CSIRTs kooperieren laufend miteinander. Auf freiwilliger Basis werden Informationen zu relevanten Sicherheitsvorfällen ausgetauscht und Erkenntnisse zur Sicherheit von Netz- und Informationssystemen erörtert.

Die Treffen des CNW dienen dem Informationsaustausch bezüglich der Dienste, Tätigkeiten und Kooperationsfähigkeiten der CSIRTs. Zentrale Aufgabe des CNW ist der Auf- und Ausbau von Vertrauen zwischen den Mitgliedstaaten sowie die Förderung einer schnellen und effektiven operativen Zusammenarbeit. Dies dient der Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz und Informationssystemen in der EU.

Das Netzwerk trifft sich in der Regel dreimal pro Jahr. 2025 fanden diese Treffen im Jänner in Brüssel, im Mai in Krakau und im September in Kopenhagen statt. Im November 2025 wurde die vertiefte Zusammenarbeit, im Zusammenhang mit dem Cyberkrisenmangement auf Unionsebene, im Rahmen der Übung „CyberSOPEx 2025“ geprobt.

2.1.7 EU-Zertifizierungsrahmen (Cybersecurity Act)

Der europäische Rechtsakt zur Cybersicherheit (Cybersecurity Act), der bereits im Jahr 2019 in Kraft getreten ist, etabliert unter anderem einen europäischen Zertifizierungsrahmen für Cybersicherheit. Dieser legt einen Mechanismus fest, mit dem europäische Schemata für die Cybersicherheitszertifizierung geschaffen werden. In weiterer Folge soll der europäische Zertifizierungsrahmen für Cybersicherheit bescheinigen, dass IKT-Produkte, -Dienste und -Prozesse, die nach einem solchen Schema bewertet wurden, den darin festgelegten Sicherheitsanforderungen genügen. Anbieterinnen und Anbieter sowie Herstellerinnen und Hersteller von IKT-Produkten, -Diensten und -Prozessen können sich zukünftig freiwillig für eine Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen entscheiden. Ein Cybersicherheitszertifikat wird EU-weit anerkannt. Durch den Nachweis, dass ein Produkt die angegebenen Sicherheitsfunktionen erfüllt oder bestimmte Sicherheitsanforderungen einhält, kann eine Cybersicherheitszertifizierung wesentlich dazu beitragen, das Vertrauen in IKT-Produkte, -Dienste und -Prozesse zu stärken und damit das ordnungsgemäße Funktionieren des digitalen Binnenmarktes zu gewährleisten.

Die Europäische Gruppe für die Cybersicherheitszertifizierung (European Cybersecurity Certification Group - ECCG) wurde durch den Cybersecurity-Act eingesetzt und nahm

ihre Arbeit im Jahr 2019 auf. Die ECCG setzt sich aus Vertreterinnen und Vertretern der nationalen Behörden für die Cybersicherheitszertifizierung oder anderer relevanter nationaler Behörden zusammen. Österreich wird in der ECCG durch das Bundeskanzleramt (BKA) vertreten. Die ECCG traf sich im Jahr 2025 zu vier Plenarsitzungen.

Des Weiteren führt die im Jahr 2020 eingerichtete Gruppe der Interessenträger für die Cybersicherheitszertifizierung (Stakeholders Cybersecurity Certification Group - SCCG) unter dem gemeinsamen Vorsitz der Europäischen Kommission (EK) und der EU-Cybersicherheitsagentur (ENISA) ihre Arbeit fort. Die SCCG setzt sich unter anderem aus Vertreterinnen und Vertretern aus akademischen Einrichtungen, Verbraucherschutzorganisationen, Konformitätsbewertungsstellen, Organisationen, die Normen entwickeln, Unternehmen und Handelsverbänden zusammen und soll in strategischen Fragen der Cybersicherheitszertifizierung beraten.

Am 27. Februar 2025 ist die Durchführungsverordnung für das erste europäische Schema für die Cybersicherheitszertifizierung „European Union Common Criteria Scheme“ (EUCC) in Geltung getreten. Das EUCC basiert auf Freiwilligkeit und ermöglicht es den Herstellerinnen und Herstellern sowie Anbieterinnen und Anbietern, die die Cybersicherheit ihrer Produkte nachweisen wollen, ihre IKT-Produkte, -Dienste oder -Prozesse in einem europaweiten einheitlichen Bewertungsverfahren von einer Konformitätsbewertungsstelle zertifizieren zu lassen.

Die Arbeiten zum „European Union Cybersecurity Certification Scheme on Cloud Services“ (EUCS), das die Zertifizierung von Clouddiensten zum Gegenstand hat, sowie zum „EU5G“, das die Cybersicherheit von 5G-Netzwerken zum Gegenstand hat, dauern nach wie vor an.

Die Europäische Kommission hat am 20. Jänner 2026 ein neues Cybersicherheitspaket vorgelegt, um die Cyber-Resilienz der EU angesichts wachsender Cybersicherheitsbedrohungen weiter zu stärken. Dieses umfasst einen Vorschlag zur Überarbeitung des Cybersecurity Acts (Cyber Security Act 2, CSA 2). Durch den CSA 2 soll die Sicherheit der Informations- und Kommunikationstechnologie-Lieferketten in der EU verbessert werden. Durch ein vereinfachtes Zertifizierungsverfahren soll sichergestellt werden, dass Produkte von Anfang an cybersicher sind. Zudem soll die Einhaltung bestehender EU-Cybersicherheitsvorschriften erleichtert und die Rolle der Europäischen Agentur für Cybersicherheit (ENISA) bei der Unterstützung der Mitgliedstaaten und der EU beim Umgang mit Cybersicherheitsbedrohungen gestärkt werden.

2.1.8 CRA Expert Group

Die „Expert Group on Cybersecurity of Products with Digital Elements (CRA Expert Group, Art 9, (EU) 2024/2847)“ wurde geschaffen, um die Zusammenarbeit und den Austausch

von Informationen und Fachwissen zwischen der Kommission und den Stakeholdern zu erleichtern.

Die Expertengruppe stellt ein wertvolles Forum für die Kommission dar, um Beiträge einschlägiger Interessensträgerinnen und -träger einzuholen und zur erfolgreichen Umsetzung des Cyber Resilience Act beizutragen, einer Verordnung, die gewerblichen Nutzerinnen und Nutzern sowie Verbraucherinnen und Verbrauchern zugutekommt, indem sie die Transparenz der Sicherheitseigenschaften erhöht und das Vertrauen in Produkte mit digitalen Elementen fördert und zur Steigerung des Wettbewerbs- und Innovationspotenzials der EU beiträgt.

Den Vorsitz der Gruppe führt ein Vertreter der Generaldirektion Kommunikationsnetze, Inhalte und Technologien (DG CONNECT) der Europäischen Kommission.

Das erste Meeting der CRA Expert Group hat am 12. Februar 2025 stattgefunden. Insgesamt traf sich die CRA Expert Group Jahr 2025 zu drei Plenarsitzungen sowie zu einer Vielzahl von Sub-Arbeitsgruppen, die sich im Detail mit speziellen Bereichen des Cyber Resilience Act beschäftigten, wie etwa mit der Marktüberwachung, den notifizierenden Behörden und technischen Beschreibungen. Weitere Sub-Arbeitsgruppen betreffend Open Source und Risikobewertung sind für das Jahr 2026 geplant.

2.1.9 Cyberverteidigung auf europäischer Ebene

Die Cyberverteidigung auf europäischer Ebene wurde im Jahr 2025 im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) weiter umgesetzt und konsolidiert. Der Schwerpunkt lag auf der operativen Umsetzung bestehender politischer Vorgaben, der Weiterentwicklung militärischer Koordinierungsstrukturen sowie der stärkeren Berücksichtigung der Cyberdimension in Planung, Führung, Ausbildung und Übung.

Cyberverteidigungsthemen wurden weiterhin auf politisch-militärischer Ebene im Militärausschuss der Europäischen Union (EUMC) sowie in nachgeordneten militärischen Arbeitsformaten behandelt. Dabei standen insbesondere die Resilienz militärischer Führungs- und Informationssysteme, die Einbindung von Cyberbedrohungen in militärische Planungsprozesse sowie die Weiterentwicklung gemeinsamer Verfahren im Fokus. Cyberverteidigung blieb ein Querschnittsthema der militärischen Fähigkeits- und Einsatzplanung.

Im operativen Bereich wurden Cyberaspekte auch 2025 systematisch in die Arbeit der Military Planning and Conduct Capability (MPCC) integriert. Dies betraf insbesondere den Schutz von Kommunikations- und Informationssystemen (CIS) bei GSVP-Missionen und Operationen sowie die Berücksichtigung von Cyberrisiken im missionsbezogenen Risikomanagement. Die Zusammenarbeit zwischen der MPCC und den militärischen Cyberfachstellen der Mitgliedstaaten wurde fortgeführt.

Ein zentraler Entwicklungsschwerpunkt im Jahr 2025 war das Projekt Cyber and Information Domain Coordination Centre (CIDCC) der Ständig Strukturierten Zusammenarbeit (PESCO). Ziel des Projekts ist der Aufbau einer multinationalen Koordinierungs- und Analysefähigkeit zur Unterstützung der militärischen Planung und Führung durch strukturierte Lage- und Analyseprodukte aus dem Cyber- und Informationsraum. Im Berichtsjahr hat das CIDCC durch analytische Produkte (One Pager, Country Books, Actor Analyses, wöchentliche Updates, Bedrohungsberichte) konkrete Informationslücken für EU-Hauptquartiere geschlossen. In realen Operationen wie „EUNAVFOR ASPIDES“ sowie in Übungen wie „MILEX 2024“ erwiesen sich diese Produkte als entscheidend für operative Planung, Risikoeinschätzung und Entscheidungsfindung. Die operativen Führungskommanden (OHQs) bestätigten, dass durch das CIDCC erstmals ein konsistentes Lagebild im Cyber- und Informationsraum zur Verfügung stand – ein bisher fehlender Beitrag, der die Wirksamkeit von GSVP-Missionen erheblich gesteigert hat.

Entsprechend wurde parallel dazu 2025 in einschlägigen EU-Gremien die Weiterentwicklung des CIDCC in Richtung eines EU Cyber Defence Coordination Centre (EUCDCC) behandelt. Ziel dieser Entwicklung ist es, die im Rahmen des PESCO-Projekts aufgebauten Strukturen und Verfahren perspektivisch in eine dauerhafte europäische Koordinierungsfähigkeit zu überführen. Dabei wurden insbesondere Fragen der Aufgabenabgrenzung, der Einbindung in bestehende militärische Strukturen sowie der Schnittstellen zu anderen EU-weiten Lage- und Koordinierungsmechanismen berücksichtigt.

Im Bereich der Fähigkeitsentwicklung wurden unter Koordinierung der Europäischen Verteidigungsagentur (EDA) auch 2025 laufende Aktivitäten zur militärischen Cyberverteidigung fortgeführt. Diese umfassten insbesondere die Harmonisierung von Ausbildungsanforderungen, die Identifikation militärischer Fähigkeitsbedarfe sowie den Austausch bewährter Verfahren. Ergänzend dazu wurden einschlägige cyberbezogene Projekte im Rahmen von PESCO weitergeführt, mit dem Ziel, Interoperabilität und kooperative Fähigkeiten im militärischen Cyberbereich zu stärken.

Ein weiterer Schwerpunkt lag 2025 im Bereich der Ausbildung und Übung. Cyberverteidigungsaspekte wurden in militärischen EU-Übungs- und Ausbildungsformaten systematisch berücksichtigt und zunehmend in multidimensionale Szenarien integriert. Ziel war es, Führungs- und Entscheidungsprozesse unter Cyberbedrohungen zu erproben, die Zusammenarbeit zwischen den Mitgliedstaaten zu stärken sowie Schnittstellen zwischen strategischer, operativer und technischer Ebene zu testen. Erkenntnisse aus diesen Übungen fließen in die Weiterentwicklung von Verfahren und Analyseprozessen ein, unter anderem im Zusammenhang mit den im CIDCC erprobten Arbeitsweisen.

Die zivil-militärische Koordinierung blieb auch 2025 ein wesentlicher Bestandteil der europäischen Cyberverteidigung. Die Abstimmung mit zivilen EU-Strukturen im Bereich der Cybersicherheit und des Cyberkrisenmanagements wurde fortgeführt, um kohärente

Reaktionen auf Cybervorfälle mit möglichen zivilen und militärischen Auswirkungen sicherzustellen.

Die Zusammenarbeit mit der NATO wurde im Berichtsjahr im Sinne eines komplementären Ansatzes weitergeführt. Der Informationsaustausch sowie die Berücksichtigung kompatibler Standards und Übungsformate trugen zur Stärkung der kollektiven Cyberresilienz bei.

Österreich beteiligte sich 2025 in den relevanten EU-Gremien, Projekten sowie an Ausbildungs- und Übungsaktivitäten im Bereich der Cyberverteidigung. Die Mitwirkung erfolgte im Einklang mit den Vorgaben der GSVP sowie den nationalen verfassungsrechtlichen Rahmenbedingungen.

2.1.10 Cyberdiplomatie auf europäischer Ebene

Die 2017 eingerichtete EU Cyber Diplomacy Toolbox ist ein Rahmenwerk für die gemeinsame Antwort auf Cyberbedrohungen gegen die Sicherheit der EU und der Mitgliedstaaten: Das gesamte Spektrum der Maßnahmen der Gemeinsamen Außen- und Sicherheitspolitik (GASP) kann auch im Cyberbereich genutzt werden. Die Cyber Diplomacy Toolbox umfasst präventive, kooperative, stabilisierende und restriktive Maßnahmen. Zu den Werkzeugen zählen beispielsweise öffentliche Erklärungen und Demarchen, Cyberdialoge, Beiträge zum Cyber-Kapazitätenaufbau in Partnerstaaten und Sanktionen. Ein häufig genutztes Werkzeug der Cyber Diplomacy Toolbox sind gemeinsame Erklärungen („naming and shaming"): So verteilten die EU und EU-MS am 28. Mai 2025 in einer gemeinsamen Erklärung eine Cyberspionagekampagne gegen das tschechische Außenministerium, die dem chinesischen Ministerium für Staatssicherheit zugeschrieben wurde. Das seit Mai 2019 bestehende Cyber-Sanktionenregime wird regelmäßig überprüft und erweitert. Zuletzt wurden am 27. Jänner 2025 drei Personen für ihre Beteiligung an russischen Cyberangriffen auf Estland gelistet. Insgesamt waren mit Ende des Berichtszeitraums 17 Personen und vier Entitäten von den restriktiven Maßnahmen erfasst.

Ein wichtiger Teil der Cyberdiplomatie auf EU-Ebene ist die Erarbeitung gemeinsamer Positionen und Strategien zu Cyberthemen auf internationaler Ebene, allen voran im Rahmen der Vereinten Nationen (siehe 2.2). Standard- und Normensetzung für neue Technologien und Cyberaktivitäten sind längst geopolitische Konfliktzonen und die Zunahme an Cyberangriffen durch staatlich gelenkte Akteurinnen und Akteure ist Teil der geopolitischen Polarisierung. Mit dem Anspruch einer EU-Führungsrolle auf internationaler und regionaler Ebene soll die EU-Vision für das globale, sichere, freie und offene Internet verankert und dabei sichergestellt werden, dass sich neue Technologien auf Menschen und den Schutz ihrer Privatsphäre fokussieren und ihr Einsatz rechtmäßig und ethisch korrekt erfolgt.

Die zuständige Ratsarbeitsgruppe für die Koordination der EU-Cyberdiplomatie ist die Horizontal Working Party Cyber Issues, die die zwei Arbeitsstränge Cyberdiplomatie

und Cybersicherheit umfasst. Zu den Arbeiten der HWP CI im Bereich Cybersicherheit siehe oben (2.1.2).

2.2 Vereinte Nationen (VN)

Auf VN-Ebene verfolgt das 1. Komitee (Abrüstung und internationale Sicherheit) der Generalversammlung der Vereinten Nationen (VN-GV) das Ziel, die aus der Nutzung von Informations- und Kommunikationstechnologie (IKT) entstehenden Risiken für die internationale Sicherheit und Stabilität zu minimieren. Das Mandat der dazu eingerichteten Open-Ended Working Group (OEWG) zu Cybersicherheit 2021 bis 2025 endete im Sommer 2025. Der Abschlussbericht zeigte vier prioritäre Handlungsbereiche für die weitere Arbeit auf: Völkerrecht, nicht-bindende Normen für verantwortungsvolles Staatenverhalten, vertrauensbildende Maßnahmen (VBM) und Aufbau von Kapazitäten.

Im Herbst 2025 wurde durch Resolutionsannahme im 1. Komitee eine permanente Nachfolgestruktur zur OEWG eingerichtet: der „Globale Mechanismus zu Entwicklungen im Bereich von IKT im Kontext von internationaler Sicherheit und zum Voranbringen von verantwortlichem Staatenverhalten in der Nutzung von IKT“ (kurz: Globaler Mechanismus). Der Globale Mechanismus wird die Arbeit der OEWG zu Normen, Völkerrecht, vertrauensbildenden Maßnahmen und Kapazitätsaufbau weiterführen; die erste organisatorische Sitzung wird Ende März 2026 stattfinden.

Für Fragen der Internet Governance ist neben den VN-Spezialorganisationen und dem WSIS-Forum das Internet Governance Forum (IGF) die bedeutendste globale Multistakeholder-Plattform für Diskussionen und Austausch unter den relevanten Akteurinnen und Akteuren, einschließlich Regierungen, Zivilgesellschaft, Privatsektor, Wissenschaft und technischen Gemeinschaften. Das IGF befasst sich mit aktuellen Herausforderungen der Internetpolitik und der digitalen Transformation wie künstliche Intelligenz, Plattformregulierung, Datenwirtschaft, Cybersicherheit sowie nachhaltige Digitalisierung. Am 16. und 17. Dezember 2025 fand in New York ein hochrangiges Treffen zur Überprüfung der Umsetzung des Weltinformationsgipfels (World Summit on the Information Society, WSIS+20) statt, wo u. a. dem IGF ein permanentes Mandat verliehen wurde.

Der Anstieg und die zunehmende Komplexität der Cyberkriminalität wurden 2025 in allen relevanten Gremien thematisiert, darunter in der Kommission für Verbrechensverhütung und Strafrechtspflege (CCPCJ) und in der 11. Vertragsstaatenkonferenz des VN-Übereinkommens gegen Korruption (UNCAC CoSP).

Das VN-Büro für Drogen- und Verbrechensbekämpfung (UNODC) in Wien ist eine tragende Säule der effektiven weltweiten Bekämpfung von Cyberkriminalität. Durch das „Global Programme on Cybercrime“ erhalten Staaten aktive und gezielte Unterstützung bei der

Stärkung nationaler Kapazitäten im Kampf gegen Cyberkriminalität. UNODC unterstützt Mitgliedstaaten auch im Bereich der Prävention und Bewusstseinsbildung.

Im Jahr 2025 standen die Vorbereitung und Einleitung der Umsetzung der VN-Cybercrimekonvention im Mittelpunkt der internationalen Bemühungen zur Bekämpfung der Cyberkriminalität. Nach Abschluss der Verhandlungen über den Text, die von Februar 2022 bis August 2024 in Wien und New York stattfanden, konnte die VN-GV am 24. Dezember 2024 die VN-Cybercrimekonvention im Konsens annehmen. Österreich hatte sich in den Verhandlungen zusammen mit seinen internationalen Partnerinnen und Partnern erfolgreich dafür eingesetzt, dass die VN-Konvention starke menschenrechtliche Bestimmungen enthält. Österreich unterzeichnete die Konvention als einer der ersten Staaten im Rahmen der Unterzeichnungskonferenz am 25. Oktober 2025 in Hanoi, Vietnam. Insgesamt haben bisher 74 VN-Mitgliedsstaaten die Konvention unterzeichnet, die 90 Tage nach der Ratifizierung durch den 40. Mitgliedstaat in Kraft treten wird. Ab Herbst 2025 fanden (im Vorfeld der Verhandlungen im Jänner 2026) informelle Vorgespräche zur Verhandlung der Verfahrensordnung der künftigen Vertragsstaatenkonferenz statt. Österreich setzt sich dabei gemeinsam mit Gleichgesinnten für eine effektive Stakeholder-Beteiligung ein und wird in weiterer Folge auch in der Umsetzung für einen effektiven, inklusiven und transparenten Mechanismus eintreten.

Als Sekretariat für die Umsetzung des VN-Übereinkommens übernimmt UNODC eine zentrale Rolle, wodurch die VN-Kompetenz im Bereich der Cyberkriminalitätsbekämpfung sowie der Amtssitz Wien weiter gestärkt werden. Damit wird ein weiteres Zukunftsthema dauerhaft in Wien verankert und der Amtssitz Wien als multilateraler Hub für Sicherheit und Innovation gefestigt.

Bei der 59. Tagung des VN-MRR präsentierte Österreich gemeinsam mit Brasilien, Dänemark, Marokko, der Republik Korea und Singapur eine im Konsens angenommene Resolution zu neuen und aufkommenden digitalen Technologien. Mit dieser wurde das Büro des VN-Hochkommissars für Menschenrechte beauftragt, einen Menschenrechtsbasierten Zugang bei der Arbeit der Vereinten Nationen zu digitalen Technologien zu koordinieren. Zudem wurde der Hochkommissar beauftragt, ein Multi-Stakeholder Meeting zur Diskussion der besseren Umsetzung der menschenrechtlichen Verpflichtungen in Bezug auf die Entwicklung und Anwendung digitaler Technologien zu organisieren.

Im Rahmen der 80. VN-GV unterstützte Österreich die Resolution zu „Förderung und Schutz der Menschenrechte im Kontext digitaler Technologien“. Die Resolution unterstreicht die Notwendigkeit eines menschenrechtsbasierten Ansatzes bei der Gestaltung und Regulierung digitaler Technologien und baut auf der im Rahmen der 78. VN-GV verabschiedeten ersten Resolution der VN-GV zu den Auswirkungen von künstlicher Intelligenz auf die Menschenrechte auf. Inhaltlich wurde die Resolution insbesondere im Hinblick auf künstliche Intelligenz, Desinformation, Cyberbullying, digitale Bildung und

digitale Inklusion weiterentwickelt. Zudem wurden geschlechterspezifische Aspekte sowie ein menschenrechtsbasierter Umgang mit neuen Technologien stärker hervorgehoben.

2.3 Organisation des Nordatlantikvertrages (NATO)

Cyberaktivitäten als eine militärische Domäne für die NATO und ihre Alliierten – neben Land, See, Luft und Weltraum – finden in den drei Kernaufgaben der NATO Niederschlag:

- Abschreckung und Verteidigung,
- Krisenprävention und -management sowie
- kooperative Sicherheit.

Der Cyberspace ist die einzige Domäne, in dem die NATO und die NATO-Bündnispartner tagtäglich in direkten Kontakt mit Gegnerinnen und Gegnern sowie Konkurrentinnen und Konkurrenten kommen. Cyberangriffe sind zu einer permanenten Herausforderung für die Bündnispartner geworden und zielen häufig auf kritische Infrastrukturen wie Energie und Gesundheitswesen ab.

Als Reaktion auf die sich entwickelnde Cyber-Bedrohungslandschaft hat die NATO die Cyberverteidigung in ihren strategischen Rahmen integriert. Das Bündnis hat Mechanismen zur Erkennung, Prävention und Reaktion auf Cyberbedrohungen etabliert, wobei der Schutz kritischer Infrastrukturen und der Austausch von Informationen und Best Practices unter den Alliierten im Vordergrund steht. Die Annahme des Cyber Defence Pledge im Jahr 2016 und dessen anschließende Verbesserung im Jahr 2023 unterstreichen das kollektive Engagement zur Stärkung der nationalen Cyberverteidigungsfähigkeiten. Auf dem NATO-Gipfel 2024 in Washington, D.C., einigten sich die Bündnispartner darauf, das Integrierte Cyberverteidigungszentrum der NATO einzurichten, um den Schutz der Netze, das Lagebewusstsein und die Nutzung des Cyberraums als Operationsgebiet zu verbessern.

Die Cyber-Defence-Strategie der NATO umfasst Governance, Fähigkeitenaufbau und Zusammenarbeit mit internationalen Partnerinnen und Partnern sowie dem privaten Sektor. Die Governance-Struktur des Bündnisses erleichtert die politische, militärische und technische Koordination, wobei das Cyber Defence Committee (CDC) und die NATO Communications and Information Agency (NCIA) eine Schlüsselrolle bei der Implementierung der Strategie und der operativen Unterstützung spielen.

Die Zusammenarbeit mit Partnerländern, internationalen Organisationen und dem privaten Sektor ist integraler Bestandteil der Cyberverteidigungsbemühungen der NATO. Kooperative Initiativen mit der EU, den Vereinten Nationen (VN) und der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) sowie das Engagement mit Industrie

und Wissenschaft verbessern die Kapazität des Bündnisses, Cyberbedrohungen effektiv zu adressieren. Zum Beispiel werden im 10. Fortschrittsbericht über die EU-NATO Kooperation vom Juni 2025 zum Thema Cybersicherheit und Verteidigung, Fortschritte zum Thema festgestellt. Das Engagement der NATO für ein freies, offenes und sicheres Umfeld für Cyberaktivitäten, ausgerichtet an internationalem Recht und Normen, untermauert den Ansatz zur Förderung von Stabilität und zur Verringerung des Risikos von Konflikten im digitalen Raum.

Österreich kooperiert als Partnerland eng mit der NATO und beteiligt sich auf technischer Ebene an Sitzungen des Digital Policy Committee sowie jenen im Zusammenhang mit einschlägigen Smart-Defence-Projekten, die auf die Interoperabilität für gemeinsame Operationen und Missionen abzielen. Seit 2013 stellt das Bundesministerium für Landesverteidigung (BMLV) außerdem einen Offizier im „NATO Cooperative Cyber Defence Centre of Excellence“ (CCDCOE) in Tallinn. Ziel der Zusammenarbeit ist die Steigerung der Fähigkeiten zur nationalen Cyberverteidigung.

Der umfassende Ansatz der NATO zur Cyberverteidigung, der Prävention, Resilienz und Reaktion ausbalanciert, gewährleistet die Bereitschaft des Bündnisses, Cyberbedrohungen zu bekämpfen und abzumildern. Durch kontinuierliche Anpassung, Zusammenarbeit und Investitionen in Cyberfähigkeiten zielt die NATO darauf ab, die Sicherheit und demokratischen Werte ihrer Alliierten in einer zunehmend digitalen Welt zu schützen. Zu einem verstärkten Dialog Österreichs mit der NATO im Rahmen der Partnerschaft für den Frieden trägt auch das 2025 unterzeichnete und in Kraft getretene bilaterale Abkommen über den Austausch und den gegenseitigen Schutz klassifizierter Informationen bei.

2.4 Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE)

Als größte zwischenstaatliche Sicherheitsorganisation der Welt befindet sich die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) im Bereich Cybersicherheit in einer Doppelrolle: Einerseits unterstützt sie die Umsetzung der auf Ebene der Vereinten Nationen (VN) getroffenen Beschlüsse, insbesondere den Kapazitätenaufbau durch ihre exekutiven Strukturen, vor allem das Sekretariat in Wien und das weite Netz an Feldmissionen. Andererseits übernahm die OSZE bei der Ausarbeitung vertrauensbildender Maßnahmen (VBM, engl. CBM) in Hinblick auf Cyberaktivitäten eine Vorreiterrolle. Die Annahme der 16 vertrauensbildenden Maßnahmen stellt global gesehen den ambitioniertesten Versuch zur Stärkung der internationalen Kooperation im Feld der Cybersicherheit außerhalb der VN dar. Ziel ist es, zwischenstaatliche Spannungen, die aus der Nutzung von Informations- und Kommunikationstechnologien entstehen, unter den teilnehmenden Staaten der OSZE zu minimieren. Dazu wird der Austausch von Informationen, die Etablierung von Kommunikationskanälen und der Aufbau von Kapazi-

täten angeregt. Die OSZE-Arbeit konzentriert sich darüber hinaus auf die Wahrung und Stärkung der Menschenrechte im Cyberkontext sowie die Bekämpfung von Desinformation und Hassrede, insbesondere gegen Frauen und Mädchen.

Für die Weiterentwicklung und Implementierung der VBM ist die Informelle Arbeitsgruppe zu Cyber (Cyber-IWG) vorrangig zuständig. Das der OSZE zugrundeliegende umfassende Sicherheitsverständnis leitet auch die Arbeit der Cyber-IWG: Die Thematik wird unter Berücksichtigung politisch-militärischer, wirtschaftlicher und menschenrechtlicher Aspekte behandelt, wobei der russische Angriffskrieg gegen die Ukraine und Cyberattacken in diesem Zusammenhang weiterhin einen besonderen Schwerpunkt bildeten.

2025 setzte Österreich seine Aktivitäten im Rahmen der „Adopt a CBM"-Initiative fort, im Zuge derer Staaten oder Staatengruppen die Operationalisierung der VBM vorantreiben. Dabei legt Österreich gemeinsam mit Belgien, Bosnien und Herzegowina, Estland, Finnland, Italien und Schweden einen Fokus auf die Umsetzung der VBM 14 zu Public-Private-Partnerships (PPP). Als nächstes konkretes Projekt ist in Zusammenarbeit mit dem OSZE-Sekretariat ein Workshop zum Thema PPP und kritische Infrastrukturen geplant, der sich an die OSZE-Teilnehmerstaaten in Ost- und Südosteuropa (Westbalkan, Moldau, Ukraine, Türkei) richtet. Die Vorarbeiten (Sondierung von Möglichkeiten, inhaltliche und organisatorische Konzeption, Finanzierung) für diesen Workshop, der im Mai 2026 in Moldau stattfinden wird, begannen im Herbst 2025.

Ein zentrales Element der Vertrauensbildung ist das Kontaktpunkteverzeichnis (VBM 8), das eine rasche und unkomplizierte Möglichkeit für den Austausch zwischen OSZE-Teilnehmerstaaten bietet. Durch die Nominierung von diplomatischen und technischen Ansprechpersonen in jedem OSZE-Teilnehmerstaat soll der Informationsaustausch verbessert und – im Sinne eines „roten Telefons" – eine Eskalation vermieden werden. Für Österreich sind die Leiterin des Referats Cyberdiplomatie im BMEIA als diplomatischer POC und der Leiter der Abteilung Cybersicherheit und Krisenrechenzentrum im BKA als technischer POC nominiert.

Neben der institutionalisierten Behandlung der Thematik durch die Cyber-IWG setzen seit einigen Jahren die jeweiligen Vorsitzstaaten der OSZE die Cybersicherheit auf ihre Vorsitzagenda und halten jährliche Cybersicherheitskonferenzen ab. Im Jahr 2025 fand diese Konferenz mit dem Schwerpunktthema „Stärkung der nationalen Cyberresilienz" in Helsinki statt.

2.5 Europarat

Den Kern der Aktivitäten des Europarates im Bereich Cybersicherheit bildet die „Budapest-Konvention“ aus dem Jahr 2001, die mit aktuell 81 Ratifikationen und laufend neuen Beitritten eine Bedeutung weit über Europa hinaus erlangt hat. Hauptzweck ist die Verfolgung einer gemeinsamen Strafrechtspolitik zum Schutz der Gesellschaft vor Cyberkriminalität, insbesondere durch entsprechende gesetzliche Regelungen und die Förderung internationaler Zusammenarbeit. Die Konvention wurde um zwei Zusatzprotokolle erweitert. Seit 2006 ist das erste Zusatzprotokoll betreffend die Kriminalisierung von rassistischen und fremdenfeindlichen Handlungen durch Computersysteme in Kraft. Österreich hat 2003 unterzeichnet.

Seit 12. Mai 2022 liegt das zweite Zusatzprotokoll zur Budapest-Konvention (CETS No. 224) zur Unterzeichnung auf, das sich mit internationaler Rechtshilfe und dem damit verbundenen grenzüberschreitenden Zugang zu elektronischen Beweismitteln befasst. Es wurde bislang von 52 Staaten, darunter Österreich, unterzeichnet sowie von drei Staaten ratifiziert. Es tritt in Kraft, sobald es in fünf Staaten ratifiziert wurde.

Die Umsetzung der Konvention wird vom Komitee der Konvention zu Cyberkriminalität (T-CY) überwacht. Staaten werden außerdem über kapazitätsbildende Projekte unterstützt, die durch ein Cybercrime-Programmbüro des Europarates in Bukarest (C-PROC) koordiniert werden. Hierzu gehören auch die Beratung bei einschlägigen Legislativmaßnahmen und Hilfe bei der Ausbildung von Richterinnen und Richtern sowie Staatsanwältinnen und Staatsanwälten.

Das „Octopus Project“ fördert die Umsetzung der Budapest-Konvention und damit zusammenhängende Standards. Die sogenannten „Oktopus-Konferenzen“, die alle zwölf bis 18 Monate stattfinden, dienen Expertinnen und Experten sowie Organisationen als wichtige Plattform im Bereich Cyberkriminalität. Die nächste Oktopuskonferenz wird vom 14. bis 16. Oktober 2026 in Straßburg stattfinden.

Seit 2012 wurden bislang 13 Leitfäden (Guidance Notes) zur Budapest-Konvention erarbeitet und veröffentlicht. Diese sollen den Vertragsstaaten die effektive Anwendung und Umsetzung erleichtern.

Am 5. September 2024 wurde die Rahmenkonvention zu künstlicher Intelligenz und Menschenrechte, Demokratie und Rechtsstaatlichkeit des Europarates in Vilnius zur Unterzeichnung aufgelegt. 19 Unterzeichnungen gibt es bisher, darunter die EU für ihre 27 Mitgliedstaaten.

Zu den weiteren Instrumenten des Europarats zählt die 2018 modernisierte Datenschutzkonvention des Europarates (ETS 108). Österreich hat das entsprechende Änderungs-

protokoll 2022 ratifiziert. Die Lanzarote-Konvention zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch leistet einen wesentlichen Beitrag zum Online-Schutz von Kindern.

2.6 Andere Gremien und Initiativen

2.6.1 Freedom Online Coalition

Die „Freedom Online Coalition" ist eine informelle Gruppierung von Staaten, die sich für die effektive Online-Umsetzung weltweiter Menschenrechte einsetzt. Auch Österreich gehört dieser Initiative an, die im Dezember 2011 von den Niederlanden gegründet wurde und mittlerweile 41 Mitgliedstaaten umfasst.

2.6.2 International Counter Ransomware Initiative

Die 2021 ins Leben gerufene International Counter Ransomware Initiative (CRI) zählt mittlerweile ca. 70 gleichgesinnte Staaten, aber auch Organisationen wie Interpol und die EU zu ihren Mitgliedern. Das Bundesministerium für Inneres (BMI), das Bundesministerium für Finanzen (BMF) und das Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) bringen sich für Österreich in den drei Arbeitsfeldern der CRI ein: International Counter Ransomware Task Force (ICRTF), Policy Pillar und Diplomacy and Capacity Building Pillar. Österreich setzt sich u. a. für eine Einbindung der Westbalkanstaaten (von denen bislang nur Albanien Mitglied ist) in die Initiative ein.

2.6.3 Joint Statement on Efforts to Counter the Proliferation & Misuse of Commercial Spyware

Die Verbreitung und der Missbrauch von Spionagesoftware stellen eine steigende Sicherheitsbedrohung dar. Daher hat sich Österreich am 22. September 2024 dem von den USA initiierten Joint Statement zum Thema angeschlossen, das ein Bekenntnis zu folgenden Themen umfasst:

- Verhütung des Exports von Software, Technologie und Ausrüstung an Endabnehmerinnen und -abnehmer, die Güter für bösartige Cyberaktivitäten nutzen
- Informationsaustausch
- Zusammenarbeit mit Partnerinnen und Partnern in Industrie und Zivilgesellschaft in Hinblick auf Bewusstseinsbildung und Standard-Setting
- Internationales Engagement

2.6.4 Pall-Mall-Process

Der von Frankreich und dem Vereinigten Königreich initiierte „Pall-Mall"-Prozess befasst sich mit der Problematik des Missbrauchs und der Verbreitung von kommerziellen Cyber-Intrusion-Fähigkeiten (commercial cyber intrusion capabilities, CCICs), die auch aus österreichischer Sicht eine ernsthafte Sicherheitsbedrohung darstellen. Die Initiative

ist komplementär zum oben genannten Joint Statement zu Spyware zu sehen, wobei bewusst ein breiterer Teilnehmerinnen- und Teilnehmerkreis angesprochen wird. Positiv hervorzuheben ist der Multi-Stakeholder-Ansatz des Pall-Mall-Prozesses.

Im Rahmen des Pall-Mall-Prozesses brachte sich Österreich von Jänner bis März 2025 aktiv in die Ausarbeitung eines Verhaltenskodex für Staaten („Code of Practice for States“) ein. Dabei handelt es sich um einen Katalog von Empfehlungen und freiwilligen Selbstverpflichtungen. Diese sind ein wertvoller Beitrag zur Bewusstseinsbildung und zum Austausch von guter Praxis unter Gleichgesinnten. Das Dokument ersetzt rechtsverbindliche Instrumente wie Exportkontrollen nicht, sondern ergänzt diese. Im Diskussionsprozess wurde auch auf die Unterscheidung zwischen dem Missbrauch und der legitimen Verwendung von CCICs Wert gelegt: Ziel ist nicht ein Verbot von CCICs, sondern deren verantwortungsvolle und rechtskonforme Nutzung, einschließlich der Achtung von Völkerrecht und der Menschenrechte.

3 Nationale Akteure

3.1 NIS-Behörde - Abteilung IV/S/2

Für die Abteilung IV/S/2 – Netz- und Informationssystemsicherheit (NIS) im Bundesministerium für Inneres brachte das Jahr 2025 sowohl auf organisatorischer Ebene als auch in Bezug auf die konkrete Aufgabenerfüllung erhebliche Änderungen mit sich. Am **1. April 2025 trat eine Novelle des Bundesministeriengesetzes (BMG)** in Kraft, die unter anderem die Aufgabenverteilung zwischen Bundeskanzleramt (BKA) und Bundesministerium für Inneres (BMI) neu regelte.

Grundsätzlich normiert das Netz- und Informationssystemsicherheitsgesetz (NISG) den Aufgabenbereich einer nationalen NIS-Behörde auf zwei unterschiedlichen Ebenen:

- § 4 NISG enthält die konkreten Aufgaben auf strategischer Ebene. Diese wurden bis 30. April 2025 durch das Bundeskanzleramt koordiniert. Mit Inkrafttreten der Novelle des Bundesministeriengesetzes (BMG) ging gemäß Abschnitt H Z 12 von Teil 2 der Anlage zu § 2 BMG die Koordination der Aufgabenerfüllung an das Bundesministerium für Inneres über (siehe auch 3.1.4).
- § 5 NISG enthält die konkreten Aufgaben auf operativer Ebene. Die Koordination der Aufgabenerfüllung in diesem Bereich wird wie bisher ebenfalls durch das Bundesministerium für Inneres erbracht.

Im Jahr 2025 wurde im Rahmen einer Novelle des Bundesministeriengesetzes (BMG) erste Maßnahmen gesetzt, um die NIS-Agenden in Österreich zu konsolidieren. Die Aufgaben der strategischen NIS-Behörde und des NCC-AT wurden mit dieser Novelle vom BKA in das BMI transferiert und dort in der Abteilung IV/S/2 zusammengeführt. Es wurde weiterhin im Rahmen des Programms zur Umsetzung der EU-Cybersicherheitspakete 2020 und 2023 umfangreiche Maßnahmen zur Umsetzung des NISG und des Cybersolidarity Acts gesetzt. Ziel der diesbezüglichen Aktivitäten war, neben Optimierung des NIS-Vollzuges, die inhaltlichen Vorbereitungen auf den zukünftigen Vollzug des NISG 2026. Im Dezember 2025 wurde in Umsetzung der europäischen Richtlinie 2022/2555 das Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026) im Parlament angenommen und anschließend im Bundesgesetzblatt veröffentlicht.

Im Zentrum der Tätigkeiten der Abteilung stand im Beobachtungszeitraum – wie auch zuvor – die behördliche Aufsicht über die Umsetzung der Vorgaben des Netz- und Informationssystemsicherheitsgesetzes (NISG) durch Betreiberinnen und Betreiber wesentlicher Dienste, Anbieterinnen und Anbieter digitaler Dienste sowie Einrichtungen der öffentlichen Verwaltung.

Darüber hinaus nimmt die Abteilung eine koordinierende Rolle innerhalb der gesamtstaatlichen Operativen Koordinierungsstruktur (OpKoord) und ihres Inneren Kreises der Operativen Koordinierungsstruktur (IKDOK) wahr und unterstützt darüber hinaus die

dem NISG unterworfenen Entitäten im Bereich der Bewusstseinsbildung (Awareness) hinsichtlich möglicher Bedrohungen im Cyberraum.

Die Arbeit der NIS-Behörde auf strategischer und operativer Ebene ist **seit 1. Mai 2025 nunmehr auf vier Referate verteilt:**

3.1.1 Referat IV/S/2/a (Recht und Audit)

Das Referat IV/S/2/a (Recht und Audit) erfüllt einen wesentlichen Teil der Aufgabenstellungen der NIS-Behörde. Die Hauptaufgaben umfassen folgende Bereiche:

- Regelmäßige Überprüfung der Umsetzung verpflichtender Sicherheitsmaßnahmen bei den dem NISG unterstellten Unternehmen und Organisationen
- Anlassbezogene Überprüfung dieser Umsetzungen durch die Behörde im Rahmen von Einschauen
- Sicherstellung des notwendigen Sicherheitsniveaus durch Aussprechen von Empfehlungen und bescheidmäßigen Anordnungen
- Verfahrensführung im Rahmen des NISG
- Feststellung der mit der Durchführung der Überprüfungen beauftragten qualifizierten Stellen
- Allgemeine und sektorspezifische Risikoanalysen
- Teilnahme an Arbeitsgruppen auf nationaler und internationaler Ebene

Im Rahmen der behördlichen Aktivität werden auch Empfehlungen und bescheidmäßige Anordnungen zur Umsetzung oder Anpassung von Sicherheitsvorkehrungen ausgesprochen. In den vergangenen Jahren gab es rund 2.500 Empfehlungen. Im Fokus standen vor allem Themen der technischen Umsetzung, z. B. im Bereich der Sicherheitsarchitektur, Systemwartung oder das Erkennen von und die Reaktion auf Vorfälle sowie der organisatorischen Rahmenbedingungen, z. B. im Bereich der Risikoanalyse oder des Umgangs mit Dienstleisterinnen und Dienstleistern, Lieferantinnen und Lieferanten sowie Dritten.

Zu den Aufgaben des Referats zählt auch das Einbringen von Sachverhaltsdarstellungen an Verwaltungsstrafbehörden. Der überwiegende Teil der Sachverhaltsdarstellungen beruhte auf Fristversäumnissen und Feststellungen von Nicht-Umsetzungen von Sicherheitsmaßnahmen im Sinne des NISG und der Netz- und Informationssystemsicherheitsverordnung (NISV).

3.1.2 Referat IV/S/2/b (Cyberlagezentrum, Prävention, Kommunikation)

Das Referat IV/S/2/b (Cyberlagezentrum, Prävention, Kommunikation) vereint eine Vielzahl von Aufgaben innerhalb der NIS-Behörde. Ein Schwerpunkt liegt auf der ressortinternen und ressortübergreifenden Koordination sowie auf der Erstellung des gesamtstaatlichen

Cyberlagebildes. Zudem werden IKDOK- und OpKoord-Lagebilder sowie Sonderlagebilder regelmäßig erstellt und den Bedarfsträgerinnen und Bedarfsträgern innerhalb des Bundesministeriums für Inneres sowie den anderen Ressorts, den Betreiberinnen und Betreibern kritischer Infrastruktur und wesentlicher Dienste zur Verfügung gestellt. Um die Qualität der Arbeit und die Akzeptanz der Partnerinnen und Partner sicherzustellen, wird laufend ein Feedback von der jeweiligen Zielgruppe eingeholt. Darüber hinaus werden Beiträge zu Cybersicherheit für andere ressortinterne Lagebilder erstellt.

Zudem wird die **Meldesammelstelle und der Single Point of Contact** als zentrale Anlaufstelle für NIS-Behörden anderer Mitgliedstaaten der EU vom Referat betreut. Ein wesentlicher Bestandteil dieser Tätigkeit ist die Analyse und Weiterverarbeitung der einlangenden Pflicht- und Freiwilligenmeldungen.

Die Zahl der Pflicht- und Freiwilligenmeldungen wächst stetig an. Waren es 2020 noch 36 Meldungen, so waren es im Jahr 2025 bereits 239 Meldungen.

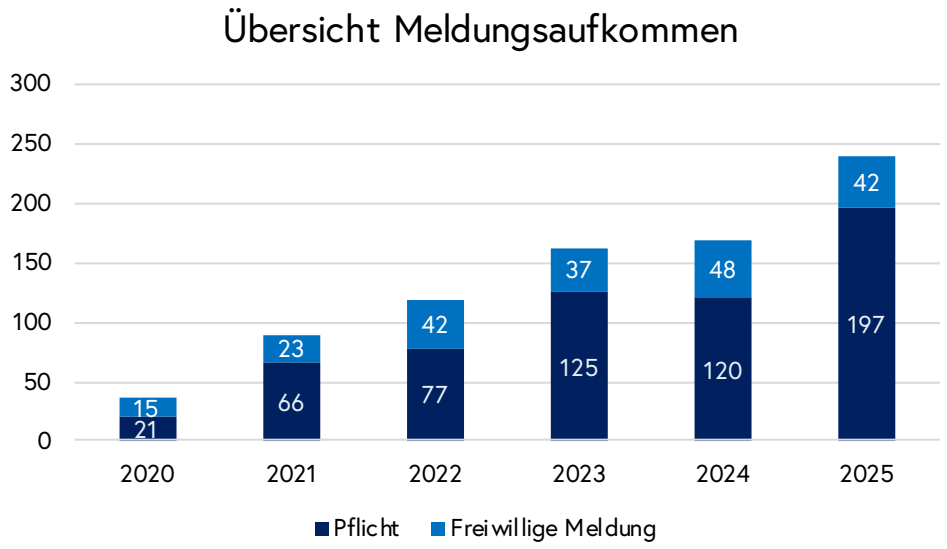


Abbildung 9: Übersicht Meldungsaufkommen: Pflichtmeldungen und Freiwillige Meldungen von 2020 bis 2025

Der **Fachbereich Awareness** im Referat IV/S/2/b ist für die Planung, Koordination und Durchführung von Awareness-Veranstaltungen, Workshops und Beratungen bei Betreiberinnen und Betreibern wesentlicher Dienste, Anbieterinnen und Anbietern digitaler Dienste, Einrichtungen der öffentlichen Verwaltung und weiteren Unternehmen oder Organisationen sowie für die Konzeption und Erstellung von Unterlagen und Publikationen verantwortlich. Im Jahr 2025 wurden 96 Awareness-Veranstaltungen bzw. -beratungen durchgeführt.

Auch koordinierende Aufgaben auf nationaler sowie auf EU-Ebene werden vom Referat IV/S/2/b wahrgenommen. Hierzu zählen die Abhaltung regelmäßiger bzw. anlassbezogener Sitzungen der **operativen Koordinierungsstrukturen** gemäß NISG sowie die **Kooperation im Rahmen von EU-CyCLONe** (European Cyber Crisis Liaison Organisation Network) zur Bewältigung großer, grenzüberschreitender Cybersicherheitsvorfälle mit Vertreterinnen und Vertretern der EU-Mitgliedstaaten.

3.1.3 Referat IV/S/2/c (NIS Technische Einrichtungen)

Das Referat IV/S/2/c (NIS Technische Einrichtungen) ist die technische Fachstelle der NIS-Behörde. Das Referat konzipiert und begleitet die Entwicklung spezifischer IKT-Lösungen, die zur Erfüllung der Anforderungen des NIS-Gesetzes erforderlich sind, sowie IT-Anwendungen, die die NIS-Behörde gezielt in ihren Aufgaben unterstützen. Zu den IKT-Lösungen nach dem NISG zählen unter anderem:

Meldeanalysesystem: Zur Analyse von Meldungen zu Cybersicherheitsvorfällen kümmert sich das Referat um den technischen Betrieb eines Meldeanalysesystems (§ 11 NISG / § 18 NISG2026). Dieses reichert eingehende Meldungen zu Cybersicherheitsvorfällen mit Informationen aus Open Source Intelligence (OSINT) an und unterstützt die Erstellung von Lagebildern zur Cybersicherheitslandschaft in Österreich.

IOC-Frühwarnsystem: Das Referat ist verantwortlich für die Konzeption, den Aufbau sowie den kontinuierlichen fachlichen Betrieb eines IOC-Frühwarnsystems (§ 13 NISG / § 17 NISG2026). Indicators of Compromise (IOCs) sind erkennbare Merkmale oder Spuren, die auf eine potenzielle oder bereits erfolgte Sicherheitsverletzung hinweisen. Das IOC-Frühwarnsystem dient der frühzeitigen Erkennung und Analyse von sicherheitsrelevanten Vorfällen in den IT-Infrastrukturen der NIS-Normunterworfenen, die hauptsächlich österreichische Unternehmen der kritischen Infrastruktur sind.

Zur Unterstützung der operativen Tätigkeiten der NIS-Behörde entwickelt und betreibt das Referat verschiedene IKT-Lösungen, darunter **Anwendungen zur Registrierung (§ 29 NISG 2026)** und Verwaltung von Stammdaten und Prüfberichten. Zudem ist das Referat für den Aufbau der erforderlichen IT-Infrastruktur sowie die Verwaltung der Schnittstellen zu anderen BMI-Anwendungen verantwortlich und leistet einen wesentlichen Beitrag im **Projekt European Network of SOC (ENSOC)** sowie in der dafür notwendigen Umsetzung eines **nationalen Cyber-Hubs** und dem Aufbau der dafür notwendigen Werkzeuge zum Informationsaustausch.

ENSOC ist ein von der Europäischen Union gefördertes Projekt, das einen grenzüberschreitenden Cyber-Hub entwickelt. Dieser Hub ermöglicht den Austausch von Cyber Threat Intelligence (CTI) mit derzeit sechs anderen EU-Mitgliedstaaten.

3.1.4 Referat IV/S/2/d (Strategische Netz- und Informationssicherheit)

Um die mit der BMG-Novelle 2025 geänderte Zuständigkeitsverteilung im NIS-Bereich widerzuspiegeln, wurde mit der aktualisierten Geschäftseinteilung des BMI das Referat IV/S/2/d – Strategische Netz- und Informationssicherheit ins Leben gerufen. Das Referat befasst sich neben den namensgebenden strategischen NIS-Agenden im Allgemeinen auch mit der Koordination von nationalen und internationalen Cyberthemen. Darunter fällt etwa die Vertretung Österreichs in der HWP Cyber, der NIS-Kooperationsgruppe, bei der ENISA und in der ECCC. Darüber hinaus ist dem Referat die Koordination der öffentlich-privaten Zusammenarbeit und der Cyber Security Steuerungsgruppe des Bundes (CSS) zugeordnet. Auch die Entwicklung von Strategien für die Cybersicherheit – etwa der ÖSCS – fällt in den Zuständigkeitsbereich. Ausgenommen sind allerdings die Angelegenheiten der Cybersicherheitszertifizierung. Diese verblieben in der Zuständigkeit des Bundeskanzleramts.

3.2 Verfassungsschutzrelevante Cybersicherheit

Die Direktion Staatsschutz und Nachrichtendienst (DSN) fungiert als operative Koordinierungsstelle für Meldungen und Anfragen zu Angriffen auf Systeme und Infrastrukturen von verfassungsmäßigen Einrichtungen sowie auf Systeme von Unternehmen der kritischen Infrastruktur. Hierfür bedient sich die DSN eines breiten Spektrums an Fähigkeiten und Techniken, wie beispielsweise Cyber Threat Intelligence, Malware Analysis und Reverse Engineering. Im Zuge der Tätigkeit ergibt sich die Taxonomie und Beschäftigung mit neuen Phänomenen im Cyberbereich und die Reaktion auf aktuelle Trends. Um einen Erfahrungs- und Wissensaustausch zu ermöglichen und zu fördern, setzt die DSN auf die Zusammenarbeit mit Strafverfolgungsbehörden und der Cybersicherheitscommunity, zu der Stakeholder aus Wirtschaft und Forschung zählen. Ziel ist es, gemeinsam die Resilienz und die Kommunikation im Bereich der Cybersicherheit zu fördern. Ebenso findet ein Austausch mit ausländischen Sicherheitsbehörden statt, um die eigenen Erkenntnisse zu teilen und eine globale Sicht auf Bedrohungen zu gewinnen.

Im Berichtsjahr 2025 wurden unterschiedliche verfassungsschutzrelevante Phänomene behandelt. Diese stellen Weiterentwicklungen von bereits in der Vergangenheit behandelten Bedrohungen dar. Dies sind vor allem Advanced Persistent Threat (APT), Hacktivistinnen und Hacktivisten und Ransomware-Gruppierungen. Sie stellen die Bearbeitung des Aufgabenspektrums Cybersicherheit vor anhaltende und dynamische Herausforderungen. Zusätzlich spielen auch geopolitische Konflikte eine große Rolle in der Cyberdomäne.

3.3 Cyber Crime Competence Center (C4)

Das Cybercrime Competence Center (C4) ist die nationale und internationale Koordinierungs- und Meldestelle zur Bekämpfung von Cybercrime. Das Zentrum setzt sich aus technisch und fachlich hochspezialisierten Expertinnen und Experten aus den Bereichen Ermittlung, Forensik und Technik zusammen.

Die sowohl für Cybercrime im engeren Sinn als auch für digitale Forensik und Datensicherung in Österreich zuständigen Polizeibehörden sind auf drei Ebenen tätig. Auf Bundesebene und als übergeordnete Organisation ist das C4 im Bundeskriminalamt angesiedelt. In jeder der neun Landespolizeidirektionen sind spezialisierte Assistenzbereiche für den Cybercrime- und Forensik-Bereich als Teil der Landeskriminalämter etabliert. Auf Bezirks- bzw. Regionalebene stehen Cybercrimeermittlerinnen und -ermittler sowie Cybercrimeforensikerinnen und -forensiker als erste Ansprechpersonen zur Verfügung.

Im Jahr 2024 erfolgte die Umstrukturierung des C4 mit einer Erweiterung der Ressourcen und gliedert sich nun wie folgt:

3.3.1 Zentrale Aufgaben

Hierbei handelt es sich um die zentrale Koordinationsstelle bei der Bekämpfung von Cyberkriminalität. Die Zuständigkeit umfasst die zentrale Administration und Organisation von Projekten und Förderprogrammen, internationalen Kooperationen, die Entwicklung und Organisation nationaler und internationaler Ausbildungsprogramme, das Beschaffungswesen für IKT-Hardware und Software und die Koordinierung sämtlicher fachbereichsübergreifender Angelegenheiten.

3.3.2 IT-Beweissicherung

Die Fachexpertise zur Sicherung und Auswertung von elektronischen Beweismitteln bildet das Kernstück des C4. Neben der IT-Forensik und Mobilen Forensik haben sich weitere Fachbereiche entwickelt, die zunehmend an Bedeutung gewinnen. Dazu gehören die Multimedia-Forensik, die Elektronik- und IoT-Forensik sowie die Automotive-IT.

3.3.3 Ermittlungen

Spezialisierte Ermittlungseinheiten für die Fachrichtungen Darknet sowie Kryptowährungen und Blockchain (einschließlich der Sicherstellung und Verwertung von Kryptowährungen) wurden eingerichtet, um die erforderliche Expertise bei Ermittlungen bereitzustellen. Auch der Bereich „Complex Cybercrime“, der sich mit Cybercrime-Delikten und Massenphänomenen befasst, deren Ermittlungsansätze überwiegend im digitalen Bereich liegen, wird abgedeckt. Dieser Bereich umfasst Delikte mit hohem Schadenspotenzial und internationalen Zusammenhängen. Zu den IT-Ermittlungen zählen zudem die Meldestelle für Internetkriminalität sowie die Zentrale Anfragestelle Social Media & Online-Service-

Provider (ZASP). Die ZASP führt zentrale Abfragen bei Social-Media-Plattformen und Internetdienstanbieterinnen und -anbietern durch. Die Meldestelle gegen Cybercrime unter against-cybercrime@bmi.gv.at ist die Ansprechstelle für Bürgerinnen und Bürger sowie für nationale Strafverfolgungsbehörden im Zusammenhang mit IT-Delikten.

3.3.4 Entwicklung und Innovation

Aufgabe ist die Unterstützung von digitaler Forensik und digitalen Ermittlungen mit wissenschaftlicher Expertise sowie die bedarfsorientierte Entwicklung von Tools und Skripten, die international auch für andere Strafverfolgungsbehörden zur Verfügung gestellt werden. Ein wesentlicher Teil ist darüber hinaus die internationale Zusammenarbeit mit Forschungsinstituten und -institutionen.

3.3.5 Digitales Beweismittelmanagement

Das digitale Beweismittelmanagement fasst jene Kompetenzen zusammen, die für eine zeitgemäße kriminalpolizeiliche Bearbeitung komplexer Fälle mit großen Datenmengen notwendig sind. Dies umfasst die technische Aufbereitung sichergestellter digitaler Beweismittel zur systematischen Indizierung und nachfolgenden Bereitstellung für die Ermittlungsbereiche im Bundeskriminalamt und bei Bedarf in den Landeskriminalämtern. Ebenso gehört das Fallmanagement dazu, das als Schnittstelle zwischen Forensikerinnen und Forensikern, Ermittlerinnen und Ermittlern, Technikerinnen und Technikern sowie gegebenenfalls der Justiz fungiert.

3.4 Direktion IKT & Cyber

Die Direktion 6 – IKT & Cyber im BMLV führt die Cyber- und Informationskräfte des Österreichischen Bundesheeres (ÖBH) und ist damit für folgende fünf Waffengattungen zuständig:

- Cybertruppe
- Elektromagnetischer-Kampf-(EloKa-)-Truppe
- Führungsunterstützung (FüU)/IKT-Truppe
- Kommunikations-(Komm-)-Truppe
- Psychological Operations-(PsyOps-)-Truppe

Das sind jene Elemente im ÖBH, die die anderen Teilstreitkräfte (Land, Luft), aber auch alle Führungsebenen miteinander verbinden und damit die Kommunikations- und Führungsfähigkeit herstellen. Sie sind unter anderem zuständig für alle Einsatzarten im Cyberraum und im Elektromagnetischen Umfeld, für das Errichten und sichere Betreiben von Einsatznetzwerken, für die Awareness im Bereich der IKT-Sicherheit, die Überwachung des Informationsumfeldes sowie für das Bereitstellen von Informationen über verschiedene Medienkanäle.

Organisatorisch besteht die Direktion IKT & Cyber aus den drei Abteilungen:

- IKT & Cyber Planung (IKTCyPl),
- IKT & Cyber Einsatz (IKTCyE) und
- IKT Bereitstellung und Nutzungsmanagement (IKTBstg&NuMngt).

Die Abteilung IKTCyPl ist die Planungskomponente der Direktion und unter anderem zuständig für die Fähigkeitsplanung und -weiterentwicklung sowie für die Erstellung von Grundlagen für alle o. a. Waffengattungen der Cyber- und Informationskräfte des ÖBH.

Die Abteilung IKTCyE ist die Einsatzkomponente der Direktion. Sie ist für die Führungsunterstützung, die elektromagnetische Kampfführung und für die Kampfführung im Cyberraum bei allen Einsätzen des Bundesheeres verantwortlich.

Die Abteilung IKTBstg&NuMngt koordiniert und steuert alle Querschnittsaufgaben in der Direktion, und nimmt neben Informations- und Wissensmanagement auch die Wirkungssteuerung und Koordinierung des Controllings sowie die Koordinierung im Forschungsmanagement und in der Zukunftsentwicklung wahr.

Im IKT & Cybersicherheitszentrum, einer der Dion 6 nachgeordneten Dienststelle und zentraler IKT-Provider des ÖBH, sind fünf Fachbereiche zusammengefasst, die sich mit der Umsetzung der planerischen Vorgaben und der Integration von beschafften Systemen in das ÖBH-eigene IKT-System beschäftigen. Die Mitarbeiter des IKT & Cybersicherheitszentrums schaffen die Voraussetzungen für die Verlegbarkeit, Mobilität, Autarkie, Resilienz und internationale Interoperabilität sowie die Basis für die Informationsüberlegenheit des ÖBH auf dem modernen, digitalen und hybriden Gefechtsfeld.

Das Leistungsspektrum erstreckt sich somit von Beiträgen zur strategischen Planung, über die operative Umsetzung, bis hin zur taktischen Durchführung sämtlicher Belange der IKT- und geoinformationsbezogenen Aufgaben des Bundesheeres.

3.5 Abwehramt (AbwA)

Unter dem Begriff der Cyberverteidigung werden alle Anstrengungen des ÖBH im Zusammenhang mit Cyberaktivitäten als Gesamtes verstanden. Das Abwehramt (AbwA) wirkt mit seinen Kompetenzen und nachrichtendienstlichen Zugängen an dieser mit. Es stellt hierzu sein Lagebild zur Verfügung, das gesamtstaatliche und auch nachrichtendienstliche Informationen zur Cyberbedrohungslandschaft zusammenführt, analysiert und als Grundlage der Beurteilung von Gegenmaßnahmen dient. Durch diese und weitere Maßnahmen soll kontinuierlich ein hohes Maß an Sicherheit der militärischen IKT-Infrastruktur gewährleistet werden.

3.6 Heeresnachrichtenamt (HNaA)

Das Heeresnachrichtenamt (HNaA) ist der strategische Auslandsnachrichtendienst Österreichs. Als solcher beschafft er Informationen über das Ausland, wertet sie aus und stellt die Ergebnisse der obersten politischen und militärischen Führung zur Verfügung. Dazu gehört auch die Beobachtung nachrichtendienstlich relevanter Entwicklungen und Vorgänge von Cyberaktivitäten als Aspekt des gesamtheitlichen nachrichtendienstlichen Lagebildes. Durch das Erkennen von Cyberbedrohungen leistet es einen wesentlichen Beitrag zur Entscheidungsfindung bezüglich einzuleitender gesamtstaatlicher Gegenmaßnahmen und einer möglichen Attribuierung.

3.7 GovCERT, nationales CERT und sektorspezifische CERTs

Das GovCERT Austria ist gemäß Netz- und Informationssystemsicherheitsgesetz (NISG) das Computer-Notfallteam der öffentlichen Verwaltung und Mitglied des Inneren Kreises der Operativen Koordinierungsstruktur (IKDOK). Ab dem 1. April 2025 ist es laut der Bundesministeriengesetz-Novelle 2025 nicht mehr im Bundeskanzleramt, sondern im Innenministerium angesiedelt. Die Erbringung operativer und operationeller Leistungen erfolgt im Rahmen einer Public-Private-Partnership mit CERT.at. Das GovCERT Austria stellt den Kontaktpunkt des Computer Emergency Response Teams (CERT) für Österreich in Bezug auf die Netze der öffentlichen Verwaltung dar und steht mit internationalen Organisationen und Kontakten wie der European Government CERTs (EGC) Group oder der Central European Cyber Security Plattform (CECSP) im engen Austausch.

Bereits seit März 2019 nimmt CERT.at die Rolle des nationalen Computer-Notfallteams gemäß NIS-Gesetz wahr. CERT.at versteht sich als Kontaktpunkt für sicherheitsrelevante IKT-Ereignisse in Österreich und dient als vertrauenswürdige und anerkannte Informationsdrehscheibe innerhalb österreichischer Organisationen und Unternehmen im Bereich der Cybersicherheit. Dazu nutzt CERT.at sein Kontaktnetzwerk zu internationalen CERTs und anderen Cybersicherheits-Organisationen sowie eigens dafür entwickelte Software und ist an zahlreichen nationalen und europäischen Projekten beteiligt. Darüber hinaus informiert CERT.at über Social Media und Mailinglisten über aktuelle Bedrohungen und Schutzmaßnahmen.

Das Austrian Energy CERT (AEC) ist ein akkreditiertes, brancheneigenes Computer Emergency Response Team (CERT, oft auch CSIRT für Computer Security Incident Response Team genannt) für die österreichische Energieindustrie. Das Ziel des AEC ist die Stärkung der IT-Sicherheitskompetenz des Energiesektors und die Erhöhung der Resilienz des Sektors gegenüber Cyberangriffen. Zu den Aufgaben gehört neben dem Sicherheitsvorfalls-Management die Bearbeitung täglich eingehender Anfragen und

Sicherheitsmeldungen, die Durchführung von Schulungstätigkeiten, die Teilnahme an internationalen Cybersicherheitsübungen sowie die Mitarbeit bei der Erstellung technischer Sicherheitskonzepte für die Elektrizitäts- und Erdgaswirtschaft. Darüber hinaus erfüllt das AEC die Rolle des primären Ansprechpartners bei nationalen und internationalen Security Incidents im Energiesektor. Damit wird neben schneller und effizienter Kommunikation auch die Koordination der IT-Sicherheitsexpertinnen und -experten und Behörden innerhalb der Branche gewährleistet.

Mit der Wahrnehmung der Aufgaben gemäß NISG 2026 und dem Gesundheitstelematikgesetz leistet das Austrian HealthCERT einen wichtigen Beitrag zur Sicherstellung der Betriebskontinuität der öffentlichen Gesundheits-Telematik-Infrastruktur, die unter anderem ELGA, Gesundheitsnetze und eHealth-Anwendungen umfasst. In diesem Zusammenhang hat das Austrian HealthCERT im Jahr 2025 gemeinsam mit verschiedenen Einrichtungen des Gesundheitssektors präventive Maßnahmen zur Vermeidung konkreter kritischer Cyberbedrohungen umgesetzt. Als Mitglied des European CSIRT Networks konnten sektorspezifische Anliegen des Gesundheitswesens auf europäischer CSIRT-Ebene eingebracht werden. Besonderes Augenmerk galt dabei der Anregung eines fachlichen Austauschs zum Thema Sicherheitsvorfälle im Zusammenhang mit Medizingeräten. Im Berichtsjahr wurde erstmals in Kooperation mit dem Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz ein „Netzwerktreffen Cybersicherheit im Gesundheitssektor“ veranstaltet. Die Veranstaltung umfasste Fachvorträge zu aktuellen Fragestellungen der Cybersicherheit sowie zu praktischen Erfahrungen mit der Umsetzung der NIS1-Vorgaben. Die Beiträge zielten insbesondere auch darauf ab, Wissen und Erfahrungswerte für jene Organisationen im Gesundheitssektor bereitzustellen, die im Hinblick auf das NISG 2026 künftig in den Anwendungsbereich fallen und bislang keine Erfahrung mit der entsprechenden Vorbereitung aufweisen. Zur weiteren Stärkung der sektoralen Vernetzung im Bereich Cybersecurity wurde eine Kommunikationsplattform etabliert, die sich insbesondere in der präventiven Kommunikation bereits als wirkungsvolles Instrument bewährt hat. In Kooperation mit dem nationalen CyCLONe Point of Contact, vertreten durch das Bundesministerium für Inneres, der Barmherzige Brüder Ordensprovinz Europa Mitte als sektorspezifischer Partner und der ENISA, wurde eine Übung zur Aktivierung der EU-Cybersicherheitsreserve erfolgreich durchgeführt.

Gemeinsam erfüllen die vier CERTs die Aufgaben gemäß NISG und decken damit die Vorgaben der europäischen Richtlinie für Netz- und Informationssicherheit sowie die Empfehlungen der EU-Cybersicherheitsagentur (ENISA) zur Erhöhung der IT-Sicherheit bei kritischen Infrastrukturen. Sie stellen auch die österreichischen Mitglieder des Computer Security Incident Response Team (CSIRT)-Netzwerks der EU (siehe 2.7). Die genannten vier CERTs werden in erster Linie bei Sicherheitsbedrohungen und -ereignissen aktiv. Dies geschieht durch Verständigung der betroffenen Stellen oder auf Basis eigener Recherchen. Darüber hinaus führen alle vier Computer-Notfallteams auch vorbeugende

Maßnahmen wie Früherkennung, Öffentlichkeitsarbeit, Beratung und Unterstützung im Anlassfall sowie auf Anfrage durch.

Das NISG sieht in der Umsetzung unter anderem für Betreiberinnen und Betreiber wesentlicher Dienste sowie Anbieterinnen und Anbieter digitaler Dienste eine Meldeverpflichtung für schwerwiegende Sicherheitsvorfälle vor. Diese verpflichtenden Meldungen werden von den Betroffenen an bestimmte, sektorenspezifische Meldestellen (sektorenspezifische Computer-Notfallteams) gesendet und von dort an das Bundesministerium für Inneres (BMI) weitergeleitet. Auf freiwillige Meldungen trifft dies ebenfalls zu, allerdings können diese Meldungen vor der Weiterleitung an das BMI von den Sektor-CERTs anonymisiert und aggregiert werden.

Für die Einrichtungen der öffentlichen Verwaltung, mit Ausnahme jener im IKDOK vertretenen, nimmt GovCERT Austria die Entgegennahme und Weiterleitung solcher Meldungen vor. Zusätzlich kann GovCERT Austria auch Frühwarnungen, Alarmmeldungen, Handlungsempfehlungen und Bekanntmachungen herausgeben, erste allgemeine technische Unterstützung bei der Reaktion auf Sicherheitsvorfälle leisten, Risiken, Vorfälle und Sicherheitsvorfälle beobachten und analysieren sowie die Lage beurteilen.

Das NISG sieht zur Wahrnehmung dieser Meldestellenfunktion die Etablierung eigener Branchen- oder Sektoren-CERTs in jedem Sektor vor. Wurde in einem Bereich noch kein eigenes CERT etabliert, werden die Aufgaben des Computer-Notfallteams und die der Meldestelle durch das nationale Computer-Notfallteam wahrgenommen. CERT.at hat dafür eine Meldeplattform unter https://nis.cert.at/ eingerichtet. Dort können auch von jeder Organisation freiwillige Meldungen eingetragen werden, die helfen, ein besseres Cyberlagebild zu schaffen.

3.8 Nationales Koordinierungszentrum für Cybersicherheit

Das Nationale Koordinierungszentrum für Cybersicherheit (NCC-AT) bildet als Teil des EU-weiten Netzwerks nationaler Koordinierungszentren, zusammen mit dem Europäischen Kompetenzzentrum für Industrie, Technologie und Forschung, im Bereich der Cybersicherheit (ECCC) den europäischen Rahmen zur Unterstützung der Innovations- und Industriepolitik im Bereich der Cybersicherheit. Ziel ist es, durch Community Building und Koordinierung der Bemühungen im Bereich Kompetenzaufbau, die Kapazitäten im Bereich Cybersicherheit in Österreich und der Europäischen Union zu stärken, Resilienz auszubauen und so die Gesellschaft und Wirtschaft vor Cyberbedrohungen zu schützen. Zudem soll die Exzellenz in der Forschung gesichert und die Wettbewerbsfähigkeit der europäischen Industrie ermöglicht werden.

Das Bundeskanzleramt setzte das NCC-AT in Kooperation mit der Österreichischen Forschungsförderungsgesellschaft (FFG) bis Herbst 2025 um und erfüllte damit den rechtlichen Auftrag der 2021 in Kraft getretenen Verordnung (EU) 2021/887 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren.

Mit dem Bundesgesetz über die Zahl, den Wirkungsbereich und die Einrichtung der Bundesministerien (Bundesministeriengesetz 1986 – BMG) idF BGBl. I Nr. 10/2025 sind die Zuständigkeiten mit November 2025 dem Bundesministerium für Inneres übertragen worden.

Um einen nachhaltigen Beitrag zum Ausbau der Cybersicherheitskompetenzen in Europa zu leisten, ist das österreichische Nationale Koordinierungszentrum einem Konsortium mit weiteren europäischen Partnerstaaten unter der Leitung von Griechenland beigetreten. Im Rahmen dieses Konsortiums sollen Maßnahmen und Strategien entwickelt werden, um Cybersicherheitsfähigkeiten in Europa systematisch auf- und auszubauen sowie Synergien zwischen bestehenden Initiativen gezielt zu nutzen. Dadurch soll ein effizienter und ressourcenschonender Einsatz der zur Verfügung stehenden Mittel gewährleistet werden. Darüber hinaus ist eine enge Zusammenarbeit mit der ECCC Cybersecurity Skills Academy vorgesehen, um einen gemeinschaftlichen und strukturierten Zugang zu Cybersicherheitsaus- und -weiterbildungsangeboten zu schaffen. Ein besonderer Fokus liegt dabei auf der aktiven Einbindung relevanter Stakeholder, um eine nachhaltige und bedarfsgerechte Entwicklung der europäischen Cybersicherheitskompetenzen sicherzustellen.

3.9 Nationale Behörde für die Cybersicherheitszertifizierung

Die nationale Behörde für die Cybersicherheitszertifizierung ist im Bundeskanzleramt eingerichtet. Ihr kommen unter anderem die Überprüfung der Übereinstimmung von IKT-Produkten, -Diensten und -Prozessen mit den in Österreich ausgestellten europäischen Cybersicherheitszertifikaten, die Überwachung und Durchsetzung der Verpflichtungen gegenüber Ausstellerinnen und Ausstellern von EU-Konformitätserklärungen und die Zusammenarbeit mit anderen nationalen Behörden für die Cybersicherheitszertifizierung und anderen öffentlichen Stellen zu.

Während mit dem EUCC am 27. Februar 2025 das erste europäische Cybersicherheitsschema in Geltung getreten ist, gab es im Berichtszeitraum keine akkreditierte Konformitätsbewertungsstelle.

4 Nationale Strukturen

4.1 Operative Koordinierungsstruktur (OpKoord) und Innerer Kreis der Operativen Koordinierungsstruktur (IKDOK)

Das Netz- und Informationssicherheitsgesetz (NISG) stellt die Grundlage zur ressortübergreifenden Zusammenarbeit im Bereich der Sicherheit von Netz- und Informationssystemen in Österreich dar. Dieses Gesetz ist damit die Rechtsgrundlage für die Operative Koordinierungsstruktur (OpKoord) und den Inneren Kreis der Operativen Koordinierungsstruktur (IKDOK).

Der **Innere Kreis der Operativen Koordinierungsstruktur (IKDOK)** setzt sich aus Vertreterinnen und Vertretern des Bundesministeriums für Inneres (Operative NIS-Behörde – IV/S/2 mit GovCERT, Direktion Staatsschutz und Nachrichtendienst — DSN, Cybercrime Competence Center – BK/C4), des Bundeskanzleramts (BKA), des Bundesministeriums für europäische und internationale Angelegenheiten (BMEIA) sowie des Bundesministeriums für Landesverteidigung (Abwehramt – AbwA, Direktion IKT & Cyber, Heeres-Nachrichtenamt – HNaA) zusammen. Die Abteilung IV/S/2 des BMI übernimmt dabei administrative und koordinierende Aufgaben des Gremiums und leitet die Sitzungen. Die anlassbezogen bzw. regelmäßig erstellten Lagebilder sowie weitere Informationen der einzelnen Organisationseinheiten des IKDOK und der OpKoord werden den jeweiligen Zielgruppen zur Verfügung gestellt. Die Hauptaufgaben des IKDOK sind die Erfassung und Bewertung eines monatlichen Lagebildes über Risiken, Vorfälle und Sicherheitsvorfälle, die Erstellung von situativen Lagebildern, der regelmäßige Austausch sowie die Unterstützung des Koordinationsausschusses im Cyberkrisenmanagement (CKM). Dem IKDOK, unterstützt durch die OpKoord, kommt dabei im Krisenfall die Funktion einer direkten Schnittstelle zum gesamtstaatlichen Cyber-Krisenmanagement zu.

Die **Operative Koordinierungsstruktur (OpKoord)** ist eine Erweiterung des IKDOK und besteht demnach aus den im IKDOK vertretenen Teilnehmerinnen- und Teilnehmerorganisationseinheiten sowie den nach dem NISG festgestellten und eingerichteten Computer-Notfallteams. Die OpKoord kann im Anlassfall um Teilnehmerinnen und Teilnehmer wie Betreiberinnen und Betreiber wesentlicher Dienste, Anbieterinnen und Anbieter digitaler Dienste oder Einrichtungen der öffentlichen Verwaltung erweitert werden („erweiterte OpKoord“).

Auswahl von Tätigkeiten des IKDOK für das Jahr 2025: Die Arbeit von OpKoord und IKDOK findet im Rahmen von wöchentlichen Jours Fixes (online) und monatlichen Lagebildsitzungen (in Präsenz) statt. Im Beobachtungszeitraum wurden folgende Sitzungen abgehalten:

- 47 IKDOK Jours Fixes,
- zwölf Lagebild-Sitzungen und

- zehn Fragestunden mit den Bundesländern zu den aktuellen Lagebildern.

Gemäß seiner primären Aufgabenstellung wurden in diesem Zusammenhang 26 anlassbezogene bzw. regelmäßige Lagebilder erstellt, die sich wie folgt gliedern:

- Zwölf IKDOK Lagebilder
- Zwölf OpKoord Lagebilder
- Ein Sonderlagebild
- Ein Teillagebild nach Bundes-Krisensicherheitsgesetz (B-KSG)

Um die Qualität der Arbeit sicherstellen zu können, wird laufend Feedback von den jeweiligen Zielgruppen eingeholt. Im Bereich der OpKoord-Lagebilder wurde die Arbeit des Gremiums im Jahr 2025 mit 4,45 von 5 Sternen bewertet.

4.2 Cyber Sicherheit Plattform (CSP)

Die Cyber Sicherheit Plattform (CSP) hat als nationales Kooperations- und Austauschformat im November 2025 ihr zehnjähriges Bestehen gefeiert. Die Public-Private-Partnership wurde auf Basis der „Österreichischen Strategie der Cybersicherheit“ (ÖSCS) mit dem Ziel eingerichtet, einen strukturierten, sektorübergreifenden Dialog zwischen staatlichen Einrichtungen, Wirtschaft, Wissenschaft sowie Betreiberinnen und Betreibern kritischer Infrastrukturen zu ermöglichen und damit einen Beitrag zur gesamtstaatlichen Cybersicherheitsresilienz zu leisten.

Vor dem Hintergrund der zunehmenden Digitalisierung und der damit einhergehenden Komplexität von Cyberbedrohungen adressiert die CSP insbesondere die Notwendigkeit koordinierter Informationsflüsse, eines gemeinsamen Lageverständnisses sowie die Etablierung von Kooperationen in den Bereichen Sensibilisierung und Awareness sowie Forschung und Entwicklung. Die Plattform fungiert dabei als Schnittstelle zwischen unterschiedlichen Stakeholdern und unterstützt die Entwicklung gemeinsamer Problemdefinitionen, Prioritäten und Handlungsoptionen.

Mit der organisatorischen Zuordnung der Cybersicherheitsplattform Österreich zum Bundesministerium für Inneres (BMI) erfolgt eine institutionelle Weiterentwicklung der CSP. Diese Einbettung reflektiert die sicherheitspolitische Relevanz von Cybersicherheit und stärkt die Anbindung der Plattform an nationale Sicherheitsstrukturen und Entscheidungsprozesse. Auch 2026 wird die CSP die Rollen als koordinierendes Element innerhalb des Cybersicherheits-Ökosystems und etabliertes Instrument der kooperativen Cybersicherheitsstrategie in Österreich konsolidieren.

4.3 CERT-Verbund Austria

Das Computer Emergency Response Team bzw. Computersicherheits-Ereignis- und Reak-tionsteam-(CERT)-Verbund Austria wurde 2011 als Kooperation aller damals existierenden österreichischen CERTs des öffentlichen Bereichs und jener der privaten Sektoren gegründet. Ziel war, die verfügbaren Kräfte zu bündeln und das gemeinsame Know-how der CERTs optimal zu nutzen. Die Teilnahme am CERT-Verbund Austria ist freiwillig. Teilnehmende verpflichten sich zu regelmäßigem Informations- und Erfahrungsaustausch, zur Identifikation und Bereitstellung von Kernkompetenzen sowie zur Förderung der CERTs in allen Sektoren – im Sinne eines kooperativen, gemeinschaftlich geführten Verbundes.

Einer der Unterschiede zwischen einem klassischen IT-Sicherheitsteam und einem CERT ist, dass die Kommunikations- und Zusammenarbeitsbereitschaft mit Dritten ein Teil des Kernauftrags ist. Ein CERT soll Schnittstellen nach außen bieten, sich vernetzen und mit anderen Teams zusammenarbeiten. International sind die CERTs weltweit im FIRST (Forum of Incident Response and Security Teams) sowie in Europa in der Task Force CSIRT (die wörtliche Übersetzung auf „Einsatzkommando“ ist hier unpassend, es entspricht eher der Natur einer Arbeitsgruppe) und im CSIRTs-Netzwerk (siehe 2.1.6) organisiert. Ein flächendeckendes Netz an CERTs ist eines der wirksamsten Mittel zur Absicherung der vernetzten Informations- und Kommunikationssysteme. Die stetig wachsende Anzahl an CERTs, CSIRTs, Security Operations Centers (SOC) und Cyber-Defence-Teams in den österreichischen Unternehmen sowie deren gelebte enge Partnerschaft bestätigen dies.

Die aktuell 18 mitwirkenden Teams haben sich 2025 in sechs Treffen, die jeweils von ei-nem der Teilnehmenden ausgerichtet werden, ausgetauscht. Dabei steht jeder Termin unter einem Hauptthema, zu dem alle CERTs ihre Erfahrungen beitragen. Sie kommunizieren aber auch außerhalb der regelmäßigen Treffen über sichere Kommunikationskanäle bzw. persönlich, wenn es die Situation erfordert. So können über Organisations- und Unternehmensgrenzen hinweg Lagebilder rasch erstellt und Maßnahmen abgestimmt werden.

4.4 Austrian Trust Circle (ATC)

Der Austrian Trust Circle (ATC) ist eine nationale Initiative für den fachlichen Informationsaustausch zu Cybersicherheit und damit in Zusammenhang stehender Vorfälle. Der Austrian Trust Circle ist eine Initiative von CERT.at und wird in Kooperation und mit der Unterstützung der für das GovCERT zuständigen Behörde (aktuell das Bundesministerium für Inneres) und der Österreichischen Agentur für Gesundheit und Ernährungssicherheit (AGES, Betreiber des Austrian Health CERT) – den „Organisatoren“ - durchgeführt. Die Zielgruppen sind alle Sektoren der strategischen Infrastruktur sowie die öffentliche Verwaltung in Österreich. Der ATC bietet Teilnehmenden einen formellen Rahmen für praxisnahen Informationsaustausch und gemeinsame Projekte im Sicherheitsbereich.

Um das für einen „Trust Circle“ notwendige Vertrauen zu schaffen, verpflichten sich alle Teilnehmenden, den Code of Conduct einzuhalten und das Traffic-Light-Protokoll (TLP) gemäß der Definition des Forum of Incident Response and Security Teams (FIRST) zu befolgen.

Die wesentlichen Ziele des ATC sind:

- Schaffen einer Vertrauensbasis, um im Ernstfall gemeinsam agieren zu können
- Vernetzung und Informationsaustausch in und zwischen den Sektoren der kritischen Infrastruktur und der öffentlichen Verwaltung
- Kontaktaustausch zwischen den CERTs und den teilnehmenden Unternehmen, Organisationen und Behörden
- Unterstützung zur Selbsthilfe in den Sektoren im Bereich IT-Sicherheit
  - Operative Kontakte zu den CERTs, beispielsweise bei der Information über die Behandlung
  - Bei der Behandlung von Sicherheitsvorfällen in den Organisationen

Der Austrian Trust Circle besteht aus einzelnen Sektoren-Circles, die durch die Organisatoren auch durch weitere Circle erweitert werden können. Aktuell besteht der ATC aus den folgenden Circles:

- Energy/Energieerzeugung und -transport
- Finance/Finanzwesen
- ISP/Internet Service Provider
- Transportation/Transportwesen und Logistik
- Industry/Industrie
- Health/Gesundheit (gemeinsam mit der AGES organisiert)
- Government/Öffentliche Verwaltung (gemeinsam mit dem BMI organisiert)

Neben regelmäßigen Treffen innerhalb der einzelnen Sektoren-Circles wird der Austausch zwischen den Sektoren, inklusive der öffentlichen Verwaltung, jährlich im Rahmen einer zweitägigen Veranstaltung gefördert. 2025 fand diese in Kitzbühel statt.

In den vergangenen Jahren lag der Schwerpunkt der behandelten Themen bei den Vorbereitungen zur NIS-2-Richtlinie. Der Trust Circle wurde genutzt, um die aus der NIS-2-Richtlinie erwarteten Vorgaben mit den Praxiserfahrungen der Teilnehmenden zu vergleichen. Im Finanzbereich waren DORA und die daraus entstehenden Aufgaben für Unternehmen ein wichtiges Thema. 2025 gewann der Austausch rund um Aktivitäten zur Erhöhung der digitalen Souveränität an Bedeutung.

Der Trust Circle wurde auch 2025 um weitere Mitglieder erweitert. Die Teilnehmenden werden dabei in den meisten Fällen durch bereits aktive Organisationen angesprochen

und eingeladen – ein Nachweis für den Nutzen des Trust Circles in der Praxis. Aufgrund des Wachstums des ATC und um den Teilnehmenden aus den Bundesländern einen regelmäßigen Austausch zu ermöglichen, wurden die Circle-Treffen ab 2024 hybrid (online und vor Ort bei CERT.at in Wien) abgehalten.

4.5 Nationales Cybersicherheitsforschungsprogramm K-PASS

Das im Jahr 2023 ins Leben gerufene nationale Cybersicherheitsforschungsprogramm Kybernet-Pass (K-PASS) ist die erstmalige Etablierung eines vollständig auf Cybersicherheit ausgelegten Forschungsförderungsinstrumentes in Österreich. Das unter Verantwortung des Bundesministeriums für Finanzen stehende K-PASS unterstützt primär österreichische Unternehmen und Forschungseinrichtungen bei der Entwicklung neuer Technologien und der Gewinnung des erforderlichen Wissens, um die digitale Sicherheit Österreichs zu erhöhen und Wertschöpfung zu generieren. Ziel ist die Schaffung marktnaher Forschungsergebnisse zu digitaler Sicherheit für sämtliche Sicherheitsanwenderinnen und -anwender bzw. Bedarfsträgerinnen und -träger, beispielsweise die Polizei oder Feuerwehr, aber auch sicherheitsrelevante Unternehmen wie der Verbund oder der Flughafen Wien-Schwechat.

Budget	5 - 6 Mio. € für jährliche Ausschreibungen
Rechtliche Grundlage	Verwaltungsübereinkommen zwischen BKA und BMF
Programmeigentümer	BMF
Programmabwicklung	FFG
Erfolgreich geförderte Projekte	24
Ausschreibungszeitraum 2025/2026	6. Oktober 2025 bis 6. März 2026
Forschungszeitraum	Ø 2 Jahre
TRL & Förderungsintensität	Bis zum Technologiereifegrad (TRL) 6, Finanzierung bis zu 85% (Ausnahme Instrument F&E-Dienstleistungen: Finanzierung bis zu 100%)
Adressaten	Bundesministerien und sonstige Behörden, Betreiberinnen und Betreiber kritischer Infrastrukturen, Unternehmen, Forschungseinrichtungen und Universitäten

5 Cyberübungen

5.1 BlueOLEx 2025

Die „BlueOLEx“ (Blueprint Operational Level Exercise) ist eine jährlich stattfindende europäische Cyber-Krisenübung auf strategischer bzw. Führungsebene. Sie wird von der European Union Agency for Cybersecurity (ENISA) organisiert und richtet sich vor allem an hochrangige Entscheidungsträgerinnen und -träger im Bereich Cyberkrisenmanagement aus den EU-Mitgliedstaaten, die zumeist die Rolle der Executives im Netzwerk EU-CyCLONe (European Cyber Crisis Liaison Organisation Network), das für die Koordination zwischen den Mitgliedstaaten bei großen Cyberkrisen zuständig ist, innehaben. An der Übung nimmt neben den Vertreterinnen und Vertretern nationaler Behörden für Cybersicherheit und der ENISA auch die Europäische Kommission teil. Für Österreich nahm hier der EU-CyCLONe Executive teil, der im Bundesministerium für Inneres angesiedelt ist. Die Ausgabe 2025 fand am 4. November in Zypern statt und wurde von den zypriotischen Behörden, mit organisatorischer Unterstützung der ENISA, ausgerichtet. Ziel der Übung ist es, die Zusammenarbeit und Entscheidungsprozesse der EU-Mitgliedstaaten bei groß angelegten Cyberangriffen zu testen und zu verbessern. Dabei wird insbesondere überprüft, wie nationale Behörden, europäische Institutionen und Kooperationsnetzwerke in einer Krise miteinander kommunizieren, Informationen austauschen und gemeinsame Maßnahmen koordinieren. Die Übung 2025 stand im Zusammenhang mit dem aktualisierten europäischen Cyber-Blueprint, der Rollen und Verantwortlichkeiten im Fall einer Cyberkrise festlegt.

Szenario der Cyberübung: Das Szenario der BlueOLEx 2025 basierte auf realitätsnahen Cybervorfällen und simulierte groß angelegte Cyberangriffe, die mehrere kritische Sektoren innerhalb der Europäischen Union gleichzeitig betreffen könnten. Dabei wurde angenommen, dass zentrale Infrastrukturen und essenzielle Dienstleistungen – etwa Energieversorgung, Kommunikation oder digitale Dienstleistungen – durch koordinierte Cyberangriffe beeinträchtigt werden.

Im Rahmen der Übung mussten die teilnehmenden Entscheidungsträgerinnen und -träger auf diese fiktive Krise reagieren. Sie diskutierten mögliche Gegenmaßnahmen, tauschten Lageinformationen aus und koordinierten Entscheidungen zwischen nationaler und europäischer Ebene. Ein besonderer Fokus lag auf strategischen Fragen wie Krisenkommunikation, politischer Koordination sowie der Abstimmung zwischen verschiedenen Institutionen. Ziel war es, zu testen, ob bestehende Prozesse und Kommunikationswege im Ernstfall effizient funktionieren und ob eine schnelle gemeinsame Reaktion der EU möglich ist.

Die Ergebnisse der Übung zeigten vor allem, wie wichtig eine enge Zusammenarbeit zwischen den EU-Mitgliedstaaten und den europäischen Institutionen im Bereich Cybersicherheit ist. Die BlueOLEx 2025 trug dazu bei, Vertrauen und operative Zusammenarbeit zwischen den beteiligten Akteurinnen und Akteuren zu stärken. Gleichzeitig

konnten Schwachstellen in bestehenden Abläufen identifiziert werden, die dem Netzwerk später mitgeteilt wurden, und die Lücken dadurch geschlossen werden konnten. Die gewonnenen Erkenntnisse fließen also in die Weiterentwicklung des europäischen Cyberkrisenmanagements ein. Dadurch soll langfristig sichergestellt werden, dass Europa im Falle einer Cyberkrise koordiniert, schnell und effektiv handeln kann.

5.2 Locked Shields 25

Im Mai 2025 fand die „Locked Shields 2025“ statt, die größte und anspruchsvollste Live-Cyber-Verteidigungsübung der Welt. Ausgerichtet vom Cooperative Cyber Defence Centre of Excellence (CCDCOE), brachte diese Übung über 4.000 Teilnehmerinnen und Teilnehmer aus 41 Nationen zusammen. Gleichzeitig feierte sie ihr 15-jähriges Jubiläum als einzigartiges Trainingsformat.

Die Vorbereitung umfasste den Aufbau der IT-Infrastruktur, das Kennenlernen der zu schützenden Systeme in einer virtuellen Cyber Range sowie die Integration von Expertinnen und Experten aus verschiedenen Ländern sowie zivilen Partnerinnen und Partnern.

Die Teilnehmerinnen und Teilnehmer mussten unter hohem Zeitdruck nicht nur technische, sondern auch strategische Entscheidungen treffen. Diese beinhalteten rechtliche, kommunikative und politische Aspekte, die auch in realen Krisensituationen von entscheidender Bedeutung sind. Der Fokus lag auf dem Schutz kritischer Infrastrukturen, der Verfügbarkeit militärischer Systeme und der strategischen Entscheidungsfindung unter realistischen Krisenbedingungen.

Die Übung konzentrierte sich auf lebenswichtige Dienste wie Stromversorgung, Wasser und 5G-Infrastruktur sowie militärische Systeme, etwa für Luftverteidigung oder taktische Kommunikation. Die Szenarien waren an aktuellen geopolitischen Herausforderungen angelehnt. Die Locked Shields bot eine realistische Umgebung, in der nationale und internationale Cyberverteidigungsteams (Blue Teams) zivile und militärische IT-Systeme sowie kritische Infrastrukturen vor intensiven Cyberangriffen schützten. Insgesamt waren über 8.000 virtualisierte Systeme mehr als 8.000 Angriffen ausgesetzt.

Österreich nahm mit einem hochqualifizierten Team teil. Neben den heereseigenen Cyber- und Informationsspezialistinnen und -spezialisten gehörten hierzu Cyberexpertinnen und -experten aus den Niederlanden und der National Guard Vermont (USA). Ebenso verstärkten Spezialistinnen und Spezialisten aus der kritischen Infrastruktur das über 100 Personen starke multinationale „Blue Team“ in Österreich.

5.3 Cyber Coalition 25

Die Übungsserie „Cyber Coalition“ ist eine jährliche Initiative, die darauf abzielt, die Fähigkeiten zur Bekämpfung von Cyberbedrohungen zu verbessern. Im Jahr 2025 nahm Österreich nach 2016 erstmals wieder an dieser Übung teil, um den neuen Charakter der Übung kennenzulernen und die eigenen Fähigkeiten zu stärken. Die Übung fand vom 25. November bis 5. Dezember 2025 statt und konzentrierte sich auf die Verbesserung der kollektiven Verteidigung und Resilienz gegenüber Cyberbedrohungen, von Phishing bis hin zu fortgeschrittener Cyberspionage.

Die Übung umfasste 1.300 Teilnehmerinnen und Teilnehmer aus den NATO-Mitgliedstaaten und mehreren Partnerländern. Sie bestand aus mehreren realistischen Szenarien, darunter Angriffe auf kritische Infrastrukturen und Satellitensysteme, um die Reaktionen der Teilnehmer auf komplexe Cybervorfälle zu testen. Österreich beteiligte sich an der Übung sowohl bei der Übungsleitung in Tallinn sowie mit lokalen Trainerinnen und Trainern und mehreren Cyberspezialistinnen und -spezialisten in Wien.

Die Schlüsselziele der Übung waren die Verbesserung der Interaktionsmechanismen zwischen Nationen und Partnerorganisationen, die Stärkung der operativen Fähigkeiten bei der Planung und Durchführung von Cyberoperationen sowie die Identifizierung von Fähigkeitslücken und das Testen neuer Technologien. Die Übung unterstrich die Bedeutung von modernen Cyberoperationen und förderte die Zusammenarbeit und den Wissensaustausch zwischen den Teilnehmerinnen und Teilnehmern.

Die Cyber Coalition 2025 bietet eine Plattform, um neue Verfahren und Prozesse zu testen, von den Übungserfahrungen zu lernen und sich mit der dynamischen Bedrohungslandschaft vertraut zu machen. Durch diese Übung wird das Bewusstsein für die zukünftigen Herausforderungen im Cyberraum gestärkt.

5.4 Bold Quest 25

Die „Bold Quest 2025“ fand vom 14. bis 28. September 2025 im Rahmen des State Partnership Program in den USA im Fort Barfoot in Virginia statt. Die Übung wurde von den USA geleitet und umfasste eine Mischung aus Command Post und Simulation Exercise.

An der Übung nahmen ungefähr 1.850 Teilnehmerinnen und Teilnehmer aus 21 Ländern teil, darunter auch Österreich, u. a. mit zivilen Expertinnen und Experten. Die Schwerpunkte lagen in den Bereichen Cyber und Coalition Intelligence, Surveillance and Reconaissance (CyISR).

Im Cyber-Bereich stand die Verteidigung gegen Cyber-Angriffe in einer realistischen Umgebung im Mittelpunkt. Im CyISR-Bereich nahmen 14 Nationen teil, mit dem Ziel, einen vollständigen ISR-Zyklus inklusive Cyber- und Weltraumkomponenten zu implementieren. Ein besonderer Fokus lag auf der Integration von künstlicher Intelligenz.

Das nationale Ziel Österreichs war die Stärkung und Entwicklung von Fähigkeiten im Cyber-Schutz und in der Cyber-Bedrohungsanalyse in einem realistischen Szenario. Die österreichischen Teilnehmerinnen und Teilnehmer profitieren von einer Bewusstseinsbildung über die Digitalisierung von Führungsprozessen in einem höheren Kommando, das sie bei den eigenen, nationalen Abläufen nutzen können.

Zusammenfassend ist die Teilnahme an der Bold Quest ein wichtiger Schritt zur Stärkung internationaler Zusammenarbeit und zur Weiterentwicklung von Fähigkeiten der Cyberkräfte.

6 Zusammen-fassung

Die Lage der Cybersicherheit in Österreich im Jahr 2025 war geprägt von einer Vielzahl von Bedrohungen und Herausforderungen. Ransomware-Angriffe stellten eine der zentralen Cyberbedrohungen dar. Die Angriffsmethoden wurden immer komplexer, und Cybergruppierungen nutzten automatisierte Prozesse und Technologien wie künstliche Intelligenz (KI), um Phishing-Kampagnen authentischer und wirksamer zu gestalten. Ein weiterer Trend war die Zunahme von „Ransomware-as-a-Service"-Angriffen, bei denen spezialisierte Gruppen ihre Schadsoftware anderen Kriminellen zur Verfügung stellten. Dies führte zu einer Senkung der Einstiegshürde für Angriffe und einer Steigerung der Qualität der Angriffe.

Die Bedrohungslage im Cyberraum wurde auch durch geopolitische Konflikte und nachrichtendienstliche Aktivitäten verschärft. Der Israel-Palästina-Konflikt hatte ein weiteres Konfliktfeld im Cyberbereich geöffnet, in dem staatliche Akteurinnen und Akteure, hacktivistische Tätergruppierungen und cyberkriminelle Netzwerke agierten. Es kam zu einem erhöhten Aufkommen von Denial-of-Service-(DDoS)-Angriffen und Hack-and-Leak-Aktivitäten.

Die jährliche Befragung von Unternehmen der kritischen Infrastruktur sowie von führenden privaten Unternehmen der Cybersicherheitsbranche zeigte, dass die Mehrheit der befragten österreichischen Unternehmen aus diesem Bereich in Maßnahmen zur Cybersicherheit investierte. Lediglich rund vier Prozent der befragten Organisationen reduzierten ihr Budget für IT-Sicherheit im Vergleich zum Vorjahr. Die im Beobachtungszeitraum umgesetzten Maßnahmen umfassten sowohl technische als auch organisatorische Initiativen zur Stärkung der Informationssicherheit sowie zur Verbesserung der Transparenz in der IT- und Infrastrukturumgebung. Zu den zentralen Maßnahmen zählten insbesondere der Einsatz beziehungsweise die Weiterentwicklung von Security-Information-and-Event-Management-(SIEM)-Lösungen und Security Operations Centers (SOC) zur kontinuierlichen Überwachung sicherheitsrelevanter Ereignisse.

Die Betrachtung der polizeilichen Kriminalstatistik zeigte, dass die Zahl der angezeigten Delikte im Jahr 2025 um 1,8 Prozent gegenüber dem Jahr 2024 gestiegen war. Die genauen Deliktszahlen wurden jährlich im Frühjahr mit der kriminalpolizeilichen Kriminalstatistik veröffentlicht. Eine tiefergehende Analyse und Beschreibung der kriminalpolizeilichen Phänomene erfolgten mit dem jährlichen Cybercrime-Report des Bundeskriminalamts.

Die Cyberlage im Jahr 2025 war aus Sicht der Landesverteidigung weiterhin von hoher Volatilität geprägt. Die Entwicklungen des Vorjahres haben deutlich gezeigt, dass sich der Cyberraum dauerhaft als eigenständige militärische Domäne etabliert hat und in modernen Konflikten und insbesondere im Rahmen der „Hybriden Kriegsführung" eine zentrale Rolle einnimmt. Cyberangriffe waren längst nicht mehr nur Begleiterscheinung klassischer militärischer Auseinandersetzungen, sondern wurden gezielt als strategisches

Instrument zur Destabilisierung von Staaten, zur Beeinflussung politischer Entscheidungsprozesse sowie zur Schwächung militärischer Führungs- und Einsatzfähigkeit eingesetzt.

Die verfassungsschutzrelevante Cyberlage in Österreich im Jahr 2025 war geprägt von einer Vielzahl von Bedrohungen und Herausforderungen. Österreich stand unverändert im Fokus fremdstaatlicher, nachrichtendienstlicher Aktivitäten. Dies hatte einerseits historische Gründe, lag andererseits aber vor allem in der geografischen Lage des Landes, seiner EU-Mitgliedschaft, im Vorhandensein von speziellem Know-how in Forschung und Technik sowie in der Funktion Österreichs als Gastgeberstaat der Vereinten Nationen und anderer internationaler Organisationen begründet.

Insgesamt war die Lage der Cybersicherheit in Österreich im Jahr 2025 komplex und vielschichtig. Die Bedrohungen kamen von verschiedenen Seiten, und die Abwehr dieser Bedrohungen erforderte eine enge Zusammenarbeit zwischen den verschiedenen Akteurinnen und Akteuren, einschließlich der Behörden, der Wirtschaft und der Zivilgesellschaft. Die Zukunft der Cybersicherheit in Österreich würde von der Fähigkeit abhängen, diese Bedrohungen zu erkennen und abzuwehren, und von der Entwicklung von Strategien und Maßnahmen, um die Cybersicherheit zu stärken und die Resilienz gegenüber Cyberangriffen zu erhöhen.

Bundesministerium für Inneres
Herrengasse 7, 1010 Wien
post@nis.gv.at
bmi.gv.at