

2025

Verfassungs- schutzbericht

Verfassungsschutzbericht 2025

Wien, 2026

Impressum

Medieninhaber, Verleger und Herausgeber:

Bundesministerium für Inneres (BMI)
Direktion Staatsschutz und Nachrichtendienst (DSN)
1010 Wien, Herrengasse 7
+43 1 531 26-0
bmi.gv.at

Fotos:

Bundesministerium für Inneres (BMI), Direktion Staatsschutz und Nachrichtendienst (DSN)

Gestaltung:

BMI Referat I/C/10/a (Strategische Kommunikation und Kreation)

Druck:

Digitalprintcenter des BMI
1010 Wien, Herrengasse 7

Wien, 2026

Copyright und Haftung:

Auszugsweiser Abdruck ist nur mit Quellenangabe gestattet, alle sonstigen Rechte sind ohne schriftliche Zustimmung des Medieninhabers unzulässig.

Es wird darauf verwiesen, dass alle Angaben in dieser Publikation trotz sorgfältiger Bearbeitung ohne Gewähr erfolgen und eine Haftung des Bundesministeriums und der Autorin / des Autors ausgeschlossen ist. Rechtsausführungen stellen die unverbindliche Meinung der Autorin / des Autors dar und können der Rechtsprechung der unabhängigen Gerichte keinesfalls vorgreifen.

Rückmeldungen: Ihre Überlegungen zu vorliegender Publikation übermitteln Sie bitte an empfaenger@bmi.gv.at.

Inhalt

Vorwort I.....	6
Vorwort II.....	7
Vorwort III	8
Abkürzungsverzeichnis	10
1 Über den Verfassungsschutz.....	16
1.1 Aufgaben und Aufbau des Verfassungsschutzes in Österreich.....	17
1.2 Rechtliche Kontrolle im Verfassungsschutz.....	19
1.2.1 Operative Kontrolle	19
1.2.2 Strukturelle Kontrolle	20
1.2.3 Parlamentarische Kontrolle	21
1.2.4 Weitere Kontrollinstanzen.....	21
1.3 SNG-Novelle.....	21
2 Verfassungsschutzrelevante Phänomenbereiche.....	23
2.1 Rechtsextremismus	24
2.1.1 Überblick.....	24
2.1.2 Aktuelle Lage	24
2.1.3 Fälle 2025.....	35
2.1.4 Trends und Entwicklungstendenzen	37
2.1.5 Zahlen/Daten/Fakten	43
2.2 Heterodoxer Extremismus	49
2.2.1 Überblick.....	49
2.2.2 Aktuelle Lage	51
2.2.3 Fälle 2025.....	56
2.2.4 Trends und Entwicklungstendenzen	57
2.2.5 Zahlen/Daten/Fakten	60
2.3 Linksextremismus.....	63
2.3.1 Überblick.....	63
2.3.2 Aktuelle Lage	65
2.3.3 Fälle 2025.....	68
2.3.4 Trends und Entwicklungstendenzen	69
2.3.5 Zahlen/Daten/Fakten	73
2.4 Auslandsbezogener Extremismus	78

2.4.1 Überblick.....	79
2.4.2 Aktuelle Lage.....	79
2.4.3 Trends und Entwicklungstendenzen	88
2.4.4 Zahlen/Daten/Fakten	91
2.5 Islamistischer Extremismus und Terrorismus.....	95
2.5.1 Überblick.....	97
2.5.2 Aktuelle Lage.....	98
2.5.3 Fälle 2025.....	109
2.5.4 Trends und Entwicklungstendenzen	112
2.5.5 Zahlen/Daten/Fakten	117
2.6 Spionage und nachrichtendienstliche Aktivitäten.....	121
2.6.1 Überblick.....	121
2.6.2 Aktuelle Lage.....	123
2.6.3 Fälle 2025.....	145
2.6.4 Trends und Entwicklungstendenzen	147
2.6.5 Zahlen/Daten/Fakten Spionage.....	155
2.6.6 Zahlen/Daten/Fakten staatschutzrelevante Cyberangriffe	156
2.7 Internationaler illegaler Waffenhandel	157
2.7.1 Überblick.....	157
2.7.2 Aktuelle Lage.....	158
2.7.3 Fälle 2025.....	160
2.7.4 Trends und Entwicklungstendenzen	162
2.7.5 Zahlen/Daten/Fakten	165
2.8 Proliferation	167
2.8.1 Überblick.....	167
2.8.2 Aktuelle Lage.....	169
2.8.3 Fälle 2025.....	172
2.8.4 Trends und Entwicklungstendenzen	174
2.8.5 Zahlen/Daten/Fakten	177
3 Schutz und Prävention	178
3.1 Schutz der Obersten Organe und verfassungsmäßigen Einrichtungen	179
3.1.1 Überblick.....	179
3.1.2 Aktuelle Lage.....	180
3.1.3 Fälle 2025.....	182
3.1.4 Trends und Entwicklungstendenzen	183

3.1.5	Initiativen und Maßnahmen	186
3.2	Schutz ausländischer Vertretungen, Vertreterinnen und Vertreter ausländischer Staaten und internationaler Organisationen	186
3.2.1	Überblick.....	186
3.2.2	Aktuelle Lage	186
3.2.3	Trends und Entwicklungstendenzen	187
3.2.4	Zahlen/Daten/Fakten	190
3.3	Schutz kritischer Infrastruktur	192
3.3.1	Überblick.....	192
3.3.2	Aktuelle Lage	193
3.3.3	Vorfälle 2025	196
3.3.4	Trends und Entwicklungstendenzen	198
3.3.5	Zahlen/Daten/Fakten	200
3.3.6	Initiativen und Maßnahmen der DSN.....	200
3.4	Wirtschaftsschutz.....	204
3.4.1	Innentäterschaft im Kontext des Wirtschaftsschutzes.....	206
3.4.2	Mobiles Präventionsteam als Instrument zur Stärkung der betrieblichen Resilienz.....	206
3.4.3	Mehrwert für Unternehmen und Hochschulen	208
3.4.4	Unternehmen mit erhöhtem Risikoprofil: Start-ups, KMU und innovationsgetriebene Betriebe im Fokus	208
3.4.5	Kleine und mittlere Unternehmen: Hidden Champions im Schatten des globalen Wettbewerbs.....	209
3.4.6	Wirtschaftsschutz 2025: Risikoabschätzung im Kontext chinesischer Joint Ventures.....	209
3.4.7	Radikalisierung im öffentlichen Diskurs im Kontext des Wirtschaftsschutzes	210
3.5	Cyber Security Center	212
3.6	Extremismusprävention und Deradikalisierung.....	213
3.6.1	Strategische Prävention.....	213
3.6.2	Staatsschutzprävention	219
3.6.3	Radikalisierungs- und Rückfallprävention.....	223
3.7	Sicherheitsüberprüfungen im Rahmen des Sicherheitspolizeigesetzes	225
3.8	Zuverlässigkeitsüberprüfungen im Kontext des Luftfahrtgesetzes.....	227

Vorwort I



A handwritten signature in black ink, appearing to read 'G. Karner', written in a cursive style.

Gerhard Karner
Bundesminister
für Inneres



A handwritten signature in black ink, appearing to read 'F. Ruf', written in a stylized, cursive font.

Franz Ruf
Generaldirektor für die
öffentliche Sicherheit

Sehr geehrte Damen und Herren,

der Verfassungsschutz ist eine der fundamentalen Säulen unserer demokratischen Gesellschaft. Er sorgt dafür, dass unsere Grundrechte und Freiheiten geschützt werden und dass die Bürgerinnen und Bürger Österreichs in Sicherheit leben können. In einer Zeit, in der sich die Bedrohungslage ständig wandelt und neue Herausforderungen entstehen, ist die Arbeit des Verfassungsschutzes von entscheidender Bedeutung. Sie verbindet Expertise und Analyse, um Österreich vor aktuellen und zukünftigen Bedrohungen zu schützen.

Der Verfassungsschutz muss in der Lage sein, Gefahren frühzeitig zu erkennen und entsprechende Maßnahmen zu ergreifen. Dies erfordert nicht nur moderne Technologien und rechtliche Rahmenbedingungen, sondern auch eine enge Zusammenarbeit mit nationalen und internationalen Partnern. Nur durch ein gemeinsames Vorgehen können wir den Herausforderungen der heutigen Zeit gerecht werden.

Im Jahr 2025 standen die Sicherheitspolitik und der Verfassungsschutz vor neuen Herausforderungen. Die Bedrohung durch extremistische Bestrebungen bleibt auf einem hohen Niveau. Eine besondere Herausforderung stellt die zunehmende Radikalisierung im digitalen Raum dar. Der Terroranschlag in Villach im Februar 2025 hat uns die unmittelbaren Auswirkungen der Online-Radikalisierungsprozesse aufgezeigt. Extremistische Inhalte verbreiten sich rasant über Online-Plattformen und verschlüsselte Kommunikationsdienste. Dies macht es notwendig, dass wir auch in Zukunft unsere Fähigkeiten zur Überwachung und Analyse dieser Kommunikationswege weiterentwickeln.

Ausländische Akteure versuchen durch die Verbreitung von Desinformation und hybride Aktivitäten die Stabilität der Republik zu schwächen. Diese Bedrohungen erfordern ständige Aufmerksamkeit und proaktive Herangehensweise, um sie effektiv zu bekämpfen. Wer unsere Verfassung angreift, trifft auf einen entschlossenen Rechtsstaat.

Die Direktion Staatsschutz und Nachrichtendienst (DSN) leistet hierzu einen unverzichtbaren Beitrag. Ihre Mitarbeiterinnen und Mitarbeiter sorgen durch ihre professionelle und sorgfältige Arbeit für die Aufrechterhaltung der Sicherheit Österreichs. Angesichts der aktuellen Bedrohungslage wird deutlich: Wachsamkeit bleibt notwendig. Doch unsere Verfassung ist stark und wir werden sie entschlossen schützen.

Vorwort II

Sehr geehrte Leserinnen und Leser,

in einer Demokratie sind Sicherheit und Freiheit untrennbar miteinander verbunden. Beide Aspekte sind entscheidend für das Wohl und die Stabilität unserer Gesellschaft. Die Direktion Staatsschutz und Nachrichtendienst sowie die Landesämter Staatsschutz und Extremismusbekämpfung (LSE) sind in allen Bundesländern Österreichs tätig, wenn verfassungsfeindliche Angriffe drohen. Als erste rote Linie des demokratischen Rechtsstaates sorgt der Verfassungsschutz dafür, dass Bedrohungslagen weit im Vorfeld erkannt und abgewehrt werden. Er ist ein zentraler Pfeiler im Schnittpunkt der inneren und äußeren Sicherheit, der besonders in angespannten Zeiten Österreichs Sicherheit gewährleistet.

Im Jahr 2025 sahen wir uns mit einer Vielzahl unterschiedlicher Gefahren konfrontiert, die zunehmend vernetzt auftraten. Die anhaltenden Bedrohungen durch transnationale Terrororganisationen, die Zunahme extremistischer Akteure mit erhöhter Gewaltbereitschaft und die Herausforderungen durch Spionageaktivitäten machten dies besonders deutlich. Digitale Bedrohungen, die Verdichtung von Desinformation und Cyberangriffe standen im Fokus der Arbeit des Verfassungsschutzes. Der Online-Raum hat sich zu einem entscheidenden Faktor entwickelt, der sich durch alle verfassungsschutzrelevanten Aufgabenbereiche zieht. Die rasant steigende Anzahl von radikalen, digitalen Inhalten und die damit verbundenen Radikalisierungsprozesse erfordern unsere volle Aufmerksamkeit. Die Anziehungskraft extremistischer Gruppierungen jeglicher Ideologie, insbesondere auf Jugendliche und junge Erwachsene, verstärkte sich, terroristische Online-Propaganda nahm laufend zu und Radikalisierung fand größtenteils in sozialen Netzwerken statt.

Die aktuelle Lage erfordert unsere volle Aufmerksamkeit und unser Engagement. Der Verfassungsschutz arbeitet in diesem Zusammenhang auf nationaler und internationaler Ebene vernetzt mit Partnerinnen und Partnern zusammen, um die Sicherheit unserer Bürgerinnen und Bürger in Österreich zu gewährleisten. Prävention ist dabei das Schlüsselwort. Ich danke allen Mitarbeiterinnen und Mitarbeitern des Verfassungsschutzes für ihren unermüdlichen Einsatz und ihre wertvolle Arbeit.

Der Schutz unserer Verfassung ist nicht allein Aufgabe staatlicher Institutionen. Demokratie lebt vom Engagement ihrer Bürgerinnen und Bürger. Ein starker gesellschaftlicher Zusammenhalt, basierend auf unseren gemeinsamen demokratischen Werten, ist der Grundpfeiler einer widerstandsfähigen Republik. Unsere Demokratie ist stark – wenn wir sie gemeinsam schützen.



A handwritten signature in black ink, appearing to read 'J. Leichtfried', written in a cursive style.

Jörg Leichtfried
Staatssekretär im
Bundesministerium für
Inneres

Vorwort III



Moderne Kontinuität zur Sicherheit der Republik – Einleitende Worte der Direktorin der DSN

Sehr geehrte Leserinnen und Leser,

der jährliche Verfassungsschutzbericht der Direktion Staatsschutz und Nachrichtendienst ist ein zentraler Bestandteil unserer Arbeit im Dienste der Sicherheit für die Republik Österreich. Der Verfassungsschutz, bestehend aus der DSN und den neun Landesämtern Staatsschutz und Extremismusbekämpfung, steht im Mittelpunkt der Gewährleistung der Sicherheit für die Bürgerinnen und Bürger Österreichs – ein Auftrag, der uns täglich vor komplexe und sich stetig wandelnde Herausforderungen stellt. Dabei waren in den vergangenen Jahren diverser werdende Bedrohungslagen zu bewältigen. In solchen Zeiten erfüllt die DSN eine besonders verantwortungsvolle Aufgabe: Als Frühwarnsystem blickt der Nachrichtendienst dorthin, wo potenzielle Gefahren entstehen, und der Staatsschutz sichert deren effektive Abwehr. Dieses Zusammenspiel zwischen Vorausschau und Reaktion ist in volatilen Sicherheitslagen entscheidend.

Sylvia Mayer
Direktorin der DSN

Das Jahr 2025 war besonders durch dynamische Entwicklungen in drei Bereichen geprägt: Extremismus, Terrorismus und staatliche Einflussnahme. Der Schutz der Bevölkerung vor diesen Gefahren blieb daher ebenso ein zentraler Schwerpunkt des Verfassungsschutzes wie auch der Schutz Oberster Organe sowie verfassungsmäßiger und kritischer Einrichtungen.

Die höchste Gefährdungslage im vergangenen Jahr ging vom islamistischen Terrorismus aus. Die Radikalisierung im digitalen Raum, insbesondere durch die Verbreitung extremistischer Inhalte auf Online-Plattformen und verschlüsselten Kommunikationsdiensten, stellte eine besondere Herausforderung dar. Der islamistische Extremismus war aufgrund der anhaltenden Attraktivität einzelner terroristischer Gruppierungen, der Zunahme von Aktivitäten im digitalen Raum innerhalb der letzten Jahre und der Mobilisierung durch Ereignisse wie den 7. Oktober 2023 ein zentraler Risikofaktor. In Österreich konnten 2025 mehrere Radikalisierungsnetzwerke identifiziert werden, die versuchen, vor allem die junge Generation zu indoktrinieren. Dies geschieht neben der Verbreitung radikaler und gewaltvoller Botschaften auch durch Inhalte, die sich an der Grenze des Legalen bewegen und – unterstützt durch entsprechende Algorithmen – Radikalisierungsprozesse beschleunigen. Dies äußerte sich in der gegenüber dem Vorjahr um über 40 Prozent gestiegenen Anzahl islamistisch motivierter Tathandlungen.

Gleichzeitig haben sich sowohl der Links- als auch der Rechtsextremismus weiter verfestigt, wobei der rechtsextreme Akzelerationismus ein zunehmend transnational geprägtes Teilphänomen darstellt. Das dabei offene Bekenntnis zur Zerstörung der bestehenden demokratischen Ordnung sowie die erkennbaren Verbindungen zu anderen Subkulturen wie der „Incel“-Szene oder misanthropischen Online-Gemeinschaften stellen einen 2025

hervorstechenden Trend dar. Auch die Mobilisierung und Vernetzung über Online-Gruppen, darunter auch Gaming-Chaträume, steigt weiter an. Der Linksextremismus, insbesondere im Zusammenhang mit Antisemitismus und radikalem Aktionismus, stellt ebenfalls eine Bedrohung dar. Dabei ist eine evidente Akzeptanz rechtswidriger Aktionsformen zu erkennen, wobei die Bandbreite von symbolischem Protest bis zu sicherheitsgefährdenden Mitteln reicht.

Neben der innerstaatlichen Bedrohung durch Extremismus und Terrorismus bleibt die Gefahr durch nachrichten- und geheimdienstliche Tätigkeiten staatlicher Akteure, darunter Russland, China und der Iran, unvermindert. Russland verfolgt eine Strategie der hybriden Bedrohung, die durch Cyberangriffe, Spionage und Desinformation geprägt ist. Die Bereiche Politik, Wirtschaft, Wissenschaft und Forschung sind relevante Aufklärungsziele für ausländische Nachrichtendienste in Österreich und somit besonders schützenswert, denn die Folgen von Spionage und Einflussnahme führen zur langfristigen Destabilisierung eines Landes. Die DSN verfolgt hier eine strategische Herangehensweise, die sich durch enge Zusammenarbeit sowohl mit relevanten Behörden als auch Unternehmen sowie Wissenschaft und Forschung zeigt.

Zur Bewältigung dieser durch zahlreiche Herausforderungen geprägten Bedrohungslage setzt die DSN intern auf Stabilität und Kontinuität, während gleichzeitig die Digitalisierung und Weiterentwicklung rechtlicher sowie technischer Möglichkeiten priorisiert werden. Ein ausdrücklicher Fortschritt wurde durch die Möglichkeit der Überwachung verschlüsselter Kommunikation von Hochrisikogefährdern erzielt, an deren Umsetzung seit dem entsprechenden Beschluss im vergangenen Jahr gearbeitet wird. Die DSN investiert darüber hinaus in moderne Technologien sowie Aus- und Fortbildungen, um die Effizienz und Effektivität ihrer Arbeit zu steigern. Auch die Kooperation mit nationalen und internationalen Partnern bleibt ein Schlüssel für die Bewältigung der komplexen Sicherheitslage. Gleichzeitig wurde die Zusammenarbeit mit der Zivilgesellschaft und der Wissenschaft verstärkt, um eine umfassende Sicherheitsstrategie zu etablieren.

Sicherheit erfordert das Zusammenspiel unterschiedlicher Faktoren: Prävention, Früherkennung von Gefahren und eine konsequente Umsetzung der Strafverfolgung sind entscheidende Maßnahmen, die der Verfassungsschutz in seiner täglichen Arbeit setzt. Mit dieser Arbeit sichert die DSN gemeinsam mit den LSE die Grundlagen der Demokratie und schützt Österreich vor allen Formen verfassungsfeindlicher Bedrohungen.

Ich danke allen Mitarbeiterinnen und Mitarbeitern der DSN und LSE für ihre unerlässliche Arbeit und unseren Partnerinnen und Partnern sowie der Bevölkerung für ihr Vertrauen und ihre Unterstützung. Der vorliegende Verfassungsschutzbericht soll nicht nur eine Bilanz ziehen, sondern auch einen Blick in die Zukunft werfen – auf die kontinuierliche Weiterentwicklung unseres Aufgabenfeldes und die Stärkung der Sicherheitsinfrastruktur in Österreich.

Abkürzungsverzeichnis

AbzG	Abzeichengesetz
AGE	Anti-Government Extremism; dt.: Anti-Regierungs-Extremismus
AGesVG	Anti-Gesichtsverhüllungsgesetz
APCIP	Austrian Program for Critical Infrastructure Protection; dt.: Österreichisches Programm zum Schutz kritischer Infrastrukturen
APT	Advanced Persistent Threat
AQ	al-Qaida
AQAP	al-Qaida in the Arabian Peninsula; dt.: al-Qaida auf der Arabischen Halbinsel
ASAGE	Anti-System-Anti-Government Extremism; dt.: Anti-System-Anti-Regierungs-Extremismus
AußWG	Außenwirtschaftsgesetz
AWD	Atomwaffen-Division
BAK	Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung
BBU	Bundesagentur für Betreuungs- und Unterstützungsleistungen
BFA	Bundesamt für Fremdenwesen und Asyl
BK	Bundeskriminalamt
BKA	Bundeskanzleramt
BMAW	Bundesministerium für Arbeit und Wirtschaft
BMEIA	Bundesministerium für europäische und internationale Angelegenheiten
BMI	Bundesministerium für Inneres
BMIMI	Bundesministerium für Innovation, Mobilität und Infrastruktur
BMJ	Bundesministerium für Justiz
BMWET	Bundesministerium für Wirtschaft, Energie und Tourismus
BNED	Bundesweites Netzwerk Extremismusprävention und Deradikalisierung
BPD	Bundespolizeidirektion
B-VG	Bundes-Verfassungsgesetz
BVwG	Bundesverwaltungsgericht
bzw.	beziehungsweise
CEB	Cultural Exchange Bureau; dt.: Kulturaustauschbüro (nordkoreanischer Nachrichtendienst)
ChemG	Chemikaliengesetz
ca.	circa
CMG	Corona-Maßnahmen-Gegner
CNE	Computer Network Exploitation; dt.: Ausbeutung von Computernetzwerken
CNC	Computerized Numerical Control; dt.: Computerisierte numerische Steuerung
COVID-19	Coronavirus Disease-2019; dt.: Coronavirus-Krankheit 2019

CSAIR	Center for Security Analysis and Intelligence Research; dt.: Zentrum für Sicherheitsanalysen und nachrichtendienstliche Forschung
CSC	Cyber Security Center; dt.: Zentrum für Cybersicherheit
DACH-Region	Deutschland, Österreich und Schweiz
DDoS	Distributed Denial of Service; dt.: Verteilte Verweigerung des Dienstes
d. h.	das heißt
DHKP/C	Devrimci Halk Kurtuluş Partisi-Cephesi, dt.: Revolutionäre Volksbefreiungspartei/Front
DSN	Direktion Staatsschutz und Nachrichtendienst
dt.	deutsch
DWR	Die wahre Religion (Verein)
EGVG	Einführungsgesetz zu den Verwaltungsverfahrensgesetzen
etc.	et cetera
EU	Europäische Union
FEYKOM	Rat der kurdischen Gesellschaft in Österreich
FKD	Feuerkrieg-Division
FPÖ	Freiheitliche Partei Österreichs
FSB	Federalnaja Sluschba Besopasnosti; dt.: Föderaler Dienst für Sicherheit (russischer Inlandsnachrichtendienst)
FTF	Foreign Terrorist Fighters; dt.: Ausländische terroristische Kämpfer
GEAS	Gemeinsames Europäisches Asylsystem
GewO	Gewerbeordnung
GP	Gesetzgebungsperiode
GPS	Global Positioning System; dt.: Globales Positionsbestimmungssystem
GU	Glawnoje Uprawlenije; dt.: Hauptverwaltung für Aufklärung (militärischer Nachrichtendienst Russlands)
HEX	Heterodoxer Extremismus
HTS	Hayat Tahrir al-Sham; dt.: Komitee zur Befreiung Syriens/der Levante
HUMINT	Human Intelligence; dt.: Menschliche Aufklärung
HuT	Hizb ut-Tahrir; dt.: Partei der Befreiung
IBÖ	Identitäre Bewegung Österreich
ICS	Industry Control System; dt.: Industrielles Steuerungssystem
IDCPC	International Department of the Central Committee of the Communist Party of China; dt.: Internationale Abteilung des Zentralkomitees der Kommunistischen Partei Chinas
inkl.	inklusive
InvKG	Investitionskontrollgesetz
IoT	Internet of Things; dt.: Internet der Dinge
IRGC	Islamic Revolutionary Guard Corps; dt.: Korps der Islamischen Revolutionsgarden
IRGC-IO	Intelligence Organization of the Islamic Revolutionary Guard Corps; dt.: Geheimdienstorganisation des Korps der Islamischen Revolutionsgarden

IS	Islamischer Staat
ISKP	Islamischer Staat Khorasan Provinz
ISSP	Islamischer Staat Sahel Provinz
ISIS	Islamischer Staat im Irak und Syrien
IT	Informationstechnologie
i. V. m.	in Verbindung mit
IZH	Islamisches Zentrum Hamburg
IZIA	Islamisches Zentrum Imam Ali
KED	Koordinationsstelle Extremismusprävention und Deradikalisierung
KGB	Komitet gossudarstwennoi besopasnosti; dt.: Komitee für Staatssicherheit (sowjetischer In- und Auslandsgeheimdienst bis 1991; Nachfolgeorganisationen → FSB und SWR)
KI	Künstliche Intelligenz
KMG	Kriegsmaterialgesetz
KPCh	Kommunistische Partei Chinas
KSÖ	Kompetenzzentrum Sicheres Österreich
LEX	Linksextremismus
LFG	Luftfahrtgesetz
LGBTQIA+	Lesbian, Gay, Bisexual, Transsexual/Transgender, Queer, Intersexual and Asexual; dt.: Lesbisch, Schwul, Bisexuell, Transsexuell/Transgender, Queer, Intersexuell und Asexuell
LKA	Landeskriminalamt
LLZ	Landesleitzentrale
LSE	Landesamt Staatsschutz und Extremismusbekämpfung
MB	Muslimbruderschaft
MEG	Maß- und Eichgesetz
MeldeG	Meldegesezt
MHP	Milliyetçi Hareket Partisi; dt.: Partei der Nationalistischen Bewegung
MID	Military Intelligence Directorate; dt.: Militärischer Nachrichtendienst (militärischer Nachrichtendienst Chinas)
MKS	Maul- und Klauenseuche
MOIS	Ministry of Intelligence and Security; dt.: Ministerium für Nachrichtendienst und Staatssicherheit (ziviler In- und Auslandsnachrichtendienst Irans)
MPS	Ministry of Public Security; dt.: Ministerium für Öffentliche Sicherheit (ziviler Nachrichtendienst Chinas)
MSS	Ministry of State Security; dt.: Ministerium für Staatssicherheit (ziviler Nachrichtendienst Chinas)
NATO	North Atlantic Treaty Organization; dt.: Nordatlantikpakt-Organisation
NAP REX	Nationaler Aktionsplan Rechtsextremismus
NGO	Non-governmental Organization; dt.: Nichtregierungsorganisation
NIS	Netz- und Informationssystemicherheit

NSD	Network Systems Department; dt.: Abteilung Netzwerksysteme (militärischer Nachrichtendienst Chinas zur Fernmeldeaufklärung und Cyberspionage)
NSG	Nuclear Suppliers Group; dt.: Gruppe der nuklearen Zulieferer
Oö. PolStG	Oberösterreichisches Polizeistrafgesetz
OFAC	Office of Foreign Assets Control; dt.: Amt für die Kontrolle ausländischer Vermögenswerte
OSINT	Open Source Intelligence; dt.: öffentlich zugängliche Informationen
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
ÖVP	Österreichische Volkspartei
PBC	Project Based Collaborations; dt.: Projektbasierte Zusammenarbeit
P/CVE	Preventing/Countering Violent Extremism; dt.: Prävention/Bekämpfung von gewalttätigem Extremismus
PKK	Partiya Karkerên Kurdistanê; dt.: Arbeiterpartei Kurdistans
PPP	Public Private Partnership; dt.: Öffentlich-private Partnerschaft
PrAG	Preisauszeichnungsgesetz
RAN	Radicalisation Awareness Network; dt.: Netzwerk zur Sensibilisierung für Radikalisierung
REX	Rechtsextremismus
RGB	Reconnaissance General Bureau; dt.: Generalbüro für Aufklärung (militärischer Nachrichtendienst Nordkoreas)
RKE	Resilienz kritischer Einrichtungen
RKEG	Resilienz kritischer Einrichtungen-Gesetz
RSB	Rechtsschutzbeauftragte/r
RV	Regierungsvorlage
RWE/RMVE	Right-wing extremism / racially or ethnically motivated violent extremism; dt.: Rechtsextremismus / rassistisch oder ethnisch motivierter gewalttätiger Extremismus
SanktionenG	Sanktionengesetz
SAVAK	Sazam-e ettelaât va amniyat-e keshvar; dt.: Organisation für Information und Sicherheit des Landes (bis 1979 Bezeichnung für den iranischen Nachrichtendienst; Nachfolgeorganisation seit 1984 → MOIS, auch VAJA genannt und früher als VEVAK bekannt)
SDF	Syrian Democratic Forces; dt.: Syrische Demokratische Kräfte
SfV	Staatsfeindliche Verbindungen
SIAK	Sicherheitsakademie des Bundes
SIGINT	Signal Intelligence; dt.: Signalaufklärung
SMG	Suchtmittelgesetz
SNG	Staatsschutz- und Nachrichtendienstgesetz
SPG	Sicherheitspolizeigesetz
StA	Staatsanwaltschaft
StGB	Strafgesetzbuch

StGG	Staatsgrundgesetz
StVG	Strafvollzugsgesetz
SWR	Sluschba Wneschnei Raswedki; dt.: Dienst der Außenaufklärung (ziviler Auslandsnachrichtendienst Russlands)
TeBG	Terrorbekämpfungsgesetz
u. a.	und andere
udgl.	und dergleichen
UFWD	United Front Work Department; dt.: Abteilung Vereinigte Frontarbeit
UN	United Nations; dt.: Vereinte Nationen
usw.	und so weiter
USA	United States of America; dt.: Vereinigte Staaten von Amerika
VAJA	Wezārat-e Eṭṭelā'āt-e Ğomhūrī-ye Eslāmī-ye Īrān; dt.: Iranisches Ministerium für Nachrichtenwesen
VAPO	Volkstreue Außerparlamentarische Opposition
VbtG	Verbotsgesetz
VersG	Versammlungsgesetz
VGT	Verein gegen Tierfabriken
WA	Wassenaar-Abkommen
WaffG	Waffengesetz
WHO	World Health Organization; dt.: Weltgesundheitsorganisation
WiEReG	Register der wirtschaftlichen Eigentümer
WrJSchG	Wiener Jugendschutzgesetz
z. B.	zum Beispiel
ZÜP	Zuverlässigkeitsüberprüfung

1 Über den Verfassungsschutz



1.1 Aufgaben und Aufbau des Verfassungsschutzes in Österreich

Die Direktion Staatsschutz und Nachrichtendienst, gegründet 2021 mit Inkrafttreten des Staatsschutz- und Nachrichtendienstgesetzes (SNG), ist sowohl polizeiliche Staatsschutzbehörde als auch ziviler Inlandsnachrichtendienst. In enger Zusammenarbeit mit den neun Landesämtern Staatsschutz und Extremismusbekämpfung werden die demokratischen und rechtsstaatlichen Prinzipien Österreichs verteidigt.

Das oberste Ziel der DSN ist der Schutz der Republik Österreich sowie ihrer verfassungsmäßigen Einrichtungen und deren Handlungsfähigkeit, der Schutz der Vertreterinnen und Vertreter ausländischer Staaten, internationaler Organisationen und anderer Völkerrechtssubjekte sowie aller in Österreich lebenden Menschen vor terroristisch, ideologisch oder religiös motiviertem Extremismus und Terrorismus, vor fremder nachrichtendienstlicher Tätigkeit, vor Spionage- und Cyberangriffen sowie vor Proliferation und illegalem Waffenhandel.

Um diese Mission, den Schutz der demokratischen Freiheit und Sicherheit Österreichs, zu erfüllen, arbeiten die zwei Bereiche der DSN – der Nachrichtendienst als präventives Frühwarnsystem mitsamt der Gefahrenerforschung und der Staatsschutz als sicherheitspolizeiliche Gefahrenabwehr – eng zusammen. Das Ergebnis dieser engen Kooperation ist eine effiziente Gefahrenkontrolle, um mögliche verfassungsgefährdende Angriffe früh zu erkennen und zu verhindern.

Der Nachrichtendienst innerhalb der DSN umfasst die Gewinnung und Analyse von Informationen für die Zwecke des Verfassungsschutzes und die erweiterte Gefahrenerforschung zur Beobachtung von Gruppierungen. Der Staatsschutz hingegen umfasst den vorbeugenden Schutz vor verfassungsgefährdenden Angriffen sowie die dahingehende Gefahrenabwehr und kriminalpolizeiliche Ermittlung. Zudem finden sich im SNG besondere Befugnisse zum Zwecke der verfassungsschutzbehördlichen Aufgaben. Um die gesetzeskonforme Ausführung dieser Aufgaben sicherzustellen, unterliegen die DSN und ihre Tätigkeiten strengen gesetzlichen und demokratischen Kontrollen durch verschiedene rechtsstaatliche Einrichtungen.

Damit verfassungsschutzrelevanten Phänomenen ehestmöglich und effektiv begegnet werden kann, ist ein gesamtgesellschaftlicher Ansatz nötig. Daher misst die DSN der Prävention eine bedeutende Rolle bei der Erfüllung ihrer Aufgaben zu. Mithilfe von speziell ausgebildeten Präventionsbediensteten sowie durch Workshops zur Steigerung der Resilienz wird bei drohender oder tatsächlicher Entwicklung von Radikalisierung frühzeitig angesetzt. Die Kooperation mit nationalen Partnerorganisationen aus den Bereichen Wirtschaft, Wissenschaft und Zivilgesellschaft ist für eine flächendeckende Prävention unabdinglich und hat für die DSN Priorität.

Aufgrund der Vielseitigkeit und Komplexität des Aufgabenbereiches der DSN bedarf es der Expertisen und des Wissens aus unterschiedlichsten Bereichen. Verfassungsschützerinnen und Verfassungsschützer weisen daher bewusst unterschiedliche fachliche und berufliche Hintergründe auf, um die komplexen Aufgaben des Schutzes der demokratischen Ordnung bestmöglich abzudecken.

Alle Bediensteten der DSN haben sich vor Dienstantritt sowohl einer Sicherheitsüberprüfung als auch einer Vertrauenswürdigkeitsprüfung zu unterziehen. Um zudem ein dauerhaft hohes Maß an Professionalität, Kompetenz und Integrität sicherstellen zu können, durchlaufen alle Bewerberinnen und Bewerber ein mehrstufiges Aufnahmeverfahren. Regelmäßige Kontrollen und hohe interne Sicherheitsstandards erhalten das Sicherheitsniveau der DSN und stärken das Vertrauen internationaler Partnerorganisationen in den österreichischen Verfassungsschutz.

Vernetzung ist ein weiterer Eckpfeiler, der für die effektive Aufgabenerfüllung des Verfassungsschutzes von großer Bedeutung ist. Die globalen Veränderungen – insbesondere im virtuellen Raum – lassen Ländergrenzen verschwimmen und eine nachhaltige Gewährleistung der Sicherheit nur durch internationale Kooperation gelingen.

Aufgrund rechtlicher Vorgaben und Kontrollmechanismen sowie zur weiteren Optimierung der Aufgabenerfüllung werden die Regelungen des am 1. Dezember 2021 in Kraft getretenen Staatsschutz- und Nachrichtendienst-Gesetzes bis Ende 2026 einer Evaluierung unterzogen. Diese Evaluierung wurde im Herbst 2025 beauftragt und soll Verbesserungsmöglichkeiten im Arbeitsablauf und in der Struktur feststellen und umsetzen. Dieses Vorhaben stellt sicher, dass der österreichische Verfassungsschutz seine Aufgaben weiterhin in bestmöglichem Umfang erfüllen kann und die Sicherheit Österreichs und aller hier lebenden Menschen sichergestellt ist.

In den jährlich erscheinenden Verfassungsschutzberichten veröffentlicht die DSN ihre Arbeitsschwerpunkte des jeweiligen Jahres und ihre Einschätzungen bezüglich der ihr zugewiesenen Aufgabenbereiche. Dies beinhaltet auch entsprechende statistische Erfassungen, die auf Basis der tatsächlichen Tatzeit erfolgen. Abweichungen gegenüber anderen Auswertungen, beispielsweise jenen des Bundesministeriums für Justiz (BMJ), die auf das Datum der Berichtslegung oder des Verfahrensabschlusses abstellen und somit eine andere Zielrichtung verfolgen, sind möglich.

Nach dem Grundsatz „So viel Transparenz wie möglich – so viel Geheimhaltung wie nötig“ gibt die DSN einerseits in ihren Verfassungsschutzberichten, andererseits durch aktive Öffentlichkeitsarbeit Einblicke in die aktuellen Entwicklungen der verfassungsschutzrelevanten Phänomenbereiche. Die entsprechenden Lagebeschreibungen machen die Arbeit der österreichischen Verfassungsschützerinnen und Verfassungsschützer sichtbar. Sie agieren täglich in einem Umfeld sensibler Informationen, die akribisch zu

einem Gesamtbild über die verfassungsgefährdenden Bedrohungen gegen die Republik zusammengefügt werden.

Mit dem Ziel: Verfassung schützen – Sicherheit gewährleisten.



1.2 Rechtliche Kontrolle im Verfassungsschutz

Der Rechtsschutz stellt ein zentrales Element jedes funktionierenden Rechtsstaates dar. Die im SNG und im Sicherheitspolizeigesetz (SPG) normierten Rechtsschutzbestimmungen stellen sicher, dass der Verfassungsschutz seine Aufgaben unter Einhaltung der gesetzlichen Bestimmungen erfüllt und eine regelmäßige Kontrolle durch unterschiedliche Institutionen erfolgt.

1.2.1 Operative Kontrolle

Der Rechtsschutzbeauftragte (RSB) des Bundesministeriums für Inneres ist eine unabhängige und weisungsfreie Kontrollinstanz, die den Rechtsschutz im Bereich sicherheitspolizeilicher und verfassungsschutzrechtlicher Maßnahmen sicherstellt. Die Aufgabe des RSB sowie seiner fünf Stellvertreterinnen und Stellvertreter ist es, den Schutz der Grund- und Freiheitsrechte in jenen Bereichen sicherzustellen, in denen Bürgerinnen und Bürger von behördlichen Maßnahmen betroffen sein können, ohne davon Kenntnis zu erlangen – insbesondere im Bereich verdeckter Ermittlungs- und Überwachungsmaßnahmen. Vor dem Setzen besonderer Ermittlungsmaßnahmen nach dem SNG ist die Genehmigung des RSB einzuholen. Beabsichtigt der Verfassungsschutz die Durchführung einer Nachrichtenüberwachung, ist dem RSB Gelegenheit zu geben, sich zu dem Vorhaben zu äußern – noch vor Übermittlung des Antrags an das Bundesverwaltungsgericht (BVwG). Zudem obliegt dem RSB auch die Prüfung der gerichtlichen Entscheidung sowie die begleitende Kontrolle der Überwachung. Der RSB ist berechtigt, Rechtsmittel zugunsten der betroffenen Person gegen die Entscheidung des BVwG zu erheben. Überdies obliegt dem RSB die Kontrolle der nationalen und internationalen Datenverarbeitung des Verfassungsschutzes. Zur Erfüllung seiner Aufgaben ist dem RSB jederzeit Einblick in alle

1 Wir sind die Direktion Staatsschutz und Nachrichtendienst (DSN) – <https://www.youtube.com/watch?v=lpPSSn4YKsU>

erforderlichen Unterlagen und Aufzeichnungen zu gewähren. Stellt der RSB im Rahmen seiner Kontrolltätigkeit fest, dass durch die Verarbeitung personenbezogener Daten die Rechte von Personen verletzt wurden, die von dieser Verarbeitung keine Kenntnis haben, hat er die Pflicht, die Personen zu informieren. Sofern dies aus bestimmten, im Gesetz normierten Gründen nicht erfolgen kann, ist der RSB verpflichtet, Beschwerde bei der Datenschutzbehörde zu erheben. Der RSB erstattet dem Bundesminister für Inneres jährlich bis spätestens 31. März des Folgejahres einen Bericht über seine Tätigkeit und Wahrnehmungen im Rahmen seiner Aufgabenerfüllung.

Mit der im September 2025 in Kraft getretenen Novelle des SNG sowie der damit verbundenen Umsetzung der Gefährderüberwachung (hierzu wird auf die Ausführungen unter Punkt 1.3 verwiesen) wurde das bisherige Rechtsschutzsystem des Verfassungsschutzes um eine weitere Institution ergänzt – das Bundesverwaltungsgericht. Das BVwG wurde im Zuge der Verwaltungsgerichtsbarkeits-Novelle 2012 geschaffen und ist Teil der zweistufigen Verwaltungsgerichtsbarkeit. Es dient der gerichtlichen Kontrolle der Verwaltung und nimmt eine zentrale Rolle im verwaltungsrechtlichen Rechtsschutzsystem ein. Die Aufgabe des BVwG im Zusammenhang mit dem Verfassungsschutz erstreckt sich auf die Bewilligung der Anträge zur Durchführung jener neu geschaffenen Ermittlungsmaßnahmen, die nur in bestimmten, gesetzlich klar definierten Fällen eingesetzt werden dürfen. Die Bewilligung unterliegt strengen Voraussetzungen und darf nur in jenem Umfang erteilt werden, der zur Erfüllung der Aufgabe erforderlich ist. Erst nach Befassung des RSB sowie Bewilligung des BVwG dürfen die Maßnahmen gesetzt werden. Mit Erweiterung der Rechtsschutzinstitutionen des Verfassungsschutzes etablierte der Gesetzgeber eine unabhängige gerichtliche Kontrolle sowie verstärkten Rechtsschutz zur Gewährleistung der Verhältnismäßigkeit und des Grundrechtsschutzes.

1.2.2 Strukturelle Kontrolle

Zum Zweck der Sicherstellung der gesetzmäßigen Aufgabenerfüllung ist eine unabhängige Kontrollkommission Verfassungsschutz eingerichtet. Die Kommission setzt sich aus fünf Mitgliedern zusammen, die vom Nationalrat für eine Funktionsperiode von zehn Jahren gewählt werden. Die Mitglieder der Kontrollkommission sind bei der Ausübung ihrer Aufgaben unabhängig und weisungsfrei. Der Kommission obliegt die begleitende Kontrolle der Tätigkeit des Verfassungsschutzes in Angelegenheiten, die nicht in die Zuständigkeit des RSB oder einer sonstigen Rechtsschutzeinrichtung fallen. Die Kontrolle ist primär auf die systemische bzw. strukturelle Überprüfung ausgerichtet. Dazu zählt etwa die Prüfung der Ablauforganisation sowie von Personal- und Sachressourcen. Die DSN und die Landesämter Staatsschutz und Extremismusbekämpfung sind verpflichtet, die Kontrollkommission bei der Wahrnehmung ihrer Aufgaben zu unterstützen und ihr jederzeit Einblick in alle erforderlichen Unterlagen und Aufzeichnungen zu gewähren. Die Kommission hat dem Bundesminister für Inneres, dem Ständigen Unterausschuss des Ausschusses für innere Angelegenheiten sowie der Öffentlichkeit jährlich zu berichten.

1.2.3 Parlamentarische Kontrolle

Art. 52 Bundes-Verfassungsgesetz (B-VG) normiert die Befugnis des Nationalrats und des Bundesrats, die Geschäftsführung der Bundesregierung zu überprüfen, deren Mitglieder über alle Gegenstände der Vollziehung zu befragen und alle einschlägigen Auskünfte zu verlangen. Die parlamentarische Kontrolle dient der Kontrolle der Vollziehung durch das Parlament und ist Ausdruck des Rechtsstaats- und Demokratieprinzips. Das Interpellationsrecht gewährt den Abgeordneten die Möglichkeit, schriftliche und mündliche Anfragen an Mitglieder der Bundesregierung, und damit auch an den Bundesminister für Inneres, zu stellen. Ferner stellt der Ständige Unterausschuss des Ausschusses für innere Angelegenheiten eine wichtige Kontrollinstitution des Verfassungsschutzes (im Rahmen der parlamentarischen Kontrolle) dar. Dieser ist zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit eingerichtet. Der Ausschuss ist berechtigt, vom Bundesminister für Inneres alle einschlägigen Auskünfte sowie Einsicht in relevante Unterlagen zu begehren. Die Sitzungen des Ständigen Unterausschusses des Ausschusses für innere Angelegenheiten sind grundsätzlich geheim.

1.2.4 Weitere Kontrollinstanzen

Unbeschadet der Kontrolle des Verfassungsschutzes im Rahmen der Dienst- und Fachaufsicht durch übergeordnete Funktionsträgerinnen und Funktionsträger des BMI zählen auch die Datenschutzbehörde, die Volksanwaltschaft und der Rechnungshof zu den Kontrolleinrichtungen des Verfassungsschutzes. Sofern sicherheitspolizeiliche Maßnahmen gegen eine Person nicht unter Einhaltung der gesetzlichen Voraussetzungen durchgeführt wurden, hat jede Person das Recht auf Beschwerde bei den Verwaltungsgerichten.

1.3 SNG-Novelle

Mit RV 136 XXVIII.GP² kam es im Sommer 2025 zu einer Novelle des SNG, deren Kernstück die Einführung der Gefährderüberwachung darstellt. Der Begriff Gefährderüberwachung umfasst dabei die Telekommunikationsüberwachung (§ 11 Abs. 1 Z 8 SNG) sowie die Quellen-Telekommunikationsüberwachung (§ 11 Abs. 1 Z 9 SNG). Die Einführung der Gefährderüberwachung erfolgte dabei vor dem Hintergrund fehlender Befugnisse zur Überwachung von Gesprächsinhalten im Vorfeld von besonders schweren Straftaten. Unter solchen ist nach § 11 Abs. 1 Z 8 SNG ein verfassungsgefährdender Angriff zu verstehen, dessen Verwirklichung mit einer Freiheitsstrafe, deren Obergrenze mindestens zehn Jahre beträgt, bedroht ist. Zudem umfasst § 11 Abs. 1 Z 8 SNG auch das tatbestandsmäßige Handeln nach § 256 StGB.

² Staatsschutz- und Nachrichtendienst-Gesetz, Sicherheitspolizeigesetz u. a., Änderung (136 d. B.) | Parlament Österreich

Im Zuge der legislativen Erarbeitung dienten vor allem die verfassungsgerichtlichen Feststellungen zur strafprozessualen Quellen-Telekommunikationsüberwachung aus 2019 als maßgebliche Leitlinien. Dementsprechend basiert § 11 Abs. 1 Z 9 SNG auf einem technisch begrenzten Ansatz (Begrenzung auf Nachrichten von Applikationen), der in ein System effektiver und unabhängiger (begleitender) Kontrolle eingebettet wurde und nur einem eingeschränkten Deliktskatalog vorbehalten bleibt. Auf diesem Weg kann eine effektive Ausübung der Befugnis gewährleistet werden, ohne dabei eine rechtlich unzulässige „Online-Durchsuchung“ durchzuführen. Die dabei eingesetzte Software wird entsprechend den rechtlichen Vorgaben abgestimmt und entspricht somit den (grund)rechtlichen Anforderungen. Letztere wurden im Rahmen der RV 136 auch durch eine Zufallsfundregelung sowie einem zeitgemäßen Schutz von Berufsgeheimnisträgern erweitert.

Da gemäß Art. 10a Staatsgrundgesetz (StGG) das Fernmeldegeheimnis unter Richtervorbehalt steht, wurde zudem ein neuartiges Rechtsschutzsystem unter Einbeziehung des Bundesverwaltungsgerichts für § 11 Abs. 1 Z 8 und 9 SNG konzipiert.

Gesamthaft wird die Gefährderüberwachung künftig ihren Platz in einem dreistufigen Ermittlungsmodell finden. Dabei gilt es, in einem ersten Schritt verfassungsschutzrelevante Bedrohungslagen – vornehmlich im virtuellen Raum – möglichst früh zu erkennen. Diese Früherkennung soll in Gestalt eines Internet-Screenings ermöglicht werden. Dabei wird insbesondere durch die Sichtung offener Inhalte in sozialen Medien (OSINT) die Identifizierung und Substantiierung von frühzeitigen Anzeichen einer Radikalisierung vorangetrieben.

Darauf basierend können in einem zweiten Schritt Befugnisse des § 11 Abs. 1 bis 7 SNG eingesetzt werden, um den Gefährdungsgrad bestmöglich einordnen zu können. Sofern diese Befugnisse nicht ausreichen, kommen schließlich in einem dritten und letzten Schritt im Fall von Hochrisikogefährdern und im Vorfeld der Begehung von schweren Straftaten die Befugnisse der Gefährderüberwachung zur Anwendung, um den gesetzlichen Auftrag der Verhinderung dieser Straftaten gewährleisten zu können.

Die Telekommunikationsüberwachung gem. § 11 Abs. 1 Z 8 SNG ist mit 30. September 2025 in Kraft getreten. Demgegenüber darf die Quellen-Telekommunikationsüberwachung gem. § 11 Abs. 1 Z 9 SNG erst zum Einsatz gelangen, wenn die technischen Voraussetzungen zur rechtskonformen Durchführung vorliegen. Dieser Zeitpunkt wird seitens des Bundesministers für Inneres im Verordnungsweg kundgemacht werden.

2

Verfassungs- schutzrelevante Phänomen- bereiche

2.1 Rechtsextremismus

„**Rechtsextremismus**“ (REX) ist die Sammelbezeichnung für politische Auffassungen und Bestrebungen – von fremdenfeindlich/rassistisch/antisemitisch bis hin zur nationalsozialistischen Wiederbetätigung –, die im Namen der Forderung nach einer von sozialer Ungleichheit geprägten Gesellschaftsordnung die Normen und Regeln eines demokratischen liberalen Rechtsstaats ablehnen und diesen insbesondere/auch mit Mitteln bzw. unter Gutheißung oder Inkaufnahme von Gewalt bekämpfen.

2.1.1 Überblick

Der Begriff Rechtsextremismus bezeichnet verschiedene extremistische Strömungen, deren gemeinsames Kennzeichen es ist, dass sie die Zugehörigkeit zu einer Nation, einem Volk, einer Ethnie oder einer Kultur als entscheidend für den „Wert“ eines Menschen ansehen und folglich die Gleichwertigkeit aller Menschen ablehnen. Damit stehen sie in fundamentalem Widerspruch zur österreichischen Verfassung, zu den Grundsätzen bzw. zentralen Werten unserer demokratischen Grundordnung und zu den universellen Menschenrechten.

Weitere Gemeinsamkeiten aller Ausprägungen des Rechtsextremismus sind Antisemitismus, Fremdenfeindlichkeit, Islam- bzw. Muslimfeindlichkeit, Chauvinismus, Antipluralismus, Sozialdarwinismus und Rassismus, die Ablehnung von Migration aus bestimmten Ländern oder Regionen der Welt sowie ein autoritär geprägtes Staatsverständnis, das oftmals mit der Ablehnung der in Demokratien üblichen Gewaltenteilung einhergeht.

Als Geschichtsrevisionisten verharmlosen viele Rechtsextremistinnen und Rechtsextremisten zudem den historischen Nationalsozialismus; manche – insbesondere die Neonationalsozialistinnen und -sozialisten (Neonazis) – verherrlichen ihn und wollen eine Gesellschaft errichten, die sich grundsätzlich am Dritten Reich der Jahre 1933 bis 1945 orientiert.

In seiner extremsten Form kann sich Rechtsextremismus als (Rechts-)Terrorismus äußern, der darauf abzielt, politische Gegnerinnen und Gegner, Feindbilder und staatliche Institutionen durch Gewalt zu schwächen oder zu beseitigen.

2.1.2 Aktuelle Lage

Alte Rechte

Die Alte Rechte kann als rechtsextreme Strömung beschrieben werden, die im Unterschied zur Neuen Rechten eine eindeutig positive Haltung gegenüber dem historischen Nationalsozialismus einnimmt und (insbesondere im subkulturellen Rechtsextremismus)

Gewalt als legitimes Mittel zur Umsetzung ihrer Ziele in Betracht zieht. Folglich finden sich in den Reihen der Alten Rechten sowohl Neonationalsozialistinnen und Neonationalsozialisten, die das nationalsozialistische Dritte Reich als Zielvorstellung propagieren, als auch Gruppierungen des sogenannten subkulturell geprägten Rechtsextremismus, die sich neben ihrer ideologischen Ausrichtung oftmals auch durch ein bestimmtes Erscheinungsbild (z. B. Bekleidung) definieren, wie bspw. die Hooliganszene oder rechtsextreme Musik- und Kampfsportgruppen.

Sowohl bei der Verbreitung gemeinsam vertretener Ideologeelemente³ (die sich innerhalb der Alten Rechten in unterschiedlichem Ausmaß zeigen) als auch bei der Rekrutierung (online und offline) und dem Ausbau internationaler Kontakte agiert die Alte Rechte konspirativ und verdeckt. Zudem nutzt sie tagespolitische Themen und gesellschaftliche Krisen für ihre antidemokratischen Ziele, während sie gleichzeitig nationalsozialistisch geprägte Auffassungen (virtuell und realweltlich) propagiert und verbreitet. Damit sollen unterschiedliche Bevölkerungsschichten erreicht, beeinflusst und vereinnahmt werden.

Weiters ist bei der Alten Rechten eine deutliche Waffenaffinität zu erkennen. Diese kann sich unter anderem durch den Besitz von oder die Faszination für Waffen äußern. Als Beleg hierfür konnten im Herbst 2025 im Rahmen von Hausdurchsuchungen gegen Führungskader der rechtsextremen Szene Waffen, Munition, Kriegsmaterial sowie zahlreiche NS-Devotionalien sichergestellt werden.

Im Berichtsjahr waren weiterhin Vernetzungsbestrebungen seitens der Alten Rechten im Rahmen von Gedenkmärschen, Fußballspielen, Konferenzen, Demonstrationen sowie konspirativen Musik- und Kampfsportveranstaltungen im In- bzw. Ausland festzustellen. Insbesondere der Kampfsport dient im subkulturellen Freizeitkontext nicht nur der Vernetzung neonazistischer Gruppen, sondern auch der Glorifizierung von maskuliner Gewalt und nimmt dadurch eine strategische Bedeutung ein.

Im Jahr 2025 lässt sich im Vergleich zum Vorjahr eine intensiviertere Verbreitung von rechtsextremem Gedankengut feststellen. Verstärkt konnten im Zusammenhang mit neonazistischen Jugendgruppen (im Stil der Skinheadszenen der 1990er-Jahre) politisch motivierte Gewaltakte und Drohungen gegenüber jüdischen Personen, queeren und homosexuellen Menschen sowie politisch linksorientierten Personen festgestellt werden. Während viele dieser Zusammenschlüsse über das Internet erfolgen und oftmals nur temporär sind, können andere über den Anschluss an erfahrene Akteurinnen und Akteure oder Gruppierungen fortbestehen.

³ Zu den gemeinsam geteilten Ideologeelementen innerhalb der Alten Rechten zählen Rassismus, Islam- und Fremdenfeindlichkeit, Revisionismus, Homophobie, Antisemitismus, übersteigerter Nationalismus sowie Antipluralismus.

Vernetzungsräume

Gedenkveranstaltungen / internationale Treffen

National wie international nehmen rechtsextreme Gedenkveranstaltungen für die Alte Rechte einen zentralen Stellenwert ein. Dafür werden historische Ereignisse und Opfer von Attentaten zum Anlass genommen, um extreme Weltanschauungen zu legitimieren, rassistische sowie fremdenfeindliche Ideologien zu festigen und zu verbreiten. Daneben dienen sogenannte Trauermärsche strategisch auch der Vernetzung und Mobilisierung neuer Anhängerinnen und Anhänger.

Als Beispiele für inländische Gedenkmärsche können die von der neurechten IBÖ initiierten Veranstaltungen „Trauerzug für Alex“⁴ und „Gedenkveranstaltung für Charlie Kirk⁵ und Iryna Zarutska⁶“ sowie die „Gedenkveranstaltung Arbeitsgemeinschaft 1683“⁷ genannt werden, an denen neben Anhängerinnen und Anhänger der Neuen Rechten auch Vertreterinnen und Vertreter der Alten Rechten teilnahmen.

Auf internationaler Ebene besteht mit dem jährlich im Februar durchgeführten NS-glorifizierenden Gedenkmarsch zum sogenannten „Tag der Ehre“⁸ in Budapest ein wichtiges Vernetzungstreffen für die europäische Neonazi-Szene. Als Beweggründe für eine Teilnahme können unter anderem das ungestrafte Tragen von SS-Symbolen und Hakenkreuzen⁹ sowie die im selben Zeitraum stattfindenden Rechtsrockkonzerte in Ungarn erwähnt werden. Im Rahmen des Gedenkmarsches 2025 wurde von einem der Hauptorganisatoren zudem eine Konferenz abgehalten, bei der geschichtliche und politische Themen im Fokus standen. An den am 8. und 9. Februar 2025 in Budapest abgehaltenen Veranstaltungen nahmen mehrere rechtsextreme Akteure aus Österreich teil.

Darüber hinaus sollte am 12. April 2025 anlässlich des 81. Jahrestages der Bombardierung der Stadt Győr ein Gedenkmarsch abgehalten werden. Da der Bürgermeister von Győr den Gedenkzug in der Stadt untersagte, wurde dieser im Honvéd-Park südöstlich der

4 Bei Alex handelt es sich um jenen 14-jährigen Österreicher, der bei einem islamistischen Terroranschlag in Villach am 15. Februar 2025 getötet wurde.

5 Charlie Kirk war ein US-amerikanischer, rechtskonservativer Aktivist, der bei einem politisch motivierten Attentat am 10. September 2025 getötet wurde. Kirk wird international in rechtsextremen Kreisen als Märtyrer gefeiert.

6 Die ukrainisch stämmige Iryna Zarutska floh im Zuge des russischen Angriffskrieges gegen die Ukraine 2022 in die USA. Zarutska wurde am 22. August 2025 Opfer eines tödlichen Messerangriffs. Die Tat wird in rechtsextremen Kreisen als rassistisch motiviert gedeutet.

7 Mit der „Gedenkveranstaltung Arbeitsgemeinschaft 1683“ soll an die Türkenbelagerung Wiens im Jahr 1683 erinnert werden.

8 Bei dem NS-glorifizierenden Marsch wird auf die Schlacht um Budapest im Winter 1944/45 Bezug genommen. Rechtsextreme Akteurinnen und Akteure gedenken durch ihre Teilnahme dem Kampf der ungarischen und deutschen Soldaten gegen die Rote Armee in der Endphase des Zweiten Weltkrieges.

9 Durch eine österreichische Staatsbürgerin oder einen österreichischen Staatsbürger im Ausland gesetzte strafrechtlich relevante Handlungen nach dem Verbotsgesetz können in gewissen Fällen auch eine Strafbarkeit nach dem Verbotsgesetz in Österreich darstellen.

Hauptstadt Budapest durchgeführt. Etwa 300 Akteurinnen und Akteure nahmen an diesem Aufmarsch teil, darunter auch österreichische Neonazis.

Kampfsport

Der Neonazismus manifestiert sich nicht nur in Vereinen und festen Kameradschaften, sondern auch in subkulturellen Milieus, wie etwa in Teilen der Kampfsportszene.¹⁰ Dabei wird der Kampfsport nicht nur als Aktionsraum zur Glorifizierung von Gewalt und Männlichkeit, der Inszenierung von Kampfsport-Techniken oder dem Tragen von einschlägigen Kampfsportmarken genutzt, sondern dient auch dem Ausbau der internationalen Kontakte im Rahmen neonazistischer Veranstaltungen.

Insbesondere in subkulturell geprägten Milieus ist ein martialisches Auftreten (etwa durch die Vermummung mittels eines Tuches mit einem Totenkopf-Motiv) beim Kampfsporttraining (bspw. in Parkanlagen oder im Rahmen von gemeinsamen „Wanderausflügen“) keine Seltenheit, um Kampfsport-Techniken zu inszenieren und in Verbindung damit die Kampfbereitschaft gegenüber politischen Gegnern (wie etwa die Antifa) zu demonstrieren.¹¹

Hinsichtlich der Kampfsportkultur spielt auch die Demonstration von Macht und Gewalt zwischen rivalisierenden Hooligangruppierungen im Rahmen von sogenannten „Acker-Matches“¹² eine Rolle.

Darüber hinaus werden in kampfsportaffinen Kreisen Kleidungsstücke mit Schriftzügen rechtsextremer Kampfsportveranstaltungen oder einschlägiger Kampfsportlabels symbolisch und zur Verbreitung rechtsextremer Propaganda getragen.

Länder wie Ungarn und Tschechien gelten nicht nur für Rechtsrockkonzerte und Aufmärsche, sondern auch für einschlägige Kampfsportveranstaltungen als zentrale Anlaufstellen für viele europäische Neonazis. Dies bestätigt auch die Teilnahme von etwa 100 Personen aus Zentral- und Osteuropa am Kampfsportevent „Virtus et Honor IV“ am

10 Auf europäischer Ebene ist weiterhin eine Ausbreitung der sogenannten Active Clubs zu beobachten. Bei Active Clubs handelt es sich um ein transnationales Kampfsportnetzwerk, das sich von den USA nach Kanada und weiter nach Europa (u. a. Deutschland, Dänemark, Frankreich, Niederlande, Norwegen, Polen, Portugal und Großbritannien) ausgebreitet hat. Nach wie vor gibt es keine Anhaltspunkte dafür, dass sich der Active-Club-Trend auch in Österreich etabliert hat.

11 Rechtsextreme Gruppierungen aus subkulturell geprägten Milieus inszenieren (oft auf amateurhaftem Niveau) Kampfsport-Techniken, um diese zu filmen und über ihre Social-Media-Kanäle zu teilen. Die Videos werden mit elektronischer Techno-Musik untermalt, um das martialische Auftreten zu unterstreichen. Darüber hinaus werden diese Videos mit einem politischen Statement, wie beispielsweise „Wien bleibt Antifa Frei! Wien gehört uns“, ergänzt.

12 „Acker-Matches“ sind organisierte Treffen rivalisierender Hooligan-Gruppen außerhalb städtischer Zentren. Diese Treffen werden häufig dazu genutzt, um gewalttätige Auseinandersetzungen zu provozieren oder zu ermöglichen. Der Zeitraum nach einem Fußballspiel, die sogenannte Dritte Halbzeit, bietet dafür eine Gelegenheit.

22. März 2025 in Olmütz (Tschechien). Unter den teilnehmenden Personen befanden sich neben zahlreichen österreichischen Neonazis (unter anderem aus dem ALPEN-DONAU BOXING-Umfeld) auch deutsche Proponenten aus dem Umfeld der Veranstaltung „Kampf der Nibelungen“, der slowakischen Neonazi-Hooligan-Gruppierung Ultras Slovan Pressburg sowie der Gemer Division.

Internationale Vernetzung

Die internationalen Vernetzungsaktivitäten der Alten Rechten beschränken sich nicht allein auf die Kampfsportszene, sondern sind durchaus vielfältig. Neben Verbindungen der Hooliganszene mit nationalen und internationalen Fußballfanklubs sind internationale Vernetzungen auch bei Demonstrationen und konspirativen Musikveranstaltungen in Österreich zu beobachten.

Dabei spielen die innerhalb des Hooliganismus geteilten transnationalen Feindbilder für grenzüberschreitende Verbindungen eine zentrale Rolle. So besuchen bspw. Anhängerinnen und Anhänger der Alten Rechten nicht nur Spiele bestimmter Mannschaften im Ausland, sondern haben auch enge Verbindungen zu den lokalen rechtsextremen Hooligan-Fanszenen. Darüber hinaus werden auch konspirative Rechtsrockkonzerte von österreichischen Neonazis zum Anlass genommen, um sich mit Gleichgesinnten aus dem europäischen Ausland zu vernetzen.

Neben ihren eigenen Vernetzungsaktivitäten nutzt die Alte Rechte auch Veranstaltungen der Neuen Rechten für ihre Ziele. Beide Strömungen – die Alte wie die Neue Rechte – verfolgen zwar unterschiedliche Herangehensweisen, haben jedoch ein ähnliches Weltbild und vergleichbare Ziele. Dies erklärt auch die internationale Mobilisierung der Alten Rechten für die von der neurechten IBÖ am 26. Juli 2025 organisierte Sommerdemo bzw. Remigrationsdemo.

Gemeinsam mit erfahrenen Gruppierungen aus dem subkulturell geprägten Rechtsextremismus nahmen auch Nachwuchsgenerationen der Alten Rechten die Sommerdemo zum Anlass, um ihre Vernetzungen auszubauen und sich prominent in Szene zu setzen. Neben der rhetorischen Übernahme verschleierter Ausrufe der Neuen Rechten (wie „Remigration“) traten die Akteurinnen und Akteure aus dem subkulturell geprägten Umfeld vor allem durch ihre aggressiven und offen rechtsextremen Parolen in Erscheinung.

Social-Media-Nutzung / Social-Media-Auftritte

Neben der physischen Vernetzung der altrechten Szene sind auch soziale Medien bei der Verbreitung rechtsextremer Propaganda und der nationalen wie internationalen Vernetzung von großer Bedeutung. Neben Mainstream-Plattformen (wie X, Instagram oder YouTube) spielen für die Alte Rechte alternative Netzwerke (wie Telegram oder Threema) beim Austausch abseits der Öffentlichkeit und zur Verbreitung verschlüsselter rechtsextremer Botschaften eine große Rolle. Codes bzw. Symbole sowie vermeintlich

humoristische Darstellungen werden herangezogen, um rechtsextreme Inhalte verschleiert darzustellen und folglich nicht gegen das Verbotsgesetz zu verstoßen.

Im Zentrum des altrechten Narrativs steht die Abschaffung des Verbotsgesetzes als „Gesinnungsparagraph“, der nach Ansicht der Alten Rechten die Meinungsfreiheit einschränkt. Nach dem Verbotsgesetz angeklagte Gesinnungsgenossen werden als Opfer der Justiz dargestellt. Durch die Behauptung, dass die Angeklagten lediglich einen „Scherz“ machen wollten und daher nicht so ernst genommen werden sollten, werden nationalsozialistische Taten verharmlost und als Bagatelle dargestellt. Solidaritätsbekundungen mit verurteilten Straftätern nach dem Verbotsgesetz bekräftigen die Verharmlosungsstrategie in der altrechten Szene.

Die allgemeine Unzufriedenheit mit der Regierung ist zudem ein Nährboden für rechtsextreme Propaganda. Rechtsextreme Akteurinnen und Akteure wissen, wie sie diese Unzufriedenheit durch populistische, radikale und stark emotionalisierende Inhalte weiter befeuern und für ihre Zwecke nutzen können. Darüber hinaus wird auf weitere gesellschaftspolitische Themen wie Migration und Asyl in einer abwertenden und rassistischen Weise Bezug genommen (mit Umschreibungen bzw. Codes wie beispielsweise „Mohammedaner“), die für islamfeindliche Diskurse charakteristisch ist.

In subkulturell geprägten rechtsextremen Kreisen bewegen sich die Online-Inhalte an der Schnittstelle von rechtsextremer Propaganda (die u. a. mit Hilfe von Zahlencodes¹³ transportiert wird), transnationaler White-Power-Solidarität, militant-neonazistischem Hooligan-Lifestyle (wie Kampfsport oder Fußball-Fankultur) und „Straßenkunst“ (wie Graffiti, vgl. Abb. 1). Hiermit und mit Hilfe von Symbolen oder humoristisch bzw. absurd wirkenden Darstellungen, welche die rechtsextremen Inhalte verharmlosen, wird strategisch versucht, rechtsextreme Ideologien zu verbreiten und jüngere Zielgruppen anzusprechen.

13 So steht in rechtsextremen Kreisen beispielsweise „88“ für „HH“, also „Heil Hitler“, da „H“ der achte Buchstabe des Alphabets ist.



Abbildung 1: Graffito der „Tanzbrigade Wien“ mit einem aggressiven Statement gegen ihr linkes Feindbild „Antifa“.

Wiederaufleben der Skinhead-Subkultur der 1990er-Jahre durch Neonazi-Jugend-Subgruppen

Seit dem letzten Quartal 2024 können in Österreich Neugründungen von gewaltaffinen und militant in Erscheinung tretenden Neonazi-Jugend-Subgruppen beobachtet werden, die stark an die Skinhead-Bewegung der 1990er-Jahre erinnern. Während viele dieser Jugendgruppen bereits nach kurzer Zeit an mangelnder Struktur und fehlenden Verbindungen zu Schlüsselfiguren bzw. etablierten Gruppierungen scheitern, sichern sich andere Gruppierungen ihr Bestehen durch die Anbindung an etablierte Zusammenschlüsse. Markant für viele dieser spontan und lose organisierten Neonazi-Jugendgruppen ist die Nutzung von Mainstream-Plattformen, insbesondere TikTok oder Instagram, für ihre Vernetzungs- und Rekrutierungszwecke. Neben der Nutzung von Social-Media-Plattformen werden auch Kundgebungen bzw. Veranstaltungen im Ausland für Rekrutierungs- bzw. Vernetzungs- und Propagandazwecke genutzt.

Unter den zahlreichen Gruppierungen, deren stereotype Merkmale¹⁴ stark an die Skinheadszenen der 1990er-Jahre erinnern, trat 2025 die Division Wien wiederholt durch

¹⁴ Als Beispiele für stereotype Merkmale, die stark an die Skinheadszenen der 1990er-Jahre erinnern, sind insbesondere Springerstiefel, Bomberjacken und Frisuren (Glatzen) anzuführen.

politisch motivierte Gewaltakte¹⁵ prominent in Erscheinung. Dazu zählen etwa die Pedo Hunting-Hassverbrechen gegenüber homosexuellen oder vermeintlich pädophilen Männern.¹⁶ Als informelle Gruppe hat sich diese mutmaßlich aus dem Umfeld der Tanzbrigade Wien, einer seit Jahrzehnten bestehenden Gruppierung an der Schnittstelle von Neonazismus, Hooliganismus, Straßenkunst, Kampfsport, Clubkultur und elektronischer Musik, entwickelt. Über die Verbindung zu Schlüsselfiguren der rechtsextremen Szene gelang es der Division Wien, ihre Kontakte im Rahmen von Veranstaltungen, Aufmärschen und Kundgebungen im In- bzw. Ausland auszubauen. Darüber hinaus werden Social-Media-Plattformen wie die der Tanzbrigade Wien mitgenutzt, um ihre Reichweite und ihren Einfluss zu vergrößern.

Auch wenn sich die Division Wien ihr Fortbestehen bisher über etablierte Zusammenschlüsse und Szene-Akteure sichert, handelt es sich um keine in sich geschlossene Gruppierung. Zu erwähnen ist in diesem Kontext etwa die fluktuierende Anhängerschaft, wengleich auch ein fester Personenkreis festzustellen ist. Zu den wechselnden Personen zählen Akteurinnen und Akteure aus bereits aufgelösten Gruppen, die beispielsweise Kundgebungen als Gelegenheiten nutzen, um sich der bestehenden Gruppe anzuschließen.

Rechtsterroristische Onlinesubkulturen

Rechtsterroristische Onlinesubkulturen stellen seit mehreren Jahren ein zentrales Sicherheitsrisiko im Bereich des gewaltorientierten Rechtsextremismus dar. Akteurinnen und Akteure, die diesem Spektrum zugeordnet werden können, operieren weitgehend dezentral und nutzen digitale Kommunikationsräume zur Verbreitung extremistischer Inhalte, zur ideologischen Schulung und zur Anstiftung zu Gewalttaten. Die Online-Milieus, in denen sich solche Akteurinnen und Akteure bewegen, sind durch eine hybride Struktur aus Propaganda, Subkultur-Ästhetik und strategischer Vernetzung gekennzeichnet. Gewalt wird dort als legitimes Mittel der politischen Veränderung verherrlicht und propagiert, wobei die Grenzen zwischen virtueller Radikalisierung und realer Gewaltanwendung zunehmend verschwimmen.

15 Politisch motivierte Gewaltakte gegen People of Colour, jüdische Personen, queere und homosexuelle Menschen, die verstärkt im ersten Halbjahr 2025 beobachtet werden konnten.

16 Im Zusammenhang mit den „Pedo Hunting“-Verbrechen wurden 13 Personen festgenommen. Das Netzwerk „Pedo Hunting Austria“ agierte über mehrere Monate und lockte homosexuelle Männer sowie vermeintlich Pädophile über Fake-Accounts zu vorab ausgemachten Treffpunkten. Zu diesen Treffen erschienen die Täter maskiert, fügten den Opfern körperliche Misshandlungen zu und demütigten sie. Bei den schwersten Fällen ermittelt das LKA Steiermark unter anderem wegen den strafrechtlichen Tatbeständen Raub und versuchter Mord. Die Vorfälle wurden gefilmt und in die Telegramgruppe „Pedo Hunting Austria“ hochgeladen. Hinsichtlich der Motivation der Pedo Hunting-Täter muss aktuell davon ausgegangen werden, dass es sich um einen Akt der Selbstjustiz gehandelt hat. Bei Hausdurchsuchungen wurde aufgrund der sichergestellten NS-Devotionalien und Waffen zudem ein Konnex zum Rechtsextremismus festgestellt.

Besonders bedeutsam innerhalb dieses Spektrums ist die Ideologie des rechtsextremen Akzelerationismus. Anhängerinnen und Anhänger dieses Konzepts propagieren den beschleunigten Zusammenbruch der bestehenden demokratischen Ordnung durch gezielte Gewaltakte. Ausgangspunkt sind unter anderem die Schriften des US-amerikanischen Neonazis James Mason sowie deren moderne Adaptionen in rechtsterroristischen Netzwerken wie der Atomwaffen-Division oder der Feuerkrieg-Division. Diese Gruppierungen und ihre Nachfolgeformationen dienen Szeneakteuren als ideologische Referenzpunkte und liefern den Rahmen für eine strategische Legitimation von Terror, um den aus ihrer Sicht notwendigen Zusammenbruch des demokratischen Systems herbeizuführen.

Die Szene agiert überwiegend anonym in Chatgruppen, Internetforen und Imageboards. Dort werden Propagandamaterialien, extrem gewaltverherrlichende Inhalte sowie technische Anleitungen zur Tatplanung bzw. -umsetzung verbreitet. Diese Kommunikationsräume fördern Selbstradikalisierungsprozesse, insbesondere bei jungen Personen, die über Meme-Kulturen¹⁷, Gaming Communities oder zum Teil ironisch codierte Inhalte schrittweise in ein gewaltverherrlichendes Weltbild eingeführt werden. Die mediale Ästhetik dieser Milieus ist stark an Subkulturformen angelehnt und dient der Rekrutierung neuer Anhängerinnen und Anhänger sowie der Normalisierung extremistischer Narrative.

Auch in Österreich gibt es Anhaltspunkte für die Rezeption akzelerationistischer Ideologeme in Online-Foren und sozialen Medien. Die Verbindung zu international vernetzten Akteurinnen und Akteuren erfolgt dabei meist virtuell, wobei Einzelpersonen und Kleingruppen Inhalte aus transnationalen Kanälen übernehmen und adaptieren. Diese Entwicklungen bilden ein kontinuierliches Gefährdungspotenzial durch selbstständig handelnde, digital radikalisierte Einzeltäterinnen und Einzeltäter, die sich ohne organisatorische Einbindung zu Gewalttaten entschließen.

Neue Rechte

Unter dem Begriff Neue Rechte wird ein loses Netzwerk von Gruppen, Einzelpersonen und Organisationen verstanden, in dem rechtsextremistische Kräfte zur Durchsetzung antiliberaler, gegen demokratische Grundnormen gerichteter Positionen in Gesellschaft und Politik kooperieren. In Österreich ist die Identitäre Bewegung Österreich (IBÖ) die Hauptgruppierung der Neuen Rechten. Diese stellt den Anspruch, sich bewusst von der Alten Rechten und vom historischen Nationalsozialismus abzugrenzen. Dies geschieht durch die Verwendung einer Sprache, die die eigentlichen Ziele verschleiern soll und hierfür neue Begriffe wie „Remigration“¹⁸, „Bevölkerungsaustausch“ oder „Demokratiesimulation“ einführt. Diese Begriffe werden öffentlich verbreitet, um breite Gesellschafts-

¹⁷ „Meme-Kultur“ bezieht sich auf das Internetphänomen, bei dem üblicherweise „humorvolle“, satirische oder politische Inhalte wie Bilder, Videos und Texte viral geteilt und immer wieder neu interpretiert werden. Die rechtsextreme Szene nutzt Memes dazu, Hassbotschaften bzw. teils verbotene Inhalte zu tarnen und subtil zu verbreiten.

¹⁸ Mit dem völkisch aufgeladenen Begriff „Remigration“ ist gemeint, dass Asylwerberinnen und Asylwerber, Fremde und nicht assimilierte Staatsbürgerinnen und Staatsbürger zwangsweise außer Landes gebracht werden sollen.

schichten zu erreichen. Zusätzlich wird versucht, mittels Kundgebungen, Kampagnen sowie spezieller Rhetorik und Propaganda die Denkweisen der Neuen Rechten in der Gesellschaft zu verankern. Ein wesentlicher Grundgedanke dabei ist die propagierte Trennung von Menschen nach Herkunft und Kultur aufgrund der Vorstellung, wonach verschiedene Ethnien nicht zusammenleben sollten (Ethnopluralismus). Weitere thematische Schwerpunkte sind die Rückbesinnung auf traditionelle Rollenbilder der Geschlechter und die Bewahrung einer als bedroht dargestellten kulturellen Identität. Langfristiges Ziel ist es, kulturelle Akzeptanz für rechtsextreme Themen zu schaffen, um damit die bestehende liberale Demokratie schrittweise in eine autoritäre Staatsform umzugestalten.

Das Konzept der „Remigration“ und weitere Entwicklungen

Die Entwicklungen hinsichtlich der Verbreitung des Begriffs „Remigration“ setzten sich im Berichtsjahr unverändert fort. Es zeichnet sich ab, dass die Neue Rechte beabsichtigt, diese Wortschöpfung nicht nur in das Parteiprogramm rechter Parteien zu bringen, sondern europaweit zu verbreiten. Der „Remigration Summit“ im Mai 2025 in einem Vorort von Mailand kann für diese Bemühungen als exemplarisches Beispiel dienen. Diese Veranstaltung wurde federführend von Martin Sellner und weiteren europäischen Aktivisten organisiert und sollte als Meilenstein dienen, um das Konzept der „Remigration“ europaweit bekannt zu machen. Es nahmen dabei Journalistinnen und Journalisten, Politikerinnen und Politiker, Influencerinnen und Influencer sowie fast ausschließlich männliche Aktivisten der europaweiten identitären Szene teil. Neben Ansprachen gab es diverse Vorlesungen sowie Diskussionsrunden.

Der Begriff „Remigration“ wurde Anfang 2024 durch die Enthüllung eines Mediums über ein konspiratives Treffen in Deutschland erstmals einer breiteren Öffentlichkeit bekannt. An diesem Treffen nahm auch Martin Sellner teil, der vor AfD-Politikerinnen und AfD-Politikern und weiteren einflussreichen Personen die Inhalte seines Buches „Remigration. Ein Vorschlag“ präsentierte. Das darin propagierte Konzept der pauschalen Rückführungen widerspricht verfassungsrechtlichen Prinzipien wie der Menschenwürde, der kulturellen Vielfalt und der Gleichheit aller Staatsbürgerinnen und Staatsbürger vor dem Gesetz.

Bei Martin Sellner handelt es sich nach wie vor um die wichtigste Führungsperson der Identitären Bewegung Österreich, wenngleich er sich vom Straßenaktivismus zurückgezogen hat und den Fokus seiner Aktivitäten verstärkt auf seine Rolle als rechter Influencer, Netzwerker und Einzelunternehmer setzt. Als Autor diverser Bücher reiste er 2025 in regelmäßigen Abständen ins deutschsprachige Ausland, um für diese zu werben. Während Sellner in Österreich das letzte noch aktive Gründungsmitglied der IBÖ ist, fand innerhalb der Gruppierung ein Generationenwechsel statt. Mittlerweile sind zwei deutsche Staatsbürger die Gesichter und Sprachrohre der Wiener IB-Gruppe. Diese Personalrochade zeigt, dass rechtsextreme Gruppen wie die IBÖ den deutschsprachigen Raum als einen gemeinsamen Kultur- und Aktionsraum sehen, in dem ein gemeinsames „Volk“ (in Differenzierung zu anderen „Völkern“) propagiert wird.

Aktionismus und Veranstaltungen

Störaktionen der IBÖ mit Bannern und Pyrotechnik entsprachen im Beobachtungszeitraum dem bekannten Muster. Tagesaktuelle Vorfälle und islamistisch motivierte Anschläge wurden zum Anlass genommen, um Aktionen im öffentlichen Raum durchzuführen. Nach der Ermordung eines Jugendlichen in Villach im Februar 2025 durch einen Migranten organisierte die IBÖ in der Wiener Innenstadt einen Trauermarsch, an dem ca. 150 Personen teilnahmen, darunter einschlägige Gruppierungen und Personen aus dem militanten neonazistischen Spektrum. Im Vorfeld dieser Veranstaltung wurde massiv gegen Migrantinnen und Migranten gehetzt und der Vorfall durch das rechte Lager instrumentalisiert. Wenige Tage nach der Kundgebung in Wien entrollten mehrere vermummte männliche Aktivisten auf einem Wohngebäude in Villach ein Banner mit der Aufschrift: „Alexander – Opfer von Multikulti. Remigration für unsere Jugend“ und entzündeten bengalische Fackeln.

Im Juli 2025 organisierte die IBÖ erneut eine Remigrationsdemo, die in dieser Form seit 2023 jährlich stattfindet. Wie in den beiden Jahren zuvor fand am Vorabend in Kellerräumen im fünften Wiener Bezirk eine Kampfsportveranstaltung statt. Die Teilnehmerzahl der Remigrationsdemo belief sich trotz wochenlanger europaweiter Mobilisierung lediglich auf ungefähr 350 Personen. Neben der großen Zahl an Teilnehmerinnen und Teilnehmern aus dem Ausland fiel dieses Jahr auch eine größere Gruppe auf, die äußerlich dem neonazistischen Hooliganmilieu zuzuordnen ist. Sie machte im Rahmen der Veranstaltung mit für Fußballstadien typischen Fanchören auf sich aufmerksam und sorgte so für eine aufgeheizte Stimmung.

Die Aktivitäten der im November 2023 gegründeten Studentengruppe Aktion 451, mit der versucht wird, um die Deutungshoheit in den für die neurechte Szene „zu linken“ Universitäten und Hochschulen zu kämpfen, nahmen 2025 spürbar ab. Während im Jahr 2024 vor allem in Wien noch regelmäßig Lesekreise organisiert wurden und rechte Influencer sowie Autoren aus einem neurechten deutschen Verlag Vorträge hielten, kamen die Aktivitäten dieser IBÖ-Tarngruppe im Berichtszeitraum in Österreich weitestgehend zum Stillstand. Erst gegen Ende 2025 erlebte die Gruppe wieder eine Belebung mit neuem Auftreten und neben neuen Lesekreisen wurden nun auch Freizeitaktivitäten, wie Sport und Wandergruppen, für das Wintersemester 2025/2026 angeboten. Hinsichtlich des Personenkreises gab es klare Überschneidungen mit der IBÖ, ergänzt durch einige weibliche Proponentinnen sowie Personen aus der Jugendorganisation einer rechten Partei.

Vernetzungen ins Parteienspektrum

Die Vernetzung zwischen der Neuen Rechten und dem rechten Parteienspektrum ist unverändert eng. Mittlerweile sind mindestens vier ehemalige IBÖ-Aktivisten als parlamentarische Mitarbeiter für eine rechte Partei tätig. Das jüngste Beispiel ist eine Person, die bis vor kurzem eine Führungsfunktion im aktivistischen Flügel der IBÖ innehatte. Bei der diesjährigen Remigrationsdemo war diese Person als Ordner und bei der Kampf-

sportveranstaltung am Vorabend als Schiedsrichter tätig. Sie nahm zudem gemeinsam mit einem Dutzend weiterer IBÖ-Aktivisten am diesjährigen IB-Sommerlager in Oberösterreich teil. Eine weitere Person, die ins Parteienspektrum wechselte, fungierte in der jüngeren Vergangenheit als eines der Gesichter der Aktion 451. Zu beobachten ist, dass alle parlamentarischen Mitarbeiter mit identitärem Hintergrund auch Mitglieder bei deutschnationalen Burschenschaften sind. Das korporierte Vereinswesen mit seiner Rolle als Verbindungselement innerhalb des Rechtsextremismus dient offenkundig auch dazu, entsprechenden Personen Laufbahnen in einer rechten Partei zu ermöglichen. Die enge Vernetzung ist nicht nur personell sichtbar, sondern auch thematisch. Dies zeigte sich im Wahlprogramm einer rechten Partei zur Nationalratswahl 2024, in der das identitäre Schlagwort „Remigration“ mehrmals enthalten war.

2.1.3 Fälle 2025

Fall SÄCHSISCHE SEPARATISTEN

Unter der Leitung der Generalbundesanwaltschaft Karlsruhe führte das Bundeskriminalamt Deutschland ein Strafverfahren gegen eine rechtsterroristische Gruppierung. Dabei handelte es sich um eine militante Gruppierung, die das Ziel verfolgte, an einem erwarteten und erhofften zukünftigen gewaltsamen Umsturz¹⁹ des gesellschaftlichen und politischen Systems in Deutschland mitzuwirken, um unter Einsatz von Waffengewalt auf einem möglichst großen Gebiet (vor allem der ostdeutschen Bundesländer) ein von der Bundesrepublik Deutschland losgelöstes, an der Ideologie des Nationalsozialismus ausgerichtetes Staats- und Gesellschaftswesen zu errichten.

Die DSN vollzog am 5. November 2024 auf Grundlage einer Europäischen Ermittlungsanordnung der deutschen Generalbundesanwaltschaft und einer Anordnung der Staatsanwaltschaft Krems a. d. Donau Hausdurchsuchungen in Wien und bei der Burg ruine Kronsegg in Niederösterreich. Die Beamtinnen und Beamten stellten bei dieser Amtshandlung elektronische Datenträger, NS-Propagandamaterial, NS-Devotionalien, Waffenteile und Munition sicher.

Aufgrund dieser Funde leitete die Staatsanwaltschaft Krems gegen zwei österreichische und einen deutschen Staatsbürger sowie gegen eine deutsche Staatsbürgerin ein separates Strafverfahren gemäß § 3g Verbotsgesetz (Nationalsozialistische Wiederbetätigung) sowie gemäß § 50 Waffengesetz ein. Zudem erfolgten Berichtslegungen der DSN an das Bundeskriminalamt Deutschland für dessen Verfahren.

Angemerkt wird, dass ein österreichischer Beschuldigter bereits seit Jahrzehnten in der nationalen rechtsextremistischen Szene aktiv ist. Er nahm in den 1980er- bzw. 1990er-

19 In der rechtsextremen Szene auch als „Tag X“ bezeichnet.



Jahren an Veranstaltungen und Wehrsportübungen der neonazistischen Gruppierung Volkstreue Außerparlamentarische Opposition (VAPO)²⁰ teil.

Die Abschlussberichte an die zuständigen Staatsanwaltschaften Krems a. d. Donau und Wien durch die DSN erfolgten im Sommer 2025. Im eigens geführten deutschen Strafverfahren der Generalbundesanwaltschaft Karlsruhe wurde im Sommer 2025 Anklage erhoben.

Fall DRUCKER

Ein österreichischer Staatsangehöriger veröffentlichte auf der Social-Media-Plattform Telegram Lichtbilder, die ihn beim Schießtraining und der Herstellung von Handgranaten zeigten. Zudem sprach er davon, dass er „auf halbem Weg“ wäre, der „zukünftige Hitler“ zu werden. Überdies verbreitete er antisemitische Verschwörungserzählungen und bezeichnete Menschen jüdischen Glaubens als Tiere, die man verbrennen müsse.

Aus diesem Grund werden Ermittlungen wegen des Verdachts der Wiederbetätigung im Sinne des Verbotsgesetzes (Nationalsozialistische Wiederbetätigung), der Verhetzung, der Vorbereitung eines Verbrechens durch Sprengmittel sowie Vergehen nach dem Waffengesetz geführt. Der Verdächtige wies keine strafrechtlichen Verurteilungen auf und besaß bis zum polizeilichen Einschreiten zwei legale Langwaffen sowie eine Pistole.

Am 16. September 2025 setzten Bedienstete des Landesamts Staatsschutz und Extremismusbekämpfung Niederösterreich eine durch die Staatsanwaltschaft Wiener Neustadt angeordnete Hausdurchsuchung an der Wohnörtlichkeit des Beschuldigten um. Dabei stellten die Bediensteten eine mittels 3D-Drucker selbst hergestellte Pistole sowie weitere Waffenteile, einen Schalldämpfer, Sprengmittel, NS-Literatur, NS-Devotionalien, einen 3D-Drucker sowie elektronische Datenträger sicher.

Die zuständige Waffenbehörde verhängte gegen den Beschuldigten ein Waffenverbot. Bis zum Zeitpunkt der gegenständlichen Berichtslegung äußerte sich der Verdächtige nicht zu den Vorhalten, die Auswertung der elektronischen Datenträger dauert aktuell noch an. Das Gerichtsverfahren wird für das Jahr 2026 erwartet.

²⁰ Die „VAPO“ (gegründet 1986) war eine weder als Partei noch als Verein konstituierte militante neonazistische Gruppe. Ideologisch orientierten sich die VAPO bzw. ihre Mitglieder am Nationalsozialismus. In einem Schulungsbrief der VAPO wurden, ausgehend von einer Mitarbeit in der „Gesinnungsgemeinschaft der Neuen Front“, als Zielvorstellungen die „Neugründung der NSDAP“ und die „erneute Machtergreifung“ angegeben. Dazu: Dokumentationsarchiv des österreichischen Widerstands (o. J.): Volkstreue außerparlamentarische Opposition (VAPO); online unter: <https://www.doew.at/erkennen/rechtsextremismus/rechtsextreme-organisationen/volkstreue-auszerparlamentarische-opposition-vapo> (Abruf am 13.10.2025).

2.1.4 Trends und Entwicklungstendenzen

Alte Rechte

National wie international erfolgt weiterhin ein reger Austausch unter Gleichgesinnten des altrechten Milieus. Während die physische Vernetzung vor allem zur internen Stabilität und ideologischen Festigung rechtsextremer Gruppen beiträgt, geht die eigentliche Gefahr zunehmend von der Online-Vernetzung aus. Da im virtuellen Raum mehr Menschen erreicht werden können und rechtsextreme Propaganda schneller und vor allem verschlüsselt verbreitet wird, erhöht sich die Gefahr, dass der online verbreitete Hass auch in reale Gewaltakte übergeht.

Die zu beobachtende Trendentwicklung gewaltbereiter und militanter neonazistischer Jugend-Subgruppen im Stil der 1990er-Jahre-Skinheadszenen könnte unter anderem damit zusammenhängen, dass Jugendliche anfällig für extreme Weltanschauungen sind und sich noch in der Identitätsfindung befinden. Hinzu kommt, dass rechtsextreme Propaganda überwiegend über soziale Medien verbreitet wird. Da Mainstream-Plattformen von Minderjährigen und Jugendlichen in einem großen Ausmaß genutzt werden, können diese einfacher erreicht werden bzw. wird ihnen dadurch rechtsextreme Propaganda leicht zugänglich gemacht.

Überdies trägt die Vernetzung junger Akteure mit etablierten Gruppierungen (oder älteren Generationen) nicht nur zur Weitergabe von Ideologien und Wissen bei, sondern sichert auch den Fortbestand von rechtsextremen Bestrebungen.

Gewalt als strategisches Element und legitimes Mittel wird von den Anhängerinnen und Anhängern der Alten Rechten nicht nur über die Ästhetik oder mittels Kampfsport-Techniken inszeniert, sondern auch aktiv im Rahmen von Vernetzungsaktivitäten, vor allem bei neonazistischen Kampfsportveranstaltungen, eingesetzt. Darüber hinaus kann sich neonazistische Gewalt durch Hasskriminalität, Drohungen, gezielte Einschüchterungen sowie körperliche, rassistische und antisemitisch motivierte Angriffe auf Personen oder Gruppen, die dem völkischen Weltbild widersprechen, äußern.

Rechtsextremer Akzelerationismus

Der rechtsextreme Akzelerationismus stellt innerhalb des rechtsextremistischen Spektrums ein dynamisches und zunehmend transnational geprägtes Teilphänomen dar. Während klassische neonazistische Organisationen in Österreich weiterhin über ein stabiles, aber strukturell überschaubares Personenpotenzial verfügen, entwickelt sich im digitalen Raum ein ideologisches Submilieu, das über die Grenzen traditioneller Organisationsformen hinausweist. Dieses Milieu strebt keinen politischen Reformprozess an, sondern bekennt sich offen zur gewaltsamen Zerstörung der bestehenden demokratischen Ordnung. Ziel ist die Beschleunigung gesellschaftlicher Destabilisierung durch Anschläge, Morde oder bewaffnete Auseinandersetzungen, um einen Zusammenbruch des Staates und die Etablierung eines „rassistisch homogenen“ Systems herbeizuführen.

Zentral bleibt die Rezeption der sogenannten Siege²¹-Ideologie und deren Grundlagentexte, die nach wie vor in einschlägigen Online-Communities kursieren. Im Jahr 2025 war eine zunehmende Fragmentierung und zugleich Internationalisierung dieses Gedankenguts zu beobachten. Während klassische Bezugspunkte wie die Atomwaffen-Division oder die Feuerkrieg-Division in ihrer ursprünglichen Form kaum noch aktiv sind, entstehen beständig neue Ableger und informelle Netzwerke, die unter wechselnden Symbolen und Namen operieren. Diese Gruppen propagieren einen individualisierten „führerlosen“ Kampf und verlagern ihre Kommunikation in verschlüsselte Chatkanäle und auf kleine Plattformen.

Die in diesen Räumen verbreitete Propaganda zeigt eine hybride Ästhetik aus Popkultur, Gaming-Elementen und Kriegsikonographie sowie die Verherrlichung von Amokläufern und Rechtsterroristen. 2025 wurde deutlich, dass Memes, Musik und visuelle Codes gezielt eingesetzt werden, um den Zugang für junge, online-affine Zielgruppen zu erleichtern. Dabei dient „Humor“ als Tarnung und Normalisierung für terroristische Inhalte. Diese Form der Radikalisierung ist nicht auf klassische rechtsextreme Milieus beschränkt, sondern spricht zunehmend auch desorientierte oder sozial isolierte junge Menschen an, die in der Folge unter anderem über popkulturelle Bezüge in extremistisches Gedankengut hineinwachsen.

Die Szene des rechtsextremen Akzelerationismus in Österreich ist zwar zahlenmäßig klein, weist aber ein hohes Risikopotenzial auf. Einzelne Fälle – etwa Selbstinszenierungen in Online-Kanälen mit Bezug zu internationalen Netzwerken – verdeutlichen eine enge Einbindung in transnationale Kommunikationsstrukturen. Im Jahr 2025 zeigten Monitoring-Daten, dass österreichische IP-Adressen regelmäßig in einschlägigen internationalen Gruppen auftauchen, wobei die Beteiligten selten als eigenständige Organisatoren auftreten, sondern als lose vernetzte Unterstützerinnen und Unterstützer agieren.

Diese Dezentralisierung ist ein zentrales Strukturmerkmal des rechtsextremen Akzelerationismus. Die Szene lehnt eine hierarchische Organisation bewusst ab, um eine Entdeckung durch die Polizei zu erschweren und Eigeninitiative zu fördern. Diese Netzwerk-im-Netzwerk-Struktur begünstigt die Entstehung autonomer, schwer erkennbarer Kleingruppen oder Einzeltäterinnen und Einzeltäter, die über Online-Materialien radikalisiert und operativ inspiriert werden. Der Austausch umfasst dabei nicht nur Ideologie, sondern auch technische Informationen über Waffenbeschaffung, Tatplanung und Kommunikationssicherheit.

21 „Siege“ (dt.: Belagerung) ist der Name der Newsletter-Sammlung des US-amerikanischen Rechtsextremisten und Neonazis James Mason, in der er die Beseitigung liberaler Demokratien mittels terroristischer Anschläge propagiert. Diese Texte sind für rechtsextreme akzelerationistische Netzwerke als ideologische Grundlage von zentraler Bedeutung.

Im Berichtszeitraum 2025 zeigte sich eine deutliche Verlagerung extremistischer Kommunikation in geschlossene Plattformen, insbesondere zu Telegram. Parallel entstanden neue, auf Gaming Communities aufbauende Kommunikationsräume, in denen extremistische Inhalte verbreitet werden. Akzelerationistische Gruppierungen nutzen zudem zunehmend audiovisuelle Medien – etwa animierte Videos, Musikstücke oder pseudo-dokumentarische Clips – um Gewalttaten zu ästhetisieren und deren Nachahmung zu fördern. Diese Form der medialen Inszenierung dient der Herstellung von Symbolfiguren („Saints“) ebenso wie der Heroisierung von Attentätern und Rechtsterroristen. Ferner setzten Akteure dieser hybriden Mischszene bewusst auf „plausible deniability“, indem sie ironische, parodistische oder ästhetisch überformte Inhalte veröffentlichten, die strafrechtlich schwer fassbar sind, aber dennoch klar extremistisches Gedankengut transportieren. Diese Taktik erschwert die frühzeitige Identifikation potenzieller Täterinnen und Täter.

Ein Trend, der 2025 besonders hervorsteicht, ist die Überschneidung mit anderen digitalen Subkulturen, etwa der sogenannten „Incel“²²-Szene oder misanthropischen Online-Gemeinschaften. Der gemeinsame Nenner besteht in nihilistischen bzw. (rechts)esoterischen Weltbildern, der Ablehnung pluralistischer Gesellschaftsformen und der Verherrlichung von Gewalt als Ausdruck persönlicher und politischer „Reinigung“. Dadurch entsteht ein fließender Übergang zwischen ideologisch gefestigtem Rechtsextremismus und einer amorphen, gewaltorientierten Online-Subkultur.

Misogynie fungiert im rechtsextremen Akzelerationismus häufig als verbindendes ideologisches Element, das disparate Milieus über gemeinsame Feindbilder und Deutungsmuster zusammenführt. Weibliche Selbstbestimmung, Gleichstellungspolitik und queere Lebensweisen werden dabei als Symbole eines „dekadenten Systems“ konstruiert, dessen vermeintlicher Niedergang beschleunigt werden soll. Die Abwertung von Frauen und feminisierten Gruppen dient zugleich der inneren Kohäsion: sie stabilisiert autoritäre Männlichkeitsideale, legitimiert hierarchische Geschlechtervorstellungen und ermöglicht niederschwellige Mobilisierung über anschlussfähige Online-Narrative (bspw. Anti-Feminismus, „Tradwife“²³-Idealisierung, „Incel“-Bezüge). In digitalen Räumen wirkt Misogynie

22 „Incel“ ist ein englisches Akronym aus „involuntary celibate“, englisch für „unfreiwillig sexuell enthaltsam“. Es ist die Selbstbezeichnung einer in den USA entstandenen Internet-Subkultur heterosexueller Männer, die nach Eigenaussage unfreiwillig keinen Geschlechtsverkehr bzw. keine romantische Beziehung haben und der Ideologie einer hegemonialen Männlichkeit anhängen.

23 „Tradwives“ sind Influencerinnen auf Social Media, die ein neokonservatives und stark patriarchales Rollenbild propagieren, das die Rolle der Frau als Hausfrau, Mutter und Versorgerin der Familie idealisiert, weibliche Erwerbstätigkeit weitgehend ablehnt und damit klassische Abhängigkeitsverhältnisse reproduziert. Auffällig ist dabei, dass diese Inhalte häufig von Influencerinnen verbreitet werden, die selbst durch diese Tätigkeit ein Einkommen erzielen und damit faktisch wirtschaftlich unabhängig sind – ein Umstand, der in den entsprechenden Darstellungen regelmäßig ausgeblendet bleibt.

zudem als Radikalisierungsbeschleuniger, indem sie soziale Frustration in politisierte Gewaltfantasien überführt und Brücken zu anderen extremistischen Subkulturen schlägt.

Das Bedrohungspotenzial des rechtsextremen Akzelerationismus liegt weniger in der Masse seiner Anhängerinnen und Anhänger als vielmehr in der strategischen Wirkung seiner Ideologie. Die bewusste Dezentralität, die Betonung individueller Tatinitiativen und die digitale Vernetzung mit internationalen Propagandastrukturen schaffen ein Umfeld, in dem einzelne, nicht prognostizierbare Gewalttaten jederzeit möglich sind.

In diesem Kontext darf zurückgehende Organisationsdichte folglich nicht als Entwarnung verstanden werden. Vielmehr hat sich der Akzelerationismus zu einem stabilen ideologischen Setzkastensystem entwickelt, der durch seine Anschlussfähigkeit an globale Kommunikationsräume fortbesteht. Für die kommenden Jahre ist mit einer weiteren Hybridisierung von Online-Radikalisierung, dezentraler Kommunikation und spontaner Gewaltbereitschaft zu rechnen.

Neue Rechte

Angetrieben durch die aktuellen Umfragewerte zu den österreichischen Parlamentsparteien und die Geschehnisse in den USA ist davon auszugehen, dass die Neue Rechte in Österreich an ihrer Taktik festhält und weiterhin beabsichtigt, ihre rechtsextreme Propaganda durch verschleierte Sprache in die Mitte der Gesellschaft zu tragen. Wiederholt hat sie in der Vergangenheit tagesaktuelle, politische Ereignisse instrumentalisiert und für ihre Zwecke umgedeutet. Es lässt sich beobachten, dass Entwicklungen in anderen Ländern als Beispiele für ihre Propaganda herangezogen werden. So hatte etwa die Einstufung der Antifa als Terrororganisation in den USA zur Folge, dass das Thema auch in Österreich aufgegriffen wurde und ähnliche Maßnahmen gefordert wurden.

Hinsichtlich des Straßenaktivismus der IBÖ ist anzunehmen, dass sich in naher Zukunft wenig ändern wird. Aktionen dieser Art finden in unregelmäßigen Abständen statt und dienen in erster Linie dazu, bildgewaltige Fotos für die sozialen Medien zu produzieren und ihren Inhalt popkulturell aufzubereiten. Medial wird darüber kaum berichtet. Die seit 2023 jährlich stattfindenden Sommerdemos bzw. Remigrationsdemos zeigen, dass sich Wien zu einem der zentralen Orte der europaweiten Identitären Bewegung entwickelt hat. Die Demonstrationen haben das Potenzial, mittels der dabei verbreiteten Ideologie die Hemmungen zur Gewaltausübung bis hin zum Rechtsterrorismus als legitimes Mittel zur Zielerreichung abzubauen. Obwohl sich Gruppierungen wie die IBÖ öffentlich von direkter Gewalt distanzieren, stehen ihr Auftreten und ihre Rhetorik im Widerspruch dazu. Ohne offen zu Gewalt aufzurufen, schafft die von der Neuen Rechten genutzte Sprache ein Umfeld indirekter Unterstützung, die das Umsetzen von Gewalttaten, insbesondere durch Einzeltäterinnen und Einzeltäter, begünstigt, weshalb diese nicht ausgeschlossen werden können.



© DSN

Rechtsextremismus



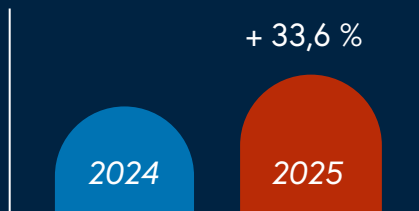
Aufklärungsquote



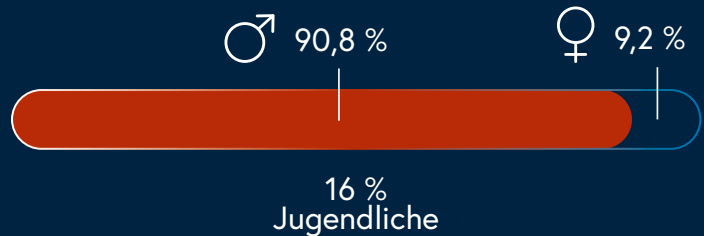
3.053

Zur Anzeige gebrachte Delikte

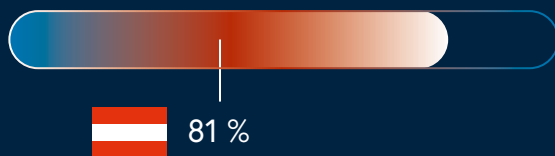
Anstieg zum Vorjahr



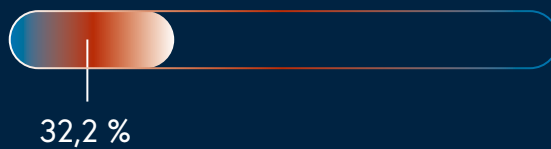
Täterinnen und Täter



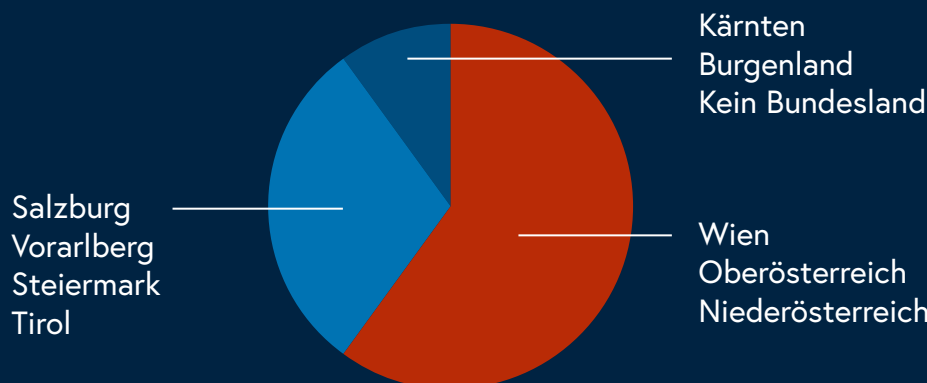
Staatsbürgerschaft der Täterinnen und Täter



Internetdelikte



Bundesländeraufteilung



2.1.5 Zahlen/Daten/Fakten

Im Jahr 2025 wurden den Sicherheitsbehörden in Österreich insgesamt **1.986 Tathandlungen**²⁴ mit rechtsextremistischer, fremdenfeindlicher/rassistischer, islamfeindlicher, antisemitischer sowie unspezifischer oder sonstiger Motivlage bekannt. Gegenüber dem Jahr 2024 (1.486 Tathandlungen) bedeutet dies einen **Anstieg um 33,6 Prozent**. **1.301** Tathandlungen (**65,5 Prozent**) wurden aufgeklärt. 2024 lag die Aufklärungsquote bei 64,1 Prozent (952 Tathandlungen).

Im Zusammenhang mit den angeführten Tathandlungen wurden 2025 bundesweit **3.053 Delikte** zur Anzeige gebracht, das sind um **30,1 Prozent mehr** als im Jahr 2024 (2.346 Delikte)²⁵. Unter den insgesamt 1.986 bekannt gewordenen und zur Anzeige gelangten Tathandlungen im Jahr 2025 befanden sich **640 Tathandlungen** (32,2 Prozent), bei denen die gesetzeswidrige Agitation im **Internet** stattfand. Im Jahr 2024 lag der Anteil der Internetdelikte bei 27,2 Prozent (404 Tathandlungen).

Im Zuge der Aufklärung rechtsextremer Straftaten wurden im Jahr 2025 insgesamt **1.518 Personen** durch die Sicherheitsbehörden zur Anzeige gebracht (2024: 1.116). Dabei handelte es sich um 1.379 Personen männlichen (90,8 Prozent) und 139 Personen weiblichen Geschlechts (9,2 Prozent). Unter den Beschuldigten befanden sich 243 Jugendliche (16 Prozent). Im Jahr 2024 gelangten 1.013 männliche und 103 weibliche Personen, davon 277 Jugendliche (24,8 Prozent), zur Anzeige.

1.229 der in diesem Spektrum angezeigten Personen (81,0 Prozent) besitzen die österreichische Staatsbürgerschaft (2024: 910, das entspricht 81,5 Prozent).

Neben den ausgeforschten Personen erfolgten im Berichtsjahr **749 Anzeigen** gegen **unbekannte Täterinnen oder Täter** (2024: 571).

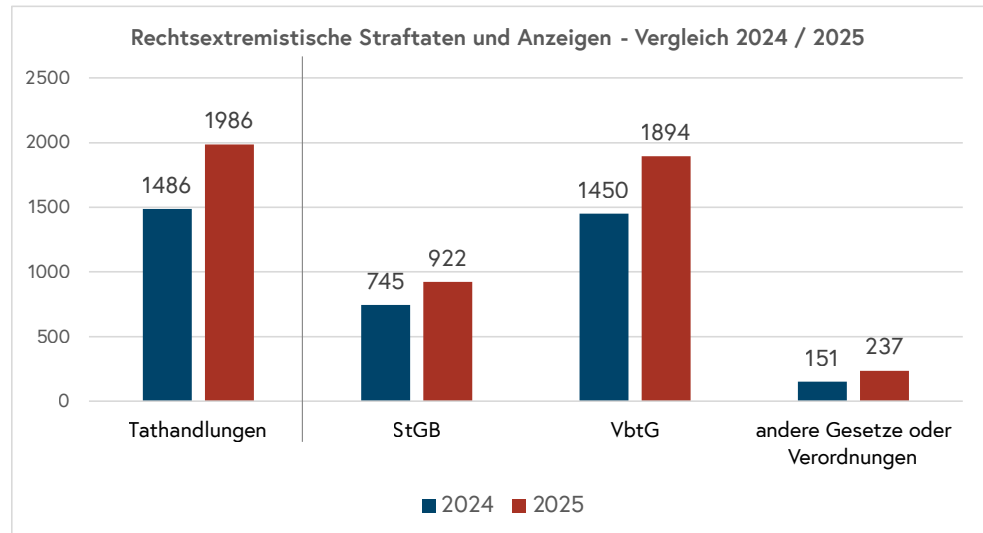
Im Zusammenhang mit der Bekämpfung rechtsextremer Aktivitäten wurden im Jahr 2025 in Österreich insgesamt **277 Hausdurchsuchungen** (inklusive freiwilliger Nachschauen; 2024: 260) durchgeführt und **75 Festnahmen** (2024: 53) vollzogen.

Bei diesen Maßnahmen wurden unter anderem NS-Devotionalien, Waffen und Munition sowie elektronische Geräte wie Mobiltelefone, Computer und Datenträger sichergestellt.

24 Eine Tathandlung kann mehrere Delikte mit gesonderten Personenanzeigen beinhalten.

25 Anzeigen zu strafbaren Handlungen mit einem rechtsextremen Hintergrund, siehe Tabelle.

Bei der **Internet-Meldestelle NS-Wiederbetätigung** sind im Jahr 2025 insgesamt 2.719 Informationen und Hinweise (davon 1.054 relevant)²⁶ eingegangen (2024: 2.210 Eingänge – 1.300 relevant).



Zu einem **Anstieg**²⁷ kam es unter anderem bei den Anzeigen nach dem Verbotsgesetz (1.450 auf 1.894), dem Delikt der Körperverletzung gemäß § 83 StGB (36 auf 41), dem Delikt der Gefährdung der körperlichen Sicherheit gemäß § 89 StGB (0 auf 5), dem Delikt der Gefährlichen Drohung nach § 107 StGB (54 auf 75), dem Delikt der Beleidigung gemäß § 115 StGB (5 auf 22), dem Delikt des Diebstahls durch Einbruch oder mit Waffen gemäß § 129 StGB (4 auf 7), dem Delikt der Aufforderung zu mit Strafe bedrohten Handlungen und Gutheißung mit Strafe bedrohter Handlungen gemäß § 282 StGB (18 auf 34), wegen Aufforderung zu terroristischen Straftaten und Gutheißung mit Strafe bedrohter Handlungen gemäß § 282a StGB (1 auf 3), wegen Verhetzung gemäß § 283 StGB (156 auf 262), dem Art III Abs 1 Z 4 EGVG²⁸ (46 auf 134), dem Waffengesetz (46 auf 66) und dem Sprengmittelgesetz (0 auf 3).

Etwa auf gleichem Niveau blieben die Anzeigen wegen Sachbeschädigungsdelikten nach den §§ 125 oder 126 StGB (386 vs. 391).

²⁶ Dabei handelte es sich um staatschutzrelevante Sachverhalte oder sonstige von Amtswegen zu bearbeitende Anliegen und Hinweise. Hier ist insbesondere zu beachten, dass in dieser Zahl Doppel- bzw. Mehrfachmeldungen durch Anzeiger an die Meldestelle enthalten sind.

²⁷ Die statistische Erfassung erfolgt auf Basis des tatsächlichen Tatzeitpunkts. Abweichungen gegenüber anderen Auswertungen, die auf das Datum des Abschlussberichts oder Verfahrensabschlusses abstellen, sind möglich.

²⁸ Der Anstieg resultiert aus der nunmehr gesetzlichen Regelung, dass Verwaltungsbehörden rechtskräftige Straferkenntnisse bzw. Strafverfügungen, unter anderem nach Art. III Abs. 1 Z 4 EGVG, den Sicherheitsbehörden für Zwecke der Sicherheitspolizei zu übermitteln haben, soweit diese deren Inhalt zur Erfüllung ihrer gesetzmäßigen Aufgaben benötigen.

Zu einem **Rückgang** kam es unter anderem bei Anzeigen wegen des Delikts der Schwere Körperverletzung gemäß § 84 StGB (16 auf 5), nach dem Delikt des Diebstahls gemäß § 127 StGB (10 auf 7), nach dem Delikt der Beharrlichen Verfolgung gemäß § 107a StGB (3 auf 1), dem Symbole-Gesetz (9 auf 2), dem Suchtmittelgesetz (14 auf 5), dem Sicherheitspolizeigesetz (6 auf 3) und nach dem Versammlungsgesetz (21 auf 0).

Anzeigen nach dem StGB	2024	2025
Mord (§ 75 StGB)	0	1 ²⁹
Körperverletzung (§ 83 StGB)	36	41 ³⁰
Schwere Körperverletzung (§ 84 StGB)	16	5 ³¹
Absichtliche schwere Körperverletzung (§ 87 StGB)	0	1
Gefährdung der körperlichen Sicherheit (§ 89 StGB)	0	5
Quälen oder Vernachlässigen unmündiger, jüngerer oder wehrloser Personen (§ 92 StGB)	0	1
Nötigung (§ 105 StGB)	3	5
Schwere Nötigung (§ 106 StGB)	7	5
Gefährliche Drohung (§ 107 StGB)	54	75
Beharrliche Verfolgung (§ 107a StGB)	3	1
Fortgesetzte Gewaltausübung (§ 107b StGB)	1	2
Hausfriedensbruch (§ 109 StGB)	1	3
Üble Nachrede (§ 111 StGB)	0	3
Beleidigung (§ 115 StGB)	5	22
Öffentliche Beleidigung eines verfassungsmäßigen Vertretungskörpers, des Bundesheeres oder einer Behörde (§ 116 StGB)	0	1
Berechtigung zur Anklage (§ 117 StGB)	0	4
Sachbeschädigung (§ 125 StGB)	358	370
Schwere Sachbeschädigung (§ 126 StGB)	28	21
Diebstahl (§ 127 StGB)	10	7
Schwerer Diebstahl (§ 128 StGB)	1	1
Diebstahl durch Einbruch oder mit Waffen (§ 129 StGB)	4	7
Raub (§ 142 StGB)	0	1
Erpressung (§ 144 StGB)	0	1

29 Im Oktober 2025 soll der Beschuldigte in Wien seinen iranischen Nachbarn erschossen haben. Zuvor soll der Tatverdächtige gegenüber dem Opfer mehrfach nationalsozialistische sowie fremdenfeindliche Aussagen getätigt haben, wobei die Tat nach Streitigkeiten im Drogenmilieu stattfand.

30 Durch fünf fremdenfeindlich/rassistisch motivierte Tathandlungen wurden fünf Personen verletzt; durch zwei islamfeindlich motivierte Tathandlungen wurden zwei Personen verletzt. Bei einer antisemitisch motivierten Tathandlung kam es zu einer versuchten Körperverletzung.

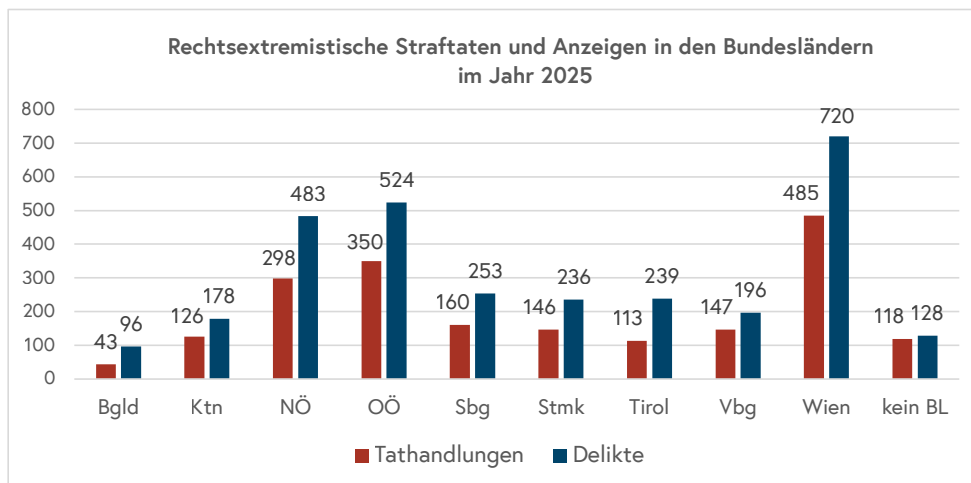
31 Durch eine fremdenfeindlich/rassistisch motivierte Tathandlung wurde eine Person verletzt.

Anzeigen nach dem StGB	2024	2025
Brandstiftung (§ 169 StGB)	0	2
Vorbereitung eines Verbrechens durch Kernenergie, ionisierende Strahlen oder Sprengmittel (§ 175 StGB)	0	3
Herabwürdigung religiöser Lehren (§ 188 StGB)	3	6
Bildliches sexualbezogenes Kindesmissbrauchsmaterial und bildliche sexualbezogene Darstellung minderjähriger Personen (§ 207a StGB)	6	6
Sexuelle Belästigung und öffentliche geschlechtliche Handlungen (§ 218 StGB)	2	1
Tierquälerei (§ 222 StGB)	0	1
Urkundenunterdrückung (§ 229 StGB)	4	3
Widerstand gegen die Staatsgewalt (§ 269 StGB)	12	10
Tätlicher Angriff auf einen Beamten (§ 270 StGB)	0	1
Terroristische Vereinigung (§ 278b StGB)	1	1
Aufforderung zu mit Strafe bedrohten Handlungen und Gutheißung mit Strafe bedrohter Handlungen (§ 282 StGB)	18	34
Aufforderung zu terroristischen Straftaten und Gutheißung mit Strafe bedrohter Handlungen (§ 282a StGB)	1	3
Verhetzung (§ 283 StGB)	156	262
Falsche Beweisaussage (§ 288 StGB)	0	4
Verleumdung (§ 297 StGB)	0	2
Sonstige StGB-Delikte	15	0
Anzeigen nach dem Verbotsgesetz (VbtG)	1.450	1.894
Anzeigen nach anderen Gesetzen oder Verordnungen		
Abzeichengesetz (AbzG)	1	2
Symbole-Gesetz (SG)	9	2
Art III Abs 1 Z 3 EGVG	4	10
Art III Abs 1 Z 4 EGVG	46	134 ³²
§ 50 Waffengesetz (WaffG)	42	53
§ 51 Waffengesetz (WaffG)	0	2
§ 13 Waffengesetz (WaffG)	4	11
§ 7 Kriegsmaterialgesetz (KMG)	0	2

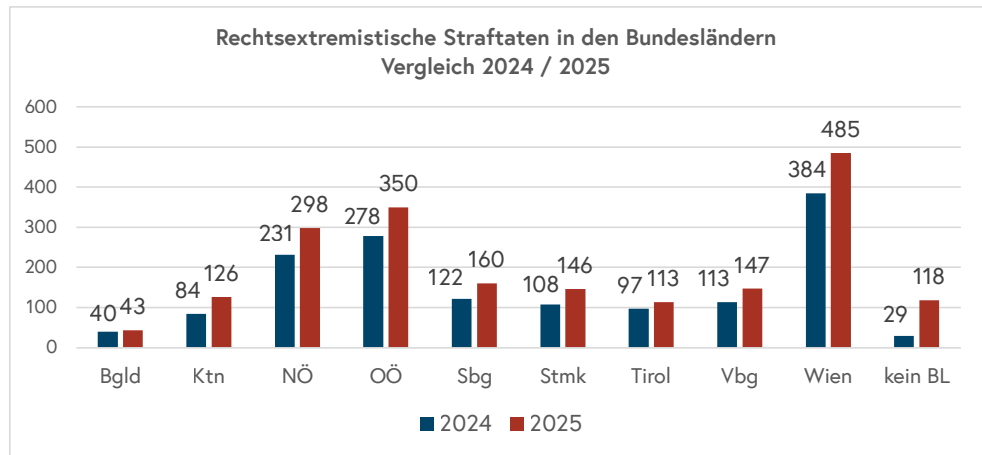
32 Der Anstieg resultiert aus der nunmehr gesetzlichen Regelung, dass Verwaltungsbehörden rechtskräftige Straferkenntnisse bzw. Strafverfügungen, unter anderen nach Art. III Abs. 1 Z 4 EGVG, den Sicherheitsbehörden für Zwecke der Sicherheitspolizei zu übermitteln haben, soweit diese deren Inhalt zur Erfüllung ihrer gesetzmäßigen Aufgaben benötigen.

Sprengmittelgesetz (SprG)	0	3
Suchtmittelgesetz (SMG)	14	5
Sicherheitspolizeigesetz (SPG)	6	3
Versammlungsgesetz (VersG)	21	0
Sonstige Gesetze oder Verordnungen	4	10
Summe	2.346	3.053

Von den insgesamt 1.986 im Phänomenbereich Rechtsextremismus bekanntgewordenen Tathandlungen waren 1.701 (85,6 Prozent) rechtsextremistisch im engeren Sinn (2024: 1.296, 87,2 Prozent), 127 (6,4 Prozent) fremdenfeindlich/rassistisch (2024: 97, 6,5 Prozent), 93 (4,7 Prozent) antisemitisch (2024: 59, 4 Prozent) und 16 (0,8 Prozent) islamfeindlich (2024: 9, 0,6 Prozent) motiviert. Bei 49 (2,5 Prozent) Tathandlungen war eine unspezifische oder sonstige Motivlage³³ hinsichtlich der Tatausführung vorhanden (2024: 25, 1,7 Prozent).

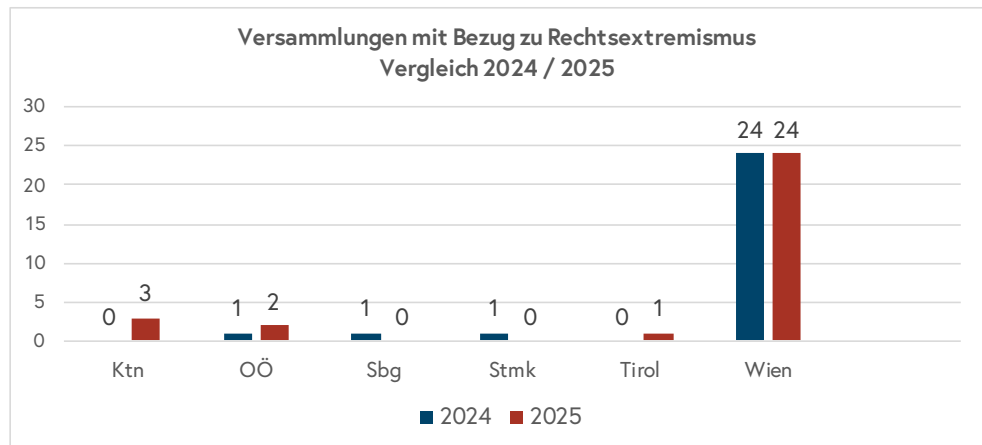


³³ Diese Zuordnung / Motivlage ermöglicht die Einordnung von Tathandlungen, die objektiv dem Rechtsextremismus zugeordnet werden, wenngleich die subjektive Tatseite nicht erfüllt ist. Beispiel: Flohmarktverkäufer veräußert NS-Devotionalien in reiner Gewinnabsicht.



In Zusammenhang mit dem **Nahostkonflikt** wurden im Phänomenbereich Rechtsextremismus im Jahr 2025 bundesweit **sieben Tathandlungen** registriert (2024: 5). Sechs davon waren rechtsextremistisch im engeren Sinn, eine fremdenfeindlich/rassistisch motiviert. Es erfolgten Anzeigen nach dem Verbotsgesetz, nach dem Delikt der Verhetzung gemäß § 283 StGB, dem Delikt der Sachbeschädigung gemäß § 125 StGB und wegen Übler Nachrede gemäß § 111 StGB.

Im Berichtsjahr 2025 wurden insgesamt **30 Versammlungen** (2024: 27), die einen Bezug zu Rechtsextremismus aufwiesen, registriert. Davon wurden 29 Versammlungen angemeldet. Die Themenfelder gliederten sich in Regierung (Bund/Land) (5) und sonstige Themen (25).



2.2 Heterodoxer Extremismus

Unter „Heterodoxem Extremismus“ (HEX) wird eine neuartige, eigenständige und stark heterogene Form von Extremismus verstanden, die sich nicht im Sinne der herkömmlichen politischen Klassifikation unter den Begriffen Links- oder Rechtsextremismus subsumieren lässt. Diese neue Form des Extremismus ist im Zuge des COVID-19-Protestgeschehens entstanden, als es zu engen, persönlichen Vernetzungen zwischen unterschiedlichsten Akteurinnen und Akteuren, beispielsweise aus dem staatsfeindlichen Milieu, der Esoterik, aus Sekten, dem Rechtsextremismus, der Impf- und Abtreibungsgegnerschaft, sowie zu einer Vermischung der inhaltlichen Ausrichtungen derselben gekommen ist. Heterodoxer Extremismus dient dabei als Sammelbegriff zur Bezeichnung von extremistischen Strömungen, Szenen, Milieus, Gruppierungen, Protestbewegungen und Vereinen, deren verbindendes ideologisches Element die grundsätzliche Ablehnung demokratischer/bestehender staatlicher Strukturen sowie der Glaube an (antisemitische) Verschwörungsnarrative ist. Insbesondere der Verschwörungsglaube an das Meta-Narrativ einer „bösen globalen Elite“, die über einen „geheimen Plan“ verfügt, um die Normalbevölkerung zu versklaven, gilt als kohäsives Element des Heterodoxen Extremismus. Demnach können die traditionell bestehenden Phänomene der Staatsfeindlichen Verbindungen (SfV) sowie jene der Corona-Maßnahmen-Gegner (CMG) unter das Beobachtungsfeld Heterodoxer Extremismus subsumiert werden.

2.2.1 Überblick

Analog zu den Entwicklungen in anderen EU-Ländern wird auch in Österreich spätestens seit der COVID-19-Pandemie die Entstehung einer neuartigen und eigenständigen Form von Extremismus beobachtet, die sich nicht im Sinne der herkömmlichen politischen Klassifikation unter den Begriffen Links- oder Rechtsextremismus subsumieren lässt. Der zentrale Unterschied zum Links- bzw. Rechtsextremismus ist, dass der Heterodoxe Extremismus zwar das aktuelle (verfassungsrechtliche) Gesellschaftsmodell ablehnt, die einzelnen Sub-Phänomene jedoch keinen einheitlichen Idealtypus einer neuen Gesellschaftsordnung definiert haben. Während also der Rechtsextremismus eine autoritäre und der Linksextremismus eine egalitäre Gesellschaftsordnung anstreben, wird der Heterodoxe Extremismus stattdessen von einem „Wir-gegen-das-System“-Gefühl bzw. von einem „Wir-gegen-die-globale-Elite“-Narrativ getragen. Ein weiterer essenzieller Unterschied zwischen Rechtsextremismus und Heterodoxem Extremismus liegt in der Konzeption des Feindbildes. Die Feindbilder im Rechtsextremismus sind in erster Linie Ausländerinnen und Ausländer, Migrantinnen und Migranten (insbesondere Musliminnen und Muslime) sowie Jüdinnen und Juden. Um diese bekämpfen und rassistische Aktionen setzen zu können, muss das derzeitige staatliche und demokratische System überwunden

werden. Demgegenüber sehen die Akteurinnen und Akteure des Heterodoxen Extremismus trotz einer vergleichbaren rassistischen, fremdenfeindlichen und antisemitischen Weltanschauung den Staat bzw. das „System“ und die globale Elite als den absoluten Feind, mit denen sie sich „im Krieg“ befinden und die es zu bekämpfen gilt.

Das wesentlichste Merkmal des Heterodoxen Extremismus ist seine fundamentalistische Ablehnung gesetzlicher Normen, demokratischer und rechtsstaatlicher Einrichtungen und Institutionen sowie verfassungsmäßiger Werte und Prinzipien. Das dadurch bei seinen Anhängerinnen und Anhängern erzeugte Gefühl, „erwacht“ zu sein, sowie die Vorstellung, sich durch das Entziehen aus staatlichen und gesellschaftlichen Normen „frei zu fühlen“, macht die besondere Attraktivität des Heterodoxen Extremismus aus. Damit einher geht zumeist der Glaube an verfassungsfeindliche Verschwörungsideologien sowie die Verbreitung von Desinformation.

Inhaltlich-ideologisch verfügt der Heterodoxe Extremismus grundsätzlich über keine eigenständige HEX-Ideologie, bedient sich jedoch ideologischer Schlüsselkonzepte wie Antisemitismus, Rechtsextremismus, Monarchismus, Rassismus, religiöser Fundamentalismus etc. Darüber hinaus wird der Heterodoxe Extremismus von einem umfangreichen Portfolio globaler und stark antisemitisch geprägter Verschwörungsideologien sowie (pro-)russischer Desinformation angetrieben, die an nationale, regionale und lokale Bedingungen angepasst werden. Die einzelnen Verschwörungsideologien werden in ein gemeinsames Meta-Narrativ eingebettet: Eine vermeintliche globale (jüdische) Elite („das System“) nutzt und inszeniert gesellschaftliche Krisen, um einen permanenten Ausnahmezustand zu erzeugen. Dieser dient der Implementierung und Ausweitung von Überwachungs- und Kontrollmaßnahmen, um ein globales totalitäres System zu etablieren und damit eine neue Weltordnung („New World Order“) zu erschaffen. Die vermeintliche „Klimahysterie“ werde als Vorwand benutzt, um die individuelle Transport- und Reisefreiheit einzuschränken, die „Systemmedien“ würden dafür sorgen, dass die Bevölkerung „staatstreu“ bleibe, und internationale Organisationen (EU, NATO, WHO etc.) sowie westliche Staaten und ihre Geheimdienste würden mit ihrer Kriegstreiberei den Dritten Weltkrieg provozieren, um den Ausgangspunkt des „Great Resets“ und damit die Versklavung der Normalbevölkerung zu generieren.

Als Extremismus sui generis stellt das Phänomen des Heterodoxen Extremismus national und international eine wachsende Bedrohung für die öffentliche Ruhe, Ordnung und Sicherheit dar und fungiert zudem als Verstärker für andere Formen des Extremismus sowie als Eingangstor für Einflussversuche durch Drittstaaten. Vor dem Hintergrund internationaler Sicherheitsdiskurse existieren abweichende terminologische und konzeptionelle Klassifikationen des Phänomens.

2.2.2 Aktuelle Lage

Die vom Heterodoxen Extremismus ausgehende Gefahr ergibt sich im Wesentlichen aus zwei sich wechselseitig beeinflussenden Faktoren: Gewaltbereitschaft und Drang zu politischer Subversion. Im Jahr 2025 war sowohl das Bedrohungspotenzial durch Gewaltakte als auch die Zahl der Straftaten aus dem heterodox-extremistischen Milieu in Österreich niedrig. Die Tathandlungen beschränkten sich überwiegend auf umfangreiche Behördeneingaben (Papierterrorismus), Drohungen und Verhetzung. Nichtsdestotrotz handelt es sich um eine Szene mit einer hohen Affinität für Waffen, Prepping³⁴, Survivaltrainings und gewaltorientierte Verschwörungsideologien. Zudem ist festzuhalten, dass im Jahr 2025 erstmals seit dem Ende der COVID-19-Pandemie im Milieu der Staatsfeindlichen Verbindungen ein Anstieg von Behördeneingaben und eine Reaktivierung von bereits aufgelösten Gruppierungen und Strukturen zu verzeichnen ist. Explizit ist hier die Neuformierung der Gruppierung Bundesstaat Preußen zu nennen. Im Zuge der COVID-19-Pandemie hat auch die seit 2012 in Österreich aktive Anastasia Bewegung³⁵ (AB) wieder an Popularität gewonnen. Zwar ist die Anzahl konkreter Siedlungsprojekte seit Jahren gleichbleibend, jedoch hat die Anzahl der Followerinnen und Follower bzw. Interessentinnen und Interessenten im Online-Raum stark zugenommen.

Online-Trends wie jene der Tradwives oder der Manosphere³⁶ und die damit verbreiteten Narrative von klassisch-patriarchalen Geschlechterrollen, Selbstversorgung und einem konservativ-fundamentalistischen Lebensentwurf machen die heterodox-extremistische Ideologie auch attraktiv für junge Menschen. Zudem verschwimmen durch die intensiv betriebene Verbreitung von Verschwörungsnarrativen zunehmend die Grenzen zwischen den einzelnen Phänomenen sowie zwischen Rechtsextremismus und Heterodoxem Extremismus. Besonders hervorzuheben ist dabei die Rolle der sogenannten Alternativmedien,

34 „Prepping“ (von engl. „prepare“, dt.: vorbereiten) bedeutet im verfassungsschutzrelevanten Kontext eine ideologisch aufgeladene Form der Krisenvorbereitung, die mit Angstnarrativen, Radikalisierung und Staatsfeindlichkeit verbunden ist. Häufig wird dabei ein besonderer Fokus auf Militarisierung gelegt, was mit dem Sammeln von Waffen, Kampftraining und paramilitärischen Übungen einhergeht.

35 Völkische Siedlungsbestrebungen sind aufgrund ihrer ideologischen Ausrichtung besonders anfällig für rechtsextreme Agitationen und pro-russische Propaganda. Diese Entwicklung wird insbesondere in der Anastasia Bewegung deutlich. Die Lehren der Anastasia stammen ursprünglich aus Russland, verfasst vom russischen Autor Wladimir Megre, und spielen in der russischen Taiga. Es verwundert daher nicht, dass der russische Staat das Potenzial dieser (pro-)russischen Bewegung als Einfallstor verdeckter Einflussnahme entdeckt hat. Diese Art der hybriden Kriegsführung äußert sich insbesondere in Form von (pro-russischen) Influencerinnen und Influencern, slawisch-arischen Veden und einer Ahnenkult, durch die anti-europäische, rassistische und antisemitische Ideologien zur Destabilisierung Österreichs und Europas vermittelt werden. Im Zentrum steht die Bewerbung Russlands als Land der Freiheit und als Bewahrer der „arisch-slawischen Tradition und Werte“.

36 „Manosphere“ (engl. Man = Mann, sphere = Netzwerk) bezeichnet ein loses Netzwerk von Online-Communities (z. B. Youtube-Kanäle), die sich mit Männlichkeit, Beziehungen, Dating, Rollenbildern und Geschlechterpolitik beschäftigen. Meistens handelt es sich dabei um radikalisierte Männer, die Kritik am Feminismus und das Gefühl von Benachteiligung und/oder Machtverlust thematisieren. Eine bekannte und sehr extreme Strömung innerhalb der Manosphere ist jene der Incels.

die als österreichweites Sprachrohr für verfassungsfeindliche Verschwörungsnarrative fungieren und in den sozialen Medien und auf Messenger-Diensten über große Reichweiten verfügen.

Alternativmedien



Unter „**Alternativmedien**“ werden unterschiedliche Medienportale zusammengefasst, die insbesondere der heterodox-extremistischen und der neurechten Szene zuzuordnen sind und sich als Gegenentwurf zu traditionellen Medien verstehen. Sie delegitimieren die etablierten Medien als „Systemmedien“ und „Lügenpresse“, während sie gleichzeitig stark ideologisch aufgeladene Inhalte kostenlos über Plattformen wie Facebook, YouTube, X, Telegram oder eigene Webseiten verbreiten. Letzteres beinhaltet oftmals auch die Verbreitung von Fake News, (pro-russischer) Desinformation und Verschwörungsideologien. Alternativmedien können im Gegensatz zu etablierten Medien ihre Inhalte sehr kostengünstig anbieten, da auf jegliche Form der professionellen Recherche und des Fact-Checkings verzichtet wird.

Innerhalb des Überlappungsbereiches zwischen den Phänomenbereichen Heterodoxer Extremismus und Rechtsextremismus (insbesondere Neue Rechte) haben sich im Zuge der COVID-19-Pandemie und dem daraus resultierenden Misstrauen gegenüber Staat und Medien zahlreiche Alternativmedien sowie einschlägige Influencerinnen und Influencer entwickelt, die als Sprachrohr und zur Informationsbeschaffung der Szenen dienen. Die Alternativmedien agieren dabei als Bindeglied zwischen der rechtsextremen Szene, rechtspopulistischen Parteien, heterodox-extremistischen Gruppierungen und Verschwörungsnarrativen. Zusätzlich haben sich Alternativmedien in Österreich im Wahljahr 2024 als verlängerter Arm des russischen Staates erwiesen. Generell ist evident, dass Alternativmedien als Einfallstor für verdeckte Einflussnahme durch Drittstaaten genutzt werden – insbesondere für Desinformationskampagnen.

Inhaltlich und ideologisch verbreiten Alternativmedien in erster Linie Verschwörungsnarrative und (russische) Desinformation. Verpackt in Phrasen wie „Man wird ja noch Fragen stellen dürfen“ oder „Schon seltsam, dass...“ prophezeien sie angeblich drohende weitere „Corona-Diktaturen“ und behaupten, dass hinter der „Massenmigration“ das Werk einer (jüdischen) „Weltelite“ bzw. des „Deep State“ stehe. Ob Hochwasserkatastrophen, Terroranschläge oder Nahostkonflikt – hinter jeder Krise unserer Zeit wird eine große Verschwörung gesehen. Dabei bedienen sich die Alternativmedien häufig jahrhundertalter antisemitischer Denkmuster, wonach etwa eine geheime jüdische Finanzelite die Welt beherrsche, und verwenden dazu sprachliche Codes und Chiffren (z. B. Juden = Globalisten, Finanzelite). Darüber hinaus wird die Kritik an der Politik Israels als Argument für die Dämonisierung und die angebliche „Doppelmoral“ des Judentums sowie

zur Verbreitung antisemitischer Stereotype genutzt, um in weiterer Folge sogar offene Holocaust-Relativierung zu betreiben.

Untermalt werden die als eigene Meinung formulierten und häufig kodifizierten Inhalte mit KI-generierten Bildern von „Chemtrails“, Kriegsgebieten und Flüchtlingsströmen. Dabei positionieren sich Alternativmedien bewusst gegen die sogenannten „Mainstream-Medien“ und beanspruchen die absolute Wahrheit für sich. Insgesamt gehen Alternativmedien höchst professionell vor, sodass der Anschein eines „echten Medienhauses“ entsteht. So verwenden sie beispielsweise zwar journalistische Darstellungsformen, verbreiten aber im Gegensatz zu etablierten Medien ihre stark einseitig dargestellten und polarisierenden Inhalte. Die Zahl der Feindbilder ist umfangreich, vermischt sich mit jener von rechtsextremistischen Akteuren und umfasst im Wesentlichen das demokratische Staatssystem, Ausländerinnen und Ausländer sowie alles, was vermeintlich „links“, „grün“ oder „woke“³⁷ ist.

In Österreich haben sich in den letzten Jahren diverse Alternativmedien herausgebildet, die zwar nicht Teil der offiziellen Medienmessungssysteme sind, deren Reichweite und Einfluss auf extremistische Milieus aber als groß eingestuft wird:

AUF1: Der 2021 gegründete Online-TV-Sender mit Sitz in Linz gilt als das mit Abstand reichweitenstärkste rechtsextreme und heterodox-extremistische Alternativmedium in Österreich (knapp 300.000 Followerinnen und Follower auf Telegram). AUF1 verbreitet verfassungsfeindliche Inhalte, antisemitische Verschwörungsnarrative und Desinformation.

Report24: Der im Zuge der COVID-19-Pandemie im Jahr 2021 entstandene Online-Blog entwickelte sich innerhalb der letzten vier Jahre zum zweitgrößten Alternativmedium in Österreich und verbreitet rechtsextremes, staatsfeindliches sowie verschwörungsideologisches Gedankengut. Insbesondere in den Kommentarspalten werden regelmäßig Gewaltfantasien gegenüber Regierungsmitgliedern gepostet. Aufgrund der selbsterklärten „wirklichen Meinungsfreiheit“ werden diese Kommentare seitens der Redaktion nicht gelöscht. Im Redaktionsteam befinden sich unter anderem bekannte Persönlichkeiten aus den radikalen, verschwörungstheoretischen Kreisen der COVID-19-Protestszene.

RTV: Der oberösterreichische Regionalsender RTV berichtete ursprünglich von Dorffesten und Geschäftseröffnungen in Steyr und Umgebung. Seit der COVID-19-Pandemie konnte

37 „Woke“ ist ein aus dem Englischen übernommener Begriff (dt.: „aufwachen“) und bedeutet in hohem Maße politisch wachsam und engagiert gegen, insbesondere rassistische, sexistische und soziale, Diskriminierung zu sein. Der Begriff und seine Bedeutung wurden vor allem im Zuge der Black Lives Matter-Bewegung bekannt, wird mittlerweile jedoch auch als Kampfbegriff von insbesondere rechten politischen Akteuren genutzt, um progressivere Bewegungen, Akteure oder Ideen abzuwerten.

der Sender seine Reichweite stark steigern und hat sich inhaltlich auf Verschwörungsnarrative und Desinformation fokussiert. Inhaltlich sowie personell weist RTV enge Kooperationen mit dem extremistischen Sender AUF1 auf. Zudem bedient RTV rechts-extreme Agitationen, z. B. gegenüber politischen Gegnerinnen und Gegnern. Anders als die anderen Alternativmedien sendet RTV nicht nur online, sondern auch via Antenne im Großraum Linz.

Info-DIREKT: Die IBÖ-nahe Online-Plattform ist eines der größten Alternativmedien in Österreich. Inhaltlich und ideologisch versucht Info-DIREKT, einen pseudo-intellektuellen Anspruch zu befriedigen, ohne auf rechtsextreme Kernthemen wie Asyl, Zuwanderung, Verschwörungsnarrative und politische Feindbilder zu verzichten.

Der Status: Der Status ist ein relativ neues Online-Alternativmedium, das im Jahr 2023 von der Chefredakteurin des ehemaligen Alternativmediums Wochenblick gegründet wurde. Inhaltlich setzt das Medium auf eine Kombination aus Kritik am „Mainstream“, verschwörungsideologischen Inhalten und rechtsextremen Parolen.

Charakteristisch für die österreichische Alternativmedienlandschaft sind die engen personellen und inhaltlichen Vernetzungen der einzelnen Portale untereinander sowie die starken Überlappungen mit der rechtsextremen Szene. Zudem arbeiten die einzelnen Medienakteure redaktionell gezielt mit einem „Wir-gegen-die-Anderen“-Narrativ, das zu einer Aufstachelung von Bevölkerungsgruppen führt und ein wesentliches Problem für den pluralistischen, demokratischen Rechtsstaat darstellt. Neben der Verbreitung von verfassungsfeindlichen und extremistischen Inhalten sowie Verschwörungsnarrativen ergibt sich die Problematik der Alternativmedien nicht zuletzt auch aus dem Umstand, dass auf Fact-Checking bewusst verzichtet wird.

Darüber hinaus wird versucht, mittels absichtlich herbeigeführter Informationsflut (engl. Information Overload) für Verwirrung und Misstrauen in der Gesellschaft zu sorgen. Durch die gleichzeitige Verbreitung sehr vieler widersprüchlicher Informationen und dem daraus entstehenden kognitiven Stress verlieren Fakten ihr Gewicht und es kommt zu einer de facto Gleichsetzung von Wahr und Falsch. Dadurch wird das gesellschaftliche Vertrauen in Medien, Wissenschaft und Institutionen systematisch untergraben. Die fortlaufende Verbreitung von demokratieablehnender und systemfeindlicher Propaganda führt zudem zu einer zunehmenden „Normalisierung“ von extremistischen Haltungen und Einstellungen in der österreichischen Gesellschaft. Daher stellen Alternativmedien neben dem Heterodoxen Extremismus nicht nur in Österreich, sondern in ganz Europa eine hybride und wachsende Bedrohung für die öffentliche Sicherheit dar.

Staatsfeindliche Verbindungen und Staatsverweigerer

Unter „Staatsfeindlichen Verbindungen“ (SfV) werden verschiedene Gruppierungen und Akteure (= **Staatsverweigerer**) verstanden, die mithilfe unterschiedlicher Begründungen die Existenz der Republik Österreich, deren Institutionen sowie das System des Rechtsstaates ablehnen bzw. nicht anerkennen. Dazu berufen sie sich unter anderem auf das historische Deutsche Reich („Reichsbürger“), diffuse Verschwörungsnarrative oder auf ein selbst definiertes Naturrecht. In weiterer Folge wird das hoheitsrechtliche Handeln des Staates abgelehnt und versucht, das bestehende Staatswesen durch den Aufbau paralleler Strukturen zu überwinden. Staatsverweigerer definieren sich selbst als „souveräne Völkerrechtssubjekte“, die vollständig außerhalb der österreichischen Rechtsordnung stehen und per Erklärung aus dem Staat bzw. der „Firma Österreich“ austreten können.

Die Szene der Staatsfeindlichen Verbindungen in Österreich umfasst heterodox-extremistische Einzelpersonen, Klein- und Kleinstgruppen, länderübergreifende Gemeinschaften und virtuelle Netzwerke, die aus unterschiedlichen Motiven und auf Basis von verschwörungsideologischen Argumentationsmustern die Existenz der Republik Österreich und deren Rechtssystem ablehnen, den demokratisch gewählten Regierungsmitgliedern die Legitimation absprechen oder sich zur Gänze außerhalb der Rechtsordnung stehend definieren. Diese personell, organisatorisch und ideologisch stark heterogenen Gruppierungen sehen im Staat das absolute Feindbild. Daraus folgt, dass der Staat bekämpft und überwunden werden muss – notfalls auch mit Gewalt.

Inhaltlich und ideologisch berufen sich Staatsfeindliche Verbindungen in Österreich häufig auf ein selbst definiertes Naturrecht oder auf alte, aber ihrer Ansicht nach noch gültige Verfassungen. Innerhalb dieser Scheinrechte werden je nach Gruppierung unterschiedliche ideologische Annahmen getroffen, jedoch leiten sie daraus immer eine vermeintliche Souveränität ab. Ein weiteres zentrales und verbindendes ideologisches Element der SfV-Szene ist die Grundannahme, dass es zwei „Existenzen“ gibt. Einerseits gibt es den „Menschen“, der ein natürliches, freies und souveränes Lebewesen ist und als ursprüngliches, gottgegebenes Sein außerhalb der Gesetze und Institutionen der Republik Österreich steht. Staatsverweigerer behaupten, dass sie sich nur als „Mensch“ dem Zugriff des Staates entziehen und „wahre Freiheit“ leben können. Demgegenüber steht andererseits das Konzept der „Person“. Diese sei eine künstliche, juristische Konstruktion des Staates, die bei der Geburt oder durch den Eintrag ins Personenstandregister erschaffen wird. Laut der Szene sei man als „Person“ nicht mehr frei, sondern ein „Staatssklave“. Daher schicken Staatsverweigerinnen und Staatsverweigerer häufig pseudo-juristische Schriftstücke an österreichische Behörden, in denen sie entweder klarstellen, „Menschen“ zu sein, oder sich als „Person“ abmelden (= sogenannte „Lebensmeldung“).

Als Beispiel ist der fiktive Bundesstaat Preußen zu nennen. Dabei handelt es sich um eine staatsfeindliche Verbindung mit ca. 100 Mitgliedern, die erstmals 2019 in Österreich in Erscheinung getreten ist. Die Gruppierung orientiert sich an den Prinzipien der deutschen Reichsbürgerszene sowie an der ehemaligen staatsfeindlichen Verbindung Staatenbund Österreich. Unter Berufung auf die sogenannten S.H.A.E.F.-Gesetze³⁸ wird das hoheitliche Handeln des österreichischen Staates und seiner Regierungsmitglieder abgelehnt. Ziel des Bundesstaats Preußen ist es, durch konkretes Intervenieren die öffentliche Verwaltung lahmzulegen bzw. sie in ihrer Arbeit zu behindern. Dafür werden bei österreichischen Verwaltungsorganen pseudo-juristische Behördeneingaben eingereicht, mit denen die Mitglieder ihre ablehnende Haltung gegenüber dem Rechtsstaat zum Ausdruck bringen. Darin „kündigen“ die „Bürgerinnen“ und „Bürger“ des fiktiven Bundesstaats Preußen unter anderem ihre österreichische Staatsbürgerschaft. Neben diesem Papierterrorismus wird Personen des öffentlichen Dienstes (z. B. Regierungsmitglieder, Staatsanwältinnen und Staatsanwälte, Polizistinnen und Polizisten) mit der Vernichtung ihrer finanziellen Existenz gedroht, indem ihnen der Eintrag hoher Schulden in diversen (internationalen) Schuldenregistern angekündigt wird. Die Zugehörigkeit zum Bundesstaat Preußen drückt sich bei den Mitgliedern insbesondere in der Verwendung eigener Fantasiedokumente, wie etwa Reisepässe, Führerscheine und Kennzeichentafeln, aus. Diese sollen ihrer staatsverweigernden Haltung besondere Legitimität verleihen und die Lossagung vom österreichischen Staat unterstreichen. Darüber hinaus nutzen sie Fahnen und Aufkleber mit dem Adler des Bundesstaats Preußen als Hoheitssymbol.

Die Gruppierung finanziert sich durch Teilnahmegebühren für Seminare und Workshops, Spendengelder, die Ausstellung von Fantasiedokumenten sowie mittels kostenpflichtiger Rechts- und Finanzberatungen. Trotz kriminalpolizeilicher Ermittlungsmaßnahmen besteht die staatsfeindliche Verbindung Bundesstaat Preußen bis heute fort.



2.2.3 Fälle 2025

Fall PAPIER

Ein nach dem Verbotsgesetz bereits vorbestrafter 49-jähriger Tiroler, der sich Ende 2022 für mehrere Monate in Untersuchungshaft befand und im Dezember desselben Jahres zu einer 18-monatigen Haft- sowie zu einer Geldstrafe von 1.440 Euro am Landesgericht Innsbruck verurteilt wurde, verfasste bereits in den Jahren 2021 und 2022 mehr als vierzig Schreiben an unterschiedliche Behörden, Ämter, Gerichte und Ministerien. In seinen Eingaben verlangte er die Einstellung mehrerer verwaltungs- und strafrechtlicher Verfahren, forderte Geldleistungen bzw. stellte Schadenersatzforderungen und drohte bei Nichtbeachtung mit einem Eintrag im amerikanischen Schuldenregister UCC. Damit

38 Ursprünglich stand die Abkürzung „S.H.A.E.F.“ für „Supreme Headquarters Allied Expeditionary Force“, also das Oberkommando der Alliierten Expeditionstreitkräfte im Zweiten Weltkrieg, welches zur Aufhebung des NS-Regimes mehrere Militärgesetze erließ. Im Verschwörungskontext wird behauptet, dass die damaligen S.H.A.E.F.-Gesetze nach wie vor in Kraft seien und Österreich/ Deutschland noch unter alliierter Kontrolle stünden.

nicht genug, gründete der Aktivist mehrere Vereine an seinem Firmensitz (Personen-transportunternehmen) und ermöglichte Sympathisantinnen und Sympathisanten der staatsfeindlichen Szene die Errichtung weiterer Vereine auf seinem Betriebsstandort. Die verfassten Eingaben an die Behörden umfassten außerdem die Aufforderung zur Kenntnisnahme diverser Rechte von Vereinsmitgliedern, wie etwa die Befreiung von der damals gültigen Masken- und Impfpflicht sowie das offene Tragen von genehmigungspflichtigen Schusswaffen ohne waffenrechtliches Dokument. Außerdem organisierte der Beschuldigte über sein Unternehmen Busfahrten zu Demonstrationen gegen die Corona-Schutz-Maßnahmen im Bundesgebiet.

Die vom Verfasser versendeten Schreiben dienten auch als Vorlage für die Eingaben diverser anderer Vereine an seinem Sitz, weshalb ihm auch die führende Mitgliedschaft in einer staatsfeindlichen Verbindung zur Last gelegt wird. In der Folge wurde der Beschuldigte aufgrund mehrerer Delikte wie Nötigung, Erpressung, Staatsfeindliche Verbindung und Anstiftung zum Amtsmissbrauch bei der Staatsanwaltschaft Innsbruck angezeigt. Die Ermittlungen führte das LSE Tirol. Weiters konnten die Beamtinnen und Beamten im Laufe der Ermittlungen feststellen, dass auch die Lebensgefährtin des Angezeigten tief in der Ideologie verhaftet ist sowie Unterstützungsleistungen und eigene Schreiben verfasst hatte. Das LSE Tirol übermittelte am 18. August 2025 den Abschlussbericht hinsichtlich der genannten Delikte an die Staatsanwaltschaft Innsbruck.

Parallel zu den geführten Ermittlungen des LSE Tirol konnten Dienststellen in Tirol weitere Tathandlungen des Tatverdächtigen feststellen. Hierbei handelte es sich um Verstöße wegen betrügerischer Krida, Untreue, schweren Betrugs, Kurpfuscherei, Urkundenfälschung und Datenfälschung.

Aus diesem Grund fanden in den letzten Jahren mehrere Hausdurchsuchungen der involvierten Ermittlungsbehörden auf den Liegenschaften des Tatverdächtigen sowie Festnahmen der verdächtigen Personen statt. Die Ermittlerinnen und Ermittler stellten dabei elektronische Datenträger, Vereinsunterlagen (diverser Verbindungen), gefälschte COVID-Impfzertifikate und Waffen sicher.

2.2.4 Trends und Entwicklungstendenzen

In Österreich hat sich die heterodox-extremistische Szene seit dem Ende der COVID-19-Pandemie inhaltlich und strukturell weiterentwickelt und professionalisiert. In den Jahren 2022/2023 konnte eine thematische Neu- bzw. Umorientierung der HEX-Akteurinnen und HEX-Akteure beobachtet werden, da das Kernthema (Corona bzw. staatliche Maßnahmen zur Eindämmung des COVID-19-Virus) an Bedeutung verloren hat. Diese Entwicklung wurde von einer Unterwanderung der Szene durch rechtsextreme Akteurinnen und Akteure sowie einer erheblichen Reichweitensteigerung der sogenannten Alternativmedien begleitet. Insbesondere neurechte Protagonistinnen und Protagonisten kaperten hetero-

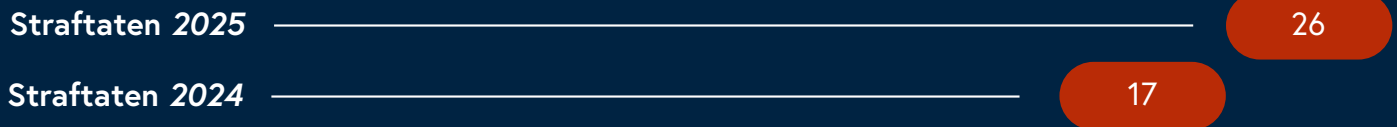
dox-extremistische Themen und nutzten die während der COVID-19-Protestbewegung gewonnenen Kontakte bewusst, um ihre Ideologie zu verbreiten.

Seit Anfang 2024 scheint diese thematische Umorientierung zumindest für die meisten heterodox-extremistischen Führungspersönlichkeiten abgeschlossen zu sein. Dieser Umstand äußert sich insbesondere durch eine Verschiebung der Mobilisierungsstrategie: Die während der Pandemie insbesondere auf Telegram aufgebauten großen Reichweiten werden nun vermehrt genutzt, um die Anhängerschaft für monetäre Zwecke anzusprechen. Anstatt für die wöchentlichen COVID-19-Demonstrationen, Stammtische und Kundgebungen zu werben, werden nun mittels diverser Verkaufs- und Vertriebsmodelle Verschwörungsnarrative und extremistisches Gedankengut finanziell profitabel gemacht. Dieses Geschäft mit der Angst basiert auf überdramatisierten Bedrohungsszenarien und den dazu passenden konsumierbaren Lösungen. Klassische Spendenaufrufe, alternativmedizinische Präparate, Nahrungsergänzungsmittel, politisiertes Merchandise, Krisenvorsorgeartikel, Verschwörungsliteratur und diverse Coaching-Formate stärken aktuell die ökonomisch-finanzielle Potenz der heterodox-extremistischen Szene in Österreich.

International zeigt die heterodox-extremistische Szene bzw. das internationale Phänomen des Anti-System-Anti-Government-Extremism (ASAGE) eine steigende Tendenz. Sowohl aus dem europäischen Ausland wie auch aus den USA werden regelmäßig Berichte von Waffenfunden, gewalttätigen Auseinandersetzungen mit Behördenvertreterinnen und Behördenvertretern sowie vereitelte Anschläge publik. In Österreich ist das Bedrohungspotenzial durch Gewaltakte aus dem heterodox-extremistischen Milieu bislang niedrig, nichtsdestotrotz wird auch Österreich im europäischen Vergleich eine relevante Szenenaktivität zugeschrieben. Das liegt einerseits am gemeinsamen Sprach- und Kulturkreis innerhalb der DACH-Region³⁹, andererseits am liberalen österreichischen Vereinsgesetz, das zur Verschleierung und Verschachtelung von Firmenkonstruktionen intensiv genutzt wird. Darüber hinaus kann beobachtet werden, dass die Anzahl und die Aktivitäten der Staatsfeindlichen Verbindungen seit Mitte 2024 zunehmen. Die Entwicklungen in Österreich entsprechen damit jenen in anderen europäischen Ländern: Das Phänomen des Heterodoxen Extremismus stellt eine verfassungsschutzrelevante Form des Extremismus dar – eine weitere quantitative und qualitative Zunahme und Stärkung ist mit hoher Wahrscheinlichkeit zu erwarten.

39 Die „DACH-Region“ umfasst den geografisch deutschsprachigen Raum; die Abkürzung setzt sich aus den Ländercodes von Deutschland (D), Österreich (AT) und der Schweiz (CH) zusammen.

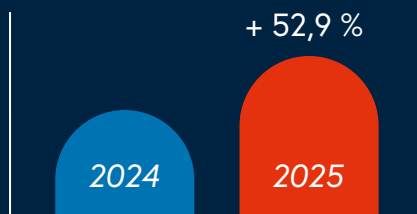
Heterodoxer Extremismus



Aufklärungsquote



Anstieg zum Vorjahr



Täterinnen und Täter



Staatsbürgerschaft der Täterinnen und Täter

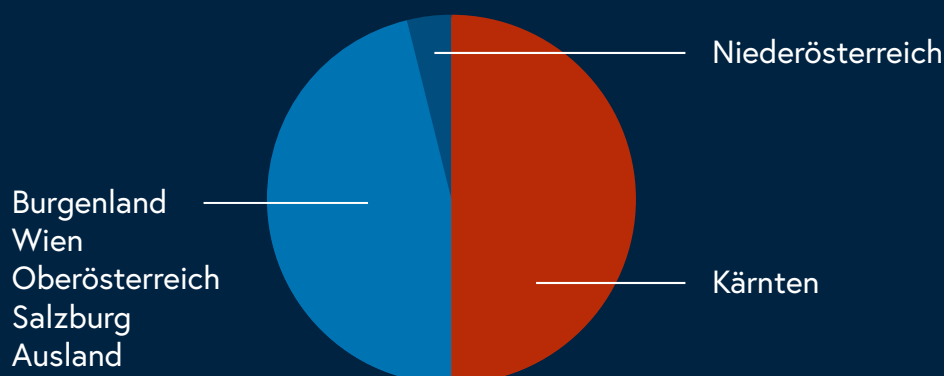


 **1**
Hausdurchsuchung

 **2**
Festnahmen

 **46**
Zur Anzeige
gebrachte Delikte

Bundesländeraufteilung



2.2.5 Zahlen/Daten/Fakten

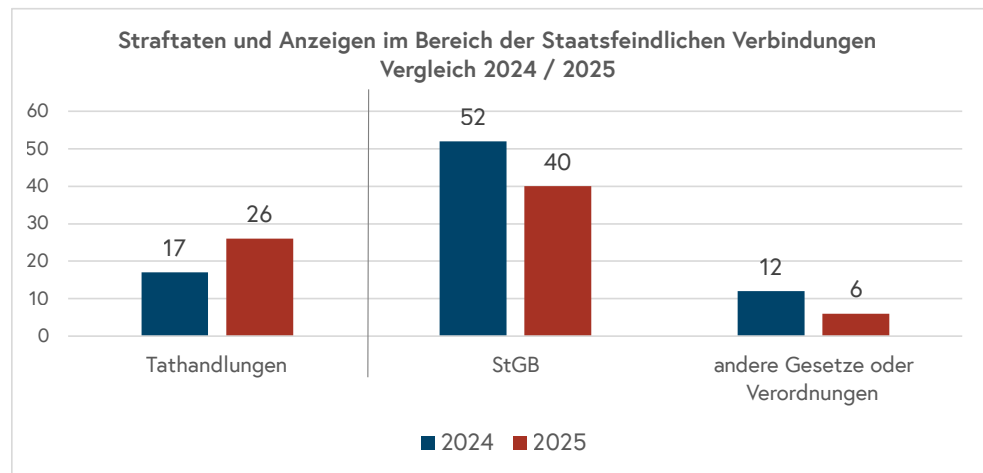
Staatsfeindliche Verbindungen

Im Jahr 2025 wurden den Sicherheitsbehörden in Österreich im Phänomenbereich **Staatsfeindliche Verbindungen** insgesamt **26 Straftaten** bekannt. Gegenüber dem Vorjahr (17 Straftaten) bedeutet dies einen **Anstieg um 52,9 Prozent**. 22 der 26 Straftaten konnten aufgeklärt werden, die **Aufklärungsquote** liegt somit bei **84,6 Prozent** (2024: 94,1 Prozent – 16 Tathandlungen).

Im Zusammenhang mit den gesetzten Tathandlungen gelangten insgesamt **46 Delikte**, davon 40 nach dem Strafgesetzbuch (StGB), zur Anzeige (2024: 64).

Insgesamt wurden **28 Tatverdächtige** (2024: 18) ausgeforscht und zur Anzeige gebracht. Dabei handelt es sich um zwölf männliche und 16 weibliche Personen. Im Jahr 2024 gelangten 13 männliche und fünf weibliche Personen zur Anzeige. Unter den Beschuldigten befanden sich, so wie im Vorjahr, keine Jugendlichen. 21 der in diesem Spektrum angezeigten Personen (75 Prozent) besitzen die österreichische Staatsbürgerschaft (2024: 13, das entspricht 72,2 Prozent).

Im Zusammenhang mit der Bekämpfung von Aktivitäten Staatsfeindlicher Verbindungen wurde **eine Hausdurchsuchung** (2024: 1) durchgeführt und **zwei Festnahmen** (2024: 4) vollzogen.



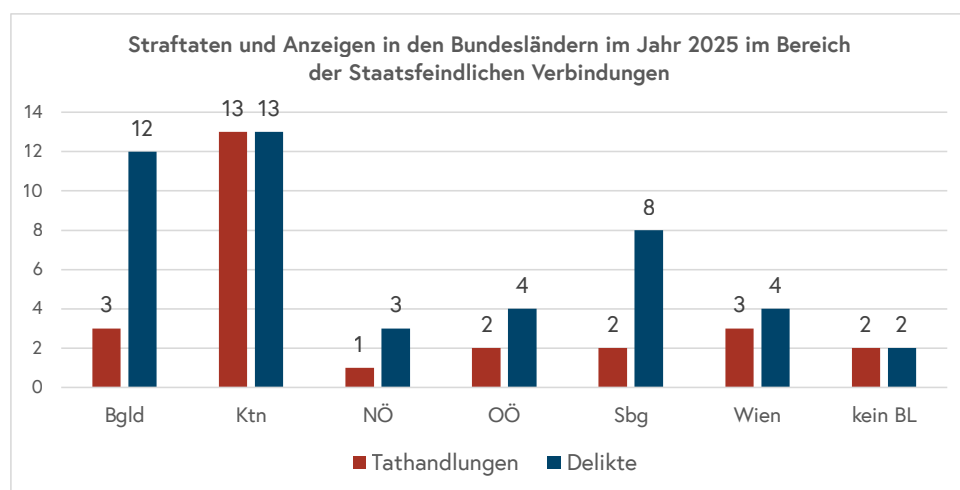
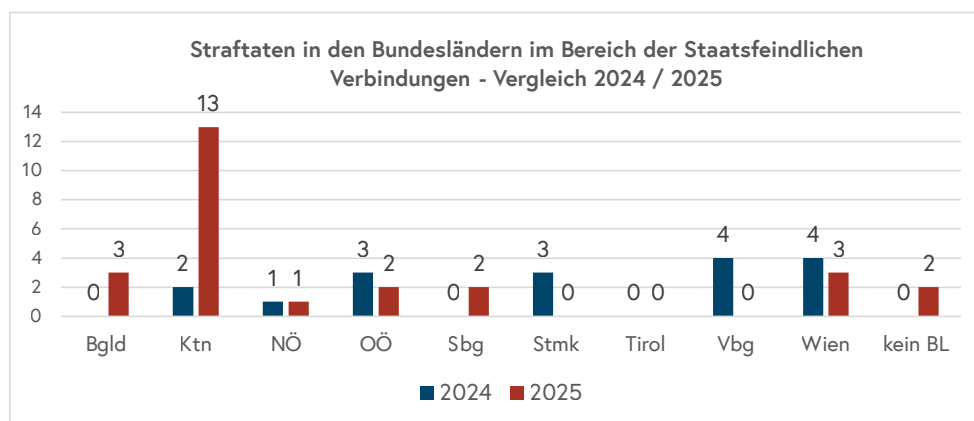
Zu einem **Anstieg** kam es beim Delikt der Gefährlichen Drohung gemäß § 107 StGB (0 auf 2), wegen Urkundenfälschung gemäß § 223 StGB (0 auf 1), dem Delikt des Widerstandes gegen die Staatsgewalt gemäß § 269 StGB (2 auf 3), dem Delikt der Kriminellen Organisation gemäß § 278a StGB (0 auf 1), wegen Aufforderung zu mit Strafe bedrohten Handlungen und Gutheißung mit Strafe bedrohter Handlungen gemäß § 282 StGB (0 auf 3), wegen Missbrauchs der Amtsgewalt gemäß § 302 StGB (1 auf 4) sowie den §§ 50 und 51 des Waffengesetzes (0 auf 5).

Rückläufig waren im Berichtsjahr Anzeigen wegen Schwerer Körperverletzung gemäß § 84 StGB (2 auf 1), wegen Nötigung gemäß § 105 StGB (4 auf 1), dem Delikt der Staatsfeindlichen Verbindungen gemäß § 246 StGB (7 auf 6), dem Delikt der Staatsfeindlichen Bewegung gemäß § 247a StGB (29 auf 18) und nach dem Verbotsgesetz (2 auf 1).

Anzeigen nach dem StGB	2024	2025
Schwere Körperverletzung (§ 84 StGB)	2	1
Nötigung (§ 105 StGB)	4	1
Gefährliche Drohung (§ 107 StGB)	0	2
Urkundenfälschung (§ 223 StGB)	0	1
Staatsfeindliche Verbindungen (§ 246 StGB)	7	6
Staatsfeindliche Bewegung (§ 247a StGB)	29	18
Widerstand gegen die Staatsgewalt (§ 269 StGB)	2	3
Kriminelle Organisation (§ 278a StGB)	0	1
Aufforderung zu mit Strafe bedrohten Handlungen und Gutheiung mit Strafe bedrohter Handlungen (§ 2 82 StGB)	0	3
Missbrauch der Amtsgewalt (§ 302 StGB)	1	4
Sonstige StGB-Delikte	7	0

Anzeigen nach anderen Gesetzen oder Verordnungen		
Verbotsgesetz (VbtG)	2	1
§ 50 Waffengesetz (WaffG)	0	3
§ 51 Waffengesetz (WaffG)	0	2
Sonstige Gesetze oder Verordnungen	10	0
Summe	64	46

Im Phänomenbereich Staatsfeindliche Verbindungen fanden 50 Prozent der Straftaten im Bundesland Kärnten statt, gefolgt von Burgenland und Wien (jeweils 11,5 Prozent), Oberösterreich und Salzburg (jeweils 7,7 Prozent) sowie Niederösterreich (3,9 Prozent). Bei zwei Tathandlungen (7,7 Prozent) befand sich der Tatort im Ausland.

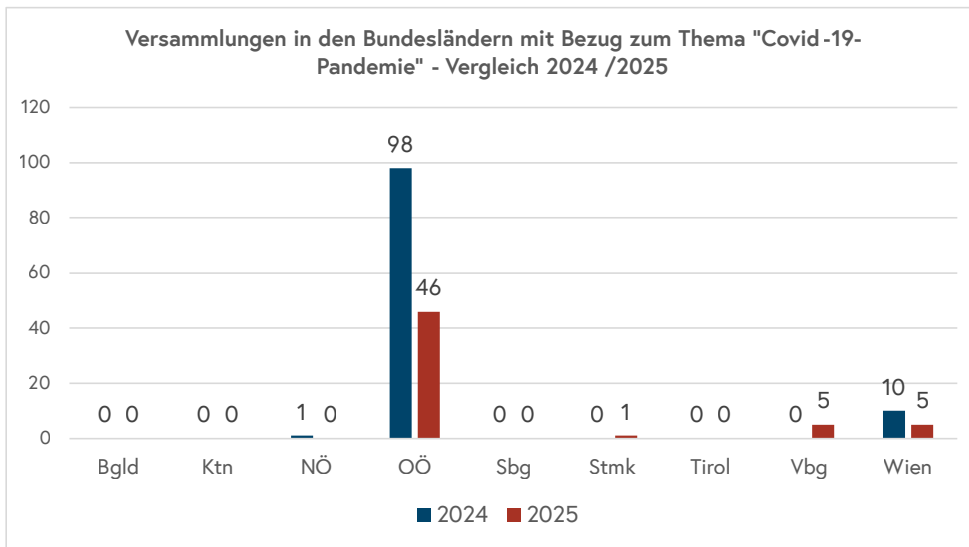


Im Berichtsjahr 2025 wurden 50 angemeldete Versammlungen (2024: 3) mit Bezug zu Staatsfeindlichen Verbindungen registriert. Alle Versammlungen fanden in Oberösterreich statt.

Corona-Maßnahmen-Gegner

Im Jahr 2025 wurde von den Sicherheitsbehörden in Österreich in der Kategorie **Corona-Maßnahmen-Gegner ein Vorfall** registriert (2024: 1 Tathandlung). Demnach wurde in Oberösterreich eine Person wegen Verhetzung gemäß § 283 StGB zur Anzeige gebracht.

Im Berichtsjahr 2025 wurden insgesamt 57 Versammlungen (2024: 109) abgehalten, bei denen inhaltlich das Thema COVID-19-Pandemie behandelt wurde. Alle Versammlungen wurden angemeldet.



2.3 Linksextremismus

„Linksextremismus“ (LEX) ist als Sammelbezeichnung für alle politischen Auffassungen und Bestrebungen zu verstehen, die im Namen der Forderung nach einer von sozialer Gleichheit geprägten Gesellschaftsordnung die Normen und Regeln eines modernen demokratischen Verfassungsstaates ablehnen und diesen mit Mitteln bzw. unter Gutheißung oder Inkaufnahme von Gewalt bekämpfen.

2.3.1 Überblick

Linksextremismus umfasst in Österreich verschiedene Strömungen, darunter auch kommunistische und anarchistische Ideologien. Diese Bewegungen lehnen die bestehende politische Ordnung, das demokratische System und den Rechtsstaat ab. Das bürgerlich-kapitalistische System wird als unterdrückerisch betrachtet und folglich bekämpft. Um ihre Ziele zu erreichen, betrachten linksextreme Gruppen Gesetzesbrüche und teils auch Gewalt als legitime Mittel.

Innerhalb der linksextremen Szene in Österreich existieren divergierende Strömungen, die eine Aufspaltung in zwei Hauptrichtungen zur Folge haben. Einerseits bestehen marxistisch-leninistisch bzw. trotzkistisch orientierte Gruppen, die auf einen revolutionären Umsturz setzen und deren Ziel es ist, eine klassenlose, kommunistische Gesellschaft zu etablieren. In der Idealvorstellung des Kommunismus würde es nach einer Übergangsphase keine politische Macht und keinen Staat im traditionellen Sinne mehr geben. Andererseits gibt es Akteurinnen und Akteure sowie Gruppierungen, die dem autonom-anarchistischen Spektrum zugeordnet werden und die für eine gänzlich herrschaftsfreie

und selbstverwaltete Gesellschaft eintreten. In diesem Zusammenhang geht die größte Gefahr für die öffentliche Sicherheit von der autonom-anarchistischen Szene aus.

„**Marxistisch-leninistische/trotzkistische Gruppierungen**“ streben die politische Umgestaltung des vorherrschenden demokratischen Systems auf Basis eines Gedankengerüsts an, das dem Marxismus-Leninismus entspringt, bzw. folgen sie der Interpretation des Marxismus von Leo Trotzki. Eine klassenlose kommunistische Gesellschaft, welche die Strukturen des Kapitalismus überwunden hat, gilt dabei als eines der wichtigsten politischen Ziele. Marxistisch-leninistische und trotzkistische Organisationen treten im Regelfall nicht offen gewalttätig auf, stehen jedoch der Gewalt als Mittel zur Umsetzung ideologischer Ziele nicht ablehnend gegenüber.

„**Autonom-anarchistische Bewegungen**“ lehnen eine feste politische Struktur in Form von Parteien oder staatlichen Verwaltungseinrichtungen sowie formale Hierarchien generell ab. Kernthematik für Autonome ist das Schaffen umfassender Freiräume, die eine uneingeschränkte Selbstbestimmung ermöglichen. Dabei wird ideologisch auf dem Anarchismus aufgebaut, der die Abschaffung jeglicher Herrschaft von Menschen über Menschen beschreibt. Inhärent ist dabei, dass Gewalt befürwortet und aktiv gegen gegnerische politische Gruppen und staatliche Institutionen angewendet wird.

In Österreich zeigen linksextreme Gruppen oft eine starke Ablehnung gegenüber staatlichen Institutionen, dem Kapitalismus und der internationalen Politik. Besonders in urbanen Zentren kommt es immer wieder zu Protesten und teils gewaltsamen Aktionen, etwa gegen die sogenannte Gentrifizierung⁴⁰, gegen Umweltzerstörung oder bei Antifaschismus-Kampagnen. Auch wenn diese Gruppen organisatorisch häufig nur lose verbunden sind, hat die Zunahme internationaler Vernetzung, insbesondere durch soziale Medien, die Mobilisierung und Radikalisierung in der Szene erleichtert und verstärkt.

Antisemitische Denkmuster sind auch im linksextremen Spektrum in unterschiedlichen Ausprägungen feststellbar. Sie treten zumeist nicht in offener Form auf, sondern äußern sich indirekt in der Delegitimierung und Dämonisierung des Staates Israel, der häufig als Symbol westlicher Machtstrukturen oder als „imperialistischer Akteur“ dargestellt wird. In diesem Zusammenhang werden antiisraelische Positionen mit antikapitalistischen und

40 „Gentrifizierung“ bezeichnet den Prozess der sozialen, kulturellen und wirtschaftlichen Umstrukturierung eines Stadtteils.

antiimperialistischen Argumentationsmustern verknüpft, wodurch klassische antisemitische Stereotype in vermeintlich „antikoloniale“ oder „solidarische“ Diskurse eingebettet werden. Besonders seit der Eskalation des Nahostkonflikts ab Oktober 2023 zeigt sich, dass linksextreme Gruppierungen an pro-palästinensischen Kundgebungen mitwirken und dort teilweise antisemitisch konnotierte Narrative verbreiten.

2.3.2 Aktuelle Lage

Im Jahr 2025 blieb der Kampf linksextremer Akteurinnen und Akteure gegen Rechtsextremismus, Rassismus und staatliche Repression ein zentrales Element der Szene. Diese Aktivitäten äußerten sich erneut in einem breiten Spektrum – von Demonstrationen und Kundgebungen bis hin zu Blockadeaktionen, Vandalismus und vereinzelt Gewalttaten. Neben dem Antifaschismus bildeten Antikapitalismus und Antiimperialismus weiterhin die zentralen ideologischen Bezugspunkte innerhalb der linksextremen Szene.

Die konsequent ablehnende Haltung gegenüber staatlichen Institutionen zeigte sich im Berichtsjahr unverändert. In zahlreichen Stellungnahmen, Aktionen und Online-Kampagnen forderten linksextreme Gruppierungen erneut die Auflösung oder Entmachtung der Sicherheitsbehörden und bezeichneten Polizei und Nachrichtendienste als „Repressionsinstrumente“. Diese Feinbildorientierung spiegelt sich sowohl in der Protestpraxis als auch in der digitalen Kommunikation wider, wobei insbesondere die sozialen Medien eine wesentliche Rolle bei der Mobilisierung einnehmen.

Im Jahr 2025 traten Akteurinnen und Akteure aus dem linksradikalen bis linksextremen Spektrum in Österreich wiederholt mit interventionsorientierten Protestformen in Erscheinung, die teils bewusst außerhalb des rechtlichen Rahmens lagen. Ein markantes Beispiel ist die Störaktion im Kontext der Eröffnung der Salzburger Festspiele am 26. Juli 2025: Aktivistinnen und Aktivisten unterbrachen den Festakt in der Felsenreitschule, entrollten Transparente und verursachten polizeiliche Maßnahmen bis hin zu Festnahmen.

Neben solchen unangemeldeten bzw. konflikträchtigen Versammlungs- und Störaktionen zeigten sich 2025 auch Anhaltspunkte für eine punktuelle Bereitschaft zur Anwendung körperlicher Gewalt gegen Personen, die als „rechts“ eingeordnet bzw. einem rechten Umfeld zugeordnet werden. Im Jänner 2025 kam es nach dem Grazer Akademikerball zu einem schweren tätlichen Angriff auf einen Ballbesucher. Solche Vorfälle sind insofern verfassungsschutzrelevant, als sie die Schwelle von konfrontativer Gegenmobilisierung zu gezielter Körperverletzung überschreiten und damit Radikalisierungs- bzw. Eskalationstendenzen einzelner Teilmilieus anzeigen.

Sachbeschädigungen und rechtswidrige Eingriffe in fremde Rechtsgüter bildeten 2025 einen wiederkehrenden Handlungsmodus. Im Zusammenhang mit einer Versammlung Ende Jänner 2025 kam es zu einer Sachbeschädigung am Haus der Wiener Burschen-

schaft Gothia. Darüber hinaus richtete sich Aktivismus wiederholt gegen Institutionen und Unternehmen: Am 21. August 2025 drangen mehrere Pro-Palästina-Aktivistinnen und Pro-Palästina-Aktivisten in das ORF-Zentrum am Wiener Königberg ein und brachten u. a. Farbschmierereien an. Am 22. August 2025 wurden bei BRP-Rotax⁴¹ in Gunskirchen Eingänge blockiert und das Firmendach besetzt. Im Kontext des Drohnensymposiums „DroneVation & Defence“ am 23. September 2025 in Wien wurde in der Nacht vor der Veranstaltung ein Behälter mit Buttersäure im Eingangsbereich ausgeschüttet.

In der Gesamtschau deuten diese Ereignisse auf eine in Teilen der Szene evidente Akzeptanz rechtswidriger Aktionsformen hin (Hausfriedensbruch, Störaktionen, Sachbeschädigung), wobei die Bandbreite von symbolischem Protest bis zu gesundheitsgefährdenden Mitteln reicht. Zugleich bleibt ein erheblicher Anteil politischer Mobilisierung im Rahmen legaler Versammlungs- und Protestpraxis. Die im Berichtsjahr dokumentierten Vorfälle sprechen dafür, dass einzelne Aktivist*innenkreise Gewalt gegen Sachen und punktuell auch gegen Personen als legitimes Mittel politischer Auseinandersetzung normalisieren. Dies kann Radikalisierungsprozesse begünstigen, weil Grenzüberschreitungen (illegaler Zutritt, Sabotage-/Störlogik) als wirksam erlebt und in Folge verstetigt werden bzw. eskalieren können.

Die linksextreme Szene in Österreich war auch 2025 von einer starken ideologischen Vernetzung geprägt. Neben klassischen Solidaritätsbekundungen zeigte sich eine zunehmende Zusammenarbeit mit Akteur*innen und Akteuren im europäischen Ausland. Exemplarisch sind das Engagement für linksextreme Aktivist*innen und Aktivisten, die in Deutschland und der Schweiz im Zusammenhang mit Angriffen auf Infrastruktur vor Gericht standen, und Protestaktionen gegen rechte Veranstaltungen (beispielsweise die Sommerdemo der IBÖ) zu nennen. Zudem blieben Solidarierungen mit marginalisierten gesellschaftlichen Gruppen und mit ethno-separatistischen Bewegungen ein zentrales Element linksextremer Ideologie. Besonders auffällig waren zudem die Verbindungen zu PKK-nahen Organisationen, die sich 2025 verstärkt im universitären Umfeld und in Städten wie Wien, Graz und Innsbruck manifestierten. Im Kontext der Situation in Syrien äußerte sich die Solidarität der Linksextremist*innen und Linksextremisten erneut in öffentlichen Kundgebungen zugunsten PKK-naher Gruppierungen. Personelle Überschneidungen, gemeinsame Veranstaltungen und eine ideologische Nähe in der Ablehnung westlicher Sicherheits- und Außenpolitik waren ebenfalls erkennbar.

Wie in anderen extremistischen Strömungen spielt auch in der linksextremen Szene der Kampfsport eine zunehmend wichtige Rolle. Trainings und Veranstaltungen werden

41 Als österreichisches Tochterunternehmen von BRP Inc. ist BRP-Rotax auf die Entwicklung und Produktion von Antriebssystemen für Produkte im Powersportsbereich spezialisiert. Aktivist*innen und Aktivisten werfen dem Unternehmen angeblich illegale Motorenlieferungen für israelische Drohnen vor.

dabei nicht nur zur physischen Stärkung, sondern auch zur Festigung des Gruppenzusammenhalts und zur internationalen Vernetzung genutzt. 2025 fanden in mehreren Städten entsprechende Veranstaltungen statt, teils unter dem Deckmantel sportlicher Initiativen, was die Bedeutung dieses Bereichs als soziales und organisatorisches Bindeglied unterstreicht.

Antifaschismus und Protestgeschehen

Das Thema Antifaschismus blieb 2025 der wichtigste Mobilisierungsfaktor innerhalb der linksextremen Szene. Besonders die mediale Präsenz rechter Gruppierungen führte zu einer Intensivierung antifaschistischer Gegenaktivitäten. In diesem Zusammenhang kam es in Wien, Linz und Salzburg zu mehreren unangemeldeten Demonstrationen und Blockadeaktionen, die teilweise in gewaltsame Auseinandersetzungen mit der Polizei mündeten. Der Antifaschismus dient weiterhin als verbindendes Narrativ unterschiedlicher linksextremer Strömungen und wird zunehmend mit kapitalismus- und systemkritischen Inhalten verknüpft.

Klimaschutz als Mobilisierungsfeld

Auch der Klimawandel war 2025 ein zentrales Thema innerhalb der linksextremen Szene in Österreich. Umwelt- und Klimafragen werden in den ideologischen Diskurs eingebettet und mit einer grundlegenden Kapitalismuskritik verknüpft. Dabei wird der Kapitalismus als Hauptverursacher globaler Krisen wie Krieg, Armut, Umweltzerstörung und sozialer Ungleichheit angeprangert.

Dennoch blieben Solidaritätsbekundungen mit der zivilgesellschaftlichen Klimabewegung häufig symbolischer Natur, während gleichzeitig ein kleiner Teil der linksextremen Szene aktiv zu radikaleren Aktionsformen aufrief.

Im Unterschied zu friedlich agierenden Gruppierungen wie Fridays for Future oder der bereits aufgelösten Gruppierung Extinction Rebellion sehen linksextreme Akteurinnen und Akteure in gezielten Sachbeschädigungen und Blockaden ein legitimes Mittel zur Zielerreichung. In mehreren europäischen Ländern kam es 2025 vermehrt zu Sabotageaktionen gegen Energie- und Verkehrsunternehmen, während in Österreich bislang keine systematische Gewaltkampagne von linksextremen Umweltgruppen festgestellt werden konnte. Einzelne Vorfälle – etwa kurzzeitige Gleisblockaden oder Farbanschläge auf Firmensitze fossiler Energieunternehmen – zeigen jedoch eine potenziell zunehmende Radikalisierungsneigung. Im Zuge einzelner Protestschauplätze im Kontext von Klimaschutzprotesten kam es vereinzelt zu Sachbeschädigungen an Baustellen, wobei eine Zuordnung dieser strafbaren Handlungen zu konkreten Akteurinnen und Akteuren nicht möglich war.

Eine gezielte Infiltration der zivilgesellschaftlichen Klimabewegung durch linksextreme Akteure oder die konsequente Übernahme des Umweltthemas konnte im Berichtsjahr

nicht beobachtet werden. Zwar bestehen punktuell personelle Überschneidungen, jedoch verhindern ideologische Differenzen eine vollständige Vereinnahmung.

Ideologische Spannungen innerhalb der Szene

Innerhalb der linksextremen Szene in Österreich bestanden auch 2025 deutliche ideologische Differenzen. Zwischen autonom-anarchistischen und marxistisch-kommunistischen Gruppierungen kam es immer wieder zu Spannungen – insbesondere in Bezug auf den Nahostkonflikt. Während Teile des autonom-anarchistischen Spektrums eine eher pro-israelische Haltung einnehmen und den Angriff der Hamas auf Israel offen verurteilen, solidarisieren sich marxistisch geprägte Gruppierungen verstärkt mit der palästinensischen Bevölkerung und sehen Israel als „imperialistische Macht“.

Diese innerlinke Spaltung trat 2025 vor allem in Wien und Graz deutlich zutage, wo es bei Demonstrationen zu offenen Konflikten zwischen den Lagern kam (beispielsweise während der Demonstrationen am 1. Mai). Trotz dieser Differenzen bleibt der Antizionismus in Teilen der Szene präsent, meist in Form von antiimperialistischen bzw. antikolonialistischen Narrativen, bei dem der Staat Israel und seine Verbündeten zum Feindbild erklärt werden.

Im Berichtsjahr wurden vereinzelt auch antizionistische und antisemitische Äußerungen und Symbole, u. a. im Zusammenhang mit pro-palästinensischer Mobilisierung, festgestellt. Kohärente Agitations- und Deutungslinien hinsichtlich dieser Thematik waren weiterhin nicht zu erkennen.

Insgesamt zeigte die linksextreme Szene in Österreich im Jahr 2025 eine stabile personelle Basis und ein hohes Maß an ideologischer Geschlossenheit innerhalb der jeweiligen Gruppierungen. Während ein Großteil der Aktivitäten weiterhin auf symbolische Aktionen und Proteste beschränkt blieb, ist in Teilsegmenten eine Übernahme militanter Taktiken und Aktionsformen feststellbar. Die Verschränkung von Antifaschismus, Klima-/Umwelt-Aktivismus und internationaler pro-palästinensischer Solidarität prägt das aktuelle Erscheinungsbild der linksextremen Szene in Österreich.



2.3.3 Fälle 2025

Fall MÜTZE

Am 25. Jänner 2025 fand der 70. Grazer Akademikerball im Congress Graz statt. Im Vorfeld kam es zu einer angemeldeten Demonstration, an der rund 1.500 Personen teilnahmen. Am Marsch bzw. der Standkundgebung nahmen unter anderem auch Personen teil, die dem linksextremen Spektrum zuzuordnen sind.

In der Nacht von 25. auf den 26. Jänner 2025 griffen sieben vorerst unbekannte Täterinnen und Täter, die dem linksextremistischen Milieu zugehörig sind, einen Ballbesucher im Beisein seiner Ehefrau am Heimweg an. Im Zuge der Tathandlung entrissen die

Aktivistinnen und Aktivisten dem Opfer seine Studentenmütze, woraufhin die Person zu Sturz kam. Die dabei erlittenen schweren Verletzungen machten einen mehrtägigen Krankenhausaufenthalt notwendig. Die Verdächtigen hingegen flüchteten mit der Kopfbedeckung des Opfers vom Tatort.

Daraufhin erfolgte gegen die insgesamt sieben Beschuldigten eine Anzeige wegen des Verdachts des schweren Raubes. Zwei unmittelbare Haupttäter und fünf Beitragstäterinnen und Beitragstäter konnten durch das Opfer und seine Ehefrau gesehen werden. Das LSE Steiermark leitete in der Folge die Ermittlungen ein.

Die Ermittlungsbehörde führte die Sichtung und Auswertung von Videoaufzeichnungen im Nahbereich des Tatortes sowie Einvernahmen von Opfer und Zeugin durch, um die Verdächtigen zu identifizieren. Dabei handelt es sich um vier österreichische weibliche und männliche Staatsbürger sowie um drei deutsche männliche Staatsbürger.

Anfang März 2025 schritten Beamtinnen und Beamte des LSE Steiermark nach Anordnung der Staatsanwaltschaft Graz gegen die Beschuldigten ein. Sie führten Hausdurchsuchungen an deren Wohnörtlichkeiten durch, wobei zwei Festnahmen sowie die Sicherstellung von zahlreichen Beweismitteln wie beispielsweise elektronischen Datenträgern erfolgte. Zwei weitere Beschuldigte mit deutscher Staatsangehörigkeit stellten sich zu einem späteren Zeitpunkt freiwillig der Exekutive und konnten daraufhin festgenommen werden.

Nach weiteren Anordnungen der Staatsanwaltschaft Graz nahmen Beamtinnen und Beamte drei weitere Tatverdächtige bei Hausdurchsuchungen an mehreren Örtlichkeiten fest. Durch die im Zuge der Hausdurchsuchungen sichergestellten Gegenstände und Auswertung der elektronischen Datenträger konnten die Verdächtigen eindeutig dem linksextremistischen Milieu zugeordnet werden.

Nach der Durchführung von Haftprüfungen sind mittlerweile alle Beschuldigten dieser Tathandlung auf freiem Fuß. Eine Abschlussberichtslegung seitens des LSE Steiermark an die Staatsanwaltschaft Graz erfolgte im Juni 2025.

2.3.4 Trends und Entwicklungstendenzen

Es ist davon auszugehen, dass sich die Aktivitäten der linksextremen Szene weiterhin primär auf den selbstdefinierten „Kampf gegen den Faschismus“ fokussieren werden. In diesem Zusammenhang ist mit einer Fortsetzung des intensiven Protest- und Veranstaltungsgeschehens zu rechnen, insbesondere im Rahmen von Demonstrationen gegen das politische Gegenüber. Es ist wahrscheinlich, dass es im Zuge linksextremer Mobilisierungen situativ und anlassbezogen auch zu physisch gewaltsamen Auseinandersetzungen kommen kann, insbesondere durch radikalisierte Akteurinnen und Akteure aus dem anarchistischen Spektrum.

Die innerhalb der Szene bestehende ideologische Heterogenität wird weiterhin bestehen bleiben und die Szene in Österreich prägen. Der szeninterne Konflikt im Kontext des Nahostkonflikts – zwischen pro-palästinensischen Positionierungen einerseits und pro-israelischen bzw. Antisemitismus ablehnenden Positionierungen andererseits – dürfte auch im Jahr 2026 fortbestehen und zu weiteren Fragmentierungs- und Polarisierungstendenzen innerhalb der Szene beitragen. Eine nachhaltige Überwindung dieser inneren Zerwürfnisse ist aus derzeitiger Sicht nicht zu erwarten. Ferner kam es im Berichtsjahr zu einer Annäherung zwischen umwelt-/klimaschutz-aktivistischen Gruppen und antimilitaristischen Netzwerken gegen die Rüstungsindustrie. Diese Annäherung könnte in Teilen der Szene auch zu einer erhöhten Aktions- und Risikobereitschaft führen. Auch könnten ungenügend erscheinende Klimaschutzmaßnahmen oder die Umsetzung von als klima- und umweltschädlich wahrgenommenen Verkehrsinfrastrukturprojekten kleinere Teile der linksextremen Szene zur Teilnahme an Blockaden, Besetzungen und Sabotageaktionen mobilisieren.

Strukturell werden die bereits bekannten Herausforderungen der Szene hinsichtlich konstanter Nachwuchsrekrutierung und langfristiger Bindung relevanter Akteurinnen und Akteure weiterhin bestehen bleiben. Der ausgeprägte Netzwerkcharakter, die freiwilligkeitsbasierte Organisationsstruktur sowie divergierende ideologische Schwerpunktsetzungen wirken nach wie vor mobilisierungshemmend. Gleichzeitig können einzelne Themenfelder weiterhin als Anknüpfungspunkte für Rekrutierungs- und Aktivierungspotenziale fungieren. Dazu zählen insbesondere die Solidarität mit gesellschaftlich marginalisierten, geflüchteten sowie als unterdrückt verstandenen Bevölkerungs- und Personengruppen, die Unterstützung separatistischer und insbesondere PKK-naher Gruppierungen sowie die oppositionelle Haltung gegenüber europäischen und nationalen migrations- und sicherheitspolitischen Maßnahmen. Zudem werden Protestformate wie die jährlich stattfindenden Demonstrationen unter dem Titel „Grenzen töten“, „EU tötet“ oder thematisch anlassbezogene Kundgebungen gegen Reformbestrebungen des Gemeinsamen Europäischen Asylsystems (GEAS) voraussichtlich auch im Jahr 2026 relevante Mobilisierungsplattformen für die Szene darstellen.

Mit Blick auf den russischen Angriffskrieg gegen die Ukraine ist weiterhin von einer tendenziell pro-ukrainischen, anti-imperialistisch begründeten Haltung innerhalb weiter Teile der linksextremen Szene in Österreich auszugehen. Russland wird dabei als imperialistischer Aggressor eingestuft, wobei diese Bewertung insbesondere im autonom-anarchistischen Spektrum stark ausgeprägt bleibt. Eine über dieses Solidaritätsmoment hinausgehende spezifische Mobilisierungsdynamik ist jedoch aktuell nicht prognostizierbar.

Insgesamt ist für das Jahr 2026 von einer anhaltenden Aktionsbereitschaft, zugleich aber auch von weiteren Fragmentierungsprozessen innerhalb der linksextremen Szene in Österreich auszugehen. Potenzielle Mobilisierungserfolge dürften daher weiterhin themen- und anlassbezogen bleiben und nur in begrenztem Umfang nachhaltige strukturelle Konsolidierungen bewirken.

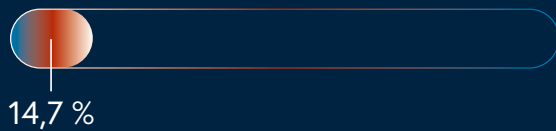


Linksextremismus

Tathandlungen 2025 136

Tathandlungen 2024 214

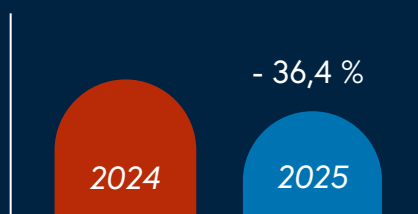
Aufklärungsquote



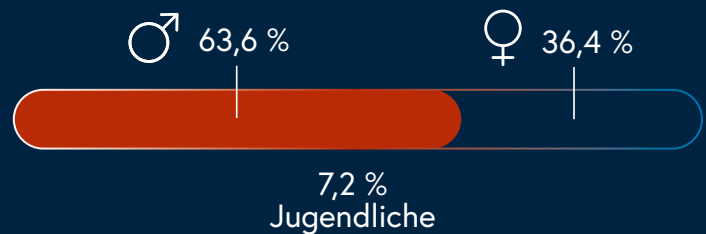
243

Zur Anzeige gebrachte Delikte

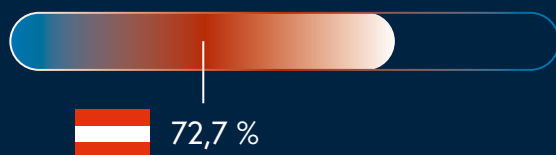
Vergleich zum Vorjahr



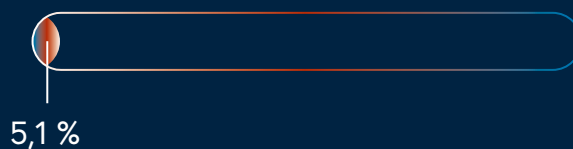
Täterinnen und Täter



Staatsbürgerschaft der Täterinnen und Täter



Internetdelikte



6

Hausdurchsuchungen



24

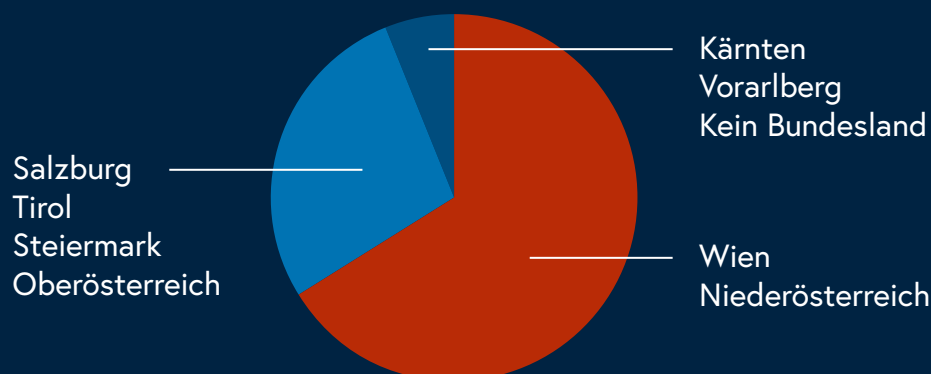
Festnahmen



141

Anzeigen gegen
Unbekannte

Bundesländeraufteilung



2.3.5 Zahlen/Daten/Fakten

Im Jahr 2025 wurden den Sicherheitsbehörden in Österreich insgesamt **136 Tathandlungen** mit erwiesenen oder vermuteten **linksextremen Tatmotiven** bekannt, wobei eine Tathandlung mehrere Delikte mit gesonderten Anzeigen beinhalten kann. Gegenüber dem Jahr 2024 (214 Tathandlungen) bedeutet dies einen zahlenmäßigen **Rückgang um 36,4 Prozent**.⁴² 20 Tathandlungen (**14,7 Prozent**) wurden **aufgeklärt** (Aufklärungsquote 2024: 10,3 Prozent – 22 Tathandlungen).

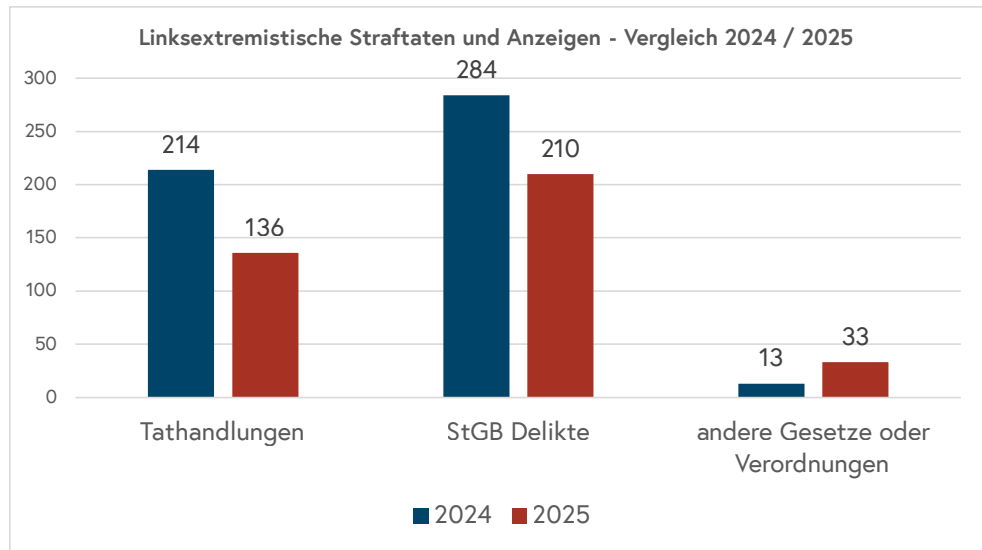
Im Zusammenhang mit den angeführten Tathandlungen wurden 2025 bundesweit insgesamt **243 Delikte** zur Anzeige gebracht, das sind **um 18,2 Prozent weniger** als im Jahr 2024 (297 Delikte). Von den 243 Delikten waren 210 nach dem StGB (2024: 284) sowie 33 Anzeigen nach anderen Gesetzen und Verordnungen (2024: 13).

Im Zuge der Aufklärung linksextremer Straftaten wurden im Jahr 2025 insgesamt **55 Personen** angezeigt (2024: 52), davon 35 Personen männlichen (63,6 Prozent) und 20 Personen weiblichen Geschlechts (36,4 Prozent). Im Jahr 2024 gelangten 39 männliche und 13 weibliche Personen zur Anzeige. Unter den Beschuldigten befanden sich vier Jugendliche (2025: 7,2 Prozent; 2024: 11 bzw. 21,2 Prozent). 40 der Beschuldigten (72,7 Prozent) besitzen die österreichische Staatsbürgerschaft (2024: 41, das entspricht 78,8 Prozent). Neben den ausgeforschten Personen erfolgten im Berichtsjahr **141 Anzeigen** gegen **unbekannte Täterinnen oder Täter** (2024: 212).

Unter den insgesamt 136 bekannt gewordenen und zur Anzeige gelangten Tathandlungen im Jahr 2025 befanden sich **sieben Tathandlungen** (5,1 Prozent), bei denen die gesetzeswidrige Agitation im **Internet** stattfand. Im Jahr 2024 wurde von den 214 Tathandlungen eine im Internet registriert (0,5 Prozent).

Im Zusammenhang mit der Bekämpfung linksextremer Aktivitäten wurden im Jahr 2025 in Österreich **sechs Hausdurchsuchungen** (2024: 1) durchgeführt sowie **24 Festnahmen** (2024: 6) vollzogen. Im Zuge dieser Hausdurchsuchungen wurde mehrere Datenträger, Laptops und Mobiltelefone sichergestellt.

⁴² Der Rückgang begründet sich vor allem mit der hohen Zahl registrierter Tathandlungen im Jahr 2024 im Zusammenhang mit den Nationalrats- und EU-Parlamentswahlen (z. B. Schmieraktionen, Beschädigung von Wahlplakaten etc.).



Zu einem **Anstieg** kam es unter anderem bei den Anzeigen wegen Körperverletzung gemäß § 83 StGB (3 auf 6), wegen Gefährdung der körperlichen Sicherheit gemäß § 89 StGB (0 auf 2), wegen Gefährlicher Drohung gemäß § 107 StGB (2 auf 6), wegen Schwerer Sachbeschädigung gemäß § 126 StGB (15 auf 33), dem Delikt des Schweren Raubes gemäß § 143 StGB (0 auf 7), wegen Urkundenfälschung gemäß § 223 StGB (0 auf 6), wegen Krimineller Vereinigung gemäß § 278 StGB (0 auf 2), dem Delikt der Terroristischen Vereinigung gemäß § 278b StGB (0 auf 2), wegen Aufforderung zu mit Strafe bedrohten Handlungen und Gutheißung mit Strafe bedrohter Handlungen gemäß § 282 StGB (1 auf 3) sowie dem Delikt der Aufforderung zu terroristischen Straftaten und Gutheißung mit Strafe bedrohter Handlungen gemäß § 282a StGB (0 auf 2), wegen Verhetzung gemäß § 283 StGB (0 auf 12), dem Versammlungsgesetz (3 auf 12) und dem Sicherheitspolizeigesetz (0 auf 19).

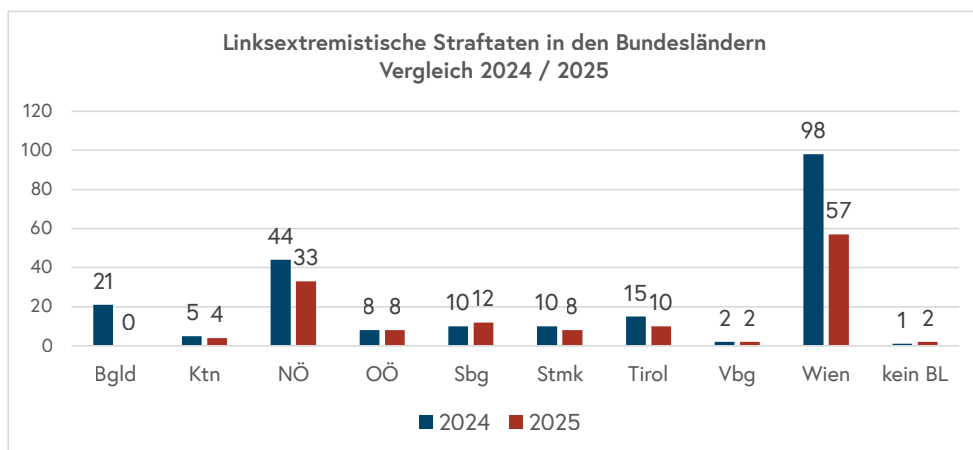
Zu einem **Rückgang** kam es bei den Anzeigen wegen Schwerer Körperverletzung gemäß § 84 StGB (11 auf 5), wegen Sachbeschädigung gemäß § 125 StGB (220 auf 113) und wegen des Widerstandes gegen die Staatsgewalt gemäß § 269 StGB (8 auf 2).

Anzeigen nach dem StGB	2024	2025
Körperverletzung (§ 83 StGB)	3	6
Schwere Körperverletzung (§ 84 StGB)	11	5
Gefährdung der körperlichen Sicherheit (§ 89 StGB)	0	2
Gefährliche Drohung (§ 107 StGB)	2	6
Beleidigung (§ 115 StGB)	0	1
Sachbeschädigung (§ 125 StGB)	220	113
Schwere Sachbeschädigung (§ 126 StGB)	15	33

Diebstahl (§ 127 StGB)	7	3
Schwerer Diebstahl (§ 128 StGB)	0	1
Diebstahl durch Einbruch oder mit Waffen (§ 129 StGB)	3	1
Eingriff in fremdes Jagd- oder Fischereirecht (§ 137 StGB)	0	3
Schwerer Raub (§ 143 StGB)	0	7
Urkundenfälschung (§ 223 StGB)	0	6
Widerstand gegen die Staatsgewalt (§ 269 StGB)	8	2
Kriminelle Vereinigung (§ 278 StGB)	0	2
Terroristische Vereinigung (§ 278b StGB)	0	2
Aufforderung zu mit Strafe bedrohten Handlungen und Gutheißung mit Strafe bedrohter Handlungen (§ 282 StGB)	1	3
Aufforderung zu terroristischen Straftaten und Gutheißung mit Strafe bedrohter Handlungen (§ 282a StGB)	0	2
Verhetzung (§ 283 StGB)	0	12
Sonstige StGB-Delikte	14	0

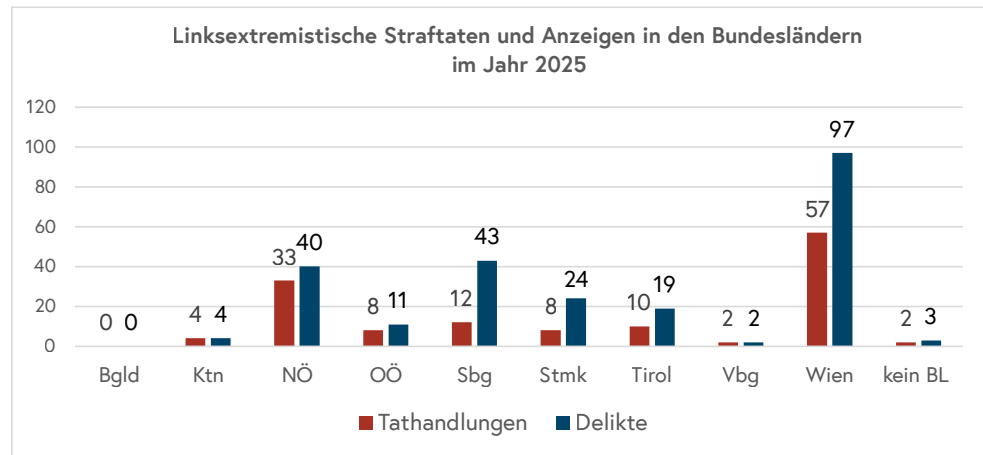
Anzeigen nach anderen Gesetzen oder Verordnungen

Versammlungsgesetz (VersG)	3	12
Sicherheitspolizeigesetz (SPG)	0	19
Straßenverkehrsordnung (StVO)	0	1
Verbotsgesetz (VbtG)	10	1
Summe	297	243



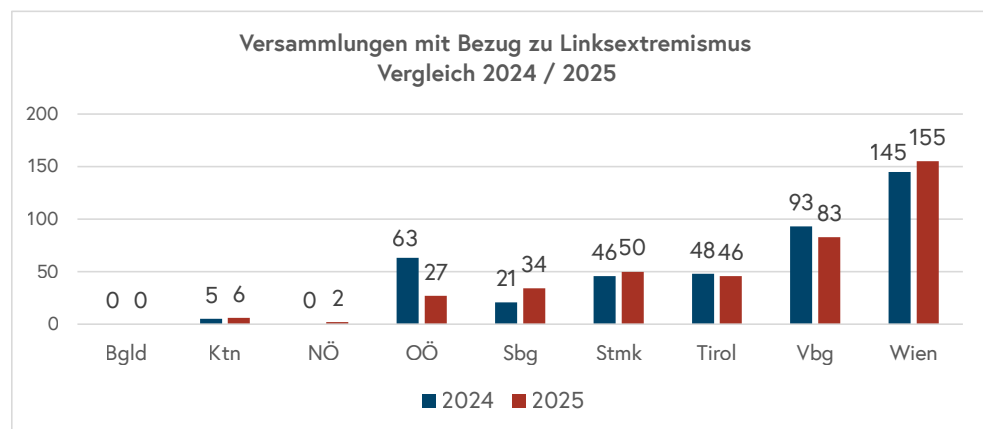
In Zusammenhang mit dem **Nahostkonflikt** wurden im Phänomenbereich Linksextremismus bundesweit **sechs Tathandlungen** (2024: 4) registriert. Es erfolgten Anzeigen wegen Sachbeschädigungsdelikten gemäß den §§ 125 und 126 StGB, wegen des Widerstandes gegen die Staatsgewalt gemäß § 269 StGB, wegen Krimineller Vereinigung gemäß § 278

StGB, wegen Terroristischer Vereinigung gemäß § 278b StGB, dem Delikt der Aufforderung zu mit Strafe bedrohten Handlungen und Gutheißung mit Strafe bedrohter Handlungen gemäß § 282 StGB, wegen Verhetzung gemäß § 283 StGB und dem Versammlungsgesetz.



Im Berichtsjahr 2025 wurden insgesamt **403 Versammlungen** (2024: 421) mit Bezug zu Linksextremismus registriert. Davon wurden 371 angemeldet, 27 nicht angemeldet und fünf aufgelöst. Die Themenfelder gliederten sich in Antifaschismus (149), Antiimperialismus (39), Regierung (35), Antikapitalismus (18), Soziales (12), Klima (10) Asylwesen (8), Bildung (1), COVID-19-Pandemie (1) und sonstige Themen (130).

Die meisten Versammlungen mit Bezug zum Linksextremismus, insgesamt 155, fanden in Wien statt (38,5 Prozent), gefolgt von Vorarlberg mit 83 (20,6 Prozent), Steiermark mit 50 (12,4 Prozent), Tirol mit 46 (11,4 Prozent), Salzburg mit 34 (8,4 Prozent), Oberösterreich mit 27 (6,7 Prozent), Kärnten mit 6 (1,5 Prozent) und Niederösterreich mit 2 (0,5 Prozent). Im Bundesland Burgenland wurden keine Versammlungen mit linksextremem Bezug registriert.

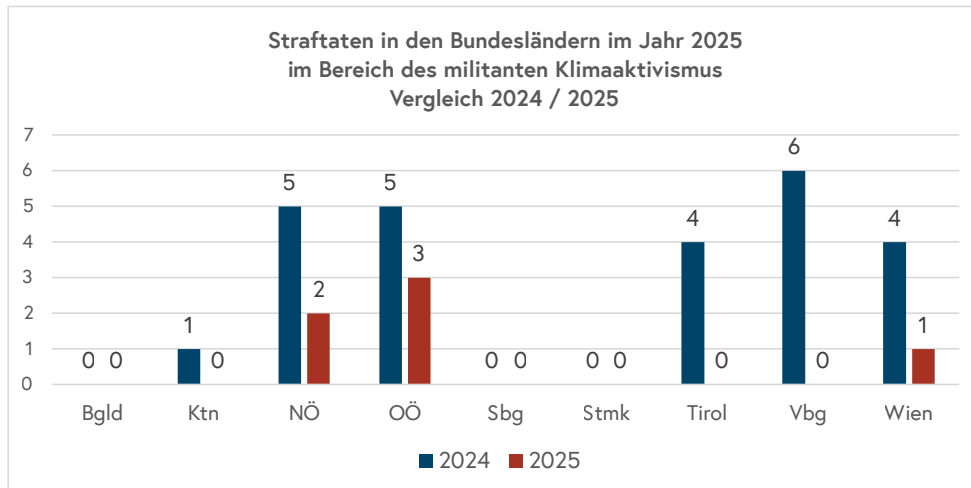


Militanter Klimaaktivismus

Im Jahr 2025 wurden den Sicherheitsbehörden in Österreich im Bereich des militanten Klimaaktivismus insgesamt sechs Tathandlungen bekannt (2024: 25). Zwei der sechs Tathandlungen (33,1 Prozent) wurden aufgeklärt (2024: 17, 68 Prozent). Im Zusammenhang mit den angeführten Tathandlungen wurden insgesamt 14 Delikte zur Anzeige gebracht (2024: 116). Von diesen Delikten waren drei nach dem Strafgesetzbuch (StGB) sowie elf Anzeigen nach anderen Gesetzen und Verordnungen.

Insgesamt konnten vier Tatverdächtige ausgeforscht und zur Anzeige gebracht werden (2024: 77, 42 männliche und 35 weibliche). Neben den ausgeforschten Personen erfolgten im Berichtsjahr fünf Anzeigen gegen unbekannte Täterinnen oder Täter (2024: 10).

Im Zusammenhang mit den genannten Tathandlungen wurden drei Personen festgenommen (2024: 7).

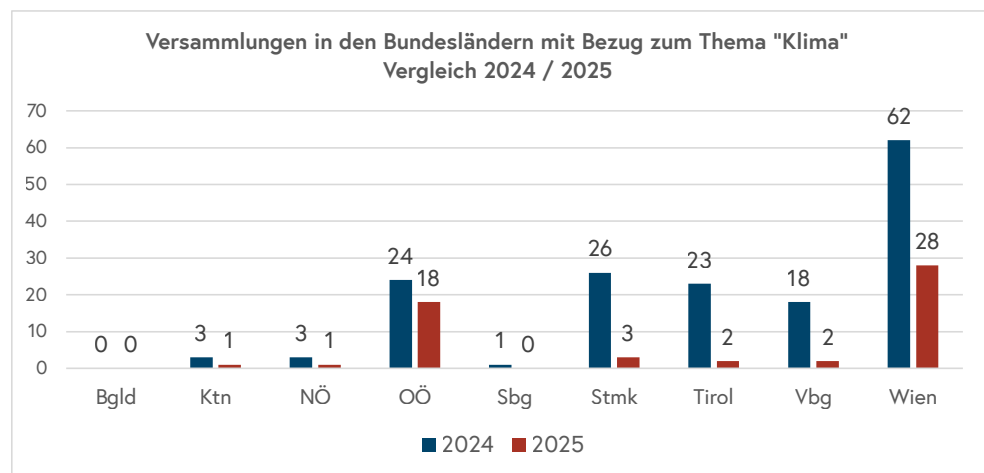


Anzeigen nach dem StGB	2024	2025
Sachbeschädigung (§ 125 StGB)	17	2
Schwere Sachbeschädigung (§ 126 StGB)	2	0
Diebstahl durch Einbruch oder mit Waffen (§ 129 StGB)	0	1

Anzeigen nach anderen Gesetzen oder Verordnungen	2024	2025
Versammlungsgesetz (VersG)	46	5
Sicherheitspolizeigesetz (SPG)	31	4
Straßenverkehrsordnung (StVO)	20	2
Summe	116	14

Im Berichtsjahr 2025 wurden insgesamt 55 Versammlungen mit Bezug zum Thema Klima registriert (2024: 160). Davon waren 48 angemeldet und sieben nicht angemeldet.

Die meisten Versammlungen mit Bezug zum Thema Klima fanden in Wien mit 28 (50,9 Prozent) statt, gefolgt von Oberösterreich mit 18 (32,7 Prozent), der Steiermark mit drei (5,5 Prozent), Tirol und Vorarlberg mit jeweils zwei (jeweils 3,65 Prozent) sowie Niederösterreich und Kärnten mit jeweils einer (jeweils 1,8 Prozent). Im Burgenland und in Salzburg wurden keine Versammlungen mit Bezug zum Thema Klima registriert.



2.4 Auslandsbezogener Extremismus

Der Begriff „**Auslandsbezogener Extremismus**“ beschreibt Formen des Extremismus, bei denen die ideologischen Zielsetzungen, Aktivitäten und Konflikte auf Ereignisse, politische Verhältnisse oder Machtkämpfe primär in anderen Staaten oder Regionen der Welt ausgerichtet sind. Organisationen im Bereich des auslandsbezogenen Extremismus vereinen oft ideologische Elemente aus dem Rechts- oder Linksextremismus oder verfolgen separatistische Ziele in ihren Herkunfts- bzw. Bezugsländern. Die politische Lage in den jeweiligen Herkunftsregionen und die Vorgaben zentraler Organisationseinheiten/Mutterorganisationen vor Ort beeinflussen maßgeblich die Strategien, Aktivitäten und Ausrichtung dieser Strukturen in Europa und somit auch in Österreich. Häufig streben sie in ihren Herkunfts- bzw. Bezugsländern tiefgreifende politische Veränderungen an, wobei sie auch Gewalt und Terror als Mittel einsetzen.

In der Bearbeitung sowie in der Beschreibung in diesem Bericht wird der islamistische Extremismus als eigenständiger Phänomenbereich behandelt.

2.4.1 Überblick

Gruppierungen, die dem sogenannten auslandsbezogenen Extremismus zugeordnet werden, sind zumeist aus den politischen, ethnischen und/oder sozialen Konflikten ihrer Herkunftsländer hervorgegangen. Sie benutzen ihre europäischen Aufenthaltsländer, darunter auch Österreich, als „sicheren“ Rückzugsraum, um von hier aus ihre extremistischen oder terroristischen Bestrebungen zur Unterstützung der entsprechenden Gruppierungen in ihren Herkunfts- bzw. Bezugsgebieten zu planen, zu propagieren und zu finanzieren. Diese Gruppen bemühen sich zumeist um ein gewaltfreies, gesetzeskonformes Erscheinungsbild, dennoch wird Gewalt gemäß ihrer ideologischen Überzeugung als legitimes Mittel zur Durchsetzung ihrer Ziele angesehen. Zudem besteht die Gefahr, dass die aus den jeweiligen Herkunftsländern übernommenen Konflikte auch hierzulande zu Gewalt zwischen den Anhängerinnen und Anhängern dieser Gruppen führen. Folglich stellen diese Gruppen eine potenzielle Bedrohung für die gesellschaftliche Stabilität und die innere Sicherheit dar.

In Österreich steht im Bereich des auslandsbezogenen Extremismus insbesondere jener mit Bezug zur Türkei im Fokus des Verfassungsschutzes. Die drei Hauptströmungen sind die Arbeiterpartei Kurdistans (PKK), die Revolutionäre Volksbefreiungspartei/Front (DHKP/C) und die Ülkücü-Bewegung (Graue Wölfe). Diese Gruppierungen haben sowohl unterschiedliche ideologische Ausrichtungen als auch unterschiedliche Interessen in ihren Herkunftsländern. Die PKK und die DHKP/C stehen für linksextremistisch orientierte, teils separatistische Bestrebungen, während die Ülkücü-Bewegung rechtsextremistisch-nationalistische Ziele verfolgt. Kooperationen zwischen ihnen sind daher nicht bzw. im Falle von DHKP/C und PKK nur anlassbezogen, teilweise auch mit österreichischen linken bzw. linksextremen Gruppierungen zu beobachten. Die Ülkücü-Bewegung hingegen steht in ihrer rechtsextremen Ausrichtung in klarer Opposition bzw. feindlich zu diesen Gruppen. Nach dem Symbole-Gesetz ist die Verwendung der Symbole aller drei Gruppierungen – der Ülkücü-Bewegung (§ 1 Abs. 4 SymboleG), der PKK (§ 1 Abs. 5 SymboleG) und der DHKP/C (§ 1 Abs. 14 SymboleG) – in Österreich verboten.

Die wichtigsten Entwicklungen im Bereich des auslandsbezogenen Extremismus im Berichtsjahr waren die formelle Auflösung der PKK und die damit einhergehenden, in ihrer Gänze noch nicht absehbaren Implikationen für Österreich.

2.4.2 Aktuelle Lage

Im Jahr 2025 war die Situation im Bereich des auslandsbezogenen Extremismus in Österreich weitgehend gleichbleibend. Hinsichtlich der Aktivitäten fanden erneut Protestaktionen sowie Solidaritäts- und Sympathiebekundungen von in Österreich ansässigen

Sympathisantinnen und Sympathisanten der Arbeiterpartei Kurdistans als auch der Revolutionären Volksbefreiungspartei/Front statt. Beide Gruppierungen unterstützten mit ihren Aktionen in Österreich die jeweils mit ihnen assoziierten Milizen bzw. „Kämpfer“ in ihren Bezugsländern. Ferner wurden im separatistischen und linksextremistischen Spektrum wiederholt sogenannte „Martyrerveranstaltungen“ abgehalten, die einen integralen Bestandteil der Rekrutierungs-, Indoktrinierungs- und Ideologisierungstrategien dieser Gruppierungen darstellen. Gleichwohl verliefen diese Kundgebungen und Veranstaltungen überwiegend friedlich und ohne sicherheitsrelevante Zwischenfälle. Dennoch bleiben sicherheitsbehördliche Schutz- und Präventivmaßnahmen weiterhin notwendig, um mögliche gegenseitige Provokationen und daraus folgende Gewalteskalationen zwischen verfeindeten Gruppierungen zu verhindern. In diesem Kontext ist zu berücksichtigen, dass die Ülkücü-Bewegung gegenüber den erstgenannten Gruppierungen eine gegnerische bzw. antagonistische Haltung einnimmt.

Eine zentrale Entwicklung im Berichtszeitraum betrifft die PKK, deren Führung beschlossen hat, die bewaffneten Strukturen aufzulösen und den bewaffneten Kampf gegen die Türkei bzw. deren Regierung zu beenden. Der mögliche Beginn eines Friedensprozesses stellt eine neue Ausgangslage und wichtige Zäsur dar, die langfristige Auswirkungen auf die Stabilität in der Region haben könnte. Hinsichtlich der PKK-Strukturen in Europa und Österreich wird jedenfalls erwartet, dass sowohl eine positive als auch eine negative Entwicklung dieses Friedensprozesses einschneidende Auswirkungen haben wird.

In diesem Zusammenhang spielt auch die Lageentwicklung in Syrien, die durch tiefgreifende politische Transformationsprozesse sowie anhaltende militärische Spannungen gekennzeichnet ist, eine wichtige Rolle. Von besonderer Bedeutung sind dabei die Dynamiken zwischen der Türkei und den in (Nord-)Syrien operierenden PKK-nahen Gruppierungen, die seitens der Türkei als terroristische Organisationen eingestuft werden. Die Türkei verfolgt das strategische Ziel, den politischen und militärischen Einfluss dieser Gruppen in der Region durch direkte und indirekte Unterstützung der neuen syrischen Regierung nachhaltig zu verringern bzw. aufzulösen. Die von kurdischen Akteurinnen und Akteuren kontrollierten Gebiete im Norden Syriens stehen daher unter erheblichem politischen und militärischen Druck. Aktuelle Entwicklungen, darunter die Verhandlungen über eine mögliche Eingliederung der Syrischen Demokratischen Kräfte (SDF) in die offiziellen syrischen Streitkräfte scheinen fortgeschritten, aber noch nicht abgeschlossen zu sein. Ein Scheitern dieser Entwicklung/Integration und ein möglicher bewaffneter Konflikt könnten zum einen die fragile Stabilität in der gesamten Region negativ beeinflussen und zum anderen den begonnenen Friedensprozess zwischen der Türkei und der PKK konterkarieren.

Oggleich die im Phänomenbereich des auslandsbezogenen Extremismus agierenden Organisationen grundsätzlich von der Anwendung von Gewalt absehen, bleibt die fortlaufende Beobachtung ihrer Aktivitäten, insbesondere auch hinsichtlich einer möglichen

Gutheiung von Terrorismus und Terrorismusfinanzierung, von zentraler Bedeutung. Sie ist wesentlich fr die Gewhrleistung der inneren Sicherheit sowie fr die prventive Bewertung potenzieller, verfassungsrelevanter Bedrohungslagen im sterreichischen Kontext.

Arbeiterpartei Kurdistans

Im Jahr 2025 trat die PKK, die seit 2002 auf der EU-Terrorliste steht, sowohl im europischen als auch im sterreichischen Kontext nicht durch offene Gewalthandlungen hervor, sondern agierte primr ber politische, kulturelle und zivilgesellschaftliche (Diaspora-) Strukturen. Diese Netzwerke dienen der Finanzierung, Propaganda und Mobilisierung, wobei vor allem Vereine als Tarnstrukturen eine wichtige Rolle spielen. Das Ziel der PKK-nahen Gruppierungen bleibt – auch nach der formellen Auflsung – die politische Rehabilitation, insbesondere die Aufhebung des Bettigungsverbots in Deutschland und schlielich die Streichung von der EU-Terrorliste. ffentlich positionieren sich die Organisationen nicht als Untersttzer einer terroristischen Bewegung, sondern als Vertreter einer kurdischen Befreiungsorganisation, die als legitimer Reprsentant der gesamten kurdischen Bevlkerung in der Trkei, im Irak, Iran und Syrien auftritt.

PKK-Auflsung

Die formelle Auflsung und die Beendigung des bewaffneten Kampfes der PKK bildete die magebliche Entwicklung im Berichtsjahr. Der erneute Friedensprozess⁴³ begann im Oktober 2024 mit einem Aufruf des Vorsitzenden der Partei der Nationalistischen Bewegung (MHP), Devlet Baheli. Die PKK-Fhrung folgte dem Aufruf calans zur Auflsung vom 27. Februar 2025 und verkndete diese am 12. Mai 2025 sowie die Beendigung des bewaffneten Kampfes. Begrndet wurde dieser Schritt unter anderem damit, dass die *„Politik der Verleugnung und Vernichtung, die unserem Volk [dem kurdischen Volk] aufgezwungen wurde, zunichtegemacht und die kurdische Frage an einen Punkt gebracht [wurde], an dem sie durch demokratische Politik gelst werden kann. [...] [D]ie PKK [hat] ihre historische Mission erfllt [...]“*⁴⁴ Weiters wurde angefhrt, dass die Entscheidung zur Auflsung und die Beendigung des bewaffneten Kampfes die Grundlage fr einen dauerhaften Frieden und eine demokratische Lsung bieten soll. Zur Umsetzung sei es jedoch notwendig, dass „Fhrer Apo“ (Abdullah calan) den Prozess fhrt und leitet, sein *„Recht zur demokratischen Politik“* anerkannt wird und umfassende, rechtliche Garantien geschaffen werden.

43 Die Friedensverhandlungen zwischen der Trkei und der PKK weisen eine Historie mit mehreren Phasen und Versuchen auf, die von Dialog, zwischenzeitlichen Waffenruhen und Eskalationen geprgt sind. Frhere Versuche gab es bereits in den 1990er-Jahren, fanden jedoch mit der Inhaftierung calans 1999 ein jhes Ende. Die ergebnislosen Oslo-Gesprche fanden zwischen 2008-2011 statt. Auch die Verhandlungen zwischen 2012-2015 fhrten zu keinem Ende des bewaffneten Konfliktes.

44 Auszug aus der Abschlusserklrung des 12. Kongresses der PKK vom 12. Mai 2025; online unter: <https://deutsch.anf-news.com/kurdistan/pkk-verkundet-auflösung-und-ende-des-bewaffneten-kampfes-46252> (Abruf am 24.11.2025).

Am 11. Juli 2025 legten die ersten PKK-„Kämpferinnen und -Kämpfer“ in der nordirakischen Stadt Sulaimaniyya öffentlichkeitswirksam ihre Waffen nieder. Die noch offenen Fragestellungen, wie etwa die Fortsetzung der Waffenniederlegung, der Abzug von PKK-„Kämpferinnen und -Kämpfern“ aus der Türkei, das weitere Vorgehen der PKK-Teilorganisationen sowie juristische Regelungen (insbesondere Haftentlassungen und eventuelle Amnestien) sollen von der am 5. August 2025 eingerichteten parlamentarischen Kommission für nationale Solidarität, Geschwisterlichkeit und Demokratie ausgearbeitet werden. Um einen erfolgreichen Abschluss des Friedensprozesses mit nachhaltiger Wirkung erreichen zu können, soll zudem ein gesamtgesellschaftlicher Ansatz angewendet werden.

Für die PKK-nahen Strukturen in Österreich kann festgehalten werden, dass seit Beginn des Friedensprozesses eine zurückhaltende, jedoch optimistische Haltung erkennbar ist. Obgleich im Jahr 2025 keine eindeutigen Erklärungen oder Stellungnahmen hinsichtlich einer eventuellen Auflösung der PKK-Strukturen in Europa wahrzunehmen waren, wird die Bereitschaft zum Frieden auch hier bekräftigt. Die Hauptverantwortung für einen erfolgreichen Abschluss des Friedensprozesses wird der türkischen Regierung zugewiesen. In einer Online-Meldung betonte der Rat der kurdischen Gesellschaft in Österreich (FEYKOM), dass ohne einen Frieden in Kurdistan weder im Nahen Osten noch weltweit ein dauerhafter Frieden erreicht werden könne.

Dies verdeutlicht auch, dass sich der Friedensprozess komplex gestaltet, sehr fragil ist und mögliche Abweichungen von Vereinbarungen eine Weiterführung des Konfliktes bedeuten könnten. Bemerkenswert an diesen Aussagen ist zudem, dass alle Kurdinnen und Kurden von der PKK fremdidentifiziert⁴⁵ werden. Damit wird das vorherrschende Narrativ verstärkt, wonach die PKK die alleinige Vertreterin aller Kurdinnen und Kurden ist.

Vernetzungen

Im Jahr 2025 war in Österreich ein bundesweit dichtes Netzwerk von Vereinen mit Nähe zu PKK-Strukturen registrierbar. Diese Organisationen treten a priori unter dem Etikett bzw. Label „Kulturverein“ auf und verfolgen das strategische Ziel, in unterschiedlichen Lebensbereichen (Kultur, Sport, Religion, Hilfsorganisationen) möglichst umfassende Vereinskonstruktionen zu etablieren. Zur Umsetzung dieser Strategie wird zum einen versucht, die vorhandenen Strukturen aufrechtzuerhalten; zum anderen wird die Gründung weiterer Vereine aktiv vorangetrieben. 2025 lag in der Umsetzung dieser Strategie ein Schwerpunkt auf dem Westen Österreichs, wo sich Vereinsstrukturen etablierten und somit eine günstige Ausgangslage für (grenzüberschreitende) Vernetzungen und Kooperationen geschaffen werden konnte. Besonders relevant waren dabei die geografische Verankerung und bundesweite Einbindung in die bereits vorhandenen PKK-nahen Strukturen. Hierbei waren eine koordinierte Zusammenarbeit und gegenseitige Unterstützung zwischen den in den einzelnen Bundesländern tätigen Vereinen deutlich erkennbar.

45 Die PKK impliziert, dass sich alle Kurdinnen und Kurden mit ihr als einziger Partei identifizieren.

Analog zu den vorangegangenen Jahren lagen die Aktivitäten der PKK-nahen Strukturen in Österreich auch im Berichtsjahr vor allem in der ideologischen Festigung der Mitglieder und in der finanziellen Unterstützung der Gesamtorganisation. Signifikant gestiegen sind zudem Lobbytätigkeiten, während gleichzeitig das Naheverhältnis zu politischen Parteien sowie Politikerinnen und Politikern ausgebaut wurde, um (symbolische) Unterstützung für die PKK-Agenden zu bekommen. Zugleich rückte das Thema des Friedensprozesses bzw. die Auflösung der PKK und ihre Auswirkungen auf die europäischen und hiesigen Strukturen sowie die seit Jahren forcierte Forderung nach Freilassung Öcalans stärker in den Fokus öffentlicher, vereinsinterner und konspirativer Debatten. In diesem Zusammenhang wurde weiterhin die türkische Sicherheitspolitik adressiert – insbesondere hinsichtlich der überwiegend kurdisch besiedelten autonomen Regionen in Nordsyrien („Rojava“). Dieser Themenschwerpunkt wurde auch seitens syrisch-kurdischer PKK-naher Jugendgruppierungen in den sozialen Medien und bei diversen Kundgebungen diskutiert.

Ähnlich wie in den letzten Jahren wurden auch 2025 Versammlungen abgehalten, die oftmals in Kooperation mit Gruppierungen aus dem österreichischen linken bis linksextremen Spektrum stattfanden. Zudem ist eine Solidarisierungsdynamik zwischen links-extremistischen Gruppierungen ohne Türkei-Bezug und PKK-nahen Jugendgruppierungen feststellbar. Hierbei wurden in der zweiten Jahreshälfte 2025 auch Themenkomplexe wie der Nahostkonflikt öffentlichkeitswirksam behandelt.

Ein großangelegtes Vernetzungstreffen fand im Februar 2025 in Wien statt. Zu den Mitorganisatoren gehörte auch die in Wien ansässige Dachorganisation FEYKOM. Nach eigenen Angaben der Organisatoren nahmen an der dreitägigen Veranstaltung rund 800 Delegierte teil, die mehr als 160 Organisationen aus 35 Ländern repräsentierten. Die Teilnehmerinnen und Teilnehmer setzten sich aus Personen aus dem linken bis linksextremen sowie aus dem PKK-nahen Spektrum zusammen. Hauptthemengebiete der Veranstaltung waren Faschismus, Imperialismus, Widerstand und Autonomiebestrebungen. Ein deutlicher PKK-Bezug konnte aufgrund der verwendeten visuellen Materialien sowie der zahlreichen Verweise der Rednerinnen und Redner auf die politischen Theorien Öcalans, insbesondere seinen demokratischen Konföderalismus⁴⁶, festgestellt werden.

Ideologisierung

Die PKK bemühte sich im Berichtszeitraum, durch gezielte öffentlichkeitswirksame Propagandamaßnahmen – darunter Großveranstaltungen – sowohl gesellschaftliche Aufmerksamkeit als auch Solidarität für ihre politischen Anliegen zu erringen. Ein zentrales

46 Der „demokratische Konföderalismus“ ist eine von Abdullah Öcalan entwickelte Theorie, die auf den Elementen Basisdemokratie, Geschlechterbefreiung und Ökologie basiert und hierarchische Strukturen im Sinne eines Nationalstaates ablehnt. Lokale Selbstverwaltung, Kommunen und Versammlungen Gleichberechtigter bilden den Kern dieser Theorie.

Ziel dieser Aktivitäten bestand in der fortlaufenden Ideologisierung und Indoktrinierung ihrer Sympathisantinnen und Sympathisanten.

Wie schon in den Vorjahren fanden auch im Jahr 2025 in mehreren österreichischen Städten die traditionellen kurdischen Neujahrsfeierlichkeiten, die sogenannten Newroz-Feste, statt. Die größte dieser Veranstaltungen wurde im März 2025 in Wien abgehalten und erzielte mit rund 3.000 Teilnehmerinnen und Teilnehmern einen vergleichbaren Andrang wie im Jahr 2024. Inhaltlich stand die Veranstaltung unter dem Eindruck der laufenden Friedensverhandlungen zwischen der PKK und der Türkei. In den Redebeiträgen zeigte sich zwar eine grundsätzlich vorsichtig-positive Haltung gegenüber dem Friedensprozess, zugleich wurde jedoch die Hauptverantwortung für dessen erfolgreiche Umsetzung überwiegend der türkischen Regierung zugeschrieben. Charakteristisch für die meisten Ansprachen war ein einleitendes Gedenken an die im bewaffneten Kampf gefallenen „Kämpferinnen und Kämpfer“, die von den Rednerinnen und Rednern als „Märtyrer“ bezeichnet wurden.

Bei den Newroz-Festen ließ sich deutlich deren politische Instrumentalisierung im Sinne der PKK-Propaganda beobachten. Dies zeigte sich vor allem in den Redebeiträgen, den an den Veranstaltungsorten angebrachten visuellen Materialien – darunter Transparente mit dem Abbild Abdullah Öcalans, Fahnen PKK-naher Organisationen sowie Darstellungen von PKK-„Kämpferinnen und -Kämpfern“ – sowie in der aktiven Teilnahme bekannter Anhängerinnen und Anhänger der PKK. Zudem konnte festgestellt werden, dass die Veranstaltungen als Plattformen zur Netzwerkbildung genutzt wurden. Für Gruppierungen mit ideologisch verwandten, jedoch unterschiedlich ausgerichteten Positionen boten die Feste ideale Gelegenheiten zum Austausch und zur gegenseitigen Vernetzung.

Im Berichtszeitraum nutzten PKK-nahe Organisationen sowohl die politischen und militärischen Geschehnisse in Nordsyrien als auch den Nahostkonflikt, um ihre Aktivitäten auf österreichischer und europäischer Ebene fortzuführen. Vor allem die PKK-nahen Jugendorganisationen betrieben eine intensive Nutzung sozialer Medien, um zu pro-palästinensischen Demonstrationen aufzurufen und entsprechende Narrative zu verbreiten. Dabei erfolgte häufig die ideologische Gleichsetzung des sogenannten „Kurdischen Freiheitskampfes“ mit dem „Palästinensischen Freiheitskampf“, wodurch beide Konflikte rhetorisch und propagandistisch miteinander verknüpft und zur Stärkung eigener politischer Positionen instrumentalisiert wurden.

Obgleich die Zahl der Demonstrationen aufgrund des Friedensprozesses zwischen der PKK und der Türkei rückläufig war, wurde beobachtet, dass thematische Schwerpunktsetzungen – insbesondere auf den Nahostkonflikt – vorgenommen wurden. Zudem wurde eine verstärkte Kooperation zwischen PKK-nahen Strukturen und österreichischen sowie europäischen linken bzw. linksextremen Gruppierungen deutlich. Diese Zusammenarbeit, die in den vorangegangenen Jahren primär anlassbezogen war und zusehends zum Usus

wird, intensivierte und manifestierte sich sowohl in gemeinsamen Mobilisierungsstrategien als auch in einer zunehmenden ideologischen Annäherung.

Revolutionäre Volksbefreiungspartei/Front

In Österreich lässt sich gegenwärtig keine gefestigte Vereinsstruktur der marxistisch-leninistischen DHKP/C identifizieren. Stattdessen existieren in den einzelnen Bundesländern Vereine, die ideologisch und aktionistisch mit der DHKP/C sympathisieren. Die Mitgliederzahlen dieser der DHKP/C nahestehenden Organisationen und Gruppierungen fallen im Vergleich zur PKK deutlich kleiner aus. Dies manifestiert sich insbesondere in der niedrigeren Frequenz sowie dem geringeren Umfang von Veranstaltungen und Demonstrationen, die von DHKP/C-nahen Akteurinnen und Akteuren besucht und organisiert werden. Dennoch weist das Sympathisantenumfeld der Organisation einen nicht zu vernachlässigenden Grad an Mobilisierungsfähigkeit und hoher ideologischer Indoktrinierung auf und ist in ein europaweites Netzwerk eingebettet. Die DHKP/C befindet sich ebenfalls auf der EU-Terrorliste. Ein zentrales Ziel der Organisation besteht in der Rekrutierung neuer, überwiegend jugendlicher Mitglieder.

Vernetzungen und Rekrutierung

Die DHKP/C agiert in Europa mit einer starken, ideologischen Motivation und einer hohen Bereitschaft, ihre Ziele mittels einer langfristigen und diszipliniert verfolgten Strategie umzusetzen. Sie versteht sich als marxistisch-leninistische Widerstandsbewegung, die gegen Kapitalismus und Imperialismus, vor allem aber gegen die türkische Regierung kämpft. Ihre Motivation speist sich aus einer tief verwurzelten revolutionären Überzeugung, wonach der Kampf für eine sozialistische Gesellschaft durch bewaffneten Widerstand erreicht werden kann. In diesem Kontext nimmt die Rekrutierung neuer Anhängerinnen und Anhänger einen besonderen Stellenwert ein. Daher versuchen DHKP/C-nahe Organisationen, durch engmaschige persönliche Sozialisation und Bindungen, insbesondere unter Jugendlichen, neue Sympathisantinnen und Sympathisanten, vor allem in urbanen Milieus, zu rekrutieren. Diesbezüglich organisierten die DHKP/C und ihre Jugendorganisationen im Sommer 2025 ein „Sommercamp“ in Südfrankreich, bei dem auch bekannte Personen aus dem DHKP/C-Umfeld in Österreich teilnahmen. Das Ziel dieser meist mehrtätigen Veranstaltungen ist – neben der Rekrutierung – vor allem die Indoktrinierung bzw. die ideologische Bindung der Jugendlichen.

Weiters konnte im Berichtszeitraum beobachtet werden, dass DHKP/C-nahe Strukturen in Österreich versuchten, ihren ideologischen Radius zu vergrößern. Dazu wurden unter dem Deckmantel von Kulturveranstaltungen Auftritte in Vereinen – zum Teil mit religiösem Bezug – organisiert und konfessionelle bzw. religiöse Überzeugungen derart instrumentalisiert, dass sie mit dem ideologischen Widerstand der DHKP/C gleichgesetzt werden konnten. Darüber hinaus wurden diese Veranstaltungen auch als Vernetzungsplattformen und zur Rekrutierung von neuen Mitgliedern verwendet.

Martyrerkult und Ideologisierungen

Innerhalb der DHKP/C kommt der Verehrung „gefallener Kämpferinnen und Kämpfern“, die als Märtyrerinnen und Märtyrer glorifiziert werden, eine zentrale ideologische und propagandistische Funktion zu. Dieser Märtyrerkult dient neben der Identitätsbildung auch der Legitimation des bewaffneten Kampfes und als emotionales Bindeglied innerhalb der Anhängerschaft. In diesem Kontext wird das Hungerfasten als ein Akt des politischen und moralischen Opfers verstanden und symbolisiert einen bewussten Verzicht auf das eigene Leben als Ausdruck des revolutionären Widerstandes. Obgleich das Hungerfasten primär einen symbolischen Charakter hat, wird es propagandistisch instrumentalisiert und dient der Mobilisierung. Auch von in Österreich lebenden Sympathisantinnen und Sympathisanten wird dieses Ideologisierungsinstrument regelmäßig angewendet. Darüber hinaus zeigt sich der Einfluss des Märtyrerkults auch im privaten und kulturellen Leben der Anhängerinnen und Anhänger. Dies wird beispielsweise bei der Namensgebung von Kindern deutlich, bei der häufig die Namen „gefallener Kämpferinnen und Kämpfer“ übernommen werden. Diese Vorgangsweise dient auch der Weiterführung symbolischer Traditionen und der Verankerung des Märtyrerkults.

Bezugnehmend auf den Nahostkonflikt wurden seitens DHKP/C-naher Gruppierungen deutliche pro-palästinensische Bekundungen sowohl in sozialen Medien getätigt als auch durch Demonstrationen manifestiert. Diese haben im Jahr 2025 deutlich zugenommen. Um ihre Haltung zu verdeutlichen, reiste eine Delegation, bestehend aus DHKP/C-, Grup Yorum- und Anti-Imperialist Front-Aktivistinnen und -Aktivisten am 8. Oktober 2025 nach Ägypten, um die Öffnung des Grenzübergangs Rafah von den ägyptischen Behörden zu erzwingen. Damit sollte der palästinensischen Zivilbevölkerung die Möglichkeit zur Flucht geboten werden. Die Delegation, der auch eine Aktivistin und ein Aktivist mit Bezug zu Österreich angehörten, wurde von ägyptischen Sicherheitsbehörden des Landes verwiesen und in die jeweiligen Herkunftsstaaten zurückgeschickt.

Grup Yorum

Die Musikgruppe Grup Yorum hat sich in den letzten Jahren zu einem der wichtigsten Propagandainstrumente der DHKP/C entwickelt. Obgleich Grup Yorum ihre Aktivitäten überwiegend von Deutschland aus steuert, betreibt sie auch dynamische Indoktrinierungs- und Rekrutierungsmaßnahmen in Österreich. So besuchten einzelne Mitglieder der Gruppe im Jahr 2025 in regelmäßigen Abständen Vereine ohne direkten DHKP/C-Bezug. Nachdem 2024 kein Konzert in Österreich stattgefunden hatte, war ein im April 2025 abgehaltenes Konzert als Indiz für eine nun stärkere Fokussierung auf Österreich zu werten. Bei dem von etwa 300 Personen besuchten Konzert wurden Propagandazeitschriften verbreitet und öffentlichkeitswirksam Plakate angebracht, auf denen pro-russische und pro-palästinensische Haltungen demonstriert wurden. Neben bekannten Aktivistinnen und Aktivisten waren auch zahlreiche Minderjährige sowie junge Erwachsene beim Konzert anwesend, was als Indoktrinierungs- bzw. Rekrutierungsstrategie der jungen Szene bewertet werden kann.

Ülkücü-Bewegung

Seit den 1960er-Jahren hat sich die Ülkücü-Bewegung sowohl in der Türkei als auch in Europa institutionell verankert und zu einem wichtigen und einflussreichen politischen und sozialen Akteur entwickelt. Sie konnte jedoch nicht nur ihre Strukturen in nahezu ganz Europa festigen, sondern steht auch in direkter Verbindung zu parteipolitischen Netzwerken in der Türkei sowie deren sozialpolitischen Agenden und wird in ihrem Handeln durch diese beeinflusst bzw. gelenkt. Das erklärte Ziel der Bewegung ist die Förderung und Festigung einer kollektiven Identität türkischer Herkunft und somit die Verteidigung des sogenannten „Türkentums“.

Allgemeine Entwicklung

Für Österreich lässt sich feststellen, dass die Ülkücü-Bewegung sowohl ihre formal rechtskonformen Vereinsstrukturen absichert, welche ideologisch und/oder personell Verbindungen zu Parteien in der Türkei aufweisen, als auch gleichzeitig Jugendliche bzw. junge Erwachsenen für ihre Ideologie zu gewinnen versucht. Gleichzeitig zeigt sich seit einigen Jahren eine zunehmende Loslösung der jungen Generation von den etablierten Vereinsstrukturen hin zu mehr Autonomie hinsichtlich ihres Organisationsgrades. Auffällig ist die fortwährende Herausbildung einer unorganisierten Ülkücü-Szene, die überwiegend von jungen Akteurinnen und Akteuren dominiert wird und traditionelle Organisationshierarchien zu überwinden scheint. 2025 kam es wiederholt zum Zeigen des durch das Symbole-Gesetz verbotenen sogenannten Wolfsgrußes. Darüber hinaus fand im Zuge einer Pro-Palästina-Demonstration in Wien im Oktober 2025 eine physische Auseinandersetzung zwischen PKK-Sympathisantinnen und -Sympathisanten und Personen aus der Ülkücü-Szene statt, die Anzeigen wegen des Verdachts der Körperverletzung zur Folge hatte. Weiters ist zu beobachten, dass die Ülkücü-Bewegung ihre Ideologie zunehmend über soziale Medien verbreitet.

Vereinsaktivitäten

In Österreich sind die Strukturen der sogenannten Ülkücü-Bewegung teils seit Jahren etabliert und historisch verwurzelt. Die ihr zugerechneten Unterstützungsvereine treten überwiegend als Kultur- und Sportorganisationen auf. In ihrer öffentlichen Selbstpositionierung präsentieren sich diese Vereine als unpolitische, kulturelle und insbesondere religiös orientierte Zusammenschlüsse. In den letzten Jahren fokussierten sie sich darauf, gesetzeskonformes Verhalten zu demonstrieren, um weder die öffentliche noch die politische Aufmerksamkeit auf sich zu ziehen. Folglich wurden Aktivitäten wie etwa größere Demonstrationen oder Protestaktionen vermieden. Auch im Jahr 2025 wurden keine Protestveranstaltungen dieser Organisationen registriert. Die Anzahl der Vereine, die der Ülkücü-Bewegung zugeordnet werden, erscheint derzeit stabil. Es ist jedoch anzumerken, dass das Potenzial der politischen Mobilisierung und Einflussnahme vor allem über soziokulturelle Netzwerke besteht. In diesem Kontext spielen sowohl Vereine, die eine bestimmte politische Haltung weiter transportieren, als auch soziopolitische Entwicklungen in der Türkei, eine bedeutende Rolle.

2.4.3 Trends und Entwicklungstendenzen

Die PKK ist nach wie vor die mitgliederstärkste Organisation im Bereich des auslandsbezogenen Extremismus in Österreich. Die Auswirkungen der formellen Auflösung der PKK und des Friedensprozesses mit dem türkischen Staat werden wahrscheinlich mittel- und langfristig bemerkbar werden. Kurzfristig wird die Organisation den Status quo aufrechterhalten, um bei einem möglichen Scheitern des Friedensprozesses handlungsfähig zu bleiben. Sollte der Friedensprozess jedoch erfolgreich verlaufen, könnte dies auch zu einer Transformation bzw. zu einem Strategiewechsel bei den europäischen PKK-Organisationen führen, vorausgesetzt, dass diese sich den Entscheidungen der Mutterorganisation unterordnen. In der Folge könnten neben politischer Lobbyarbeit vor allem Themenschwerpunkte wie kulturelle und sprachliche Autonomie, Identität und Menschenrechte in den überwiegend kurdisch besiedelten Regionen in den Fokus genommen werden. Aktuell ist eine gewisse Konsolidierungsphase festzustellen, in der im Rahmen von Panel- und Informationsveranstaltungen das weitere Vorgehen diskutiert wird. Allerdings werden die europäischen Organisationen sehr wahrscheinlich auf die Ergebnisse und Vorschläge der türkischen parlamentarischen Kommission für nationale Solidarität, Geschwisterlichkeit und Demokratie und deren Implementierung warten, bevor sie ihre Ausrichtung festlegen werden.

Ogleich Österreich und Europa seitens der PKK weiterhin primär als Rückzugsgebiete gesehen werden, bleibt Gewalt eine strategische Option der PKK und kann weiterhin durch politische und geostrategische Entwicklungen in den überwiegend kurdisch besiedelten Gebieten ausgelöst werden. Auch wenn eine Wiederaufnahme terroristischer Aktivitäten in Europa kurz- und mittelfristig eher unwahrscheinlich ist, würden die bestehenden Strukturen dies bei einem Strategiewechsel bzw. Scheitern des Friedensprozesses ermöglichen. Dementsprechend wäre die PKK in der Lage, punktuell Gewalt – primär gegen türkische Einrichtungen in Österreich – einzusetzen.

Hinsichtlich der Entwicklungen in Syrien ist zu betonen, dass der Befehlshaber der syrisch-kurdischen Streitkräfte, Mazloum Abdi, bereits im März 2024 erklärte, dass sich die SDF⁴⁷ nicht an die Aufforderung Öcalans halten müssen, da sie keine Teilorganisation der PKK seien. Darüber hinaus einigte sich die SDF bereits am 10. März 2025 mit der von Ahmed al-Sharaa geführten neuen Führung in Syrien. Obwohl die syrisch-kurdischen Kräfte ideologisch der PKK zuzuordnen sind bzw. dieser zumindest nahestehen, erscheint im Zuge dieser Entwicklungen eine organisatorische Differenzierung stattgefunden zu haben. Eine Wiederaufnahme bzw. neuerliche Verstärkung des Konfliktes zwischen der Türkei und der PKK bzw. PKK-nahen Organisationen und/oder zwischen der syrischen Regierung und der SDF in Syrien könnte auch direkte Auswirkungen auf die innere Sicherheit Österreichs haben. Die Austragung der Konflikte in der Region könnten

47 Die SDF wird von der Türkei als Ableger der PKK und damit als Terrororganisation eingestuft.

sich in der in Österreich lebenden Diaspora spiegeln, wodurch mit mehr Protesten und Demonstrationen zu rechnen wäre.

In Bezug auf den Nahostkonflikt ist zu beobachten, dass vor allem PKK-nahe Jugendgruppierungen eine pro-palästinensische Haltung einnehmen, die primär über soziale Medien und durch Teilnahme an Protesten artikuliert und manifestiert wird.

Was die künftigen Aktivitäten der DHKP/C betrifft, ist davon auszugehen, dass insbesondere die gezielte Rekrutierung von Jugendlichen weiter vorangetrieben wird. Damit einhergehend ist mit einer zunehmenden Indoktrinierung Minderjähriger zu rechnen, die dem Aufbau ideologischer Bindungen und der Gewinnung langfristiger Unterstützungspotenziale dient. Auch das Engagement der Musikgruppe Grup Yorum dürfte sich verstärken – sowohl national als auch international. Ferner lässt sich eine deutlich erhöhte Sichtbarkeit und Aktivität in den sozialen Medien beobachten, begleitet von einem zusehends selbstbewussteren Auftreten und einer zunehmenden Vernetzung.

In der Türkei unterliegt die DHKP/C weiterhin einem hohen Verfolgungsdruck, weshalb die Gefahr terroristischer Anschläge dort aufrecht bleibt. Im europäischen Raum, der von der Organisation primär als Rückzugs- und Rekrutierungsraum definiert wird, zeigen sich aktuell keine Anzeichen gewalttätiger Aktionen. Gleichzeitig ist zu bemerken, dass die DHKP/C bislang nicht eindeutig zur formellen Auflösung der PKK Stellung genommen hat. Daher ist mit hoher Wahrscheinlichkeit davon auszugehen, dass die DHKP/C ihre Aktivitäten weiterführen und dabei versuchen wird, das möglicherweise durch die formelle Auflösung der PKK entstehende Vakuum zu füllen.

Die Aktivitäten der Ülkücü-Bewegung sind weitestgehend von den politischen Geschehnissen und Konstellationen in der Türkei bestimmt. Das aktuelle Potenzial der Bewegung in Österreich wird als moderat eingestuft. Die Aktivitäten der Gruppierung scheinen temporär, spontan und anlassbezogen zu sein, ohne eine organisierte Struktur aufzuweisen. Eine Veränderung der politischen Ausgangslage bzw. mögliche Verschiebungen aufgrund der formellen Auflösung der PKK könnten Auswirkungen auf die Beschaffenheit und den Aktionismus der Bewegung in Österreich haben. Eine mögliche Zuspitzung als Folge des Scheiterns des Friedensprozesses könnte zu gewalttätigen Auseinandersetzungen von PKK Sympathisantinnen und -Sympathisanten mit türkisch-nationalistischen Gruppierungen führen.

Auslandsbezogener Extremismus

Tathandlungen 2025 153

Tathandlungen 2024 224

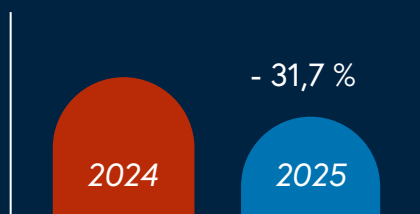
Aufklärungsquote



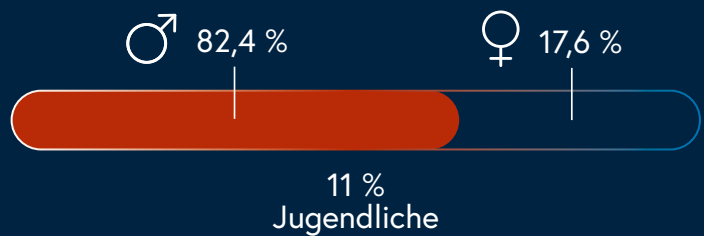
227

Zur Anzeige gebrachte Delikte

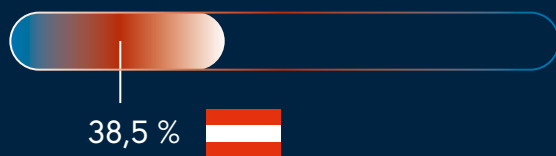
Vergleich zum Vorjahr



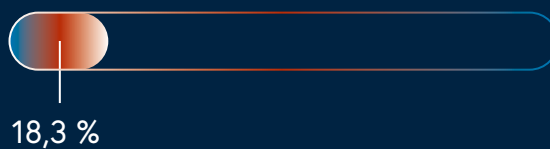
Täterinnen und Täter



Staatsbürgerschaft der Täterinnen und Täter



Internetdelikte



6

Hausdurchsuchungen



1

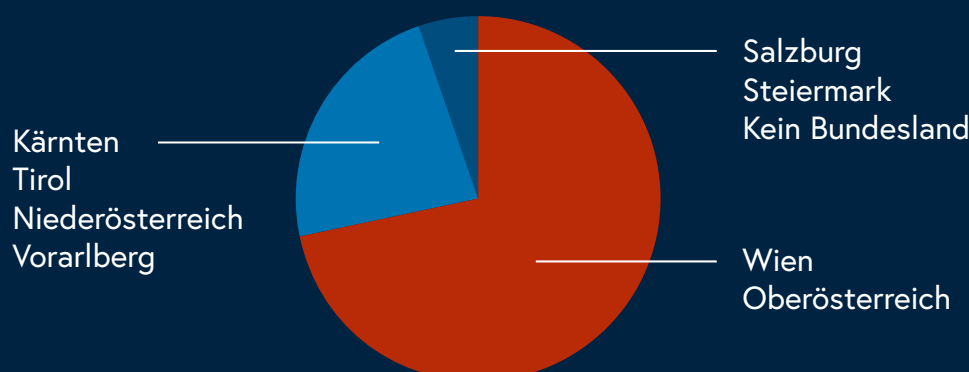
Festnahme



106

Anzeigen gegen
Unbekannte

Bundesländeraufteilung



2.4.4 Zahlen/Daten/Fakten

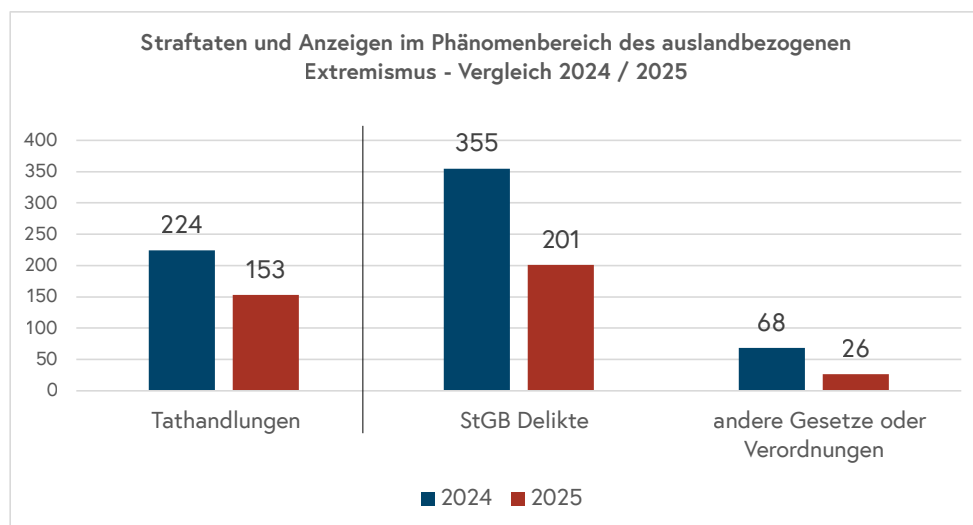
Im Jahr 2025 wurden den Sicherheitsbehörden in Österreich im Phänomenbereich des **auslandsbezogenen Extremismus** insgesamt **153 Tathandlungen** bekannt. Gegenüber dem Jahr 2024 (224 Tathandlungen) bedeutet dies einen zahlenmäßigen **Rückgang um 31,7 Prozent**. 75 Tathandlungen (**49 Prozent**) wurden **aufgeklärt** (2024: 130, 58 Prozent). Bei 62 Tathandlungen (40,5 Prozent) war ein Zusammenhang mit dem Nahostkonflikt feststellbar.

Im Zusammenhang mit den gesetzten Tathandlungen gelangten insgesamt **227 Delikte** zur Anzeige, davon 201 nach dem Strafgesetzbuch (StGB) sowie 26 Anzeigen nach anderen Gesetzen und Verordnungen. Im Jahr 2024 wurden 423 Delikte (355 nach dem StGB sowie 68 nach anderen Gesetzen und Verordnungen) angezeigt.

Insgesamt konnten **91 Tatverdächtige** ausgeforscht und zur Anzeige gebracht werden (2024: 252). Dabei handelt es sich um 75 männliche und 16 weibliche Personen (2024: 186 männliche, 66 weibliche). Unter den Beschuldigten befinden sich zehn Jugendliche (2025: 11 Prozent; 2024: 34 bzw. 13,5 Prozent). 35 (38,5 Prozent) der Beschuldigten besitzen die österreichische Staatsbürgerschaft (2024: 97, 38,5 Prozent). Neben den ausgeforschten Personen erfolgten im Berichtsjahr **106 Anzeigen gegen unbekannte Täterinnen oder Täter** (2024: 115).

Bei **28** (18,3 Prozent) der insgesamt 153 Tathandlungen fand die strafbare Handlung im **Internet**, hier vor allem in sozialen Medien und Messenger-Diensten, statt (2024: 23, 10,3 Prozent). Die Aufklärungsquote lag hier bei 89,3 Prozent (2024: 78,3 Prozent).

Im Zusammenhang mit der Bekämpfung auslandsextremistischer Aktivitäten wurden im Jahr 2025 in Österreich insgesamt **sechs Hausdurchsuchungen** (inklusive freiwilliger Nachschauen) (2024: 19) durchgeführt und **eine Festnahme** vollzogen (2024: 5).

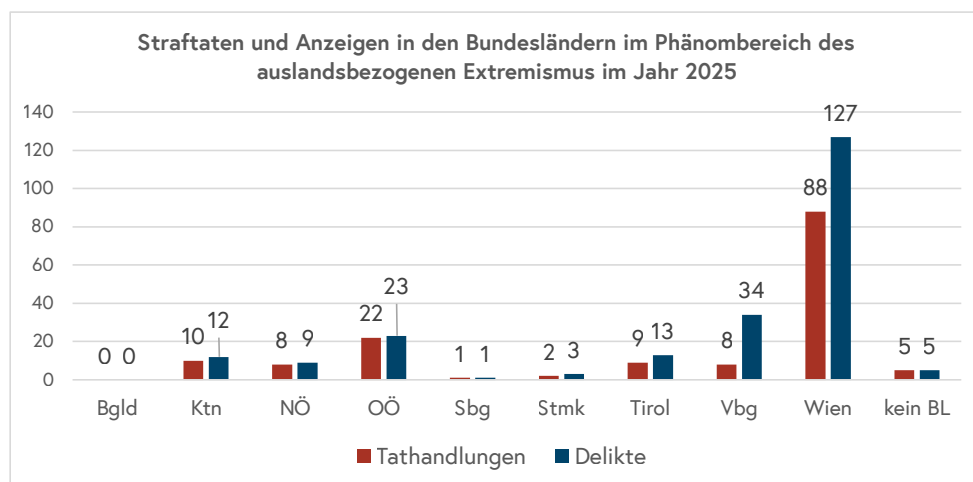
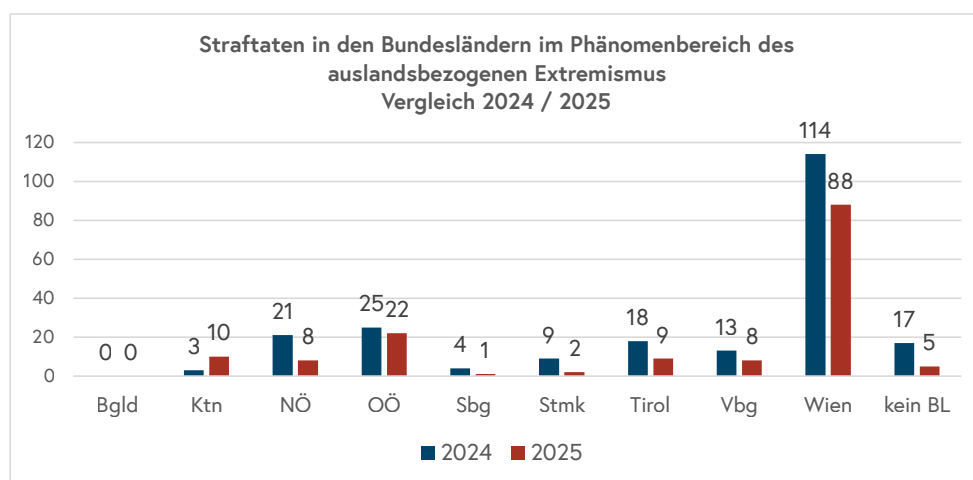


Anzeigen nach dem StGB	2024	2025
Mord (§ 75 StGB iVm. § 15 StGB), Versuch	1	1 ⁴⁸
Körperverletzung (§ 83 StGB)	7	30
Schwere Körperverletzung (§ 84 StGB)	11	0
Gefährdung der körperlichen Sicherheit (§ 89 StGB)	3	0
Raufhandel (§ 91 StGB)	12	0
Nötigung (§ 105 StGB)	4	0
Schwere Nötigung (§ 106 StGB)	5	3
Gefährliche Drohung (§ 107 StGB)	16	25
Fortgesetzte Gewaltausübung (§ 107b StGB)	3	0
Beleidigung (§ 115 StGB)	1	3
Sachbeschädigung (§ 125 StGB)	65	67
Schwere Sachbeschädigung (§ 126 StGB)	32	26
Diebstahl (§ 127 StGB)	1	1
Herabwürdigung religiöser Lehren (§ 188 StGB)	9	0
Landzwang (§ 275 StGB)	28	0
Kriminelle Organisation (§ 278a StGB)	11	2
Terroristische Vereinigung (§ 278b StGB)	16	8
Aufforderung zu mit Strafe bedrohten Handlungen und Gutheißung mit Strafe bedrohter Handlungen (§ 282 StGB)	0	7
Aufforderung zu terroristischen Straftaten und Gutheißung terroristischer Straftaten (§ 282a StGB)	54	6
Verhetzung (§ 283 StGB)	65	21
Falsche Beweisaussage (§ 288 StGB)	0	1
Sonstige StGB Delikte	11	0
Anzeigen nach anderen Gesetzen oder Verordnungen		
§ 50 Waffengesetz (WaffG)	1	3
Symbole-Gesetz (SG)	57	14
Verbotsgesetz (VbtG)	4	3
Art. III Abs. 1 Z 4 EGVG	0	1
Versammlungsgesetz (VersG)	1	5
Sonstige Gesetze oder Verordnungen	5	0
Summe	423	227

48 Ein russischer Staatsangehöriger wird der versuchten Bestimmung zum Auftragsmord eines ausländischen Regierungskritikers via Internet beschuldigt.

Von den insgesamt 153 bekannt gewordenen Tathandlungen waren 26 (17 Prozent) nationalistisch, 36 (23,5 Prozent) antisemitisch, sieben (4,6 Prozent) separatistisch, fünf fremdenfeindlich/rassistisch (3,3 Prozent) und zwei (1,3 Prozent) islamfeindlich motiviert. Bei 77 (50,3 Prozent) Tathandlungen war eine unspezifische oder sonstige Motivlage hinsichtlich der Tatausführung vorhanden.

Im Phänomenbereich auslandsbezogener Extremismus fanden 57,5 Prozent der Tathandlungen in Wien, gefolgt von Oberösterreich (14,4 Prozent), Kärnten (6,5 Prozent), Tirol (5,9 Prozent), Niederösterreich und Vorarlberg (jeweils 5,2 Prozent), der Steiermark (1,3 Prozent) und Salzburg (0,7 Prozent) statt. 3,3 Prozent der Tathandlungen konnten keinem Bundesland zugeordnet werden.



Von den 153 im genannten Phänomenbereich registrierten Tathandlungen konnte bei 14 Tathandlungen (9,2 Prozent) ein Bezug zu der nationalistischen Bewegung Graue Wölfe (2024: 39), bei sechs Tathandlungen (3,9 Prozent) zur separatistischen Organisation PKK (2024: 12) und bei fünf Tathandlungen (3,3 Prozent) zur Hamas (2024: 1) hinsichtlich der

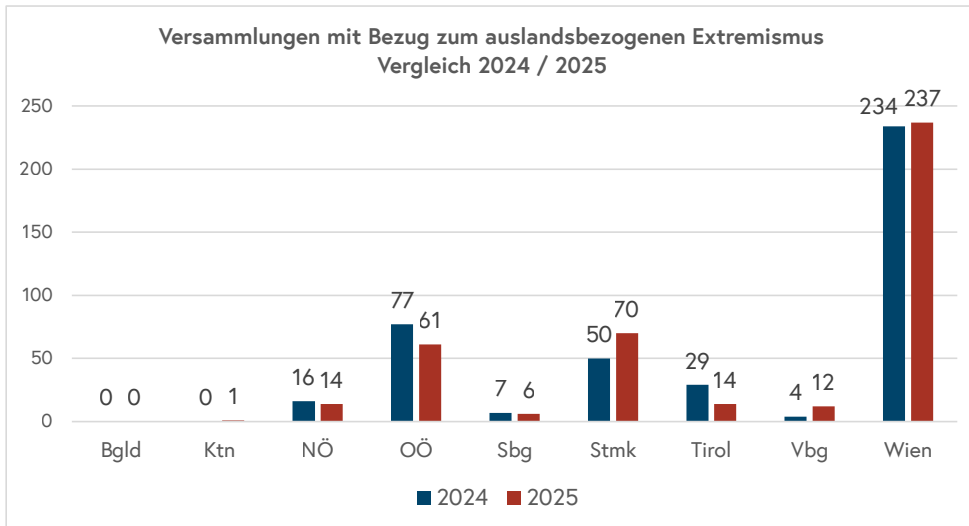
Tatausführung festgestellt werden. Im Jahr 2025 wurden keine Tathandlungen hinsichtlich der zum Marxismus Leninismus orientierten DHKP/C registriert (2024: 1). Im Rahmen dieser Tathandlungen wurden zum überwiegenden Teil Anzeigen nach dem Symbole-Gesetz erstattet. Bei sechs Tathandlungen wurden zudem das Delikt Terroristische Vereinigung gemäß § 278b StGB zur Anzeige gebracht.



In Zusammenhang mit dem **Nahostkonflikt** wurden bundesweit **62 Tathandlungen** registriert, die dem Bereich des auslandsbezogenen Extremismus zugeordnet werden konnten (2024: 80). 20 davon waren antisemitisch, zwei islamfeindlich, eine nationalistisch motiviert. Bei 39 Tathandlungen war eine unspezifische oder sonstige Motivlage hinsichtlich der Tatausführung vorhanden. Im Rahmen der 62 Tathandlungen wurden 63 Anzeigen wegen Sachbeschädigungsdelikten gemäß den §§ 125 und 126 StGB, 15 Anzeigen wegen Körperverletzung gemäß § 83 StGB, acht Anzeigen wegen Verhetzung gemäß § 283 StGB, vier Anzeigen nach dem Delikt der Aufforderung zu terroristischen Straftaten und Gutheißung terroristischer Straftaten gemäß § 282a StGB und jeweils zwei Anzeigen nach den Delikten der Kriminellen Organisation gemäß § 278a StGB und Terroristischen Vereinigung gemäß § 278b StGB erstattet.

Im Berichtsjahr 2025 wurden insgesamt **415 Versammlungen** (2024: 417) mit Bezug zum auslandsbezogenen Extremismus registriert. Davon wurden 402 angemeldet, elf nicht angemeldet und zwei aufgelöst.

Die meisten Versammlungen mit Bezug zu auslandsbezogenem Extremismus fanden in Wien statt (237), gefolgt der Steiermark (70), Oberösterreich (61), Niederösterreich und Tirol (jeweils 14), Vorarlberg (12), Salzburg (6) und Kärnten (1). Im Burgenland konnten keine Versammlungen mit Bezug zum auslandsbezogenen Extremismus festgestellt werden.



2.5 Islamistischer Extremismus und Terrorismus

Der „Islamistische Extremismus“ ist eine religiös motivierte Form des politischen Extremismus. Islamismus ist der Sammelbegriff für ein breites Spektrum an Strömungen, deren gemeinsames Merkmal in der Überzeugung besteht, dass der Islam ein umfassendes gesellschaftspolitisches Programm darstellt, das alle Aspekte und Bereiche des Lebens durchdringen soll, und die ihren ideologischen und politischen Zielen eine spezifische Interpretation des Islam zugrunde legen. Islamistinnen und Islamisten nehmen für sich in Anspruch, den „wahren“ Islam zu vertreten. Sie wollen ihre Auslegung der Scharia (= islamische Gesetze und Normen) als Herrschaftsordnung durchsetzen und die Gesellschaft insgesamt als auch sämtliche privaten Lebensbereiche entsprechend umgestalten. Ihre Deutung der Scharia steht in einem deutlichen Gegensatz zum österreichischen liberalen demokratischen Rechtsstaat und ist mit den Grundprinzipien der Verfassung nicht vereinbar. Der islamistische Extremismus setzt – im Gegensatz zum Terrorismus – nicht notwendigerweise die Bereitschaft zu ideologisch motivierter Gewalt voraus. Islamistische Extremistinnen und Extremisten in Österreich verfolgen unterschiedliche Strategien zur Durchsetzung ihrer Ziele. Während einige islamistische Gruppierungen Gewalt anwenden, sind andere nicht gewaltorientiert und bewegen sich im Rahmen der bestehenden Rechtsordnung. Die wichtigsten islamistischen Bewegungen in Österreich lassen sich in jihadistisch, salafistisch und legalistisch unterteilen.



Der Begriff „**Terrorismus**“ ist in der Wissenschaft nicht einheitlich definiert. Allgemein gilt, dass Terrorismus die bewusste Gewaltanwendung nicht staatlicher Akteurinnen und Akteure gegenüber einer oder mehrerer Personen, einer Gruppe oder der Bevölkerung zur Erreichung politischer, ideologischer und religiöser Ziele ist.

Der Begriff „**Salafismus**“ beschreibt ein spezielles Verständnis des Islam bzw. eine bestimmte ideologische Ausrichtung, die sich als eigenständige Strömung im 20. Jahrhundert bildete. Der Salafismus ist geprägt durch bestimmte theologische und islamrechtliche Grundpositionen und einen besonderen Zugang beim Umgang mit den Quellen des Islam.

Salafistinnen und Salafisten orientieren sich an einer idealisierten religiösen Praxis, den überlieferten Handlungen des Propheten Mohammed (Sunna) und der muslimischen Urgemeinde. Sie streben nach einer „Reinigung“ des Islam von „unislamischen Neuerungen“ nach dem Vorbild der sogenannten „as-salaf as-salih“ („die frommen Vorfahren“ oder „rechtschaffenen Altvorderen“), welche die ersten drei Generationen der muslimischen Gläubigen umfassen. Salafistinnen und Salafisten beanspruchen für sich, im Besitz einer absoluten Wahrheit zu sein, und fühlen sich als die einzig „wahren“ Musliminnen und Muslime. Der in ihren Augen „wahre“ Islam soll durch den direkten Rückgriff auf Koran, Sunna und das Beispiel der Altvorderen wiederbelebt werden.

Eine salafistische Ausrichtung in religiösen Fragen sagt noch nichts über die vertretenen Positionen von Predigern oder Gruppierungen in politischen Fragestellungen aus. Die Fragen nach der politischen Umsetzung salafistischer Glaubensvorstellungen führen daher regelmäßig zu Konflikten und heftigen Debatten unter Salafistinnen und Salafisten. Grundsätzlich lässt sich der Salafismus in drei Hauptströmungen unterteilen, die als Idealtypen zu sehen sind:

„**Quietistischer Salafismus**“

Der quietistische (auch: puristische) Salafismus nimmt weitgehend Abstand von aktiver politischer Partizipation und öffentlicher politischer Debatte. Stattdessen fokussiert er sich auf die Reinigung und Berichtigung des Islams von in seinen Augen falschen Vorstellungen und illegitimen Neuerungen.

„**Politischer Salafismus**“

Der politische Salafismus setzt auf intensive Propagandatätigkeit (durch da'wa, „Missionierung“), beteiligt sich zudem aber auch aktiv am politischen Geschehen (beispielsweise durch parlamentarische Aktivitäten).

„Jihadistischer Salafismus“

Im Gegensatz zu politischen und quietistischen Salafistinnen und Salafisten wollen Vertreterinnen und Vertreter des jihadistischen Salafismus ihre Ziele in erster Linie durch Gewaltanwendung durchsetzen.

Der Begriff „Jihadismus“ wird unabhängig von der langen und komplexen Tradition und den vielfältigen Bedeutungen des religiösen Konzepts des „Jihad“ definiert. Der Jihadismus ist in diesem Sinne keiner bestimmten Ideologie zuzuordnen, sondern bezeichnet den bewaffneten Kampf zur Durchsetzung eines politischen Wandels hin zu einer islamistischen Herrschafts- und Gesellschaftsordnung. Der Begriff des Jihadismus umfasst ein breites Spektrum unterschiedlicher Akteurinnen und Akteure, die zum Teil konkurrierende Ideologien vertreten. Kampfhandlungen werden dabei als religiöse Pflicht verstanden.

2.5.1 Überblick

Auch im Jahr 2025 verfolgten Islamistinnen und Islamisten in Österreich das langfristige Ziel, eine Gesellschafts- und Staatsordnung auf der Grundlage des islamischen Rechts zu errichten. In ihrem idealen Staat wären Grundprinzipien wie Meinungsfreiheit, Trennung von Staat und Religion, Gewaltenteilung und Gleichberechtigung der Geschlechter nicht gewährleistet. Der Islamismus steht somit im klaren Widerspruch zum liberalen demokratischen Rechtsstaat. Das Spektrum des Islamismus in Österreich reicht von streng hierarchisch und zentralistisch organisierten Strukturen bis hin zu hierarchiefreien Szenen und losen Netzwerken.

Während nicht alle islamistischen Extremistinnen und Extremisten direkt zu Gewalt (in ihrer extremsten Form ausgeprägt als Terrorismus) bereit sind, bergen ihre Ideologien oft Haltungen, die Gewaltbereitschaft fördern können. Die fundamentale Ablehnung bestehender Gesellschaftsordnungen in der muslimischen wie auch in der westlichen Welt ist charakteristisch. Das Ziel ist die Errichtung einer Herrschaftsordnung, die auf islamistischen Idealen basiert. Besonders betont wird die Vorstellung eines „wahren“ Islam, der andere mögliche Interpretationen ausschließt. Innerhalb dieses extremistischen Spektrums gibt es unterschiedliche Ansichten über die Methoden zur Erreichung der Ziele, vor allem im Hinblick auf die Ablehnung oder die Akzeptanz von Gewalt. Mit anderen Worten: Manche Gruppen lehnen Gewalt ab, während andere terroristische Gewalt als zentrales Mittel zur Zielerreichung betrachten. Gemeinsam ist den meisten islamistischen Ideologien jedoch ein tief verankerter Antisemitismus. Entsprechend wurde auch 2025 von islamistischen Akteuren in Österreich antisemitisches Gedankengut öffentlich in Moscheen, in sozialen Medien sowie bei Demonstrationen verbreitet.

In Österreich birgt der islamistische Extremismus und Terrorismus – insbesondere durch die Gefahr von terroristischen Anschlägen – ein erhebliches Sicherheitsrisiko. Sinn und Zweck von Anschlägen ist es, Angst und Schrecken in der Bevölkerung zu verbreiten und psychologischen Druck auf die Gesellschaft auszuüben. Des Weiteren können Anschläge sowie staatliche Reaktionen auf Anschläge zur (weiteren) Radikalisierung von Sympathisantinnen und Sympathisanten sowie zur Mobilisierung der eigenen Anhängerschaft genutzt werden. Terrorismus wird somit als eine Form politisch motivierter Gewalt eingesetzt, um die öffentliche Wahrnehmung zu beeinflussen und Unsicherheit zu erzeugen. Österreich bleibt daher im Kontext des internationalen Terrorismus wachsam, insbesondere in Bezug auf die Radikalisierung und Rekrutierung durch islamistische Netzwerke.

2.5.2 Aktuelle Lage

Risikostufe und Gefahrenpotenzial

2025 waren Österreich und Europa bereits das dritte Jahr in Folge mit mehreren Terroranschlägen und Anschlagversuchen konfrontiert. Zahlreiche Anschlagversuche in und Bedrohungen für Österreich konnten durch den Verfassungsschutz verhindert bzw. abgewehrt werden. Sowohl aufgrund weiterer konkreter Bedrohungsszenarien im In- und Ausland als auch wegen der anhaltenden abstrakten Gefährdungslage blieb die Risikostufe in Österreich während des Berichtszeitraums erhöht. Die laufende Bewertung der Risikostufe erfolgte unter anderem im Lichte des Messerattentats vom 15. Februar 2025 in Villach, weiterer Anschläge in Europa sowie mehrerer vereitelter terroristischer Gewalttaten in Österreich und in europäischen Staaten.

Der terroristische Angriff der Hamas auf Israel am 7. Oktober 2023 und die darauf folgende Eskalation des Nahostkonfliktes war auch im Jahr 2025 ein zentraler Faktor für das Fortbestehen der Bedrohungslage in Österreich und Europa. Die Geschehnisse im Nahen Osten entfalteten weiterhin eine stark emotionalisierende Wirkung und beförderten bzw. stärkten islamistische Rekrutierungs- und Mobilisierungspotenziale. Terrororganisationen wie der Islamische Staat nutzten diese Thematik propagandistisch und riefen zu Terroranschlägen – unter anderem in Österreich und Europa – auf. Mitglieder der Hamas wiederum setzten 2025 nicht nur im Nahen Osten, sondern auch in Österreich und Europa sicherheitsrelevante Handlungen. So lagerten sie beispielsweise Schusswaffen in Österreich und Deutschland, die potenziell für Anschläge auf jüdische und israelische Einrichtungen genutzt werden sollten.

Das größte Gefahrenpotenzial für Terroranschläge in Österreich und Europa ging im Berichtsjahr von radikalisierten, männlichen Einzelpersonen und autonom agierenden Kleingruppen aus. In diesem Zusammenhang setzte sich der Trend zu immer jüngeren Akteuren fort. Die Mehrheit der radikalisierten Minderjährigen und jungen Erwachsenen beteiligte sich auch 2025 hauptsächlich an der Verbreitung von Propaganda. Zuletzt waren jedoch auch vermehrt junge Akteure in die Planung und Durchführung von Terror-

anschlägen involviert. In Österreich wies der Großteil der jungen Akteure einen Bezug zum IS auf. Radikalisierungsprozesse fanden in den meisten Fällen sowohl online – gefördert durch islamistische Propaganda – als auch realweltlich statt.

Die Propagandaapparate der Terrororganisationen bestanden auch 2025 aus offiziellen und inoffiziellen (nicht mit der Führung der jeweiligen Terrororganisation akkordierten) Medieneinrichtungen. Diese veröffentlichten ihre Propaganda auf unterschiedlichen Plattformen und in verschiedenen Sprachen, um ein möglichst breites Publikum zu erreichen.

Anhängerinnen und Anhänger des IS kreierten im Jahr 2025 inoffizielle Kanäle mit dem primären Ziel, offizielle und inoffizielle IS-Propaganda in die deutsche Sprache zu übersetzen und im deutschsprachigen Raum zu verbreiten. Über diese Kanäle wurden 2025 auch Aufrufe zu Terroranschlägen mit Bezügen nach Österreich veröffentlicht. Die Verfasserinnen und Verfasser riefen unter anderem zu Anschlägen in österreichischen Großstädten auf und verwiesen auf den Villach-Attentäter. Islamistische und terroristische Organisationen nutzten zudem vermehrt Künstliche Intelligenz (KI) zur Produktion von Propaganda, vor allem zur Erstellung von Bildern, Videos, Audiomaterial sowie für Übersetzungstätigkeiten.

Die Ziele terroristischer Anschläge in Europa waren 2025 vielfältig. Von besonders großem Interesse blieben unverändert vor allem leicht zugängliche Örtlichkeiten mit einem hohen Aufkommen an Besucherinnen und Besuchern. Darüber hinaus zählten auch Polizeibedienstete sowie Angehörige der LGBTQIA+-Community im Jahr 2025 zu potenziellen Anschlagzielen. Seit der Eskalation des Nahostkonfliktes im Jahr 2023 lag der Fokus jedoch primär auf israelischen bzw. jüdischen Personengruppen und Einrichtungen. Folglich wies ein Teil der 2025 in Europa verübten Terroranschläge eindeutig antisemitische Motive auf. Beispiele hierfür sind der im Februar 2025 verübte Terroranschlag auf dem Gelände des Holocaust-Mahnmals in Berlin (Deutschland) sowie der im Oktober 2025 am jüdischen Feiertag Jom Kippur erfolgte Terroranschlag vor einer Synagoge in Manchester (Vereinigtes Königreich). Im April 2025 gelang es den österreichischen Sicherheitsbehörden einen unter anderem gegen die israelische Botschaft in Wien beabsichtigten Anschlag zu verhindern.

Die bevorzugten Tatmittel blieben in Europa auch im Jahr 2025 einfach zu beschaffende Alltagsgegenstände mit zum Teil erheblicher Schadenswirkung. In diese Kategorie fallen vor allem Hieb- und Stichwaffen sowie Fahrzeuge. Beispiele hierfür sind die im Februar und Mai 2025 verübten Stichwaffenattentate in Villach und Bielefeld (Deutschland). Österreichische IS-Akteurinnen und IS-Akteure setzten sich in den vergangenen Jahren jedoch zum Teil auch mit der Beschaffung von Schusswaffen bzw. der Herstellung von Sprengstoffen auseinander. Darüber hinaus zeigten österreichische IS-Anhängerinnen und IS-Anhänger im Berichtsjahr deutliches Interesse an der Nutzung von Drohnen für die Durchführung von Terroranschlägen.

Islamischer Staat, al-Qaida und affillierte Gruppierungen

Von Terrororganisationen wie dem IS, al-Qaida sowie affiliierten Gruppierungen ging im Jahr 2025 eine erhöhte Gefahr für Europa und Österreich aus.

Seit 2019 hat der Islamische Staat in seinen früheren Kerngebieten in Syrien und im Irak deutlich an Einfluss eingebüßt. Durch diese Entwicklungen kam es zu einer Machtverschiebung und einem Erstarren der Ableger des IS in Westafrika (ISWAP), der Sahel-Zone (ISSP) sowie in Afghanistan und Pakistan (ISKP). Zu den prominentesten und aktivsten Provinzen des IS zählten 2025 die Ableger in Somalia (IS Somalia) und in Pakistan. Der IS Somalia ist vorwiegend in Finanzierungstätigkeiten involviert, wohingegen sich der ISKP auf die externen Operationen des IS konzentrierte. 2024 leitete der ISKP mehrere großangelegte Anschläge an, insbesondere jenen auf die Crocus City Hall in Moskau am 22. März 2024. Obwohl die Kapazitäten des ISKP zur Durchführung derartiger Anschläge im Berichtsjahr abnahmen, verfolgt der ISKP weiterhin das Ziel, Anschläge im Westen durchzuführen bzw. anzuleiten.

Wie in den vorangegangenen Jahren konnten auch im Jahr 2025 Ausreiseambitionen aus Europa festgestellt werden, wobei die fraglichen Personen das Ziel hatten, sich den Ablegern des IS in Somalia oder Pakistan anzuschließen. Die Ausreiseversuche aus Österreich blieben jedoch zumeist ohne Erfolg. Zudem gab es hierzulande im Jahr 2025 keine vergleichbare Mobilisierung wie zur Zeit des Höhepunktes des IS in Syrien und im Irak zwischen 2013 und 2017, obwohl das Interesse, sich dem IS anzuschließen, unter radikalisierten Personen in Österreich nach wie vor vorhanden ist.

Die Bedrohungslage durch al-Qaida (AQ) in Österreich hat sich in den letzten Jahren gewandelt. Seit Ende August 2022 ist AQ ohne Führung. Inoffiziell soll Sayf al-Adl die zentrale Führung der Organisation innehaben. In Europa und Österreich ging von AQ im Jahr 2025 eine – verglichen mit dem IS – geringere Gefahr aus. AQ versuchte vor allem, propagandistisch Stärke zu zeigen und nutzte insbesondere den Nahostkonflikt, um Unterstützung zu generieren. Folglich konnte AQ-Propaganda auf den sichergestellten Handys radikalisierten Personen in Österreich festgestellt werden. Am bedeutendsten waren dabei die Produktionen des Ablegers der al-Qaida auf der Arabischen Halbinsel (AQAP).

Insgesamt waren der ISKP sowie AQAP 2025 federführend in der Propagandaproduktion. Der ISKP veröffentlichte durch seine Medienorganisation al-Azaim Foundation umfangreiche Propaganda in mehreren Sprachen, darunter auch in Englisch. AQAP wiederum publizierte vorwiegend über die Organisation Al-Malahem Media in Arabisch und über das Outlet Inspire in Englisch. Sowohl AQAP als auch der ISKP riefen im Berichtsjahr in ihren Medienproduktionen radikalisierte Personen in Europa zu Anschlägen auf. In den Publikationen wurde auch Österreich explizit als Anschlagziel erwähnt. Diese Aufrufe wurden 2025 zudem von inoffiziellen IS-Medienorganisationen wie Sarh al-Khilafa (Die

Struktur des Kalifats) für die Produktion weiterer Propagandamaterialien wie Poster, Videos und Texte aufgegriffen und sowohl online als auch über verschlüsselte Messenger-Dienste verbreitet. Auch deutschsprachige Propaganda war online weitläufig verfügbar. Einzelne österreichische IS-Anhänger waren 2025 bestrebt, Berichte im Auftrag offizieller IS-Medien in mehrere Sprachen zu übersetzen.

2025 ging in Österreich auch eine erhöhte Gefahr von Jihadistinnen und Jihadisten mit nordkaukasischem Hintergrund aus. Das Radikalisierungspotenzial in der tschetschenischen Community Österreichs ist aufgrund der dort vorherrschenden Geschichtsdarstellung – Stichwort: ethnische und religiöse Unterdrückung – sowie bestehender, separatistisch orientierter Familien- und Clanstrukturen signifikant hoch. Dies zeigt sich insbesondere daran, dass bereits in der Vergangenheit viele Tschetscheninnen und Tschetschenen aus Österreich nach Syrien und in den Irak ausgereist sind bzw. dies versuchten. Tschetschenische Kämpfer fanden sich danach sowohl auf Seiten des IS als auch auf Seiten AQ-naher Gruppierungen. Die jihadistische Ideologie des IS wird von vielen Angehörigen dieser Volksgruppe vertreten, auch in Österreich.

Nordkaukasische IS-Anhängerinnen und IS-Anhänger in Österreich waren 2025 teilweise gut vernetzt und hatten enge Verbindungen zu internationalen terroristischen Strukturen. So wurde beispielsweise ein tschetschenischer IS-Anhänger in Österreich zu viereinhalb Jahren Haft verurteilt, unter anderem, weil er eine führende Rolle in einem internationalen Netzwerk einnahm, das vorwiegend in der Terrorfinanzierung aktiv war. Das Netzwerk soll Beträge im mittleren zweistelligen Millionenbereich an IS-Anhängerinnen und IS-Anhänger in Syrien zur Verfügung gestellt haben.

Islamischer Staat Khorasan Provinz und Islamischer Staat Somalia

Vom Islamischen Staat Khorasan Provinz ging auch 2025 eine hohe Gefahr für die öffentliche Sicherheit in Österreich aus. Zwar war der ISKP im Vergleich zum Jahr 2024 geschwächt, nahm jedoch weiterhin eine zentrale Rolle bei der Planung internationaler Terroranschläge ein.

Der „**Islamische Staat Khorasan Provinz**“ (**ISKP**) ist eine terroristische Organisation, die 2015 als regionaler Ableger des IS in der Khorasan-Region Afghanistans und Pakistans etabliert wurde. Der Großteil der aktuell aktiven ISKP-Kämpfer besteht aus ehemaligen Mitgliedern der pakistanischen Taliban sowie ehemaligen IS-Kämpfern aus Syrien und dem Irak und umfasst Personen afghanischer und zentralasiatischer Nationalität.

In Afghanistan zählen die östlichen Provinzen zu den wichtigsten Einflussgebieten des ISKP. Trotz der Abnahme an Aktivitäten innerhalb Afghanistans versucht der ISKP weiterhin, die Regierung der Taliban zu schwächen. Der ISKP fokussiert seine



Angriffe in Afghanistan daher auf Institutionen, die Führung der Taliban sowie auf die schiitische Bevölkerung.

Der ISKP ist zudem einer der aktivsten und bedeutendsten Akteure in der Medienstrategie des IS und produziert Propaganda in zahlreichen Sprachen. Im Jänner 2025 wurde Österreich auf einem Poster des ISKP erstmals explizit als Anschlagziel genannt. So wurde neben diversen Großveranstaltungen in Europa auch die Wiener Ballsaison als Anschlagziel angeführt. Das Poster ist als Teil der Medienstrategie des ISKP zu betrachten, die das Ziel verfolgt, Personen für Anschläge in Europa zu mobilisieren. Aufgrund seiner besonders zentralen Rolle innerhalb des IS sowie seiner aktiven Medienstrategie hatte der ISKP eine große Anziehungskraft auf IS-Anhängerinnen und IS-Anhänger in Österreich.

Der IS in Somalia hat mit dem Erstarben des al-Karrar Büros⁴⁹ unter der Leitung von Abd al-Qadir Mumin im Jahr 2025 stark an Bedeutung gewonnen und nimmt mittlerweile eine führende Rolle bei der Finanzierung der Terrororganisation ein. Gegen Ende 2025 stand zur Debatte, ob Abd al-Qadir Mumin die Führung des gesamten IS und die Rolle des Kalifen innehaben könnte. Bereits im Jahr 2024 wurde unter europäischen IS-Anhängerinnen und IS-Anhängern immer öfter Somalia als Ausreiseziel diskutiert. Dieser Trend setzte sich im Berichtsjahr fort.

2025 kam es zu einem deutlichen Anstieg von IS-Terroranschlägen auf Sicherheitspersonal, Regierungseinrichtungen und öffentliche Institutionen in Somalia. Außerdem referenzierte der IS in seiner Propaganda vermehrt auf seinen Ableger in Somalia und stellte dieses Land als geeigneten Ort für Migration, Unterstützungstätigkeiten und für den bewaffneten Kampf dar. Dies zeigt, dass der Ableger in Somalia im Jahr 2025 an Bedeutung gewonnen hat und auch in Zukunft ein potenzielles Ausreiseziel für die österreichische und europäische IS-Szene darstellt.

Radikalisierungsnetzwerke

2025 konnten in Österreich mehrere Radikalisierungsnetzwerke identifiziert werden. Diese werden zum Großteil von IS-Anhängern betrieben und zielen darauf ab, die junge Generation zu indoktrinieren und systematisch heranzuziehen. Alter oder Herkunft spielen in diesen Radikalisierungsnetzwerken keine wesentliche Rolle. Die beobachtete Szene ist zudem ethnisch divers. So konnten Personen unterschiedlicher Nationalitäten wahrgenommen werden, etwa Personen mit nordkaukasischem Hintergrund, aus den Ländern des Westbalkans sowie Konvertitinnen und Konvertiten aus Österreich.

⁴⁹ „Al-Karrar“ ist ein Büro des IS, das als zentrale operative und finanzielle Einheit für den IS in Ost-, Zentral- und Südafrika fungiert. Das Büro ist mit dem IS in Somalia verbunden und koordiniert die finanzielle Unterstützung, um die Operationen des IS in der Region zu finanzieren.

Die Radikalisierungsnetzwerke boten auch 2025 Rahmenbedingungen, um Kinder, Jugendliche und junge Erwachsene zu ideologisieren und radikales Gedankengut zu verbreiten. Durch den Fokus auf Expansion und Jugendarbeit, gepaart mit direkten Kontakten erfahrener Szeneangehöriger zu IS-Führungspersonen im Ausland, versucht die Szene in Österreich neue Mitglieder zu rekrutieren.

Die DSN setzte 2025 zahlreiche Maßnahmen, um die Radikalisierungsnetzwerke zu schwächen bzw. zu beseitigen und somit weiteren Rekrutierungen und Radikalisierungsprozessen proaktiv entgegenzuwirken. Beispielsweise wurde im November 2025 in Österreich, der Schweiz und in Deutschland unter enger Absprache und Koordination ein internationaler Joint Action Day im Bereich des islamistischen Extremismus und Terrorismus durchgeführt. Weiters setzte die DSN in Zusammenarbeit mit den neun Landesämtern Staatsschutz und Extremismusbekämpfung sowie den Justizbehörden österreichweit zahlreiche Hausdurchsuchungen, Sicherstellungen, Beschuldigtenvernehmungen und Festnahmen um und führte zudem über 100 Gefährderansprachen sowie waffenrechtliche Maßnahmen durch.

2025 beobachtete der Verfassungsschutz Ausreiseambitionen von Personen aus diesen Netzwerken. Vor allem der ISKP in Pakistan wird immer noch als attraktives Ausreiseziel erachtet. Es ist wahrscheinlich, dass führende IS-Anhänger in den identifizierten Radikalisierungsnetzwerken eine wesentliche Rolle bei der Organisation von Ausreiseversuchen spielen. Zudem kann nicht ausgeschlossen werden, dass IS-Ableger ihrerseits aktiv versuchen, auf diese Netzwerke für Ausreisen und die Planung von Terroranschlägen zurückzugreifen.

Lage in Syrien

Seit dem 8. Dezember 2024 regiert in Syrien Ahmed al-Scharaa (alias Abu Muhammad al-Jawlani), der ehemalige Anführer des syrischen Milizbündnisses Hayat Tahrir al-Sham (HTS), als Übergangspräsident. Die HTS, vormals Jabhat al-Nusra, hatte sich im Jahr 2017 offiziell von AQ gelöst und jene Rebellenoffensive angeführt, die im Jahr 2024 den Sturz des Assad-Regimes herbeiführte. Die ersten Wahlen unter al-Scharaa fanden am 5. Oktober 2025 unter geringer gesamtgesellschaftlicher Beteiligung statt. Ein erheblicher Teil der Bevölkerung Syriens wurde von den Wahlen ausgeschlossen, nicht zuletzt, weil Teile des Landes nach wie vor von der kurdischen Minderheit kontrolliert werden. Die aktuelle syrische Regierung wird seither von einer sunnitischen Mehrheit dominiert. Sowohl Frauen als auch Minderheiten, insbesondere Alawiten, Christen, Schiiten und Ismailiten, sind derzeit nicht repräsentativ in der syrischen Regierung vertreten.

Bei **Hayat Tahrir al-Sham** (dt.: **Komitee zur Befreiung Syriens/der Levante**) handelt es sich um die Nachfolgeorganisation der Terrororganisation Jabhat al-Nusra unter der Leitung von Abu Muhammad al-Jawlani. Al-Jawlani radikalisierte



sich früh und schloss sich 2003 al-Qaida im Irak an. Nach Ausbruch des syrischen Bürgerkrieges 2011 wurde er von Abu Bakr al-Baghdadi – damals Anführer des Islamischen Staates im Irak – nach Syrien geschickt, um eine jihadistische Organisation aufzubauen. Dies resultierte in der Gründung der Terrororganisation Jabhat al-Nusra.

Im April 2013 forderte al-Baghdadi die Auflösung von Jabhat al-Nusra und die Eingliederung der Organisation in den neugegründeten Islamischen Staat im Irak und Syrien (ISIS). Al-Jawlani lehnte diese Forderung ab und betonte, dass er die Befehle des damaligen al-Qaida-Führers al-Zawahiri und nicht jene von al-Baghdadi befolgen werde. Diese Haltung führte nicht nur zum Konflikt zwischen al-Qaida und ISIS (später IS) in Syrien, sondern hatte auch zur Folge, dass Jabhat al-Nusra ab 2013 offiziell als al-Qaida-Ableger auftrat. Die USA erhöhten aufgrund der Nähe zu al-Qaida das Kopfgeld zur Ergreifung der Person al-Jawlani auf zehn Millionen US-Dollar.

2016 wurde die Verbindung zu al-Qaida zumindest offiziell beendet und die Jabhat al-Nusra in Jabhat Fath al-Sham umbenannt. Al-Jawlani strebte seither konsequent danach, das Image des Terroristen abzulegen und als regierungsfähiger, legitimer politischer Akteur wahrgenommen zu werden. 2017 kam es zu einem Zusammenschluss von Jabhat Fath al-Sham mit mehreren jihadistischen Organisationen, die fortan unter dem Namen Hayat Tahir al-Sham operierten. Trotz diverser Namensänderungen und Restrukturierungen blieb das wesentliche Ziel der Organisation die Errichtung eines islamistischen Staatswesens in Großsyrien.

Nach der territorialen Kapitulation des IS im Jahr 2019 inhaftierten die Syrischen Demokratischen Kräfte zahlreiche IS-Anhängerinnen und IS-Anhänger, darunter auch sogenannte Foreign Terrorist Fighters (FTF) sowie deren Kinder. Die Mehrzahl dieser Personen befand sich auch im Jahr 2025 in den Lagern und Gefängnissen der SDF in den syrischen Regionen Hasaka und Raqqa, darunter auch Österreicherinnen und Österreicher. Innerhalb dieser Lager verfügt der IS über gut ausgebaute Strukturen und Zellen, gleichzeitig versuchte er in den letzten Jahren immer wieder seine Anhängerinnen und Anhänger zu befreien. Die Befreiung ideologisch Gleichgesinnter bietet dem IS perspektivisch die Gelegenheit, Einfluss sowohl über ehemalige Lagerbewohnerinnen und Lagerbewohner als auch auf deren soziales Umfeld zu nehmen. Einen besonderen Schwerpunkt des IS bildet die Indoktrination von Kindern und Jugendlichen innerhalb der Lager. IS-Netzwerke in Österreich versuchten in den letzten Jahren, Spenden zur Unterstützung von IS-Anhängerinnen und IS-Anhängern in den Lagern zu sammeln. Die Spenden wurden sowohl online auf Plattformen wie Telegram, TikTok und Instagram als auch realweltlich lukriert.

Foreign Terrorist Fighters unbekanntem Aufenthalts

Von den insgesamt 267 Personen aus Österreich, die sich Terrororganisationen wie beispielsweise dem IS vor Ort angeschlossen haben, befand sich 2025 noch eine mittlere zweistellige Anzahl in der ehemaligen Konfliktregion von Syrien und dem Irak. Ein Teil der österreichischen FTF ist bereits ums Leben gekommen. Allerdings waren die Aufenthaltsorte mehrerer österreichischer FTF auch 2025 nicht abschließend geklärt. Es besteht die realistische Möglichkeit, dass einige unter einem falschen Namen registriert und gefangen genommen wurden. Ein Teil könnte sich in Nordwest-Syrien aufhalten und auf ein Wiedererstarken des IS hoffen, oder sich anderen Organisationen wie der HTS angeschlossen haben. Ziel der österreichischen Sicherheitsbehörden war und ist es, diese Personen ausfindig zu machen und gerichtlich zur Verantwortung zu ziehen.

„Foreign Terrorist Fighters“ (FTF) sind Personen, die aus Österreich ausgereist sind, um sich einer jihadistischen Gruppierung oder Organisation – zumeist dem IS – anzuschließen. Unter dem Begriff werden auch jene Personen subsumiert, die versuchen, sich einer jihadistischen Gruppierung oder Organisation im Ausland anzuschließen, jedoch an der Ausreise gehindert werden.



Repatriierungen

Aufgrund einer Entscheidung des Bundesverwaltungsgerichts im Jahr 2024 zur Rückführung einer weiblichen FTF samt ihren Kindern aus Syrien wurden im Berichtsjahr zwei österreichische Staatsbürgerinnen mit ihren minderjährigen Kindern nach Österreich zurückgeholt und eine davon festgenommen. Die Rückkehrerinnen wurden anschließend aufgrund der Mitgliedschaft in einer terroristischen Vereinigung zu zwei Jahren bedingter Haftstrafe verurteilt. Die Wiedereingliederung und aktive Einbindung der Betroffenen in das gesellschaftliche Leben verliefen soweit positiv.

Da die Repatriierung radikalierter IS-Unterstützerinnen und IS-Unterstützer weltweit eine neue gesellschafts- und sicherheitspolitische Herausforderung darstellt, gibt es aufgrund der kurzen Zeitspanne bislang vergleichsweise wenige für Europa gültige Erfahrungswerte. Vor allem die Integration der in den Kriegsgebieten geborenen und sozialisierten Kinder stellt eine große Herausforderung dar. Es bedarf gesamtgesellschaftlicher Anstrengungen und Ansätze, um eine erfolgreiche und nachhaltige Integration der repatriierten Familien zu erzielen.

Waffenlager der Hamas in Europa und Österreich

Der Konflikt zwischen Israel und der Hamas hatte in den letzten Jahren auch signifikante Auswirkungen auf die islamistische Szene in Europa und Österreich. In Österreich wirkte sich der Konflikt lange Zeit vor allem in Form einer ideologischen Instrumentalisierung durch islamistische Akteurinnen und Akteure aus. Der Konflikt im Gazastreifen wurde

genutzt, um antisemitisches Gedankengut zu verbreiten und islamistische Narrative gegen Israel und den Westen zu propagieren. Diese Inhalte wurden insbesondere von Akteurinnen und Akteuren des legalistischen Islamismus sowohl in Moscheen als auch in sozialen Medien verbreitet.

Die Hamas war im Westen bisher nicht in Anschlagpläne involviert, da sie sich auf den bewaffneten Kampf gegen Israel vor Ort konzentrierte. Folglich agierte die Hamas in Europa und Österreich ähnlich dem Vorbild der Muslimbruderschaft, der sie entstammt, und versuchte über lokale Vereine und paneuropäische Institutionen Einfluss auf Politik und Gesellschaft in Europa zu nehmen. Die Hamas findet in manchen mehrheitlich muslimischen Ländern Unterstützung, ist in der EU hingegen verboten.

Ende 2023 gab es erste Hinweise, dass die Hamas nun auch Europa zumindest für die Lagerung und den Transport von Waffen nutzt. Im Dezember 2023 wurden Hamas-Mitglieder in Deutschland und den Niederlanden festgenommen, die nicht nur Kontakte zur Hamas-Führung pflegten, sondern auch Zugang zu einem Waffenlager in Bulgarien gehabt haben sollen.



Die „Hamas“ bzw. „Harakat al-Muqawama al-Islamiyya“ (dt.: „Islamische Widerstandsbewegung“) ist eine sunnitische, islamistische Organisation. Sie wurde im Jahr 1987 als palästinensischer Ableger der Muslimbruderschaft gegründet. Die Hamas ist eine komplexe Organisation: Sie ist eine politische Partei, besitzt einen karitativen und militärischen Zweig und ist zugleich eine Terrororganisation. Bei den letzten Wahlen im Gazastreifen im Jahr 2006 ging sie als Wahlsiegerin hervor und kontrolliert seitdem streng autoritär den Gazastreifen. Die EU führt die gesamte Hamas auf ihrer Terrorliste. Bisher führte die Hamas ausschließlich Anschläge in Israel durch. Die derzeitigen Entwicklungen und nachrichtendienstlichen Erkenntnisse deuten jedoch einen Wandel im Modus Operandi der Hamas an. In Zukunft könnten auch jüdische und israelische Einrichtungen in Europa von der Hamas als Anschlagziele in Betracht gezogen werden.

Anfang Oktober 2025 wurden in Deutschland drei Mitglieder der Hamas festgenommen, die für die Terrororganisation Waffen organisierten. Bei den Festnahmen konnten Schusswaffen, darunter Pistolen und Sturmgewehre, sichergestellt werden.

Auch in Österreich gab es im Berichtsjahr Ermittlungen gegen Mitglieder der Hamas, die in unmittelbarem Kontakt mit den zuvor angeführten Akteuren der Hamas in Deutschland standen. In der Folge konnte Anfang Oktober 2025 in Wien ein Waffenlager ausgehoben werden, in dem mehrere Pistolen sichergestellt wurden und das den angeführten Hamas-Mitgliedern zugeordnet werden konnte. Die Mitglieder standen in Kontakt mit

Hamas-Netzwerken in Europa und im Nahen Osten, die für den Kauf und Transport von Waffen zuständig waren. Die in Österreich und Deutschland aktiven Personen könnten die Waffen möglicherweise für Anschläge auf jüdische und israelische Einrichtungen in Europa besorgt haben. Sollten sich diese Vermutungen bestätigen, würde dies einen signifikanten Wandel im Modus Operandi und in der Bedrohung Europas durch die Hamas darstellen.

Legalistischer Islamismus

Im „**Legalistischen Islamismus**“ wird nicht notwendigerweise ausschließlich im Rahmen der bestehenden Rechtsordnung agiert, um islamistische Ideale in Bezug auf jedes Individuum wie auch die Gesellschaft insgesamt umzusetzen. Vertreterinnen und Vertreter des legalistischen Islamismus agieren vorrangig gewaltfrei. Die Haltung der unterschiedlichen Bewegungen zu Gewalt bzw. Gewaltanwendung zur Verfolgung der eigenen Ziele kann aber je nach Zeit und Kontext variieren. Sie kann somit in manchen Kontexten deutlich abgelehnt, in anderen jedoch auch als gerechtfertigt angesehen oder sogar unterstützt werden. Zentrales Mittel im legalistischen Islamismus ist jedoch die Einflussnahme auf Politik und Gesellschaft auf legalem Wege. Es wird eine Langzeitperspektive zur Islamisierung verfolgt, die auf eine generationenübergreifende Veränderung der Gesellschaft und ihrer Ordnung abzielt. Neben dieser langfristigen Gefährdung des liberalen demokratischen Rechtsstaates stellt die angestrebte weitreichende Verbreitung der ideologischen Grundlagen der legalistischen islamistischen Strömungen auch eine kurzfristige Gefahr dar, da diese ebenso ein Nährboden für eine weitere Radikalisierung durch extremere – auch gewaltbereite – Strömungen sein kann.



Vertreterinnen und Vertreter des legalistischen Islamismus agieren primär gewaltfrei und innerhalb des gesetzlich vorgegebenen Rahmens. Auch 2025 versuchten Organisationen des legalistischen Islamismus in Österreich, Einfluss auf Politik und Gesellschaft zu nehmen, indem sie auf wichtige gesellschaftspolitische Schnitt- bzw. Knotenpunkte abzielten. Vor allem der Bildungs- und Erziehungsbereich sowie die Kinder- und Jugendarbeit nimmt für legalistische Islamistinnen und Islamisten eine vorrangige Rolle ein.

Zur Erreichung ihrer Ziele setzen sie auf langfristige Strategien, die sowohl auf das Individuum als auch die gesamte Gesellschaft fokussieren. Zugleich ist diesen Bewegungen jeweils ein Absolutheitsanspruch in Bezug auf die Deutung des Islam inhärent: Die von ihnen vertretene Definition des „wahren Islam“ negiert die innermuslimische Vielfalt bzw. tritt dieser aktiv entgegen.

Eine der bedeutendsten Bewegungen des legalistischen Islamismus in Österreich ist die Muslimbruderschaft (MB). Die MB versuchte im Jahr 2025 weiterhin, Einfluss innerhalb der österreichischen muslimischen Gemeinschaft und in politischen Institutionen zu erlangen und durch ihre generationenübergreifende Strategie die demokratischen Prinzipien und Strukturen zu unterminieren und zu transformieren.

Neben der Muslimbruderschaft waren 2025 im gesamten deutschsprachigen Raum – und damit auch in Österreich – Akteurinnen und Akteure der legalistisch-islamistischen Hizb ut-Tahrir (Partei der Befreiung) sowie salafistischer Organisationen aktiv. Letztere sind in Österreich sowohl online in unterschiedlichen sozialen Medien sowie offline im Zuge von Predigten, Vereinen und Straßen-da'wa (Einladung zum Islam) aktiv.

Organisationen aus dem Spektrum des quietistischen Salafismus erheben den Anspruch, den „wahren Islam“ zu vertreten und Teil der Gemeinschaft der „wahrhaft Gläubigen“ zu sein. Die religiösen Praktiken und die Glaubensauslegung der Mehrheit der Musliminnen und Muslime werden kritisch betrachtet und weitgehend abgelehnt. Erklärtes Ziel des quietistischen Salafismus ist es daher, Musliminnen und Muslime auf den vermeintlich „richtigen Weg“ zurückzuführen. Aufgrund der strengen Glaubensauslegung fokussieren sich quietistische Salafistinnen und Salafisten auf Glaubensfragen und sind bestrebt, diese in der Gesellschaft in Form von da'wa zu verbreiten.



„Da'wa“ bedeutet wörtlich „Einladung zum Islam.“ Seit Anfang der 2000er-Jahre sind salafistische da'wa-Bewegungen im deutschsprachigen Raum in der Missionierungsarbeit aktiv. Lange Zeit wurde die deutschsprachige da'wa-Szene in Österreich durch die salafistische „Lies!“-Kampagne des Vereins Die wahre Religion (DWR) geprägt. Beim Verein Die wahre Religion konnten Berührungspunkte zum jihadistischen bzw. legalistischen Islamismus festgestellt werden. Seit 2016 wurden in Österreich mehrere da'wa-Organisationen gegründet, die in vielen Aspekten die Aktivitäten von DWR weiterführen.

In Österreich sind da'wa-Organisationen aktiv, die zumindest teilweise in global agierende Netzwerke eingebettet sind. Auch 2025 unternahmen Akteurinnen und Akteure österreichischer da'wa-Bewegungen mehrere Initiativen, darunter Vorträge und Predigten, da'wa-Workshops, Infostände (vorwiegend im urbanen Bereich), Bildungsreisen und Retreats sowie Online-da'wa-Trainings. Zudem praktizieren sie einen professionellen Medienauftritt und publizieren regelmäßig Inhalte auf Plattformen wie YouTube, Instagram, TikTok und Facebook. Im Gegensatz zu den Vorgängeraktionen von „Lies!“ werden derzeit keine Koran-Exemplare bei Infoständen verteilt. Die Organisationen versuchen innerhalb des rechtlichen Rahmens zu agieren und ihre Ideologie zu verbreiten. Die Akteurinnen

und Akteure sind zudem in der Regel bemüht, nach außen keine extremistischen Inhalte zu propagieren. Allerdings können immer wieder Bezüge zu extremistischen Strukturen festgestellt werden. Die in Österreich aktiven Bewegungen stehen zumindest teilweise in Verdacht, eine verfassungsfeindliche Ideologie zu vertreten. In der Vergangenheit hatten österreichische FTF vielfach Kontakt zu da'wa-Organisationen, insbesondere im Zuge der „Lies!“-Kampagne. Zudem besteht die Gefahr, dass da'wa-Organisationen in Österreich aufgrund ihrer Organisationsstruktur und ihren breit angelegten Online- und Offline-Aktivitäten als Multiplikatoren einer verfassungsfeindlichen islamistischen Ideologie innerhalb der Gesellschaft fungieren. Der Verfassungsschutz begegnet etwaigen Verdachtslagen mit der Umsetzung von sicherheits-, vereinsbehördlichen oder strafprozessualen Maßnahmen.

2.5.3 Fälle 2025

Fall VILLACH

Am späten Nachmittag des 15. Februar 2025 kam es in der Villacher Innenstadt zu einem Terroranschlag, bei dem eine Person getötet und fünf weitere teilweise schwer verletzt wurden. Der 23-jährige Täter, ein syrischer Staatsbürger, leistete zwei Tage vor dem Anschlag via Videoaufzeichnung einen Treueschwur auf die Terrororganisation IS. Auch wenn der Täter keine strukturelle Einbindung in die Terrororganisation aufwies, kann die Treuebekundung zumindest als Gutheißung der gewaltbefürwortenden IS-Ideologie sowie als Versuch einer Zugehörigkeitserklärung verstanden werden. Die Inspiration für die Durchführung des Anschlags mit einem Messer holte sich der Täter aus einem Propaganda-Video des IS; die Tatwaffe besorgte er sich wenige Tage vor dem Anschlag in einem Geschäft.

Bei der Planung und Durchführung von Anschlägen in Österreich ziehen Täterinnen und Täter zumeist die illegale Anfertigung von Selbstlaboraten für Explosivstoffe oder den illegalen Erwerb von Schusswaffen in Betracht. Aufgrund der schwierigen Herstellung bzw. des hindernisreichen Erwerbs von Explosivstoffen/Schusswaffen wird schlussendlich aber zumeist auf Hieb- und Stichwaffen zurückgegriffen.

Dem couragierten Eingreifen eines Zeugen – ebenfalls ein syrischer Staatsbürger – war es zu verdanken, dass der Angreifer nach kurzer Zeit gestoppt wurde. Der Zeuge nahm das Messerattentat wahr und machte den Täter durch einen gezielten Zusammenstoß mit seinem Kraftfahrzeug handlungsunfähig. Etwa sechs Minuten nach Beginn der Tathandlung konnte der Täter durch ersteinschreitende Beamtinnen und Beamte des Stadtpolizeikommandos Villach festgenommen und die Tatwaffe sichergestellt werden.

Der Radikalisierungsprozess des Täters kann als kurz, intensiv und repräsentativ beschrieben werden: Aufgewachsen in einem nichtreligiösen Umfeld in Syrien, begann er im Jahr 2024 und mittlerweile wohnhaft in Europa, sich erstmals eindringlicher mit dem Islam zu beschäftigen. Über diverse Internetseiten und soziale Netzwerke versuchte



der Betroffene, Antworten auf religiöse Fragen zu finden und tat dies schlussendlich auf den Propagandaseiten des IS. Ansprachen ehemaliger Führungspersonlichkeiten der Terrororganisation sowie gewaltbefürwortender Sprechgesang (sogenannter „anashid“) spielten die tragende Rolle bei der emotionalen und ideologischen Vorbereitung auf den Terroranschlag. Die Wahrnehmung des Täters, dass physische Gewalt gegen vermeintliche Feinde des Islams eine religiöse Pflicht sei, dürfte durch die Konsumation ebenjener Propaganda gefördert worden sein. Schriftliche Aufzeichnungen, die der Täter einige Wochen vor dem Anschlag anfertigte, beinhalteten ausgeprägte Gewaltfantasien und zeigten eine intensive Beschäftigung mit „Geisterwesen“.

Der rasante Radikalisierungsprozess des Attentäters von Villach steht paradigmatisch für die Radikalisierungsverläufe zahlreicher Personen in Österreich, gegen die gegenwärtig wegen Terrorismusverdachts ermittelt wird: Wenig ideologische Festigung, dafür aber eine starke Gewaltbereitschaft, gepaart mit weiteren förderlichen Radikalisierungsfaktoren, prägen – wie auch die weiteren Fallbeispiele zeigen – häufig die Vita von Jugendlichen und jungen Erwachsenen. Dieses Leitmotiv propagiert und instrumentalisiert der IS gleichermaßen und wirkt auf die islamistisch-extremistische Szene in Österreich fortlaufend besonders anziehend.

Fall WESTBAHNHOF

Aufgrund der Veröffentlichung von Terrorpropaganda gelangte Ende 2024 ein TikTok-Profil in den Fokus des österreichischen Verfassungsschutzes. Nach Ausforschung des Profilbetreibers – ein zum Tatzeitpunkt 15-jähriger Österreicher – und einer darauffolgenden Hausdurchsuchung im Februar 2025 bestätigte sich der Verdacht einer jihadistischen und damit gewaltbefürwortenden Einstellung des Täters: Der junge Mann hegte intensiven Hass auf Un- bzw. Andersgläubige und plante im Namen des IS einen Anschlag auf den Wiener Westbahnhof. Der Fund von Anleitungen zur Sprengstoffherstellung und von Utensilien für den Bau einer Rohrbombe verdeutlichten die Ernsthaftigkeit der Anschlagpläne und die Unmittelbarkeit der Tatumsetzung.

Sowohl in Bezug auf die Vita als auch auf den Radikalisierungsverlauf sind Parallelen zwischen dem Attentäter von Villach und dem Jugendlichen aus Wien festzustellen: das (Wieder-)Entdecken islamischer Werte in Österreich und deren einseitige Interpretation, ein kurzer und intensiver Radikalisierungsverlauf, der primäre Fokus auf Schriften und „anashid“, welche die Ablehnung und Bekämpfung von „Islamfeinden“ thematisieren, sowie die vermeintliche Erfüllung durch Umsetzung der IS-Ideologie.

Im Gegensatz zum Attentäter von Villach war der radikalisierte Jugendliche von Wien jedoch sowohl virtuell als auch realweltlich stark in der islamistisch-extremistischen Szene vernetzt. Das verbindende Element der Peer-Group: der gemeinsame Hass auf Personen, die von der eigenen Weltanschauung abweichen.

„Falsche“ Musliminnen und Muslime (d. h. unislamische Herrscher oder sogar die eigene Familie), Andersgläubige und sogar der gesamte Westen werden dabei gleichermaßen zum einenden Feindbild erklärt. Die Umsetzung der Gewaltbereitschaft gegen diese Feindbilder verschafft Anerkennung und erhöht den Status innerhalb der Peer-Group. Die Gewaltideologie des IS fungiert in diesem Rahmen als identitätsstiftendes Merkmal. Sogenannte „virtuelle Plotter“, die eine tatsächliche Einbindung in IS-Netzwerke aufweisen oder vortäuschen, zielen auf radikalisierte Jugendliche und junge Erwachsene ab und leiten diese bei der Beschaffung von Waffen und der konkreten Tatausführung an. So auch im Falle des Betroffenen, der einen Anschlag auf den Westbahnhof plante: Via Messenger-Dienst tauschte er sich mit einem vermeintlichen ISKP-Mitglied über den Modus Operandi eines möglichen Terroranschlags aus.

Im Juni 2025 wurde der Täter unter anderem wegen der Vorbereitung einer terroristischen Straftat und der Mitgliedschaft in einer terroristischen Vereinigung zu einer teilbedingten Haftstrafe von 24 Monaten verurteilt.

Im November 2025, etwa einen Monat nach seiner bedingten Entlassung, griff der Jugendliche seine Pläne erneut auf: So erkundigte er sich zusammen mit einer weiteren Person in einem Geschäft über den Erwerb von Schusswaffen; darüber hinaus wurden ein Messer und Einsatzhandschuhe erworben. Die Durchsicht des Mobiltelefons des jungen Österreicher zeigte u. a. zahlreiche Web-Suchverläufe zu terroristischen Anschlägen und zur Herstellung von Explosivstoffen. Der Beschuldigte wurde erneut festgenommen und die Untersuchungshaft über ihn verhängt.

Fall AUSREISE

Im Jänner 2024 erging der Hinweis an den österreichischen Verfassungsschutz, dass ein stark radikalisierte junger Erwachsener aus Österreich den Anschluss an die Terrororganisation Hamas im Gazastreifen plane, um sich dort an Kampfhandlungen zu beteiligen.

Nach Umsetzung strafprozessualer Maßnahmen konnte im Zuge der Auswertung von Datenträgern ein bereits gebuchter Flug von Wien nach Tel Aviv (Israel) festgestellt werden. Aufgrund des fehlenden Rückflug-Tickets wurde die Flugreise von der zuständigen Airline selbstständig storniert.

Wenige Monate nach den fehlgeschlagenen Ausreisebestrebungen äußerte der Betroffene in einer Moschee im Beisein eines Zeugen die Drohung, vom „wahren“ Islam abtrünnige Personen – womit er sich auf die Moschee-Besucher bezog – töten zu wollen. In der darauffolgenden Beschuldigtenvernehmung drohte der junge Mann den Beamtinnen und Beamten damit, sie umzubringen. Zudem erklärte er, dass das Töten von Polizisten schon seit Längerem sein Ziel gewesen wäre. Im Zuge der Festnahme leistete der Betroffene aktiven Widerstand gegen die Amtshandlung und verletzte dabei einen Polizeibeamten.

Der zum Tatzeitpunkt 21-jährige Österreicher war im Jahr 2023 zum Islam konvertiert und stammt – wie auch die zuvor beschriebenen Einzeltäter – aus einem nicht-religiösen Elternhaus. Während sich der Betroffene anfangs nur oberflächlich mit der Religion befasste, übernahm er ab 2024 zunehmend extremistische Elemente, die den gewaltvollen Jihad als religiöse Pflicht befürworten. Der Betroffene dürfte dabei eher von einem jihadistischen Narrativ als von einer einzelnen Terrororganisation geprägt worden sein. Die positive Bezugnahme sowohl auf die Hamas als auch auf den IS und al-Qaida scheint trotz der realweltlichen Feindschaft zwischen diesen Terrororganisationen für den Betroffenen keinen Widerspruch dargestellt haben.

Der Hass des jungen Mannes richtete sich primär gegen andersdenkende Musliminnen und Muslime sowie Ungläubige. Sowohl die eigenen Eltern als auch bekannte salafistische Influencer-Prediger wurden wegen seiner Ansicht nach fehlenden bzw. verwässerten Islambekenntnisses zu Feinden des Islams deklariert, die es zu töten gilt.

Hervorzuheben ist weiters die beim Täter diagnostizierte psychische Beeinträchtigung sowie sein prädelinquentes (Vor-)Verhalten – zwei Faktoren, die Einfluss auf das Radikalisierungsgeschehen nehmen können und gegenwärtig bei Personen mit Bezug zum islamistischen Extremismus in Österreich vermehrt wahrgenommen werden.

Ein ausgeprägter Zusammenhang zwischen terroristischer Gewalt und psychischen Auffälligkeiten findet sich insbesondere bei Einzeltäterinnen und Einzeltätern sowie Kleinstgruppen, weil größere organisierte Gruppen von solchen Personen tendenziell Abstand nehmen.

Im Juni 2025 wurde der junge Erwachsene unter anderem wegen Mitgliedschaft in einer terroristischen Vereinigung, schwerer Nötigung und Widerstand gegen die Staatsgewalt schuldig gesprochen. Aufgrund eines psychiatrischen Gutachtens wurde er als nicht zurechnungsfähig beurteilt und in einem forensisch-therapeutischen Zentrum untergebracht.

2.5.4 Trends und Entwicklungstendenzen

2025 war in Österreich das Risiko in Bezug auf islamistisch motivierte Gewalt permanent erhöht. Aufgrund der angespannten Lage im In- und Ausland wird dieses Gefahrenpotenzial in Österreich mit hoher Wahrscheinlichkeit kurz- bis mittelfristig erhöht bleiben. Die Gefahrenlage sowie die damit einhergehende Risikostufe werden fortwährend von nationalen und internationalen Entwicklungen beeinflusst und bedürfen daher einer kontinuierlichen Evaluierung und Bewertung.

Das Jahr 2025 bestätigte für ganz Europa den Trend zu Terroranschlägen, die von Einzeltätern mit einfach zu beschaffenden Tatmitteln durchgeführt werden. Auch der Terroranschlag in Villach fiel in dieses Schema. Darüber hinaus ist davon auszugehen,

dass der IS in den kommenden Jahren gezielt zu Gewalthandlungen durch Einzelpersonen aufrufen wird. Gleichzeitig sind komplexere Attentate für die Terrororganisationen weiterhin erstrebenswert und bleiben folglich eine realistische Gefahr. Dies zeigt sich auch deutlich darin, dass im Berichtsjahr innerhalb der österreichischen radikal-islamistischen Szene ein reges Interesse an Schusswaffen, Sprengstoffen und Drohnen erkennbar war. Außerdem besteht die realistische Gefahr, dass jihadistische Akteurinnen und Akteure in Österreich und Europa zukünftig vermehrt auf neue Technologien für Anschläge zurückgreifen könnten. Bereits 2025 gab es in Europa Versuche, Anschläge mittels Drohnen durchzuführen. Auch für Österreich besteht die Möglichkeit, dass sich eine derartige Bedrohungslage manifestieren könnte, um großangelegte Anschläge umzusetzen.

2025 konnten in Österreich mehrere IS-Radikalisierungsnetzwerke festgestellt werden. Die Anzahl der jungen IS-Anhängerinnen und IS-Anhänger in Österreich wächst, was unter anderem auf die proaktiven Rekrutierungsstrategien etablierter IS-Anhängerinnen und IS-Anhänger zurückzuführen ist. Die Radikalisierung findet unter anderem über diverse Online-Plattformen statt, um neue Anhängerinnen und Anhänger zu rekrutieren. Für das Jahr 2026 besteht die hohe Wahrscheinlichkeit, dass dieses Wachstum aufgrund des Fokus auf die Rekrutierung von Jugendlichen und jungen Erwachsenen anhalten wird. Zudem besteht die realistische Möglichkeit, dass es zu Ausreisebewegungen und Anschlägen aus Radikalisierungsnetzwerken heraus kommen wird.

In den letzten Jahren wurde deutlich, dass Radikalisierungsprozesse innerhalb des islamistischen Extremismus und Terrorismus sowohl junge Männer als auch junge Frauen umfassen. Die weiblichen Extremistinnen sind vielfach hochradikalisiert und befürworten teilweise Gewalt. Obwohl Frauen vorwiegend in der Verbreitung von terroristischer Propaganda involviert sind, gab es in der Vergangenheit vereinzelt auch Anschläge von weiblichen IS-Anhängerinnen in Österreich. Daher kann nicht ausgeschlossen werden, dass Frauen in den kommenden Jahren neben der Verbreitung von Propaganda und der Durchführung von Ausreisen auch vermehrt in Anschlägen involviert sein könnten.

Des Weiteren sind auch legalistische islamistische Organisationen federführend in der Kinder- und Jugendarbeit aktiv und versuchen, ihre Ideen auf diesem Wege schrittweise innerhalb der Gesellschaft zu verbreiten. Dieses Phänomen besteht seit vielen Jahren und wird mit hoher Wahrscheinlichkeit auch 2026 fortbestehen.

Die Bedeutung der regionalen IS-Ableger ändert sich stetig und ist vielfach von geopolitischen wie auch regionalen Entwicklungen abhängig. Es ist wahrscheinlich, dass die Ableger in Pakistan, Afghanistan und Somalia in den kommenden Jahren weiterhin eine wichtige Rolle spielen werden. Obwohl der ISKP im Vergleich zum Jahr 2024 derzeit geschwächt ist, nimmt er nach wie vor eine zentrale Rolle in der Planung von internationalen Anschlägen ein und besitzt daher auch immer noch eine hohe Anziehungskraft auf hochradikalisierte IS-Anhängerinnen und IS-Anhänger. Die Bedrohung durch den ISKP

wird mit großer Wahrscheinlichkeit auch 2026 anhalten. Vor allem besteht die Gefahr, dass der ISKP seine Anhängerinnen und Anhänger zu weiteren Anschlägen in Europa anstiften wird. Eine derartige Anstiftung könnte 2026 sowohl durch direkten Kontakt mit IS-Anhängerinnen und IS-Anhängern als auch durch ISKP-Propaganda erfolgen. Die Bedeutung des IS-Ablegers in Somalia könnte im kommenden Jahr zunehmen, sollte sich herausstellen, dass der Leiter des IS in Somalia, Abd al-Qadir Mumin, tatsächlich der neue Kalif des IS ist.

Neben dem IS, insbesondere dem ISKP, war im Berichtsjahr auch der al-Qaida-Ableger AQAP in der Produktion von Propaganda aktiv. Die Propaganda von ISKP und AQAP umfasste unter anderem Aufrufe zu Anschlägen durch Einzelpersonen in Europa. Es ist wahrscheinlich, dass diese Organisationen ihre Medienstrategie auch in absehbarer Zukunft weiterverfolgen und Anhängerinnen und Anhänger zu Ausreisen und Anschlägen anstiften werden. Zudem ist anzunehmen, dass IS-Anhängerinnen und IS-Anhänger in Österreich wie im gesamten deutschsprachigen Raum auch in Übersetzungstätigkeiten für inoffizielle und offizielle IS-Medien involviert sein werden. Insgesamt wird die Bedrohungslage durch inspirierte oder angeleitete Einzeltäter in Österreich auch für das Jahr 2026 als hoch eingestuft.

Im März 2025 fanden die ersten Repatriierungen von zwei weiblichen FTF mit ihren Kindern aus Syrien nach Österreich statt. In den kommenden Jahren werden mit großer Wahrscheinlichkeit weitere Familien nach Österreich repatriiert werden. Im Falle weiterer Repatriierungen bedarf es verstärkter gesamtgesellschaftlicher Anstrengungen zur effektiven und nachhaltigen Eingliederung und Integration der betroffenen Personen.

Ein im Jahr 2024 aus Österreich ausgereister IS-Anhänger verübte im Jahr 2025 einen Anschlag in Pakistan. Innerhalb der österreichischen Szene war auch im Berichtsjahr ein hohes Interesse an Ausreisen evident, wobei vor allem der IS in Pakistan und in Somalia hohe Anziehungskraft hatten. Dies ist unter anderem auch auf die zentrale Rolle des ISKP in der Produktion von mehrsprachiger Propaganda in Form von Videos, Magazinen und Postern zurückzuführen. Es besteht die realistische Möglichkeit, dass es 2026 zu weiteren Ausreiseversuchen aus Österreich und Europa kommen wird.

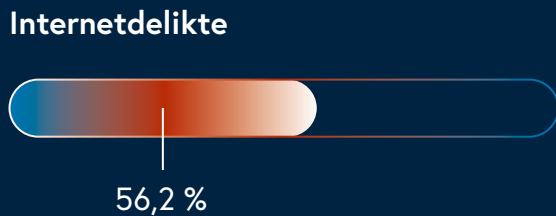
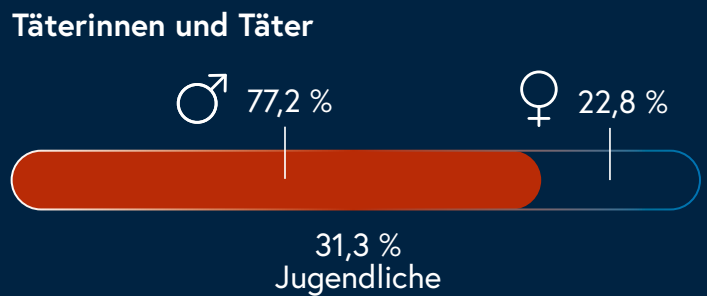
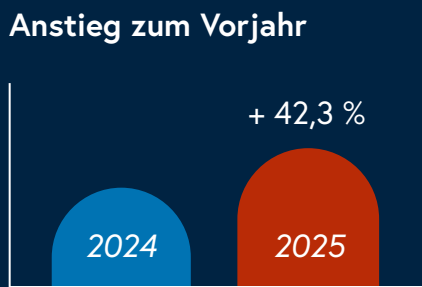
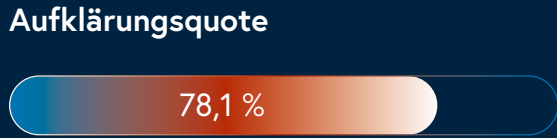
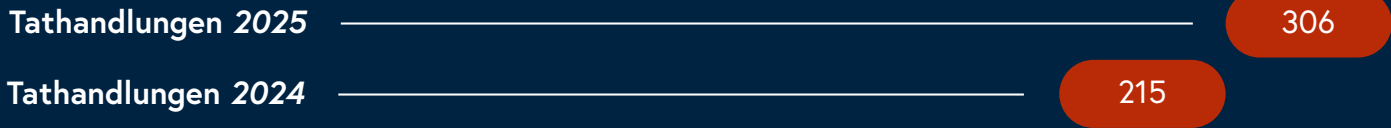
Angesichts der im Berichtsjahr erstmals in Österreich und Deutschland enttarnten Waffendepots der Terrororganisation Hamas, die möglicherweise in Zusammenhang mit Anschlagplänen auf jüdische und israelische Einrichtungen stehen, muss von einem signifikanten Wandel im Modus Operandi der Hamas hin zur Gewaltanwendung und der Durchführung von Anschlägen außerhalb von Israel ausgegangen werden. In welcher Form in den kommenden Jahren von der Hamas eine konkrete terroristische Bedrohung für Österreich ausgehen könnte, wird vom Verfassungsschutz laufend geprüft.

Künstliche Intelligenz wird in den kommenden Jahren von islamistischen und terroristischen Organisationen mit großer Wahrscheinlichkeit vermehrt zur Produktion von Propaganda genutzt werden. So besteht die Gefahr, dass KI zur Erstellung von Deepfakes sowie zur Unterstützung in der Planung diverser Aktivitäten verwendet werden wird. Das Potenzial der KI besteht sowohl für legalistische als auch für jihadistische Islamistinnen und Islamisten. Für Letztere könnte KI eine wesentliche Rolle bei der Vorbereitung von Anschlägen einnehmen. Ein Beispiel hierfür sind bereits getätigte Versuche, KI für die Erstellung von Bombenbauanleitungen zu nutzen. Die Herausforderungen durch KI sind vielfältig und werden die österreichischen Sicherheitsbehörden in den kommenden Jahren verstärkt beschäftigen.

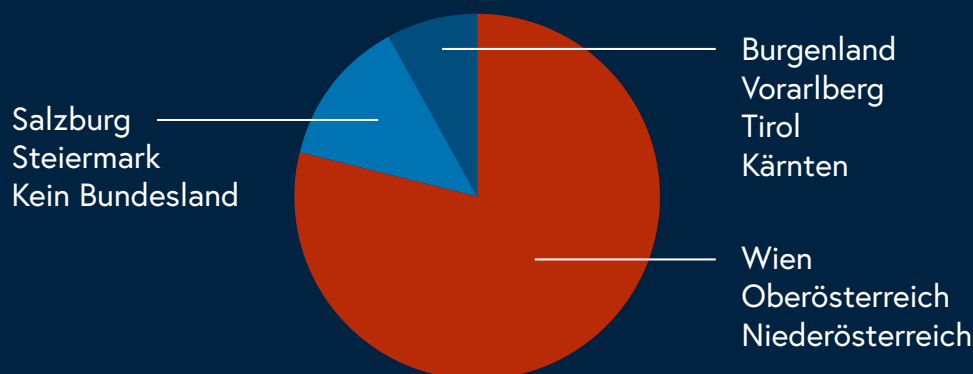
Bewegungen und Organisationen im Bereich des legalistischen Islamismus stellen vor allem langfristig eine Gefahr für die liberal-pluralistische Demokratie dar. Sie sind bestrebt, Normen und politische Grundlagen aufzuweichen und Menschenrechte durch die Verbreitung verfassungsfeindlicher Ideologien auszuhöhlen bzw. zu beschneiden. Personen und Vereine aus dem Umfeld der Muslimbruderschaft verfolgen in Österreich zudem das Ziel, Einfluss auf wesentliche politische und gesellschaftliche Institutionen zu nehmen, um so langfristig eine Transformation der Gesellschaft herbeizuführen. Diese Bedrohung konnte in Österreich schon 2025 festgestellt werden – und dies nicht nur von Seiten der legalistischen Muslimbruderschaft, sondern auch verschiedener salafistischer Organisationen sowie der Hizb ut-Tahrir. Dieses Gefahrenpotenzial wird mit hoher Wahrscheinlichkeit auch in den kommenden Jahren bestehen.



Islamistischer Extremismus und Terrorismus



Bundesländeraufteilung



2.5.5 Zahlen/Daten/Fakten

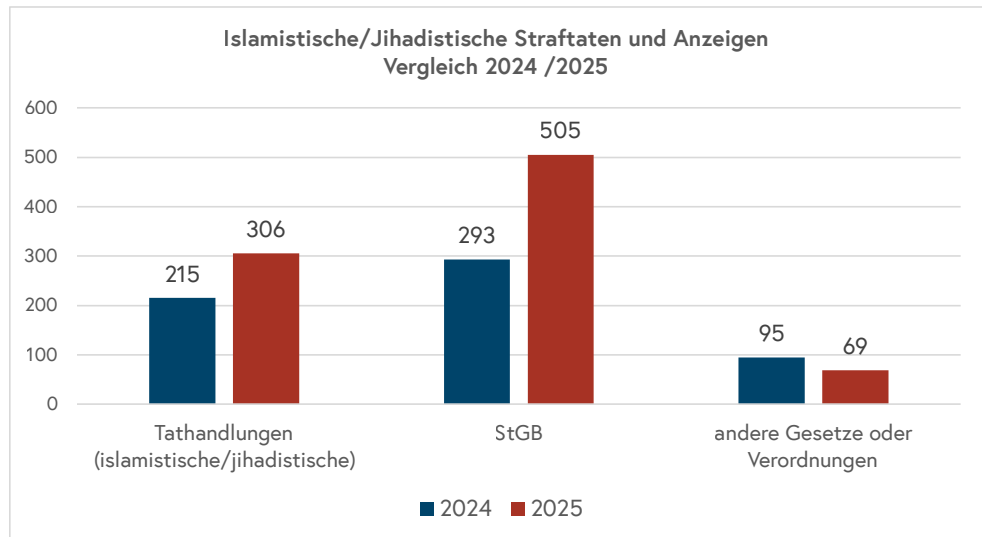
Im Jahr 2025 wurden den Sicherheitsbehörden in Österreich im Phänomenbereich **islamistischer Extremismus und Terrorismus** insgesamt **306 Tathandlungen** mit einer islamistischen/jihadistischen Motivlage bekannt. Gegenüber dem Jahr 2024 (215 Tathandlungen) bedeutet dies einen **Anstieg um 42,3 Prozent**. 239 Tathandlungen (**78,1 Prozent**) wurden **aufgeklärt** (Aufklärungsquote 2024: 84,2 Prozent – 181 Tathandlungen).

Im Zusammenhang mit den angeführten Tathandlungen wurden 2025 bundesweit insgesamt **574 Delikte** zur Anzeige gebracht, das sind **um 47,9 Prozent mehr** als im Jahr 2024 (388 Delikte). Von den 574 Delikten waren 505 nach dem Strafgesetzbuch (2024: 293) strafbar. 69 Anzeigen erfolgten nach anderen Gesetzen und Verordnungen (2024: 95).

Insgesamt konnten **272 Tatverdächtige** ausgeforscht und zur Anzeige gebracht werden (2024: 202). Dabei handelt es sich um 210 (77,2 Prozent) männliche und 62 (22,8 Prozent) weibliche Personen (2024: 118 männliche, 84 weibliche). Unter den Beschuldigten befinden sich 85 Jugendliche (2025: 31,3 Prozent; 2024: 88 bzw. 43,6 Prozent). 115 (42,3 Prozent) der Beschuldigten besitzen die österreichische Staatsbürgerschaft (2024: 106, 52,5 Prozent). Neben den ausgeforschten Personen erfolgten im Berichtsjahr **71 Anzeigen** gegen **unbekannte Täterinnen oder Täter** (2024: 43).

Bei **172** (56,2 Prozent) der insgesamt 306 **Tathandlungen** fand die strafbare Handlung im **Internet**, hier vor allem in den Sozialen Medien und Messenger-Diensten, statt. Die Aufklärungsquote lag bei 76,7 Prozent (132 Tathandlungen). Im Jahr 2024 lag der Anteil der Internetdelikte der insgesamt 215 Tathandlungen bei 37,2 Prozent (80 Tathandlungen), bei einer Aufklärungsquote von 81,3 Prozent (65 Tathandlungen).

Im Zusammenhang mit der Bekämpfung islamistischer/jihadistischer Aktivitäten wurden im Jahr 2025 in Österreich insgesamt **129 Hausdurchsuchungen** (inkl. freiwilliger Nachschauen) (2024: 68) durchgeführt und **40 Festnahmen** (2024: 26) vollzogen.



Zu einem **Anstieg** kam es unter anderem bei den Anzeigen wegen Körperverletzung gemäß § 83 StGB (3 auf 6), wegen Gefährlicher Drohung gemäß § 107 StGB (20 auf 42), wegen Landzwang gemäß § 275 StGB (3 auf 10), wegen Krimineller Organisation gemäß § 278a StGB (66 auf 143), dem Delikt der Terroristischen Vereinigung gemäß § 278b StGB (117 auf 201), wegen Terroristischer Straftaten gemäß § 278c StGB (2 auf 5), wegen Terrorismusfinanzierung gemäß § 278d (3 auf 11), dem Delikt Reisen für terroristische Zwecke gemäß § 278g StGB (1 auf 4), wegen Aufforderung zu mit Strafe bedrohten Handlungen und Gutheißung mit Strafe bedrohter Handlungen gemäß § 282 StGB (3 auf 5) sowie dem Delikt der Aufforderung zu terroristischen Straftaten und Gutheißung mit Strafe bedrohter Handlungen gemäß § 282a StGB (10 auf 25), wegen Verhetzung gemäß § 283 StGB (7 auf 13), Anzeigen gemäß § 50 Waffengesetz (4 auf 18) und dem Symbole-Gesetz (3 auf 4).

Zu einem **Rückgang** kam es bei den Anzeigen wegen Mordes gemäß § 75 StGB (4 auf 3), wegen Schwerer Körperverletzung gemäß § 84 StGB (5 auf 1), wegen Nötigung gemäß § 105 StGB (3 auf 1), wegen Schwerer Nötigung gemäß § 106 StGB (7 auf 2), wegen Sachbeschädigung gemäß § 125 StGB (18 auf 15) und dem Anti-Gesichtsverhüllungs-gesetz (68 auf 37).

Anzeigen nach dem StGB	2024	2025
Mord (§ 75 StGB) oder (§ 75 StGB iVm. § 15 StGB ⁵⁰)	4	3 ⁵¹
Körperverletzung (§ 83 StGB)	3	6
Schwere Körperverletzung (§ 84 StGB)	5	1
Erpresserische Entführung (§ 102 StGB)	0	1
Nötigung (§ 105 StGB)	3	1
Schwere Nötigung (§ 106 StGB)	7	2
Gefährliche Drohung (§ 107 StGB)	20	42
Hausfriedensbruch (§ 109 StGB)	0	3
Sachbeschädigung (§ 125 StGB)	18	15
Schwerer Diebstahl (§ 128 StGB)	0	2
Unterschlagung (§ 134 StGB)	0	1
Schwerer Raub (§ 143 StGB)	1	1
Schwere Erpressung (§ 145 StGB)	0	1
Widerstand gegen die Staatsgewalt (§ 269 StGB)	2	3
Landzwang (§ 275 StGB)	3	10
Verbrecherisches Komplott (§ 277 StGB)	1	3
Kriminelle Organisation (§ 278a StGB)	66	143
Terroristische Vereinigung (§ 278b StGB)	117	201
Terroristische Straftaten (§ 278c StGB)	2	5
Terrorismusfinanzierung (§ 278d StGB)	3	11
Reisen für terroristische Zwecke (§ 278g StGB)	1	4
Aufforderung zu mit Strafe bedrohten Handlungen und Gutheißung mit Strafe bedrohter Handlungen (§ 282 StGB)	3	5
Aufforderung zu terroristischen Straftaten und Gutheißung terroristischer Straftaten (§ 282a StGB)	10	25
Verhetzung (§ 283 StGB)	7	13
Falsche Beweisaussage (§ 288 StGB)	1	1
Verleumdung (§ 297 StGB)	0	1

50 Mordversuch (§ 75 StGB i. V. m. § 15 StGB) betraf Fälle aus dem Jahr 2024.

51 Am 15. Februar 2025 attackierte ein syrischer Staatsbürger in Villach, Kärnten, wahllos Personen mit einem Klappmesser, wobei eine Person getötet wurde und weitere fünf Personen teils schwer verletzt wurden.

In Niederösterreich steht ein inhaftierter syrischer Staatsbürger in Verdacht, in Syrien als Mitglied des IS andere Menschen getötet und vergewaltigt zu haben.

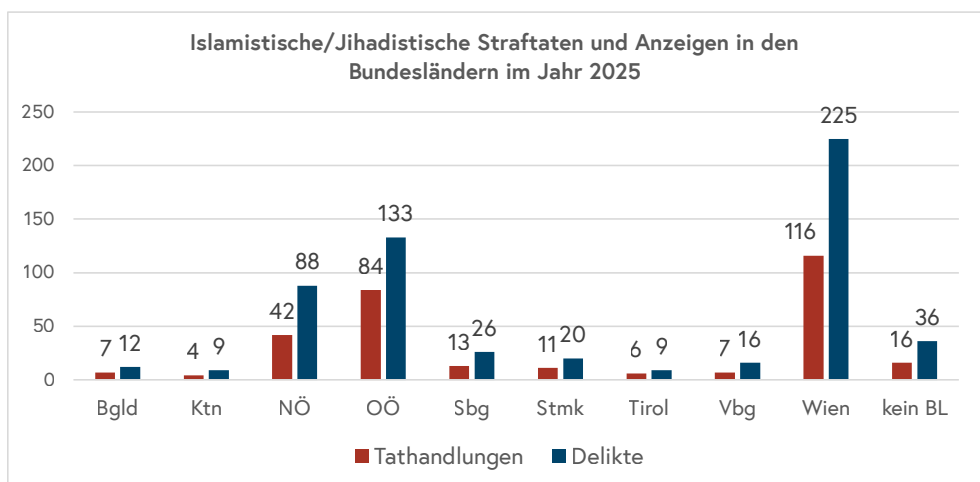
In Wien wird einem syrischen Staatsbürger die Mitgliedschaft in einer terroristischen Organisation, welche der „Jabhat al-Nusra“-Front zugeordnet wird, vorgeworfen. Es erfolgten Anzeigen wegen Mordes, Erpresserischer Entführung und den Delikten der Kriminellen Organisation und Terroristischen Vereinigung.

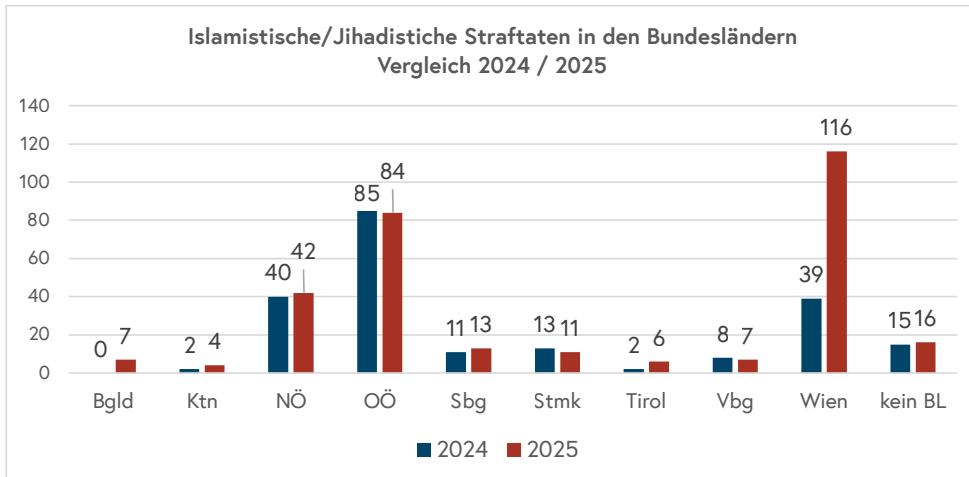
Vortäuschung einer mit Strafe bedrohten Handlung (§ 298 StGB)	0	1
Sonstige StGB Delikte	16	0

Anzeigen nach anderen Gesetzen oder Verordnungen

§ 13 Waffengesetz (WaffG)	0	1
§ 50 Waffengesetz (WaffG)	4	18
§ 51 Waffengesetz (WaffG)	1	1
Symbole-Gesetz (SG)	3	4
Abzeichengesetz (AbzG)	0	2
Anti-Gesichtsverhüllungsgesetz (AGesVG)	68	37
§ 7 Kriegsmaterialgesetz (KMG)	0	1
§ 27 Suchtmittelgesetz (SMG)	1	1
Versammlungsgesetz (VersG)	4	4
Sonstige Gesetze oder Verordnungen	14	0
Summe	388	574

Von den 306 islamistisch/jihadistisch motivierten Tathandlungen fanden die meisten im Bundesland Wien (37,9 Prozent) statt, gefolgt von Oberösterreich (27,5 Prozent), Niederösterreich (13,7 Prozent), Salzburg (4,2 Prozent), der Steiermark (3,6 Prozent), Burgenland und Vorarlberg (je 2,3 Prozent), Tirol (2 Prozent) und Kärnten (1,3 Prozent). 5,2 Prozent der Tathandlungen konnten keinem Bundesland zugeordnet werden.





In Zusammenhang mit dem **Nahostkonflikt** wurden bundesweit **neun Tathandlungen** mit einer islamistischen/jihadistischen Motivlage registriert (2024: 11).

Im Rahmen dieser Tathandlungen wurden Anzeigen wegen Sachbeschädigung gemäß § 125 StGB, dem Delikt der Schweren Erpressung gemäß § 145 StGB, nach den Delikten der Kriminellen Organisation gemäß § 278a StGB und der Terroristischen Vereinigung gemäß § 278b StGB, dem Delikt der Aufforderung zu mit Strafe bedrohten Handlungen und Gutheißung mit Strafe bedrohter Handlungen gemäß § 282 StGB, wegen Verhetzung gemäß § 283 StGB und nach dem Versammlungsgesetz erstattet.

2.6 Spionage und nachrichtendienstliche Aktivitäten

Der Phänomenbereich „**Spionage und nachrichtendienstliche Aktivitäten**“ beschreibt die Bearbeitung und Aufklärung von staatlichen nachrichtendienstlichen und geheimdienstlichen Handlungen, die einen Nachteil für das betroffene Land bzw. einen Vorteil für die Auftragsnation zur Folge haben können.

2.6.1 Überblick

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

Speziell der letztgenannte Aspekt hat eine hohe Dichte an diplomatischen Einrichtungen und Personal anderer Staaten in Österreich zur Folge. Dies ermöglicht es, sogenannte

„legal abgedeckte Residenturen“, also Botschaften und Generalkonsulate mit verdeckt nachrichtendienstlich agierendem, diplomatischem Personal, einzurichten. In diesem Kontext sind auch halboffizielle Vertretungen, wie beispielsweise Niederlassungen von Fluggesellschaften oder Presseagenturen, die als Tarnung für Spionageaktivitäten genutzt werden, zu nennen.

In Österreich besonders aktiv sind die Nachrichtendienste Russlands, Chinas und des Iran. Ihre Aktivitäten können in unterschiedlichsten Bereichen und auf verschiedensten Ebenen erfolgen, insbesondere im Zuge von Spionage (gegen Österreich wie auch andere Staaten), Einfluss- und Desinformationskampagnen und gezielten Cyberangriffen.

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 Akteure zudem aktive Maßnahmen geheim-/nachrichtendienstlichen Charakters durch, wie beispielsweise Cybersabotage oder Informationsoperationen. Zusätzlich zu diesen nachrichtendienstlichen Kernaufgaben gibt es Überschneidungen zu Cyberkriminellen und Haktivistinnen bzw. Haktivisten. Zu den Tätigkeiten klassischer Cyberkrimineller zählen Angriffe auf Computersysteme, z. B. Ransomware-Angriffe⁵². Die Entwicklungen im Bereich der Digitalisierung, die mittlerweile sämtliche Lebensbereiche betreffen, verstärken das Risiko, das von Cyberkriminellen und insbesondere von nachrichtendienstlichen 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.

Mit den geltenden Straftatbeständen der §§ 256 StGB und 319 StGB, die an eine Tätigkeit fremder Geheim- und Nachrichtendienste im Bundesgebiet anknüpfen, kann aus derzeitiger Sicht nicht das Auslangen gefunden werden. Erkenntnisse aus der Praxis, die unter anderem auch auf zahlreichen Einstellungsbeschlüssen der Staatsanwaltschaft gründen, zeigen, dass vor allem das objektive Tatbestandselement „zum Nachteil der Republik Österreich“ eine Herausforderung darstellt. Um dem entgegenzuwirken, veröffentlichte das Bundesministerium für Justiz, unvorgreiflich der unabhängigen Rechtsprechung, am 18. Dezember 2024 einen Erlass zur Auslegung des Begriffs „zum Nachteil der Republik Österreich“.

52 Ransomware-Angriffe sind Angriffe auf Computersysteme, meist mit dem Ziel durch Erpressung finanzielle Mittel zu lukrieren.

2.6.2 Aktuelle Lage

Russland

Allgemeine Vorgehensweise russischer Nachrichtendienste

Zusammenfassend ist festzustellen, dass Russland auch im Jahr 2025 ein Hauptakteur im Zusammenhang mit Spionage und Einflussnahme in und gegen Österreich war.

Im Verlauf des Berichtsjahres blieben die Spannungen zwischen Europa und Russland hoch. Diese Entwicklung ist einerseits auf den anhaltenden russischen Angriffskrieg gegen die Ukraine, andererseits auf vermehrte feindliche Aktivitäten Russlands, insbesondere durch Spionage, Sabotage und Desinformation, gegenüber europäischen Staaten zurückzuführen. Russland sieht sich in einem anhaltenden systemischen Konflikt mit „dem Westen“, dem auch Österreich angehört. Entsprechend befindet sich Österreich seit 2022 auf der russischen Liste „unfreundlicher Staaten“.

Russlands Nachrichtendienste spielen bei der Erreichung der strategischen und geopolitischen Ziele des Staates eine maßgebliche Rolle. Mithilfe unterschiedlicher Methoden verfolgen sie vor allem das Ziel, politische und gesellschaftliche Prozesse in westlichen Staaten zum Vorteil Russlands zu beeinflussen und Informationen aus relevanten Bereichen zu gewinnen. Weitere wesentliche Ziele sind die Destabilisierung des europäischen Zusammenhalts und der Einheit und Handlungsfähigkeit der NATO sowie die Abschwächung oder völlige Verhinderung der europäischen Unterstützung für die Ukraine.

Die russischen Spionageaktivitäten in Österreich stehen im Einklang mit diesen übergeordneten geopolitischen Zielsetzungen des Kremls und spiegeln zugleich die strategische Relevanz wider, die Österreich als EU-Mitglied und NATO-Partnerland einnimmt. Demzufolge sind die Bereiche Politik, Wirtschaft, Wissenschaft und Militär Aufklärungsziele für russische Nachrichtendienste in Österreich. Des Weiteren versucht Russland, mittels Beeinflussungsoperationen das Vertrauen der österreichischen Bevölkerung in die Handlungsfähigkeit sowohl der österreichischen als auch der europäischen politischen Entscheidungsträgerinnen und Entscheidungsträger zu unterminieren.

Österreich ist zudem auch aufgrund seiner geografischen Lage und seiner Rolle als Sitzstaat von rund 50 internationalen und quasi-internationalen Organisationen für die russischen Nachrichtendienste von zentraler Bedeutung. Dies spiegelt sich in den nachrichtendienstlichen Aktivitäten Russlands auf dem österreichischen Staatsgebiet wider. Die russischen Nachrichtendienste nutzen sowohl die bilateralen Vertretungsbehörden Russlands als auch die internationalen Organisationen in Österreich zum Zwecke nachrichtendienstlicher Tätigkeiten.

Darüber hinaus richten sich die Aktivitäten russischer Nachrichtendienste schon seit vielen Jahren auf die Überwachung russischer Dissidentinnen und Dissidenten bzw. russlandkritischer Akteurinnen und Akteure in europäischen Staaten. Zudem steht die

russische Diaspora mit ihren gesellschaftlichen und politischen Aktivitäten in Europa und Österreich unter Beobachtung der russischen Nachrichtendienste.



Die wesentlichen **nachrichtendienstlichen Akteure Russlands** sind der zivile russische Auslandsnachrichtendienst SWR (Slushba Wneshnej Razvedki), der militärische Nachrichtendienst GU (Glawnoje Uprawlenije) und der zivile Inlandsnachrichten- und Sicherheitsdienst FSB (Federalnaja Slushba Besopasnosti).

Die wesentlichsten Ziele des **SWR** in Österreich sind die Spionage gegen bzw. die Beeinflussung von politischen Entscheidungsträgerinnen und Entscheidungsträgern sowie das Betreiben der SIGINT⁵³-Stationen in Wien.

Das wichtigste Ziel des **GU**⁵⁴ in Österreich ist die Beschaffung militärischer, sicherheitspolitischer und technologischer Informationen. Österreich ist als Mitglied der EU, in seiner Rolle als NATO-Partner und als Teilnehmer an internationalen Militärmissionen für den GU von sicherheitspolitischer Relevanz. Der GU ist besonders daran interessiert, Wissen über militärische und Dual-Use-Technologien⁵⁵ zu erwerben.

Der **FSB** konzentriert sich in erster Linie auf die innere Sicherheit, Spionageabwehr und die Überwachung russischer Oppositioneller, die als Bedrohung für das russische Regime gelten, im In- und Ausland.

Methoden der Informationsbeschaffung

Österreich beheimatet mit der russischen Botschaft in Wien, dem Generalkonsulat in Salzburg und den russischen Vertretungen bei internationalen Organisationen in Wien eine der größten russischen Legalresidenturen⁵⁶ weltweit. Russland nutzt diese, um Mitarbeiterinnen und Mitarbeiter aller drei wesentlichen russischen Nachrichtendienste nach Österreich zu entsenden. In weiterer Folge führen diese Personen unter diplomatischer Abdeckung bzw. unter dem Schutz der diplomatischen Immunität nachrichtendienstliche Aktivitäten durch, die sich in ihrer Intensität und Methodik unterscheiden. Neben konspi-

53 Erklärung „SIGINT“ am Ende des Kapitels.

54 Die offizielle Umbenennung des russischen militärischen Nachrichtendienstes GRU (Glawnoje Raswedywatelnoje Uprawlenije/Hauptverwaltung des Generalstabs) in GU (Glawnoje Uprawlenije/Hauptverwaltung) erfolgte im Jahr 2010. Obwohl die Bezeichnung in GU geändert wurde, blieb der alte Name GRU im allgemeinen Sprachgebrauch weit verbreitet und wird auch in Verfassungsschutzberichten anderer europäischer Länder noch verwendet.

55 „Dual-Use-Technologien“ sind Technologien, die sich sowohl für den zivilen als auch militärischen Einsatz eignen.

56 „Legalresidenturen“ sind getarnte Standorte fremder Nachrichtendienste in den offiziellen Vertretungen (z. B. Botschaft) im Empfangsstaat.

rativen Tätigkeiten, wie etwa dem Anwerben und dem Führen von Personen aus für den russischen Staat relevanten Bereichen, dient auch die Teilnahme an unterschiedlichen Veranstaltungen als Beschaffungsmethode. Die Informationsabschöpfung erfolgt dabei primär über den strategischen Aufbau sowie die kontinuierliche Pflege persönlicher oder institutioneller Kontakte.

Infolge des Angriffskrieges Russlands gegen die Ukraine kam es ab 2022 europaweit zur Ausweisung zahlreicher russischer Diplomatinen und Diplomaten, womit die Verkleinerung der Legalresidenturen in den jeweiligen europäischen Ländern einherging. Die Maßnahmen führten zu einer wesentlichen Schwächung der Ressourcen und Kapazitäten russischer Nachrichtendienste in Europa, auch in Österreich. Die Zahl des diplomatischen Personals Russlands in Österreich blieb vor allem aufgrund der multilateralen Vertretungen in Wien hingegen auch nach 2022 hoch. Aus diesem Grund nutzen russische Nachrichtendienste Österreich nicht nur als Operations-, sondern auch als Planungs- und Rückzugsraum für nachrichtendienstliche Aktivitäten in ganz Europa. Die DSN arbeitet eng mit anderen österreichischen Behörden, insbesondere dem Bundesministerium für Europäische und Internationale Angelegenheiten, zusammen, um mögliche Handlungen russischer Diplomatinen und Diplomaten, die nicht mit den klassischen Aufgaben einer diplomatischen Mission vereinbar sind, zu unterbinden. Nur durch eine konsequente Vorgehensweise gegen nachrichtendienstliche Aktivitäten, die vom österreichischen Staatsgebiet ausgehen, kann ein nachhaltiges Sicherheitsrisiko und ein entscheidender Reputationsschaden für Österreich abgewendet werden.

Die Schwächung der russischen Legalresidenturen in Europa führte unter anderem dazu, dass russische Nachrichtendienste verstärkt auf sogenannte Proxy-Akteurinnen und Proxy-Akteure zurückgreifen, die im Auftrag Russlands unter anderem zur Informationsgewinnung eingesetzt werden.

Als „**Proxy-Akteurinnen und Proxy-Akteure**“ werden Personen bezeichnet, die keinem Nachrichtendienst angehören, sondern stellvertretend für diesen agieren. Die daraus resultierende schwierige Zuordnung ermöglicht es staatlichen Akteuren, ihre Verantwortung für bestimmte Handlungen zu verschleiern und politische Haftung zu vermeiden. Eine abschließende Charakterisierung von Proxy-Akteurinnen und Proxy-Akteuren gestaltet sich schwierig, da deren Motivation zur Kooperation stark variieren und von ideologischen Überzeugungen bis hin zu finanziellen Anreizen reichen kann. Auffällig ist jedoch, dass Proxy-Akteurinnen und Proxy-Akteure nicht selten in kriminelle Strukturen eingebunden sind oder aus solchen hervorgehen.



Neben der diplomatischen Abdeckung nutzen russische Nachrichtendienste auch andere Tarnmöglichkeiten, um nachrichtendienstliches Personal im Verborgenen einzusetzen. Diese Positionen werden als Non-Official-Cover, also Personen, die ohne offizielle Abdeckung agieren, bezeichnet. Russland greift in diesem Zusammenhang auch auf Personen zurück, die unter journalistischer Tarnung operieren und Aufgaben für russische Dienste wahrnehmen. Die Abdeckung ermöglicht dem nachrichtendienstlichen Personal Zugang zu relevanten Veranstaltungen und Personenkreisen, der in weiterer Folge zur nachrichtendienstlichen Informationsgewinnung genutzt wird. Auch in Österreich kam es zu Fällen, in denen Journalistinnen und Journalisten russischer Herkunft die Akkreditierung entzogen wurde, nachdem sie unter Spionageverdacht für Russland geraten waren.

Der Einsatz von „Illegalen“ ist eine weitere spezifische und meist langfristige Einsatzform russischer Nachrichtendienste. Als Illegale werden Angehörige eines Nachrichtendienstes bezeichnet, die unter Volllegendierung⁵⁷ und ohne offensichtlichen Bezug zum Herkunftsland nachrichtendienstliche Operationen durchführen.

Seit 2022 werden Staatsbürgerinnen und Staatsbürger aus sogenannten „unfreundlichen Staaten“, die nach Russland einreisen möchten, vermehrt intensiven Grenzkontrollen unterzogen und oftmals aufgefordert, ihre elektronischen Geräte auf „unerlaubte Inhalte“ überprüfen zu lassen. Reisende nach Russland stellen damit eine potenzielle Quelle für die Informationsabschöpfung seitens Russland dar, darüber hinaus sind sie aber auch als mögliche Zielgruppe für Rekrutierungsversuche russischer Nachrichtendienste einzustufen.

Schließlich blieb im Berichtsjahr auch die bereits im Verfassungsschutzbericht 2024 beschriebene SIGINT-Station in Wien ein zentrales Instrument zur Informationsbeschaffung für russische Nachrichtendienste in Österreich und Europa.



„**Signal Intelligence**“ (SIGINT) sind Informationen, die durch die Erfassung und Analyse der elektronischen Signale und Kommunikation eines bestimmten Ziels gewonnen werden. Ausländische Nachrichtendienste können SIGINT für die Erfassung geheimer und sensibler Informationen im Zielstaat nutzen. So kann auch Österreich zum Ziel der Signalaufklärung durch fremde Dienste werden.

Sabotage

Die Durchführung von Sabotageakten ist ein wichtiges Bedrohungselement im Methodenbündel der sogenannten „hybriden Bedrohungsstrategie“ Russlands gegen Europa.

⁵⁷ Nachrichtendienstoffiziere, die unter falscher Identität und oft mit komplett erfundener Biografie („Legende“) operieren.

Als „hybride Bedrohungsstrategie“ eines staatlichen Akteurs kann der abgestimmte, kombinierte und mitunter nichtlineare Einsatz verschiedener Fähigkeiten, Mittel und Methoden des gesamten „DIMEFIL-Spektrums“⁵⁸ verstanden werden. Die Planung und akkordierte Umsetzung geschieht stets mit der Zielsetzung, das Gegenüber in seiner Handlungs- und Reaktionsfähigkeit zu beeinträchtigen und so dessen Schwächung oder Destabilisierung herbeizuführen, um seine eigenen Interessen gegen den Willen des anderen durchsetzen zu können. Eine „Hybridbedrohung“ kann etwa durch die kombinierte und koordinierte Anwendung und Durchführung von Desinformation, Cyberangriffen und Sabotageakten, u. a. mittels Proxy-Akteuren, erzeugt werden.

2025 wurden in Fortsetzung der Entwicklungen des Vorjahres in mehreren europäischen Staaten vermehrt Sabotageakte registriert. Russland wird als Hauptakteur hinter diesen Vorfällen vermutet, da der Anstieg dieser sicherheitsrelevanten Vorfälle zeitlich mit dem Beginn des russischen Angriffskrieges gegen die Ukraine zusammenfällt und die Ereignisse sich überwiegend in NATO-Staaten ereigneten, die der Ukraine direkte oder indirekte militärische Unterstützung leisten.

Die bislang bekannt gewordenen Vorfälle deuten darauf hin, dass sich die mutmaßlichen russischen Sabotageakte in Europa vor allem gegen militärische und logistik- bzw. transportbezogene Ziele richteten. Betroffen waren insbesondere Einrichtungen und Infrastrukturen, die im Zusammenhang mit der militärischen Unterstützung der Ukraine stehen. Es wird angenommen, dass russische Aktivitäten darauf gerichtet sein könnten, Prozesse des öffentlichen Lebens zu stören, weshalb folglich auch Einrichtungen der kritischen Infrastruktur potenzielle Sabotageziele sind. Die Methoden der Sabotage sind mannigfaltig, wenngleich vor allem gezielte Sachbeschädigungen, Brandstiftungen und vorbereitende Ausspähungsaktionen durchgeführt werden.

Zur Durchführung von Sabotageakten bedienen sich russische Nachrichtendienste häufig sogenannter Proxy-Akteurinnen und Proxy-Akteure. Deren Anwerbung erfolgt zumeist über Social-Media-Kanäle oder Messenger-Dienste, wobei für den Fall der Durchführung der Sabotage eine Belohnung in Aussicht gestellt wird. Den angeworbenen Personen ist häufig nicht bewusst, dass es sich bei der Auftraggeberin oder dem Auftraggeber um einen staatlichen Akteur handelt. Der Einsatz von Proxy-Akteurinnen und Proxy-Akteuren erschwert zudem die eindeutige Attribution und trägt zur Verschleierung der eigentlichen Urheberchaft bei.

Österreich verzeichnete im Gegensatz zu anderen europäischen Staaten noch keinen Sabotageakt, der Russland attribuiert werden konnte. Eine zukünftige Gefährdung Österreichs durch derartige Straftaten lässt sich jedoch nicht ausschließen. Vor diesem

58 „DIMEFIL“ steht für Diplomatic/Political, Information, Military, Economic, Financial, Intelligence and Legal.

Hintergrund ist es erforderlich, insbesondere die Resilienz der kritischen Infrastruktur in Österreich weiter gezielt zu stärken.

Einflussnahme und Desinformation

Russland nutzt seine staatlichen, finanziellen und technischen Ressourcen, um die europäische Bevölkerung großflächig zu beeinflussen. Zielsetzung ist die Unterstützung russlandfreundlicher Narrative und politischer Positionen, um zukünftig russische Interessen in anderen Staaten durchsetzen zu können. Des Weiteren beobachtet Russland die politischen und gesellschaftlichen Diskurse in westlichen Ländern und versucht, mithilfe der gewonnenen Erkenntnisse gezielt die Fähigkeit der politischen Einigung in Europa zu untergraben.

Zur Erreichung dieser Ziele bedient sich Russland einerseits klassischer Einflussversuche unter Einsatz von nachrichtendienstlichem Personal. In diesem Zusammenhang spielen staatliche und staatsnahe Einrichtungen Russlands im Ausland eine zentrale Rolle. Außerdem nutzt Russland gezielt private Institute und Vereine, die auf den ersten Blick keine Verbindungen zum russischen Regime haben, zur Einflussnahme.

Darüber hinaus führt Russland großangelegte Beeinflussungsoperationen, auch in Form von Desinformationskampagnen, als Mittel der hybriden Bedrohungen in Europa durch. Desinformationsnarrative werden durch herkömmliche russische Medien, aber auch über soziale Medien und Messenger-Dienste verbreitet.



Unter „**Desinformation**“ werden falsche Inhalte und Informationen verstanden, die gezielt und mit einer Täuschungsabsicht verbreitet werden. Hier liegt auch der Unterschied zu Falschinformationen/-meldungen, die ohne Täuschungsabsicht oder irrtümlich generiert und veröffentlicht werden.

Zur Durchführung von Online-Desinformationskampagnen bedient sich Russland unterschiedlicher Methoden. Dazu zählen unter anderem Social Bots⁵⁹, Trollfabriken⁶⁰ und Doppelgänger-Kampagnen⁶¹. Russland setzt vermehrt KI-generierte Inhalte, sogenannte

59 „Social Bots“ sind automatisierte Programme, die menschliches Verhalten simulieren bzw. Nutzerinnen und Nutzer imitieren, um unentdeckt Informationen in sozialen Netzwerken zu manipulieren.

60 Als „Trolle“ werden Internetnutzerinnen und Internetnutzer bezeichnet, die bewusst Online-diskussionen stören und manipulieren.

61 Unter „Doppelgänger-Kampagnen“ wird das Klonen von Webseiten, etwa von Nachrichtenmagazinen, verstanden. Das Design und das Layout entsprechen der offiziellen Seite, die inhaltliche Ausrichtung hingegen unterscheidet sich deutlich.

Deepfakes⁶², ein, um seine Desinformationsnarrative zu verteilen. Diese imitieren typische Internetnutzerinnen und Internetnutzer nahezu perfekt und treten automatisiert mit echten Benutzerkonten in Interaktion.

Des Weiteren greift Russland zur Wahrung und Durchsetzung seiner Interessen auf vielschichtige und koordinierte Einflussstrategien im politischen Bereich zurück. Nach dem Wahljahr 2024 konnten auch im Jahr 2025 bei Wahlen in europäischen Ländern Versuche russischer Einflussnahme festgestellt werden. Es ist zu erwarten, dass Russland auch in Zukunft gezielte Maßnahmen ergreifen wird, um Wahlen in EU-Ländern, so auch in Österreich, zu seinen Gunsten zu beeinflussen.

Schon in der Vergangenheit war Österreich von russischen Desinformationsaktivitäten betroffen. Ermittlungen legen nahe, dass im Jahr 2022 in Österreich eine pro-russische Desinformationskampagne aktiv war, die mutmaßlich durch eine von einem russischen Nachrichtendienst gesteuerte Zelle koordiniert wurde. Ziel war es, pro-russische Narrative zu verbreiten, die darauf abzielten, die öffentliche Meinung im Kontext des Ukrainekriegs zu beeinflussen.

Es ist davon auszugehen, dass diese Zelle europaweit vernetzt war und sich mehrerer Akteure aus diversen europäischen Ländern bediente, unter anderem bulgarischer Staatsbürgerinnen und Staatsbürger, die in London in diesem Zusammenhang bereits verurteilt wurden. Die Zelle soll in Wien gezielte Ausspähungen gegen hochrangige Persönlichkeiten aus Politik, Medien und Sicherheitsbehörden, die Zugang zu vertraulichen und sensiblen Informationen hatten, durchgeführt haben. Ziel dürfte auch gewesen sein, Mobilgeräte dieser Personen zu beschaffen und diese Geräte in weiterer Folge nach Russland zu verbringen. Staatliche Strukturen sollen hierfür infiltriert und unterwandert worden sein.⁶³

Zudem war Österreich auch zahlreichen russischen Desinformationsnarrativen ausgesetzt, die insbesondere über soziale Medien im gesamteuropäischen Raum verbreitet wurden. Die Narrative wurden unter anderem auf russlandnahen Plattformen verteilt, die eigene Beiträge mit Österreichbezug und in deutscher Sprache veröffentlichen. Russland be-

62 „Deepfake“ setzt sich aus den Begriffen „deep learning“ (Technologie unter Nutzung von Künstlicher Intelligenz) und „fake“ (Fälschung/Verfälschung) zusammen. Manipulierte Videos oder Bilder werden mithilfe von KI erzeugt; so werden etwa Aussagen von Politikerinnen und Politikern generiert, die diese nie getätigt haben.

63 Russische Nachrichtendienste haben in zahlreichen europäischen Städten, unter anderem auch in Wien, Stützpunkte bzw. Zweigstellen eingerichtet. Um diese Zweigstellen auf Dauer für ihre Aktivitäten und Einflussnahmen, wie z. B. Desinformationskampagnen und Informationsbeschaffungen, zielgerichtet bedienen zu können, wurde eine Person aus dem inneren Kreis der russischen Nachrichtendienste, die Wissen über die europäischen Grundsätze und -strukturen besitzt und Kontakte zu Personen in der EU pflegt, eingesetzt. Diese Person baute für die Umsetzung der regelmäßig ergangenen Aufträge ein international agierendes Netzwerk auf und führte (im Auftrag russischer Nachrichtendienste) mehrere Operationen in Österreich durch.

obachtet gesellschaftliche Diskurse und Spannungsfelder sehr genau. Je stärker ein Thema die Bevölkerung polarisiert, desto größer ist sein Potenzial, von Russland strategisch aufgegriffen und für eigene Zwecke instrumentalisiert zu werden. Aktuell lässt sich eine verstärkte Schwerpunktsetzung auf Österreichs Neutralität und seine Rolle in gegenwärtigen Konflikten, insbesondere mit Bezug zum russischen Angriffskrieg gegen die Ukraine, feststellen. Darüber hinaus rücken die Themen Energiesicherheit bzw. die Preissteigerung in Österreich in den Fokus russischer und russlandnaher Social-Media-Kanäle und Onlineplattformen.

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.

Im Rahmen offensiver Cyberoperationen (CNE)⁶⁴ nutzen russische Akteure auch Schwachstellen in privaten IoT-Geräten⁶⁵, um ihre Spuren zu verschleiern. Durch das Eindringen in unsicher konfigurierte Netzwerkgeräte (beispielsweise Router) und das Installieren von zusätzlicher Proxy-Software⁶⁶ 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 Akteure verschaffen sich nicht nur Zugang zu privaten Geräten, sondern auch immer wieder zu End-of-Life-Netzwerkgeräten von Organisationen in sämtlichen Sektoren

64 „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.

65 Ein „IoT-Gerät“ (Internet-of-Things-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.

66 „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.

und unterschiedlichen Ländern. In Kombination mit dem Einsatz spezieller Schadsoftware bleiben diese Zugriffe oftmals jahrelang unentdeckt. Derartige opportunistische Kampagnen verfolgen nicht nur Spionageabsichten, sondern könnten 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 APT⁶⁷28, APT29 und Turla. APT28 ist mutmaßlich mit dem militärischen Nachrichtendienst GU affiliert. 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 schließlich wird dem FSB zugeordnet und ist auf Cyberspionageoperationen gegen Regierungsstellen und Forschungseinrichtungen spezialisiert. Zusätzlich zu den relevantesten 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 demnach ein breites Spektrum russischer Cyberoperationen ab. Die 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.

China

Allgemeine Vorgehensweise chinesischer Dienste

Der komplexe chinesische Nachrichtendienstapparat gliedert sich in vier Hauptorganisationen: zwei zivile und zwei militärische Einheiten. Das Ministerium für Staatssicherheit (MSS) bildet das Rückgrat der Auslandsaufklärung und fokussiert sich auf die Gewinnung strategischer Informationen aus Politik, Wirtschaft, Forschung, Technologie und Verteidigung. Parallel dazu operiert das Ministerium für Öffentliche Sicherheit (MPS), das als oberste Instanz der Volkspolizei primär für innere Sicherheitsbelange verantwortlich ist, jedoch auch nachrichtendienstliche Funktionen im Ausland wahrnimmt und durch transnationale Repressionsaktivitäten in Europa auffällt.

67 „APT“ steht für „Advanced Persistent Threat“. Der Begriff Akteur oder Gruppierung wird hier für die leichtere Lesbarkeit verwendet. Fachlich präzise spricht man von einem Activity Cluster. Diese Cluster ergeben sich durch ähnliche Merkmale bei beobachteten vergangenen Angriffen (z. B. verwendete Schadsoftware, Art des Vorgehens, C2 Infrastruktur). Hierbei werden mehrere ähnliche Beobachtungen zu einer Gruppe – dem Activity Cluster – zusammengefasst und mit einem Namen versehen. Unterschiedliche Sicherheitsforscher oder Firmen vergeben hierbei eigene Namen.



Als zivile Nachrichtendienste fungieren das Ministerium für Staatssicherheit (**MSS**) und das Ministerium für Öffentliche Sicherheit (**MPS**). Das Military Intelligence Department (**MID**) und das Network Systems Department (**NSD**) sind hingegen militärische Nachrichtendienste.

Im militärischen Bereich agiert das Military Intelligence Department (MID) global im HUMINT⁶⁸-Sektor und untersteht dabei dem Joint Staff Department Intelligence Bureau der Zentralen Militärkommission. Ergänzt wird es durch das Network Systems Department (NSD), dessen Schwerpunkte in der Signalaufklärung, technischen Informationsbeschaffung und Cyberspionage liegen.

Neben diesen Kernstrukturen sind diverse staatliche Institutionen mit eigenen nachrichtendienstlichen Kapazitäten ausgestattet. Hervorzuheben ist das International Department of the Central Committee of the Communist Party of China (IDCPC), das auf die Gewinnung politisch sensibler Informationen und die Manipulation ausländischer Entscheidungsträgerinnen und Entscheidungsträger spezialisiert ist. Das United Front Work Department (UFD) wiederum nutzt ein ausgedehntes Netzwerk von Vereinen und Organisationen im Ausland für nachrichtendienstliche Zwecke. Seine Aufgaben reichen von der Imagepflege der chinesischen Regierung über die Kooptierung westlicher Eliten bis zur umfassenden Überwachung der chinesischen Diaspora.

Derlei autoritäre Kontrollmechanismen kontrastieren fundamental mit Österreichs offener, demokratischer Gesellschaftsordnung. China nutzt systematisch die in liberalen Demokratien geltenden gesellschaftlichen und wissenschaftlichen Freiheiten aus, beispielsweise zur Beschaffung von Know-how und Technologien, und generiert daraus sowohl unmittelbare als auch langfristige strategische Vorteile. Der kontinuierliche Verlust von Know-how und Forschungsergebnissen untergräbt nachhaltig Österreichs Innovationskraft.

Pekings übergeordnetes Ziel bleibt die Transformation der globalen Ordnung zu Gunsten Chinas. Unter Xi Jinpings Führung strebt China danach, bis zum hundertjährigen Staatsjubiläum zur dominanten Weltmacht aufzusteigen. Der „14. Fünfjahresplan“, die Programme „Made in China 2025“ und „China Standards 2035“ sowie die „Belt and Road“-Initiative bilden die strategischen Eckpfeiler dieser Transformation. Die von der Kommunistischen Partei Chinas (KPCh) forcierte militärisch-zivile Fusion ordnet dabei alle gesellschaftlichen Kräfte dem Erreichen des „chinesischen Traums“ unter – einer Vision globaler Dominanz Chinas in Wirtschaft, Technologie und Militär.

⁶⁸ „HUMINT“ steht für „Human Intelligence“ und bezieht sich auf Informationen, die durch menschliche Quellen generiert werden.

Methoden der Informationsbeschaffung

Zur Beschaffung von Informationen greift China auf ein breites Instrumentarium zurück, bei dem der von ihm verfolgte „whole of society approach“ zentral ist. Die Möglichkeit der Miteinbeziehung aller chinesischen Firmen, Universitäten und Individuen in nachrichtendienstliche Zielsetzungen (= „Non-Professionalisierung“ chinesischer Spionage) ist eine der größten Stärken chinesischer Nachrichtendienste. Darüber hinaus werden auch unter dem Deckmantel diplomatischer und journalistischer Tätigkeit nachrichtendienstliche Operationen in Österreich durchgeführt, die von Informationssammlung über Technologieakquise und Quellenwerbung bis zur Beeinflussung von Wirtschaft und Politik reichen.

Chinas Nachrichtendienste, die weder unabhängigen politischen Gremien noch der Öffentlichkeit gegenüber rechenschaftspflichtig sind, verfolgen einen gesamtgesellschaftlichen Ansatz („**whole of society approach**“), bei dem die Gesellschaft als Ganzes der Realisierung gesamtstaatlicher Zielsetzungen zuarbeiten soll.

Im Sinne dieses gesamtgesellschaftlichen Ansatzes sind chinesische Staatsangehörige, Firmen u. a. aufgrund der Gesetzeslage dazu verpflichtet, Aufträgen nachzukommen, die chinesische Nachrichtendienste auf Begehren der KPCh erteilen. In weiterer Folge werden Einzelpersonen, Institutionen und Unternehmen zur Spionage und zum Diebstahl geistigen Eigentums von westlichen Einrichtungen angewiesen. Diese Strategie erlaubt es China, zahlreiche, höchst unterschiedliche Akteure für nachrichtendienstliche Zwecke zu mobilisieren und auf allen Ebenen der Gesellschaft zu operieren.



Das rechtliche Fundament dieser Aktivitäten wurde 2023 durch die Verschärfung des nationalen Sicherheitsgesetzes maßgeblich erweitert. Alle chinesischen Staatsangehörigen, Unternehmen und Bildungseinrichtungen – gleich, ob im In- oder Ausland tätig – sind nun zur bedingungslosen Kooperation mit den Nachrichtendiensten verpflichtet. Weiters gewährt das reformierte Anti-Spionage-Gesetz chinesischen Behörden nahezu unbegrenzte Befugnisse zur Datenerfassung bei den in China tätigen ausländischen Unternehmen. Auch sensible Daten internationaler Nutzerinnen und Nutzer chinesischer Technologieprodukte, Apps und digitaler Anwendungen können von chinesischen Behörden abgegriffen werden.

Im wirtschaftlichen Bereich nutzt China neben legalen Instrumenten, wie beispielsweise strategischen Investitionen oder Joint Ventures, auch illegale Mittel zur Technologieakquise: Scheitern offizielle Übernahmen von oder Kooperationen mit Firmen, greift China auf verdeckte Operationen und Cyberangriffe zurück. Darüber hinaus setzen

chinesische Nachrichtendienste zunehmend auf automatisierte Informationsgewinnung durch KI-gestützte Systeme, welche Daten aus sozialen Medien, Firmendatenbanken und wissenschaftlichen Publikationen systematisch auswerten und Profile von Zielpersonen erstellen. Die traditionellen Methoden der Informationsbeschaffung werden dabei wohl-gemerkt nicht ersetzt, sondern durch digitale Ansätze komplementiert.

Wissenschafts- und Wirtschaftsspionage

Der systematische Wissenstransfer aus westlichen Ländern nach China, der dessen rasanten technologischen Aufstieg der letzten Jahrzehnte mit ermöglichte, bleibt ein Kernstück der chinesischen Globalstrategie. Österreichs dynamische Forschungsland-schaft steht daher ebenso im Fokus chinesischer Nachrichtendienste wie der wirtschaft-liche Innovationssektor. Die hohe Expertise heimischer (Forschungs-)Institutionen und Unternehmen in Bereichen wie Quantentechnologie, Halbleiterforschung, KI-Entwicklung, Robotik, Biotechnologie, Luftfahrt und Überwachungssysteme macht sie zu prioritären Zielobjekten. Gleichzeitig fehlt in Österreich vielerorts noch das notwendige Sicher-heitsbewusstsein wie auch der entsprechende infrastrukturelle Schutz. Folglich sind insbesondere kleine und mittelständische Unternehmen wie auch Start-Ups leichte Ziele für chinesische Nachrichtendienste, vor allem, wenn sie auf ausländische Investitionen angewiesen sind.

Im Rahmen der nationalen Investitionskontrolle prüft der Verfassungsschutz zwar ge-plante Unternehmensbeteiligungen auf Risiken für die öffentliche Sicherheit, allerdings weiß China die Grauzone zwischen legitimen und illegitimen Aktivitäten geschickt auszunutzen. Die von China praktizierte systematische Verschmelzung ziviler und militärischer Forschung (Military-Civil Fusion) führt dazu, dass selbst harmlos erschein-ende Kooperationen mit chinesischen Start-ups oder Universitäten potenzielle Sicher-heitsrisiken darstellen. Besonders risikobehaftet sind in diesem Kontext Bereiche wie Drohnentechnologie, autonome Systeme und Materialforschung, wo es praktisch keine Grenze zwischen ziviler und militärischer Nutzung mehr gibt.



Das „**Investitionskontrollgesetz**“ (**InvKG**) regelt in Österreich die Kontrolle aus-ländischer Direktinvestitionen. Unter bestimmten Voraussetzungen unterliegt der teilweise oder vollständige Erwerb österreichischer Unternehmen durch juristische oder natürliche Personen aus Drittstaaten einer Genehmigungspflicht. Bei dieser Norm für die Investitionskontrolle geht es um Unternehmen, die der kritischen Infrastruktur zuordenbar sind oder Technologien anbieten, die von Staaten für ihre militärischen oder sicherheitspolitischen Interessen verwendet werden können. Die Aufgabe der DSN ist es, im Genehmigungsprozess zu beurteilen, ob der Erwerb eines solchen Unternehmens eine Gefährdung für die österreichische bzw. gesamteuropäische Sicherheit oder die öffentliche Ordnung darstellen kann.

Bei der Kultivierung zukünftiger Informationssammlerinnen und Informationssammler verfolgen Chinas Nachrichtendienste häufig einen generationenübergreifenden Ansatz. Aufstrebende wissenschaftliche Talente werden über Jahre hinweg finanziell unterstützt, wodurch Abhängigkeitsverhältnisse entstehen, die China später für die Abschöpfung sensibler Information nutzt („seeding campaigns“). Staatliche chinesische Stipendiengeber, wie etwa das Chinese Scholarship Council (CSC), fördern aufstrebende chinesische Forschungstalente, die an österreichischen Universitäten Zugang zu innovativen Technologien bekommen. Die Stipendiatinnen und Stipendiaten sind zur ideologischen Loyalität gegenüber der KPCh und zur regelmäßigen Berichterstattung an chinesische Vertretungen verpflichtet. Mit Abschluss ihrer Forschungstätigkeit werden chinesische Akademikerinnen und Akademiker oftmals zur Rückkehr nach China verpflichtet.

Österreichische Forschungszentren, die sich oftmals ihrer Attraktivität für chinesische Nachrichtendienste nicht ausreichend bewusst sind, kann China als Einfallstor in den europäischen Wissenschaftsraum nutzen. Vonseiten chinesischer Universitäten angestobene Forschungsk Kooperationen mit österreichischen Partnerinstitutionen dienen zwar formal dem wissenschaftlichen Austausch, fungieren faktisch jedoch oft als Kanäle für systematischen Wissenstransfer.

Verstärkt nutzen chinesische Dienste auch Talent Spotting-Programme, im Zuge derer gezielt österreichische Nachwuchswissenschaftlerinnen und Nachwuchswissenschaftler mit großzügigen Forschungsbudgets und Karriereperspektiven nach China gelockt werden, um dort ihr Fachwissen preiszugeben. Die Rekrutierung erfolgt über multiple Kanäle: persönliche Ansprache auf Konferenzen und Messen, digitale Plattformen wie LinkedIn, Forschungsprojekte oder Stipendienprogramme.

Einflussnahme auf Politik und Diaspora

Die 2024 aufgedeckten Einflussoperationen im Europäischen Parlament verdeutlichen Chinas systematische Bemühungen, die EU und ihre Mitgliedstaaten zu destabilisieren und für eigene Zwecke zu instrumentalisieren. In Österreich existiert ein dichtes Geflecht aus politischen, wirtschaftlichen und diplomatischen Verbindungen, das gezielt für pro-chinesische Einflussnahme genutzt wird. Das Konzept des „Elite Capture“ zielt darauf ab, Schlüsselfiguren in Politik und Verwaltung durch materielle Anreize oder prestigeträchtige Einladungen zu kooptieren. Chinesische Vereine, Kulturinstitutionen, wie beispielsweise Konfuzius-Institute, sowie diverse China-Zentren pflegen intensive Beziehungen zu österreichischen Entscheidungsträgerinnen und Entscheidungsträgern, die bei Bedarf aktiviert und genutzt werden können.

Die chinesische Diaspora in Österreich, die auf etwa 30.000 Personen geschätzt wird, unterliegt einem engmaschigen Kontroll- und Überwachungssystem durch chinesische Nachrichtendienste. Dabei üben diese – auch über Vereine – systematisch Druck auf Auslandschinesinnen und Auslandschinesen aus. Insbesondere die von der chinesischen

Regierung als „Fünf Gifte“ bezeichneten Gruppen – Tibeter, Uiguren, Anhängerinnen und Anhänger der religiösen Gruppierung Falun Gong, taiwanische Unabhängigkeitsbefürworterinnen und Unabhängigkeitsbefürworter und Demokratieaktivistinnen und Demokratieaktivisten – sind von Repressionsmaßnahmen betroffen. Durch die Praktizierung einer Form von „Sippenhaft“ werden Familienangehörige in China als Druckmittel eingesetzt, um in Österreich lebende Chinesinnen und Chinesen zur Kooperation zu zwingen. Dies betrifft vor allem Personen in sensiblen Positionen in Forschung, Technologie oder Verwaltung. Nicht zuletzt können Mitglieder der Diaspora gezielt für Social Engineering-Operationen eingesetzt werden, indem sie Vertrauen zu österreichischen Zielpersonen aufbauen und diese für nachrichtendienstliche Zwecke ausnutzen.

Pekings mediale Strategie, die der österreichischen Politik und Gesellschaft ein ausnahmslos positives Bild Chinas unter Auslassung jedweder kritischer Perspektiven oder unliebsamer Fakten vermitteln soll, umfasst die gezielte Verbreitung pro-chinesischer Narrative in der österreichischen Öffentlichkeit und die Beeinflussung lokaler Medien.

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 Cyberakteure weitestgehend auf die Unterstützung von Wirtschaftsspionage. Es lässt sich jedoch auch zunehmendes Interesse an politischer Spionage beobachten. Diese richtet sich zumeist 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. Cyberakteure 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 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.

Iran

Allgemeine Vorgehensweise iranischer Dienste

Die iranischen Nachrichtendienste fördern aktiv die Interessen des Iran und schützen das Regime vor Bedrohungen. In Österreich beobachten sie gezielt iranische Oppositionelle, Medien, Menschenrechtsorganisationen und Minderheiten, um diese gegebenenfalls zu unterdrücken oder für ihre Zwecke zu instrumentalisieren.

Die nachrichtendienstliche Sicherheitsarchitektur des Iran wird vorrangig durch drei Organisationen geprägt.

VAJA/MOIS⁶⁹

Das Ministerium für Nachrichtendienst VAJA, hervorgegangen aus dem Schah-Geheimdienst SAVAK, überwacht und verfolgt weltweit Feinde des Regimes. Anfänglich konzentrierte sich VAJA vorwiegend auf die Ausschaltung iranischer Oppositioneller, heute agiert der Dienst zunehmend global und umfassend.

IRGC-IO

Die Islamic Revolutionary Guard Corps-Intelligence Organization (IRGC-IO) ist im Vergleich zum zivilen Nachrichtendienst VAJA 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 Regimegegnern.

IRGC-Quds Force

Der dritte bedeutsame Akteur mit geheimdienstlicher Vorgehensweise in der iranischen Sicherheitsstruktur ist die IRGC-Quds Force, spezialisiert auf extra-



⁶⁹ International wird VAJA oft als MOIS (Ministry of Intelligence and Security) oder auch MOI bezeichnet, da das Ministerium mittlerweile nur noch den Nachrichtendienst beinhaltet.

territoriale Operationen und Kommandoaktionen, die auch in Abstimmung mit anderen iranischen Diensten ausgeführt werden. So übernimmt das Geheimdienstministerium VAJA mitunter die Planung und Steuerung staatsterroristischer Aufträge, die IRGC-Quds Force anschließend deren Ausführung.

Rivalitäten und mangelnde Koordination schwächen oftmals die Effizienz dieser Dienste. In Wien nutzen Nachrichtendienstoffiziere die bi- und multilateralen iranischen Botschaften als Tarnung. Der diplomatische Status schützt sie vor Strafverfolgung und erleichtert Kontakte zu Behörden, Unternehmen und Universitäten. Beispielhaft dafür ist ein ehemaliger Dritter Botschaftsrat der iranischen Botschaft in Wien, der als VAJA-Offizier ein Agentennetzwerk in Europa steuerte und einen Anschlag auf einen für den 30. Juni 2018 geplanten Oppositionskongress in Villepinte bei Paris plante, welcher jedoch vereitelt werden konnte.

Methoden der Informationsbeschaffung

Iranische Nachrichtendienste setzen vielfältige und zunehmend hybride Methoden ein, um Informationen zu beschaffen und Oppositionelle einzuschüchtern. Im Zentrum steht die iranische Botschaft in Wien, eine der größten diplomatischen Vertretungen Teherans in Europa. Sie dient als zentrale operative Basis und Schaltstelle für nachrichtendienstliche Aktivitäten in West- und Mitteleuropa. Nachrichtendienstoffiziere des MOIS und der IRGC sind verdeckt unter diplomatischem Schutz akkreditiert und nutzen die Immunität, um Kontakte zu Behörden, Wirtschaftsakteuren, Wissenschaftlerinnen und Wissenschaftlern sowie Universitäten aufzubauen. Ziel ist die klassische Human Intelligence: Rekrutierung von Informanten, Sammlung sensibler Daten zu Technologie, Rüstung, Energie und Politik sowie die systematische Überwachung der iranischen Diaspora.

Neben dieser traditionellen Agentenarbeit gewinnen technische und cyberbasierte Methoden stark an Bedeutung. Iranische Akteure führen gezielte Cyberangriffe durch, die sich gegen Exil-Iranerinnen und Exil-Iraner, regimekritische Medien, Journalistinnen und Journalisten und europäische Institutionen richten. Solche Operationen zielen darauf ab, E-Mails, Kommunikationsverläufe, Standortdaten und persönliche Netzwerke abzuschöpfen.

Parallel dazu dienen soziale Medien und digitale Plattformen als Überwachungsinstrumente. Iranische Dienste scannen Profile, Posts und Verbindungen von Dissidentinnen und Dissidenten, um kritische Stimmen zu identifizieren, Bewegungsprofile zu erstellen und Druckmittel (z. B. Drohungen gegen Familienangehörige im Iran) zu generieren. In der Diaspora werden zudem kulturelle und religiöse Vereine systematisch infiltriert. Schiitische Zentren, Moscheen und Kulturvereine fungieren als Plattformen zur Datensammlung: Bei Veranstaltungen, Spendenaufrufen oder Mitgliederversammlungen werden Teilnehmerlisten, Kontaktdaten und Meinungsäußerungen erfasst. Diese Informationen

fließen in zentrale Dossiers ein, die sowohl zur Loyalitätskontrolle als auch zur Vorbereitung repressiver Maßnahmen genutzt werden.

Ergänzend greifen die Dienste zunehmend auf kriminelle Netzwerke als Proxys zurück. Organisierte Gruppen in Europa werden für Einschüchterungsaktionen, Überwachungen oder sogar geplante Anschläge rekrutiert, um eine direkte Attribution an Teheran zu erschweren.

Diese Methodenvielfalt stellt aus Sicht des Verfassungsschutzes eine anhaltende und wachsende Bedrohung dar. Die Kombination aus diplomatischer Tarnung, cybergestützter Spionage, sozialer Kontrolle über religiöse Strukturen und Outsourcing an Kriminelle ermöglicht es dem Regime, effektiv und mit geringem Entdeckungsrisiko zu operieren. Dies gefährdet nicht nur die Sicherheit einzelner Personen in der Diaspora, sondern auch die Souveränität Österreichs.

Proxy-Akteure im nachrichtendienstlichen Netzwerk des Iran

Von der Islamischen Revolution 1979 bis in die 1990er-Jahre verübten iranische Nachrichtendienste mehrere Anschläge auf Oppositionelle in Europa. Attentäterinnen und Attentäter mit Verbindungen zu den iranischen Diensten wurden in mehreren europäischen Staaten verhaftet und angeklagt. Dabei konnte ein direkter Bezug zum Iran als Auftraggeber nachgewiesen werden. In Österreich wurden allerdings keine durch Proxy-Akteure ausgeführte Anschläge bekannt.

Später bedienten sich die iranischen Dienste zunehmend krimineller Netzwerke, Drogenkartelle, pro-iranischer Milizen oder Terrorgruppierungen, um gewaltsame Angriffe im Ausland umzusetzen. Diese strategische Neuorientierung dürfte sich weiter verstärken. Die sogenannten Proxy-Akteure handeln wissentlich oder unwissentlich im Auftrag des Irans. Nachrichtendienstmitarbeiterinnen und Nachrichtendienstmitarbeiter steuern solche Angriffe oft von iranischem Boden aus, um einer Verurteilung zu entgehen. Durch zwischengeschaltete Vermittlerinnen und Vermittler bleibt die Verbindung zum Iran häufig unklar, was es dem Regime ermöglicht, seine Beteiligung zu verschleiern.

Neben Kriminellen übernehmen auch unauffällige zivile Einrichtungen, wie etwa Fluggesellschaften, Vereine, Presseagenturen, Firmen, Banken oder Kulturzentren, immer wieder nachrichtendienstliche Aufgaben, so etwa Informationsbeschaffung und ideologische Einflussnahme im Sinne des Iran.

Einflussnahme auf Politik und Diaspora

In Österreich spielen schiitische Zentren, die eng mit dem Iran verwoben sind, eine zentrale Rolle bei der Ausübung von Soft Power und nachrichtendienstlicher Einflussnahme. Besonders hervorzuheben ist hierbei das Zentrum der Islamischen Kultur Imam

Ali (auch Ali-Zentrum oder IZIA) in Wien, welches 2017 von der Islamischen Republik Iran erworben und ausgebaut wurde.

Unter dem Deckmantel der Religion rechtfertigen diese Zentren ein totalitäres Herrschaftssystem, das mit pluralistischen Gesellschaften unvereinbar ist. Revolutionsführer Ajatollah Chomeini hat den religiösen Glauben in eine politische Ideologie umgeformt, die auch der aktuelle Oberste Führer⁷⁰ des Iran, Ali Chamenei, als fortlaufende Islamische Revolution versteht, mit dem Ziel einer panislamischen Zivilisation. Die „Herrschaft des Rechtsgelehrten“ (Velayat-e Faqih) wird in diesen Zentren propagiert und Regimekritik als Verrat gebrandmarkt. Die tätigen Imame und Verantwortlichen werden zum Teil direkt aus Teheran bestellt und gesteuert.

In Österreich fördern solche Zentren antisemitische Ressentiments und den Hass auf Regimegegnerinnen und Regimegegner. Sie beeinflussen die iranische Diaspora durch Veranstaltungen, Medien und soziale Netzwerke, um die Loyalität zum Regime zu stärken und gleichzeitig Dissidentinnen und Dissidenten einzuschüchtern. Exil-Iranerinnen und Exil-Iraner berichten wiederholt von Überwachungen, Bedrohungen und Einschüchterungsversuchen, die bis hin zu physischen Nachstellungen reichen können. Die iranische Botschaft in Wien dient als operative Basis für die nachrichtendienstlichen Tätigkeiten sowohl des MOIS als auch der IRGC. Der Verfassungsschutz beobachtet diese Strukturen, da sie nicht nur ideologische Einflussnahme betreiben, sondern auch Plattformen für nachrichtendienstliche Operationen sind. Dies reicht von der Sammlung von Informationen über Regimegegnerinnen und Regimegegnern über die Koordination von Proxy-Aktivitäten bis hin zur Unterstützung von Gruppierungen wie der Hisbollah. Diese wurde auch öffentlichkeitswirksam evident, als der Iranische Botschafter in Wien im August 2024 via seinem Kanal auf X die verbotene Flagge der Terrororganisation Hisbollah veröffentlichte. Konsequenterweise erfolgte eine Anzeige durch die DSN, welche jedoch aufgrund des diplomatischen Status des damaligen Botschafters ohne straf- oder verwaltungsrechtliche Folgen blieb.

Dass diese Zentren mitunter Handlungen setzen, die mit den geltenden Rechtsordnungen Europas unvereinbar sind, zeigt das Verbot des Islamischen Zentrums Hamburg (IZH) am 3. Juli 2024 durch das deutsche Bundesministerium für Inneres und Heimat. Dort wurden Vorwürfe wie die Verbreitung islamistischer Ideologien, Antisemitismus und Unterstützung der Hisbollah, die als Terrororganisation eingestuft ist, belegt. Die DSN stuft die iranischen Aktivitäten als anhaltende Bedrohung ein, die die innere Sicherheit und den Schutz vulnerabler Exilgruppen und Dissidentinnen und Dissidenten gefährdet. Eine anhaltende Beobachtung und ggf. die Durchführung restriktiver Maßnahmen gegenüber solchen Einrichtungen bleiben daher geboten, um eine weitere Instrumentalisierung religiöser Strukturen für totalitäre Zwecke zu unterbinden.

70 Zum Zeitpunkt der Berichtslegung Ali Chamenei – verstorben am 28. Februar 2026.

Nachrichtendienstliche Cyberaktivitäten

Der Fokus der iranischen Nachrichtendienste im Cyberraum liegt auf der Absicherung des Regimes. Um dies zu erreichen, betreiben sie auch Cyberspionageoperationen. Die dabei gewonnenen Erkenntnisse verwenden sie oftmals für Desinformationskampagnen (Cyber-Enabled Information Operations). Bei den Zielen handelt es sich primär um für den Iran relevante privatwirtschaftliche Organisationen, insbesondere – bzw. je nach Fokus der Desinformationskampagne – unterschiedliche 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 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 MOIS zugerechnet.

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 Personengruppen 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 Hacktivistern auf Ziele in Österreich.

Die häufigsten Methoden im Hacktivismus sind Distributed Denial of Service (DDoS)-Angriffe und Hack-and-Leak-Operationen. Bei DDoS-Angriffen wird eine Vielzahl von Anfragen 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 Industriesteueranlagen⁷¹. Meist wird hierfür vorab nach ungesicherten Zugängen gesucht. Sobald das System infiltriert ist, werden Steuerbefehle eingesetzt, um die betroffenen Anlagen zu beschädigen oder abzuschalten. Selbst wenn es den Akteuren nicht gelingt, auf kritische Systeme zuzugreifen, wird ein aus technischer Sicht fehlgeschlagener Angriffsversuch seitens der 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 Haktivistinnen und Haktivisten primär darum, einen medialen Effekt zu erzielen, indem suggeriert wird, dass es gelungen sei, tief in das System einzudringen.

Seit einigen Jahren befeuern geopolitische Spannungen die Annäherung bzw. Verflechtung von staatlichen Interessen und Strukturen mit hacktivistischen 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 zudem das Bild einer großen, öffentlichen Unterstützungsbewegung konstruieren zu können. Die wichtigsten hacktivistischen Gruppierungen auf russischer Seite waren in den letzten 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 Staatsbürger 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 besonders deutlich. Hierbei greifen iranische Nachrichtendienste gezielt Unternehmen oder Einzelpersonen an; die dabei erbeuteten Daten werden anschließend veröffentlicht. Zur Veröffentlichung verwenden iranische Dienste sogenannte hacktivistische Personas⁷². 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.

71 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 relativ einfachen Mitteln darauf zugreifen können. In wenigen Fällen können die Angreifer dabei nicht nur Daten ablesen, sondern diese auch verändern und die volle Kontrolle über die Anlage übernehmen.

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

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.

Als „**Cyber-Enabled Information Operations**“ werden Informationsoperationen in Form von Cyberangriffen verstanden, deren Ziele 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.

Angesichts der gegenwärtigen geopolitischen Spannungen und Konflikte wird der Hactivismus nicht an Relevanz verlieren – nicht zuletzt aufgrund sich verdichtender Überschneidungen und Verflechtungen zwischen staatlichen Akteuren bzw. deren Interessen und Strukturen einerseits und hacktivistischen Akteuren und deren Aktivitäten andererseits. So ist etwa eine zunehmende Konvergenz zwischen pro-russischen und pro-palästinensischen hacktivistischen 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 anti-kolonialistischen Aktivismus. Außerdem verschwimmen zusehends die Grenzen zwischen Cyber-Enabled Information Operations staatlicher 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 zur Verhinderung externer Zugriffe direkt über das Internet, wichtig und erforderlich, um hacktivistische Kampagnen mit medialer Wirkung weitestgehend verhindern zu können.

Zunehmende Auslagerung von Cyberangriffen

Staatliche Cyberakteure 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 Akteure oftmals durch eine facettenreiche Motivlage – wirtschaftlich, politisch, militärisch, ideologisch – auszeichnen, sind Cyberkriminelle in aller Regel lediglich finanziell motiviert. Staatliche Cyberakteure fokussieren sich zudem 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 sämtliche vorliegende Zugangsdaten exfiltrieren zu können. Diese Informationen werden zeitnah im Darknet zum Verkauf angeboten und dienen anderen kriminellen oder staatlichen Akteuren als Eintrittsvektor bei Folgeangriffen in diese Zielsysteme. Obwohl grundsätzlich deutliche Unterscheidungsmerkmale vorliegen, geht der Trend in Richtung einer zunehmenden Kooperation zwischen staatlichen Akteuren und der organisierten Kriminalität.

Staatliche Cyberakteure 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 diese 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 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 Cyberakteuren und 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 Cyberakteure nähert sich damit zusehends der chinesischen Vorgehensweise im Bereich der Cyberspionage an.

Die zunehmende Kooperation zwischen nachrichtendienstlichen Cyberakteuren 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.

2.6.3 Fälle 2025

Fall ENERGIEUNTERNEHMEN

Im Rahmen von Ermittlungen stieß die DSN auf verdächtige Aktivitäten eines Mitarbeiters der russischen Botschaft in Österreich im Zusammenhang mit einem größeren österreichischen Energieunternehmen. Es bestand der Verdacht, dass der Botschaftsmitarbeiter als (verdeckter) Nachrichtendienstoffizier des zivilen russischen Auslandsnachrichtendienstes SWR Handlungen zum Nachteil der Republik Österreich setzte.

Die weiteren Ermittlungen brachten die Erkenntnis, dass es zwischen dem Botschaftsmitarbeiter und einem Mitarbeiter des Energieunternehmens zu persönlichen Treffen gekommen war und weiterhin kam. Die Art und Weise, wie diese Treffen durchgeführt wurden, sowie das Verhalten der beiden Personen ließen darauf schließen, dass es sich um nachrichtendienstliche Treffen zur Übergabe sensibler Daten oder Dokumente handelte.

Die Ermittlerinnen und Ermittler nahmen Kontakt mit dem betroffenen Energieunternehmen auf, um potenzielle Schäden abzuwenden und weitere Informationen über den Aufgabenbereich und die Informationszugänge des Mitarbeiters zu erhalten, der im Ausland für die Firma tätig war. Es konnte erhoben werden, dass keine geschäftlichen Verbindungen zu Russland bestanden und die Treffen somit keine mit dem Aufgabenbereich des Mitarbeiters verbundenen Termine sein konnten. Zudem hielt sich der Mitarbeiter des Energieunternehmens nur an den Tagen der Treffen sowie unmittelbar davor und danach in Österreich auf. Es bestand daher der Verdacht, dass er ausschließlich deshalb nach Österreich reiste, um sich mit dem russischen Botschaftsmitarbeiter zu treffen.

Im Zuge von Hausdurchsuchungen bei dem Beschuldigten konnten elektronische Datenträger, eine verbotene Waffe sowie diverse firmeninterne Unterlagen des Energieunternehmens sichergestellt werden. Die Unterlagen und Gegenstände deuteten darauf hin, dass der Mitarbeiter des Energieunternehmens bereits seit längerer Zeit Geschäfts- oder



Betriebsgeheimnisse zugunsten des Auslandes ausgekundschaftet und einen geheimen Nachrichtendienst zum Nachteil Österreichs unterstützt hatte.

Derartige Ermittlungen sind in der Regel komplex und stellen die österreichischen Sicherheitsbehörden vor besondere Herausforderungen. Diplomaten haben auch in Österreich eine besondere immunitätsrechtliche Stellung. Im gegenständlichen Fall genoss der Botschaftsmitarbeiter absolute Immunität im Sinne des Art. 31 Abs. 1 Wiener Übereinkommen über diplomatische Beziehungen (WDK). Der Botschaftsmitarbeiter war daher von der Strafgerichtsbarkeit des Empfangsstaates (Österreich) ausgenommen. Eine strafrechtliche Verfolgung der Person und die Durchführung von Maßnahmen im Sinne der Strafprozessordnung waren daher ohne Aufhebung der Immunität ausgeschlossen.

Nachdem ein Ersuchen um Aufhebung der diplomatischen Immunität seitens der russischen Botschaft unbeantwortet blieb, wurde der Betroffene schließlich zur „unerwünschten Person“ erklärt und musste Österreich umgehend verlassen.

Russland reagierte auf die in Österreich gesetzten Maßnahmen spiegelbildlich mit der Ausweisung eines Mitarbeiters der österreichischen Botschaft in Moskau.

Fall IT-INFRASTRUKTUR

Im Juni 2025 stellte das Bundesministerium für Inneres Unregelmäßigkeiten in der hauseigenen IT-Infrastruktur fest. Eine weitere Untersuchung der festgestellten Abnormitäten ergab Anhaltspunkte, dass unbefugte Akteure offenbar Zugriff auf Teile der Computersysteme des Innenministeriums erlangt hatten. In Folge wurde neben der sofortigen Einbindung der zuständigen Bereiche auch die DSN zur Analyse des möglichen Sicherheitsvorfalles zugezogen.

Innerhalb kurzer Zeit konnte festgestellt werden, dass unbekannte Täter offensichtlich in das Netzwerk des Innenministeriums eingedrungen waren. Ebenso konnte verifiziert werden, dass die Zugriffe der Täter in Systembereiche nur eingeschränkt möglich waren.⁷³ Die Art und Weise der festgestellten technischen Bewegungsabläufe legten den Verdacht nahe, dass es sich um einen professionellen Angriff auf das Computersystem handelte. Durch das Vorgehen und die angewandte Methodik war die Zielsetzung einer langfristigen Etablierung im System erkennbar.

Die Täter interessierten sich insbesondere für etwa 100 persönliche Mailboxen von Führungskräften und Bediensteten, die auf Grund ihrer Tätigkeit zumindest partiell über schutzwürdige Informationen zur nationalen und internationalen sicherheitsstrategischen Ausrichtung des Innenministeriums verfügten. Erkennbar war durch das Vorgehen und

⁷³ In der Vorfallaufarbeitung und den einhergehenden Ermittlungen konnten keine Hinweise festgestellt werden, dass Zugriff auf polizeiliche Informationssysteme und Datenbanken bestand.

die Zielsetzung zudem, dass die Täter über professionelle Strukturen und Werkzeuge zur Durchführung eines solchen Angriffes verfügten.

Im Zuge der Ermittlungen wurde eine durchgehende Beobachtung der Handlungen der Täter im System durchgeführt, um Kenntnisse über die Strukturen und Methoden der Akteure feststellen zu können. Durch die kontrollierte Beobachtung der Akteure im Netzwerk war es möglich, diese in ihren Bewegungen einzuschränken und weiteren Schaden zu verhindern.

Durch die gewonnenen Erkenntnisse konnten die Täter aus dem System entfernt werden. Parallel wurden strafrechtliche Ermittlungen wegen widerrechtlichen Zugriffes auf Computersysteme geführt, die folglich auf den Tatbestand gem. § 256 StGB (Geheimer Nachrichtendienst zum Nachteil Österreichs) erweitert wurden.

Die festgestellte Methodik und eingesetzten Werkzeuge der Täter weisen Parallelen zu bereits bekannten Angriffen von staatlichen oder staatsnahen Akteuren aus dem asiatischen Raum auf.

2.6.4 Trends und Entwicklungstendenzen

Russland

Hybrider Angriff Russlands gegen Europa

Russland wird seine hybriden Angriffstaktiken auch künftig gezielt einsetzen, um die Handlungsfähigkeit und die Einheit des Westens, der NATO und der Europäischen Gemeinschaft zu unterminieren. Vor dem Hintergrund des anhaltenden russischen Angriffskrieges gegen die Ukraine wird ein strategischer Fokus Russlands weiterhin auf Maßnahmen zur Beeinträchtigung der Unterstützung der Ukraine durch den Westen liegen. Folglich ist davon auszugehen, dass die russischen Nachrichtendienste ihre in Europa bestehenden Informationsbeschaffungsnetzwerke weiter ausbauen, um Entwicklungen frühzeitig antizipieren zu können.

Im Berichtsjahr wurden in unterschiedlichen Staaten Europas Sabotagefälle festgestellt, die eine Urheberchaft Russlands aufgrund der Zielauswahl als plausibel erscheinen lassen. Sabotageakte sind ein effektives Werkzeug hybrider Angriffe, um zentrale Bereiche zu destabilisieren und ein Klima der Verunsicherung zu erzeugen. Zudem soll die Reaktions- und Handlungsfähigkeit der betroffenen Länder getestet werden. Angesichts bereits erfolgter Sabotageakte ist insbesondere im Bereich der kritischen Infrastruktur und der militärischen Transportlogistik von einem anhaltend hohen Gefahrenpotenzial auszugehen. Aus diesem Grund ist es essenziell, europaweit einen verstärkten Fokus auf die Resilienz der kritischen Infrastruktur zu legen.

Im Jahr 2025 wurde in mehreren europäischen Staaten ein signifikanter Anstieg von Drohnensichtungen verzeichnet, welche unter anderem unmittelbare Sicherheitsmaß-

nahmen wie temporäre Flughafenschließungen nach sich zogen. Ob diese Vorfälle im Kontext hybrider Bedrohungstaktiken Russlands stehen, ist bislang nicht abschließend geklärt. Die Vorkommnisse haben jedenfalls das Schadenspotenzial bzw. die Eignung von Drohnen als Mittel hybrider Bedrohungstaktiken aufgezeigt. Drohnen sind vergleichsweise leicht verfügbar, mit begrenztem technischen Aufwand steuerbar und flexibel einsetzbar. Zudem ist die Detektion der Piloten herausfordernd und ermöglicht das Abstreiten von Verantwortlichkeiten. Gleichzeitig bergen diese Vorfälle das Risiko, alle Vorkommnisse vorschnell Russland zuzurechnen. Auch dies kann ein gewünschter Effekt hybrider Bedrohungstaktiken sein. Des Weiteren können sie sowohl beträchtliche materielle Auswirkungen als auch psychologische Effekte wie gesellschaftliche Verunsicherungen hervorrufen. Jedenfalls haben die Vorfälle des Jahres 2025 die Notwendigkeit einer nationalen und internationalen Resilienz gegen Drohnenangriffe aufgezeigt.

Im Einklang mit seinen übergeordneten strategischen Zielsetzungen setzt Russland weiterhin auf Einflussnahme und Desinformation, um verschiedene gesellschaftliche und politische Bereiche im Sinne eigener Narrative zu formen. Diese Maßnahmen werden auch künftig sowohl im digitalen wie auch im physischen Raum Anwendung finden. Vor dem Hintergrund des raschen technologischen Fortschritts, insbesondere im Bereich der Künstlichen Intelligenz, die die Generierung und Verbreitung manipulativer Inhalte erheblich vereinfacht, ergibt sich ein wachsender Bedarf an effektiven Strategien zur frühzeitigen Erkennung und Offenlegung manipulierter Inhalte. Desinformation kann gesellschaftliche Spannungen verstärken und zu einer stärkeren Polarisierung der Gesellschaft beitragen. Insbesondere staatlich gelenkte russische Einflussoperationen, die mit technischer Unterstützung umgesetzt werden (z. B. Bot-Netzwerke), können Debatten maßgeblich zugunsten Russlands verzerren. Diese Narrative werden auch in Österreich durch russlandaffine Akteurinnen und Akteure über soziale Medien weiter verstärkt und in ihrer Reichweite potenziert.

Es ist zu erwarten, dass Russland auch weiterhin auf ein breites Spektrum staatlicher und nichtstaatlicher Ressourcen zur Durchführung hybrider Taktiken zurückgreifen wird. Russland wird dazu nachrichtendienstliches Personal einsetzen, welches entweder unter diplomatischer Abdeckung oder verdeckt als Non-Official-Cover in Europa operiert.

Es ist davon auszugehen, dass Russland zudem weiterhin verstärkt Proxy-Akteurinnen und Proxy-Akteure rekrutieren und einsetzen wird, um in Europa verdeckte Einfluss-, Informations- und Sabotageaktivitäten flexibel und schwer nachweisbar durchzuführen.

Sollte es zu Friedensverhandlungen zwischen Russland und der Ukraine kommen, die eine vorläufige Beendigung des russischen Angriffskrieges gegen die Ukraine zur Folge hätten, ist davon auszugehen, dass Russland – auch vor dem Hintergrund der eigenen angespannten wirtschaftlichen Lage – versuchen wird, die Beziehungen zum Westen in ausgewählten Bereichen wieder zu intensivieren. In diesem Kontext dürfte Moskau

insbesondere auf eine schrittweise Lockerung bestehender Sanktionen hinwirken. Entsprechend ist zu erwarten, dass künftige Einfluss- und Desinformationskampagnen auf jene Sektoren ausgerichtet werden, in denen eine Normalisierung der wirtschaftlichen und politischen Beziehungen als strategisch vorteilhaft erscheint. Auch das Aufklärungsinteresse der russischen Nachrichtendienste würde sich dementsprechend verschieben.

Unter der gegenwärtigen politischen Führung betrachtet Russland seine Beziehungen zum Westen als Teil eines andauernden und strukturellen Konflikts, der den russischen Angriffskrieg gegen die Ukraine deutlich übersteigt. Selbst im Falle einer Friedenslösung wäre weiterhin davon auszugehen, dass feindliche Aktivitäten gegenüber europäischen Staaten fortbestehen würden. Allerdings wäre mit einer Anpassung der eingesetzten Modi Operandi an die veränderten Rahmenbedingungen und strategischen Zielsetzungen zu rechnen.

Cyberentwicklungen

Auch in Zukunft werden sich russische Akteure im Cyberraum weitestgehend auf die Ukraine und militärisch relevante Drittstaaten fokussieren. Mittels Durchführung von Cyberspionage-Operationen wird weiterhin versucht werden, Nachschublinien und Truppenbewegungen aufzuklären. Zusätzlich ist die zunehmende Kooperation mit der organisierten Kriminalität eine relevante Entwicklung im Zusammenhang mit russischen Nachrichtendiensten.

Österreich ist im Hinblick auf den russischen Angriffskrieg in der Ukraine derzeit kein primäres Ziel russischer Cyberspionagekampagnen. Dennoch kann es zu einem Anstieg an Cyberangriffen gegen österreichische Behörden und kritische Infrastrukturen kommen, sofern aufgrund von Verhandlungen, Sanktionsmaßnahmen oder anderen geopolitischen Aktionen die Bedeutung der Positionierung Österreichs zunimmt.

China

Verstärkte Präsenz im Bereich Forschung und internationale Zusammenarbeit

Die systematische Expansion chinesischer Präsenz in der internationalen Forschungslandschaft und in multilateralen Kooperationsstrukturen hat 2025 eine neue Qualität erreicht. Zwar verschärften viele EU-Staaten ihre Schutzmaßnahmen bei internationalen Forschungsk Kooperationen, dennoch nutzt China gezielt die noch bestehenden Vulnerabilitäten zur Ausweitung seiner nachrichtendienstlichen Aktivitäten. Die von den USA im Jahr 2025 vorgenommenen Budgetkürzungen bei der internationalen Forschungszusammenarbeit und bei multilateralen Organisationen betrafen auch in Österreich ansässige Institutionen. Das dadurch entstandene Machtvakuum weiß China durch bereitgestellte Gelder und verfügbares Personal systematisch zu füllen.

Der international bedeutsame Standort Wien mit dem Sitz der Vereinten Nationen und weiterer multilateraler Institutionen ist ein Hauptziel chinesischer Einflussnahme. Mit Blick

auf das Ziel des weiteren Ausbaus seiner Präsenz auf globaler Ebene hat China seine finanziellen Beiträge für in Wien ansässige internationale Organisationen in den letzten Jahren deutlich erhöht und fordert im Gegenzug hochrangige Führungspositionen ein. Einige der multilateralen Organisationen in Wien verzeichneten in den letzten Jahren einen Anstieg chinesischen Personals in Schlüsselpositionen. Diese Platzierungen dienen nicht nur der Informationsgewinnung über westliche Strategien und Technologien, sondern auch der aktiven Beeinflussung internationaler Standards und Normen im chinesischen Interesse. Durch seine intensiviertere Involvierung in Standardisierungsgremien möchte China die Festlegung technischer Standards in Zukunftstechnologien kontrollieren. So könnte es China gelingen, eigene Produkte und Systeme als globale Norm zu etablieren, was einer Realisierung der nationalen Vorgaben der „China Standards 2035“-Initiative gleichkäme.

Die Gefahr eines massiven Know-how-Verlusts durch Wissensspionage und schleichende Unterwanderung des österreichischen Innovationssystems nahm im Jahr 2025 weiter zu. Der in Österreich lebenden chinesischen Diaspora fällt dabei eine Schlüsselrolle zu. Chinesische Studierende, Studierendenvereine sowie Wissenschaftlerinnen und Wissenschaftler werden von chinesischen Nachrichtendiensten für wissenschaftliche Spionage und Technologietransfer mobilisiert. Sie unterliegen auch in Österreich einem engmaschigen Kontrollsystem durch die chinesischen Nachrichtendienste. Sie können zur Ausspähung von Landsleuten ebenso eingesetzt werden wie als Rekrutierungspool für nachrichtendienstliche Aktivitäten.

Das „Thousand-Talents-Plan“-Programm zur Anwerbung ausländischer Fachexpertinnen und Fachexperten wird zunehmend durch subtilere Rekrutierungsmechanismen ergänzt. Statt auf offensive Abwerbung setzen chinesische Akteure vermehrt auf die diskretere, langfristige „Kultivierung“ von Talenten durch großzügige Forschungsförderung, Einladungen zu prestigeträchtigen Konferenzen und lukrative Beratungsverträge.



Der sogenannte „**Thousand-Talents-Plan**“ ist ein integraler Bestandteil der chinesischen Strategie zur Wissensbeschaffung in westlichen Ländern. Im Rahmen dieses Talentplans wirbt China u. a. Wissenschafts- und Technologieprofessorinnen und -professoren, Forschende sowie Studierende an – unabhängig von deren Staatsangehörigkeit oder nationalen Herkunft. Insbesondere Personen mit Fachwissen oder Zugang zu Technologien, über die China nicht verfügt, stehen im Fokus dieser Initiativen. Im Gegenzug für die Beschaffung ausländischer Technologien, die die KPCh für nationale, militärische und wirtschaftliche Ziele benötigt, werden den angeworbenen Talenten finanzielle, persönliche und berufliche Vorteile in Aussicht gestellt.

Die Intensivierung chinesischer Aktivitäten im österreichischen Forschungssektor erfordert dringend den weiteren Ausbau bereits bestehender Präventionsmechanismen, wie etwa tiefergehende Risikobewertungen chinesischer Akademikerinnen und Akademiker vor ihrer Zulassung. Dies ist auch deshalb notwendig, da China aufgrund der in den letzten Jahren in einigen EU-Ländern etablierten rigiden Visascreenings versuchen könnte, mit seinen dort abgelehnten Bewerberinnen und Bewerbern auf andere Länder auszuweichen. Will Österreich seine Position als attraktiver Forschungsstandort bewahren, gilt es, neben der Wissenschaftsfreiheit auch vermehrt die technologische Souveränität und die österreichischen Sicherheitsinteressen zu schützen.

Cyberentwicklungen

Die Aktivitäten chinesischer Nachrichtendienste im Cyberraum werden sich in Europa weiterhin auf Wirtschafts- und Wissenschaftsspionage fokussieren. Dabei sind vor allem Unternehmen der Halbleiterbranche und andere Pioniere der Hochtechnologie attraktive Angriffsziele. Zur Aufklärung der eigentlichen Zielsysteme kann es zu Angriffen gegen Betreiber von Telekommunikationsnetzen kommen. Dies betrifft zunehmend vor allem die digitale Infrastruktur großer Cloudanbieter. Die erlangten Zugriffe können in weiterer Folge für Cybersabotageoperationen gegen physische und digitale Infrastruktur genutzt werden. Im Zuge dessen kann es zu Spill-Over-Effekten⁷⁴ auf andere Staaten kommen. Vermehrte Vorfälle innerhalb der EU können als Indikatoren für eine zukünftig verstärkte politische Cyberspionage gewertet werden.

Iran

Proxy-Akteure als zentrales Mittel

Die nachrichtendienstlichen Aktivitäten des Iran unterliegen einem kontinuierlichen Wandel, der durch geopolitische Faktoren, technologische Fortschritte und die Notwendigkeit zur Verschleierung staatlicher Beteiligung geprägt ist. Ein zentrales Mittel dieser Strategie bleibt die Nutzung von Proxy-Akteurinnen und Proxy-Akteuren, die als Puffer zwischen dem Regime und den ausführenden Operationen dienen. Diese Entwicklung hat sich seit den 2000er-Jahren verstärkt und wird voraussichtlich auch in absehbarer Zukunft weitergeführt, insbesondere im Kontext des Konflikts zwischen Israel und dem Iran, bei der hybriden Kriegsführung und im Rahmen asymmetrischer Bedrohungen. Der Einsatz von Proxy-Akteurinnen und Proxy-Akteuren ermöglicht es dem Iran nicht nur, Einfluss auszuüben, ohne eine direkte Zuordnung zu riskieren, sondern eignet sich auch zur Anpassung an veränderte Sicherheitslandschaften, etwa durch den verstärkten Einsatz von Kriminellen, Milizen oder zivilen Tarnstrukturen.

74 Der „Spill-Over-Effekt“ bezeichnet in diesem Fall die Möglichkeit, dass ein Cyberangriff über nationale Grenzen hinaus gesellschaftliche oder wirtschaftliche Systeme beeinflussen kann. Beispielsweise kann ein Cyberangriff auf eine nationale Infrastruktur zu einem Spill-Over-Effekt in der benachbarten Wirtschaft führen, indem Lieferketten unterbrochen werden.

Ein markanter Trend ist seit einiger Zeit die zunehmende Rekrutierung sogenannter „Wegwerfagenten“ („disposable agents“), die als kurzfristig einsetzbare, „entbehrliche“ Akteurinnen und Akteure fungieren. Diese Personen werden oft über soziale Medien, kriminelle Netzwerke oder informelle Kanäle angeworben und sind in der Regel ideologisch nicht fest verankert, sondern primär durch finanzielle Anreize motivierbar. Besonders auffällig ist hierbei die Nutzung von Jugendlichen und Minderjährigen, die schon für geringe Summen zu riskanten Operationen bereit sind.

Beispiele aus Europa, die dem Iran attribuiert werden konnten, zeigen, wie junge Menschen in Attentatsversuche auf israelische oder jüdische Ziele verwickelt waren. Ein 15-Jähriger versuchte, mit einer geladenen Waffe das israelische Botschaftsgebäude in Stockholm zu erreichen; ein 13-Jähriger feuerte Schüsse auf ein israelisches Rüstungsunternehmen in Göteborg und ein 16-Jähriger platzierte Sprengsätze vor dem Haupteingang eines israelischen Rüstungsunternehmens. Diese Jugendlichen sind für iranische Dienste wenig verlässlich, da sie zumeist untrainiert, oft impulsiv und anfällig für Enttarnung sind. Dennoch erweisen sie sich als nützlich, da sie eine hohe Plausibilitätsverleugnung ermöglichen: Ihre Beteiligung kann als jugendliche Kriminalität oder lokaler Extremismus abgetan werden, was die Verbindung zu Teheran verschleiert. Diese Strategie minimiert die Risiken für das Regime und nutzt die Vulnerabilitäten bestimmter Gruppen, insbesondere Armut oder soziale Marginalisierung, aus, um kostengünstig Operationen durchführen zu können. Als Verbindungsglied agieren oftmals kriminelle Gruppen, die die tatsächlichen Attentäterinnen und Attentäter anheuern oder mit diesen affiliert sind.

In diesem Kontext kann nicht ausgeschlossen werden, dass auch hinter so manchen antisemitischen Aktionen in Europa vom Iran gesteuerte Operationen durch Proxy-Akteurinnen und Proxy-Akteure stehen. Der Iran hat eine lange Geschichte verdeckter Angriffe im Ausland, um ideologische Ziele zu verfolgen und geopolitischen Druck auszuüben. Seit 2023 deuten Berichte darauf hin, dass kriminelle Gangs und rekrutierte Individuen in solche Vorfälle involviert sind, so etwa in Australien, wo eine iranische Beteiligung an antisemitischen Attacken zur Ausweisung des Botschafters führte. Diese Entwicklung könnte sich weiter verstärken, da der Kollaps traditioneller Proxy-Strukturen im Nahen Osten, etwa durch den Verlust einflussreicher Milizen, den Iran zu neuartigen, dezentralisierten Ansätzen in Europa zwingt. Zukünftige Tendenzen umfassen möglicherweise auch die Integration von Cyber-Elementen, wie KI-gestützte Rekrutierungen oder Desinformationskampagnen, um die Effizienz solcher Operationen zu steigern. Um diese Trends einzudämmen, ist eine verstärkte Überwachung von Rekrutierungsnetzwerken und die Kooperation mit sicherheitspolitischen Partnerinnen und Partnern essenziell.

Cyberentwicklungen

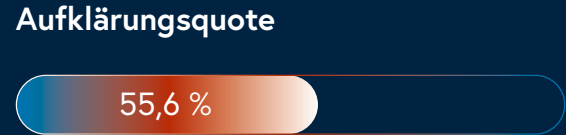
Iranische Nachrichtendienste verfolgen im Cyberraum vorrangig zwei Ziele. Zum einen betreiben sie Spionage gegen Unternehmen aus jenen Wirtschaftssektoren, die aufgrund

der gegen den Iran verhängten internationalen Sanktionen für diesen von besonderer Bedeutung sind. Zum anderen werden iranische Dissidentinnen und Dissidenten im Westen ausspioniert. Es ist davon auszugehen, dass der Iran dieses Verhalten auf absehbare Zeit fortsetzen wird. Im Zuge des anhaltenden Iran-Israel-Konflikts spielen Haktivistinnen und Haktivisten eine zunehmend wichtigere Rolle. Dem Iran gelingt es, weltweit computeraffine Bevölkerungsschichten mit Iran-nahen ideologisch-religiösen Motivlagen für sich zu gewinnen und zur Umsetzung von iranischen Zielen einzusetzen. Auch wenn die Angriffe in der Regel nur geringe Auswirkungen haben, erwecken sie dennoch den Eindruck einer globalen, modernen und militanten Solidaritätsbewegung für die Ziele des Irans.



Spionage und Cyberangriffe

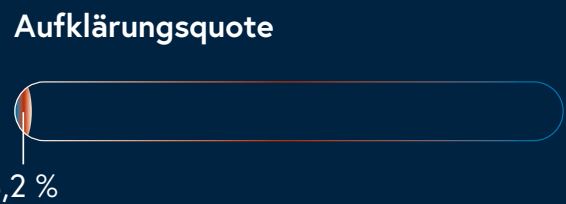
Spionage



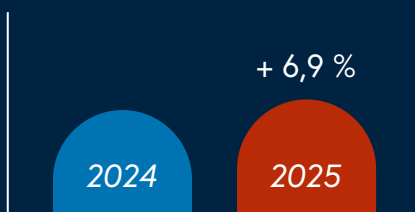
Bundesländeraufteilung



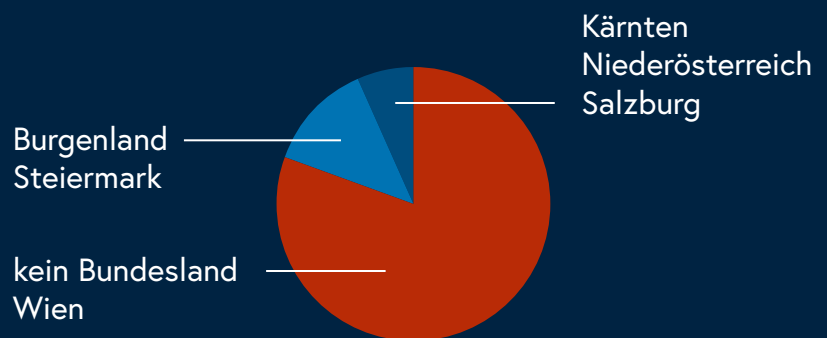
Cyberangriffe



Anstieg zum Vorjahr



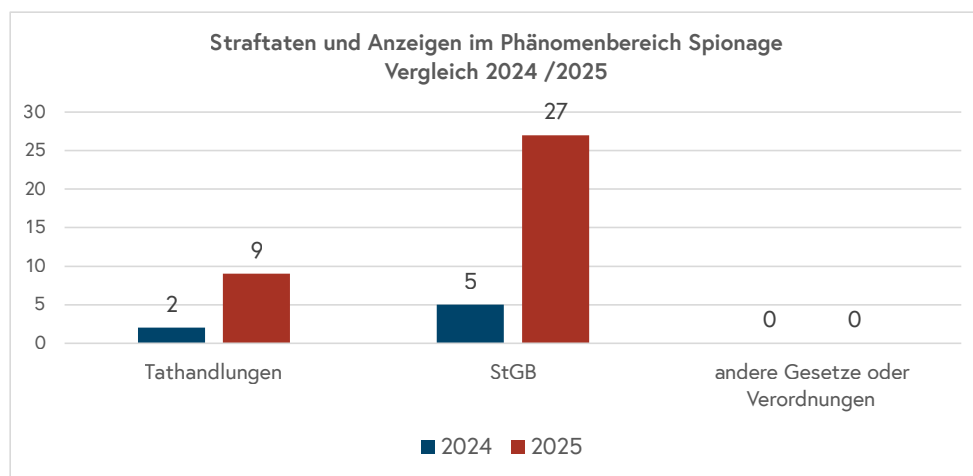
Bundesländeraufteilung



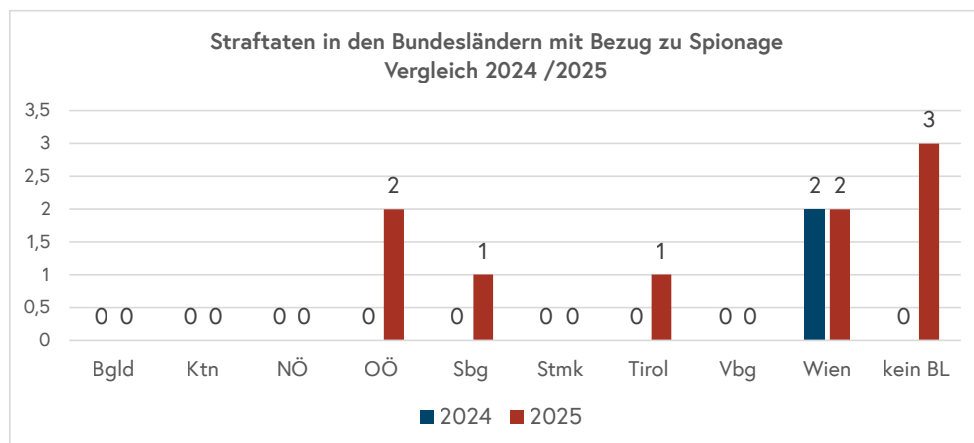
2.6.5 Zahlen/Daten/Fakten Spionage

Im Jahr 2025 wurden bei den Sicherheitsbehörden in Österreich in der Kategorie **Spionage** insgesamt **neun Tathandlungen** registriert (2024: 2). Fünf Tathandlungen wurden aufgeklärt, die Aufklärungsquote liegt somit bei 55,6 Prozent (2024: 100 Prozent).

Im Zusammenhang mit den gesetzten Tathandlungen gelangten insgesamt **27 Delikte** nach dem Strafgesetzbuch zur Anzeige (2024: 5) Insgesamt konnten **16 Tatverdächtige** **ausgeforscht** und zur Anzeige gebracht werden (2024: 2). Neben den ausgeforschten Personen erfolgten im Berichtsjahr **vier Anzeigen gegen unbekannte Täterinnen oder Täter**.



Anzeigen nach dem StGB	2024	2025
Freiheitsentziehung (§ 99 StGB)	0	1
Überlieferung an eine ausländische Macht (§ 103 StGB)	1	0
Gefährliche Drohung (§ 107 StGB)	1	0
Diebstahl (§ 127 StGB)	1	0
Entziehung von Energie (§ 132 StGB)	0	0
Geldwäscherei (§ 165 StGB)	0	3
Verrat von Staatsgeheimnissen (§ 252 StGB)	0	0
Geheimer Nachrichtendienst zum Nachteil Österreichs (§ 256 StGB)	2	20
Fälschung eines Beweismittels (§ 293 StGB)	0	3
Militärischer Nachrichtendienst für einen fremden Staat (§ 319 StGB)	0	0
Summe	5	27



2.6.6 Zahlen/Daten/Fakten staatschutzrelevante Cyberangriffe

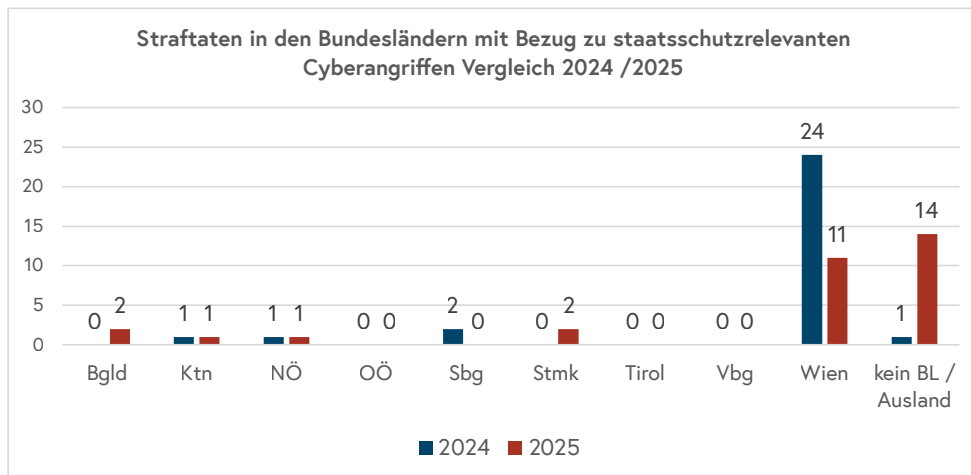
Im Phänomenbereich der **Cyberangriffe** wurden den Sicherheitsbehörden im Berichtsjahr 2025 insgesamt **31 staatschutzrelevante Tathandlungen** (2024: 29) bekannt. Gegenüber dem Jahr 2024 bedeutet dies einen **Anstieg um 6,9 Prozent**.

Im Zusammenhang mit den gesetzten Tathandlungen gelangten insgesamt **34 Delikte** (2024: 31) nach dem Strafgesetzbuch (StGB) zur Anzeige.

Eine Tathandlung wurde aufgeklärt; die **Aufklärungsquote** liegt somit bei **3,2 Prozent** (2024: 0 Prozent).

Anzeigen nach dem StGB	2024	2025
Widerrechtlicher Zugriff auf ein Computersystem (§ 118a StGB)	1	19
Datenbeschädigung (§ 126a StGB)	2	2
Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB)	26	10
Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c StGB)	0	1
Erpressung (§ 144 StGB)	2	0
Schwere Erpressung (§ 145 StGB)	0	1
Geheimer Nachrichtendienst zum Nachteil Österreichs (§ 256 StGB)	0	1
Summe	31	34

Von den 31 registrierten Tathandlungen fanden elf in Wien, jeweils zwei im Burgenland und in der Steiermark sowie jeweils eine in Niederösterreich und in Kärnten statt. Bei 14 Tathandlungen waren österreichische Botschaften im Ausland betroffen (versuchte Einbringung von Schadsoftware via Phishing-E-mails).



2.7 Internationaler illegaler Waffenhandel

Unter dem „**internationalen illegalen Waffenhandel**“ wird die Weitergabe von und der Handel mit konventionellen Waffen (in ihrer Gesamtheit oder auch in Teilen), entsprechenden Ausrüstungsgütern, Software und Technologie entgegen den gesetzlichen Bestimmungen über nationale Grenzen hinweg verstanden.

2.7.1 Überblick

Illegal gehandelte oder geschmuggelte Schusswaffen stellen nicht nur hinsichtlich ihrer möglichen Verwendung in bewaffneten Konflikten eine Bedrohung dar, sondern werden auch von extremistischen und terroristischen Akteuren für Anschläge und Gewalttaten genutzt. Der Kampf gegen den unerlaubten Handel mit bzw. Schmuggel von Waffen und Waffenteilen zählt daher zu den sicherheitspolitischen Prioritäten der Europäischen Union. Ein zentraler Baustein im Rahmen dieser Bemühungen ist der im Juli 2020 beschlossene „EU-Aktionsplan gegen den unerlaubten Handel mit Feuerwaffen (2020-2025)“. Dieser Plan definiert mehrere Handlungsfelder, darunter den „Ausbau der internationalen Zusammenarbeit“ und die „Erhöhung des Drucks auf kriminelle Märkte“, sowie gezielte Maßnahmen, um den illegalen Waffenmarkt zu bekämpfen und den legalen Handel zu stärken.

Trotz dieser verstärkten gesamteuropäischen Bemühungen blieb der illegale internationale Waffenhandel auch im Jahr 2025 eine bedeutende Herausforderung für die Sicherheit Österreichs. Dies liegt zum einen an der Tatsache, dass er oftmals in Kombination mit anderen Formen der Kriminalität auftritt, zum anderen an der geografischen Lage Österreichs, aus der eine besondere Rolle Österreichs als Transitland für den Schmuggel von Schusswaffen, Kriegsmaterial, Sprengstoff und Munition resultiert, insbesondere aus

den Ländern des Westbalkans. Der rege Güter- und Personenverkehr sowie fehlende Grenzkontrollen im Schengen-Raum erleichtern den Schmuggel zusätzlich.

2.7.2 Aktuelle Lage

Anders als häufig angenommen wird der überwiegende Teil illegal gehandelter Schusswaffen, sonstigen Kriegsmaterials, Munition und Sprengmittel nicht per se für den Schwarzmarkt produziert, sondern stammt ursprünglich aus legaler Produktion und dem legalen Handel damit. Erst im Laufe der Zeit gelangen diese Güter durch verschiedene Modi Operandi auf den Schwarzmarkt und werden dort illegal gehandelt. Dies geschieht in Österreich in der Regel durch Einzelpersonen, seltener durch organisierte Gruppen, die sich auf bestimmte Beschaffungsmethoden spezialisieren, um an illegale Schusswaffen zu gelangen und diese weiterzuverkaufen. Nationale Grenzen spielen als Behinderung dieses illegalen Waffenhandels nur mehr eine untergeordnete Rolle. Vielmehr schaffen zusammenwachsende Wirtschaftsräume für Kriminelle neue Chancen. Sie bieten ihnen die Möglichkeit, relevante politische Entwicklungen wie innerstaatliche Konflikte oder nationale legislative Unterschiede weltweit zu ihren Gunsten auszunutzen. Durch diese Entwicklung vermischen sich zunehmend die regionale, nationale und internationale Ebene des illegalen Waffenhandels. Dies zeigt sich auch am Beispiel Österreichs.

Um illegale Schusswaffen für den Schwarzmarkt zu beschaffen, werden viele verschiedene Modi Operandi genutzt. Bedingt durch die geografische Lage war Österreich viele Jahre vor allem Transit, aber auch Zielland von illegalen Schusswaffen aus den noch existierenden Beständen der ehemals sozialistischen Nachbarländer und der Nachfolgestaaten des ehemaligen Jugoslawien.

In den letzten Jahren veränderte sich diese Lage jedoch. Durch die spezifische österreichische Rechtslage hinsichtlich nicht wesentlicher Waffenteile wurde Österreich zunehmend zu einem Quellland. Solche hierorts nicht wesentlichen Waffenteile⁷⁵ – in der Regel betrifft dies Griffstücke und Gehäuse – wurden legal im heimischen Handel in großen Mengen beschafft und weltweit illegal ausgeführt. Letzten Endes wurden sie dann mit weiteren Waffenteilen, die andernorts beschafft oder illegal selbst angefertigt worden waren, zu funktionsfähigen Schusswaffen zusammengesetzt. Oft fanden in den letzten Jahren derart beschaffte freie Waffenteile aus Österreich schon kurze Zeit nach ihrem Verkauf in Österreich Verwendung bei Gewalttaten im europäischen Ausland. Durch die Novellierung des Waffengesetzes im Jahr 2025 wurde diese Rechtslücke geschlossen.

75 Nicht wesentliche Waffenteile sind Bauteile einer Schusswaffe, die nicht zu den gesetzlich als „wesentlich“ definierten Teilen gehören (z. B. Lauf oder Verschluss). Sie sind für die Schussabgabe nicht unmittelbar funktionsentscheidend und unterliegen daher in der Regel nicht den gleichen waffenrechtlichen Erlaubnispflichten wie wesentliche Teile.

Anders stellt sich die Lage in Bezug auf illegale Sprengmittel dar. Hier dominieren aktuell aus Vorläuferstoffen illegal hergestellte Sprengmittel, sogenannte Selbstlaborate, und zweckentfremdete Pyrotechnik. Wurden entsprechende Vorläuferstoffe früher hauptsächlich noch im stationären Handel bezogen, so nahm in den letzten Jahren der Erwerb derselben bei lizenzierten Onlinehändlern stetig zu. Mittlerweile können kaum noch Beschaffungsversuche im stationären Handel festgestellt werden. Anders stellt sich die Lage im Hinblick auf zweckentfremdete Pyrotechnik dar. Diese wird durch dazu nicht befugte Personen vor allem in grenznahen Märkten in bestimmten Nachbarländern erworben und dann unerlaubt nach Österreich eingeführt. Sprengmittel aus dem legalen Handel oder dem militärischen Bereich finden sich hingegen kaum am Schwarzmarkt.

Immer wieder ergeben sich vor allem bei illegalen Schusswaffen und Sprengmitteln Bezüge zur schweren und organisierten Kriminalität. Aber auch extremistische und terroristische Akteure streben danach, solche Güter als „Force Multiplier“ bzw. „Kraftverstärker“ für ihre Taten zu beschaffen, wie nationale und internationale Beispiele der jüngeren Vergangenheit zeigen.

Darüber hinaus streben auch staatliche Akteure immer wieder danach, entgegen den gesetzlichen Bestimmungen an rüstungsrelevante österreichische Güter zu gelangen. In diesen Fällen zielen die verdeckten Beschaffungsvorgänge nur selten auf Schusswaffen oder Sprengmittel ab. Vielmehr wird vorrangig versucht, Verteidigungsgüter, Dual-Use-Güter und hochwertige Freiwaren⁷⁶ für die eigenen konventionellen Rüstungsvorhaben zu beschaffen. Diese finden dann in entsprechenden Waffensystemen oder aber in der Forschung, Entwicklung sowie Produktion von Rüstungsgütern Verwendung. Als anerkannter Forschungsstandort und Sitz bedeutender Produzenten und Händler in verschiedenen Technologiebereichen steht Österreich hier besonders im Fokus. Durch konspiratives Vorgehen versuchen solche staatlichen Akteure, diese Beschaffungen verdeckt durchzuführen und bestehende Exportkontrollmechanismen zu umgehen. Dabei werden nicht nur die zuständigen Behörden über die tatsächliche Endverwendung getäuscht, sondern oft auch die involvierten österreichischen Betriebe selbst.

Das „**Wassenaar Abkommen**“ (**WA**) ist ein internationaler Vertrag von 42 Staaten zur Exportkontrolle, der darauf abzielt, destabilisierende Waffenansammlungen zu verhindern. Das Abkommen wurde 1995 ausgearbeitet und 1996 von 33 Gründungsmitgliedern, darunter Österreich, unterzeichnet. Durch die Koordination der entsprechenden Exportkontrollmaßnahmen leisten die Mitgliedsstaaten einen wichtigen Beitrag zur regionalen und internationalen Sicherheit.



⁷⁶ Dabei handelt es sich um Güter, die keinen Exportbeschränkungen unterliegen, wie beispielweise besondere Werkzeuge oder Materialien.



2.7.3 Fälle 2025

Fall *SELBSTLABORATE*

Die DSN wurde im Juli 2025 von einer ausländischen Sicherheitsbehörde in Kenntnis gesetzt, dass ein im Bundesgebiet wohnhafter polnischer Staatsbürger improvisierte Sprengsätze und mehrere Schusswaffen im Zuge seines Heimaturlaubes nach Polen verbracht hatte.

Beim Bau der bzw. Hantieren mit den Sprengsätzen kam es zu einer Explosion. Im Zuge weiterer Erhebungen konnte festgestellt werden, dass die Explosion zustande kam, während Vorprodukte zur Herstellung explosivfähiger Stoffe in Form von pyrotechnischen Gegenstände gemischt bzw. gemahlen wurden. Der Mann wurde mit lebensgefährlichen Verletzungen und schweren Verbrennungen in ein polnisches Krankenhaus eingeliefert. Der Beschuldigte verfügte über keine offizielle Ausbildung im Umgang mit Pyrotechnik bzw. Sprengstoffen. Seine amateurhaften Kenntnisse auf dem Gebiet der Sprengstoffherstellung hatte er sich autodidaktisch angeeignet.

Aufgrund dieses Vorfalls wurde der Beschuldigte bereits in Polen verdächtigt, einerseits in die Produktion von Pyrotechnik bzw. Sprengstoff involviert zu sein, und andererseits illegal Schusswaffen und Munition zu besitzen. Da nicht ausgeschlossen werden konnte, dass sich weitere explosionsgefährliche Stoffe bzw. Schusswaffen auch an der österreichischen Wohnadresse des Beschuldigten befinden, wurde unverzüglich eine Hausdurchsuchung durch die Staatsanwaltschaft Wien angeordnet.

Tatsächlich konnten in der Wohnung Chemikalien, Zünder zur Herstellung von Sprengmitteln bzw. Pyrotechnik, ein Schalldämpfer, Magazine, ein Totschläger, eine Machete und eine Vorderschaftrepetierflinte vorgefunden und sichergestellt werden. Im Zuge der waffentechnischen Untersuchung sowie waffenrechtlichen Einordnung durch das kriminaltechnische Büro im Bundeskriminalamt wurde der Totschläger als verbotene Waffe der Kategorie A eingestuft. Es stellten sich der für Schreckschusswaffen bestimmte und im vorliegenden Zustand nicht für die Verwendung an einer Schusswaffe geeignete Schalldämpfer und Magazine sowie die Vorderschaftrepetierflinte als Soft-Air-Gewehr und somit nicht dem Waffengesetz unterliegende Gegenstände heraus.

Ein dem Beschuldigten zuordenbares Kellerabteil, das ebenfalls durchsucht wurde, war mit besonderen Zutrittssperren und weiteren Sicherheitsmerkmalen versehen. In diesem Abteil konnten die Einsatzkräfte ein eingerichtetes Labor zur Herstellung von Chemikalien sowie zur Bearbeitung und Anfertigung von Schussapparaten vorfinden. Durch den beigezogenen Entschärfungsdienst konnten im Kellerbereich unter anderem zwei in Vorbereitung befindliche, sogenannte „unkonventionelle“ Spreng- und Knallvorrichtungen gesichert und beschlagnahmt werden. Zudem wurden diverse Substanzen und Suchtgifte sichergestellt. Das sichergestellte Material wurde durch Chemiker des Bundeskriminalamtes auf seine chemische Zusammensetzung analysiert, um festzu-

stellen, ob bzw. welche Explosivstoffe enthalten sind. Aufgrund der nachgewiesenen Elemente, Ionen und Verbindungen handelte es sich beim Großteil des sichergestellten Pulvers um Schwarzpulver. Gegen den Beschuldigten wurde in Abwesenheit zuerst ein vorläufiges Waffenverbot ausgesprochen, nach Prüfung durch die zuständige Behörde dann ein Waffenverbot verhängt.

In der Folge stand der Mann auch in Österreich im Verdacht, gerichtlich strafbare Handlungen begangen zu haben. Bezüglich der im Bundesgebiet verwirklichten Verstöße gegen das Waffen- und Sprengmittelgesetz wurde der zuständigen Staatsanwaltschaft berichtet.

Bei einer Hausdurchsuchung an der Wohnadresse des Beschuldigten in Polen konnten unter anderem Substanzen, die zur Herstellung von Pyrotechnik und Explosivstoffen geeignet sind, Gasdruckwaffen, Munition und ein Schalldämpfer sichergestellt werden.

Der Beschuldigte befand sich zum Zeitpunkt der Berichtslegung in einer polnischen Haftanstalt in Untersuchungshaft. Ein Abschlussbericht an die zuständige Staatsanwaltschaft Wien erfolgte.

Fall WAFFENSAMMLER

Im Mai 2025 langte bei einer oberösterreichischen Sicherheitsbehörde eine anonyme Anzeige ein, in der behauptet wurde, dass ein österreichischer Staatsbürger im Besitz illegal erworbener Waffen, darunter auch automatische Schusswaffen der Kategorie A, sei. Weiters hieß es, dass der Österreicher diese Gegenstände auch zum Verkauf anbiete, ohne über die dafür erforderlichen Berechtigungen zu verfügen.

Nach Einlangen dieses anonymen Hinweises wurden seitens des zuständigen LSE Oberösterreich unverzüglich entsprechende Ermittlungen aufgenommen, die die Verdachtsmomente verifizieren konnten. Gegen die beschuldigte Person war bereits in der Vergangenheit ein Waffenverbot verhängt worden, das jedoch wieder aufgehoben wurde, weshalb der Mann im Herbst 2023 erneut eine Waffenberechtigung erlangen konnte.

Im Zuge der Ermittlungen konnten insgesamt drei Tatverdächtige ausgeforscht werden. Durch die zuständige Staatsanwaltschaft Wels wurden mehrere Hausdurchsuchungen an den jeweiligen Wohnadressen angeordnet. Dabei konnten neben diversen Datenträgern insgesamt 374 Schusswaffen, davon 26 Stück der Kategorie A, 270 Stück der Kategorie B und 78 Stück der Kategorie C sichergestellt werden.⁷⁷

77 Kategorie A: vollautomatische Schusswaffen, Kriegsmaterial, Schalldämpfer udgl.; Kategorie B: halbautomatische Schusswaffen udgl.; Kategorie C: Langwaffen, Scharfschützengewehre, spezielle Schusswaffen für den Einsatz auf weite Distanzen.

Bei der sofort durchgeführten Einvernahme bezeichneten sich zwei der Männer als Waffensammler. Diese beiden Beschuldigten waren geständig und gaben an, die illegalen (verbotenen) Schusswaffen vom hauptverdächtigen Oberösterreicher gekauft zu haben. Letztgenannter verweigerte die Aussage zu den Vorwürfen.

Die drei Männer wurden bei der zuständigen Staatsanwaltschaft Wels angezeigt. Das Verfahren ist noch offen.

2.7.4 Trends und Entwicklungstendenzen

Aus europäischer Perspektive stellt der russische Angriffskrieg auf die Ukraine nach wie vor das größte mittel- bis langfristige Risiko im Bereich des internationalen illegalen Waffenhandels dar. Der Ausgang dieses Krieges und die daraus resultierenden Konsequenzen sind nach wie vor offen. Erfahrungswerte aus anderen Kriegen der jüngeren Vergangenheit zeigen jedoch, dass mit langfristigen Auswirkungen auf den internationalen illegalen Waffenhandel gerechnet werden muss. So besteht die reelle Gefahr, dass die in diesem Krieg eingesetzten Schusswaffen, sonstiges Kriegsmaterial, Sprengmittel und Munition auf den internationalen, insbesondere aber europäischen Schwarzmarkt fließen könnten. Österreich wäre von einer solchen Entwicklung aufgrund seiner geografischen Lage als potenzielles Transitland besonders betroffen. Während viele der aktuell in der Ukraine verwendeten Waffensysteme für die Zwecke der schweren und organisierten Kriminalität ungeeignet sind, stellt sich die Lage im Hinblick auf extremistisch oder terroristisch motivierte Tathandlungen anders dar. Die ukrainischen Sicherheitskräfte unternehmen derzeit aber (noch) umfassende Maßnahmen, um einen solchen Waffenschmuggel aus der Ukraine zu verhindern.

Bei Fortführung des Krieges ist mittelfristig weiterhin mit verstärkten illegalen Beschaffungsmaßnahmen für Güter der konventionellen Rüstung zu rechnen. Aufgrund entsprechender Exportbeschränkungen und verschiedener Sanktionsmaßnahmen sind vor allem Russland und seine Verbündeten darauf angewiesen, benötigte Güter, die in konventionellen Waffen aller Art Anwendung finden, auch hierzulande verdeckt zu beschaffen.

Mittel- bis langfristig werden auch sogenannte Privately Made Firearms (PMF) weiter an Bedeutung im internationalen illegalen Waffenhandel gewinnen. Neue und breit zugängliche Technologien sowie verstärkter Wissensaustausch werden mehr Menschen in die Lage versetzen, potenziell solche PMF anzufertigen. Die systematische Anwendung Künstlicher Intelligenz zum Entwurf und zur Verbesserung entsprechender Modelle scheint hier absehbar. Damit einhergehend wird auch die Vielfalt der auf diesem Weg herstellbaren Waffen weiter zunehmen. Während aktuell die Qualität, Verlässlichkeit und Einsatztauglichkeit selbst angefertigter Schusswaffen meist noch deutlich schlechter ist als jene der industriell hergestellten Produkte, kann sich dies rasch ändern.

Dieser Trend in Richtung Eigenanfertigung beschränkt sich mittlerweile nicht mehr allein auf Schusswaffen. Immer häufiger treten weltweit verschiedenstes Kriegsmaterial, Ausrüstung und Bauteile auf, die unter Nutzung moderner Technologien selbstangefertigt wurden. Dies reicht von unkonventionellen Spreng- und Brandvorrichtungen über Handgranaten bis hin zum Umbau frei erhältlicher Drohnen zu Waffenplattformen.

Einen Sonderfall stellen hier gefälschte Schusswaffen namhafter Hersteller, auch Counterfeit Guns genannt, dar. Diese illegal selbst hergestellten Fälschungen existenter Schusswaffen traten erst vor wenigen Jahren am Schwarzmarkt auf. In sehr kurzer Zeit entwickelten sie sich in puncto Verarbeitungs- und Materialqualität weiter und treten nun immer häufiger europa- und weltweit in Erscheinung. Ähnliche Fertigungsmerkmale verschiedener Modelle lassen auf eine Produktion in quasi-industriellem Ausmaß schließen. Aktuell betrifft dies vor allem halbautomatische Pistolen, da diese Art von Schusswaffen am Schwarzmarkt sehr begehrt sind.

Sowohl PMF als auch Counterfeit Guns werden auf absehbare Zeit große Herausforderungen für die Sicherheitsbehörden darstellen, da etablierte Methoden der Ermittlung und Informationsgewinnung hier nicht erfolgsversprechend scheinen.

„Privately Made Firearms“ (PMF) sind Schusswaffen oder Teile davon, die unerlaubt durch dazu nicht befugte Personen angefertigt werden. Dies kann sowohl mittels traditioneller Werkzeuge erfolgen, aber auch unter Nutzung moderner Technologien wie dem 3D-Druck oder CNC-Fräsen⁷⁸ für den Heimgebrauch. Der Grad der Selbstanfertigung kann variieren und von einer vollständigen Eigenanfertigung aller Waffenteile bis hin zur Nutzung von Rohlingen und bestimmten Waffenteilen aus industrieller Produktion reichen.



78 CNC-Fräsen (Computerized Numerical Control) sind Werkzeugmaschinen, die durch den Einsatz von Steuerungstechnik in der Lage sind, Werkstücke mit hoher Präzision auch für komplexe Formen automatisch herzustellen.

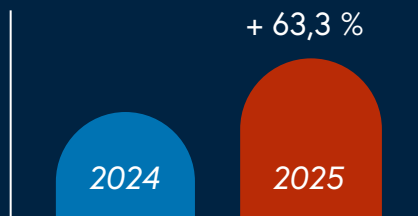
Internationaler illegaler Waffenhandel



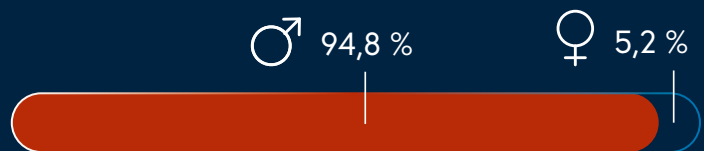
Aufklärungsquote



Anstieg zum Vorjahr



Täterinnen und Täter



Staatsbürgerschaft der Täterinnen und Täter

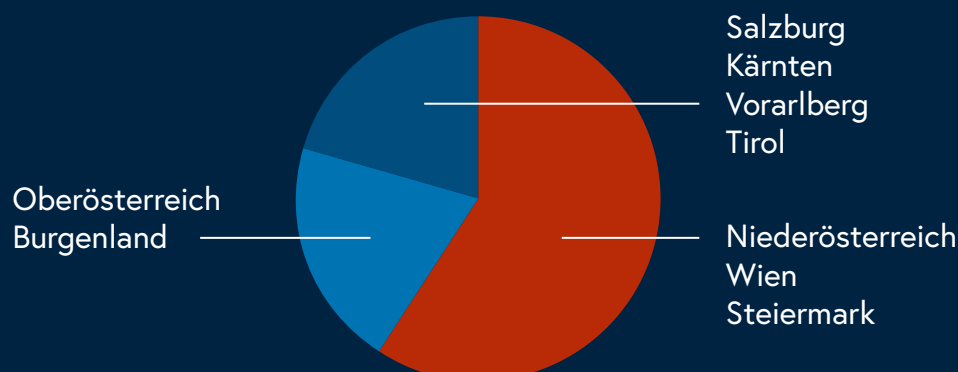


 **41**
Hausdurchsuchungen

 **24**
Festnahmen

 **108**
Zur Anzeige
gebrachte Delikte

Bundesländeraufteilung



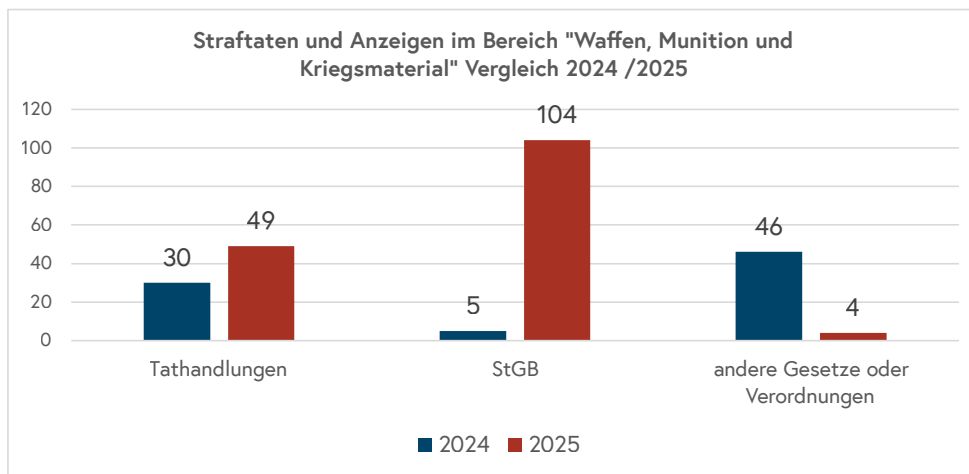
2.7.5 Zahlen/Daten/Fakten

In der Kategorie **Waffen, Munition und Kriegsmaterial** wurden den Sicherheitsbehörden im Berichtsjahr 2025 insgesamt **49 staatschutzrelevante Tathandlungen** bekannt (2024: 30). Gegenüber dem Jahr 2024 bedeutet dies einen **Anstieg um 63,3 Prozent**. 47 dieser 49 Tathandlungen wurden aufgeklärt; die **Aufklärungsquote** liegt somit bei **95,9 Prozent** (2024: 96,7 Prozent – 29 Tathandlungen).

Insgesamt konnten **77 Tatverdächtige** (2024: 32) ausgeforscht und zur Anzeige gebracht werden. Bei diesen handelt es sich um 73 männliche Personen (94,8 Prozent) und vier weibliche Personen (5,2 Prozent) (2024: 31 männliche, 96,9 Prozent und eine weibliche, 3,1 Prozent). 59 (76,6 Prozent) der Tatverdächtigen besitzen die österreichische Staatsbürgerschaft (2024: 25, 78,1 Prozent).

Im Zusammenhang mit den gesetzten Tathandlungen gelangten insgesamt **108 Delikte** (2024: 51), vier nach dem Strafgesetzbuch (StGB) sowie 104 nach anderen Gesetzen und Verordnungen, zur Anzeige.

Im Berichtsjahr 2025 erfolgten durch die Sicherheitsbehörden **41 Hausdurchsuchungen** (einschließlich freiwilliger Nachschauen) (2024: 23) und **24 Festnahmen** (2024: 1).

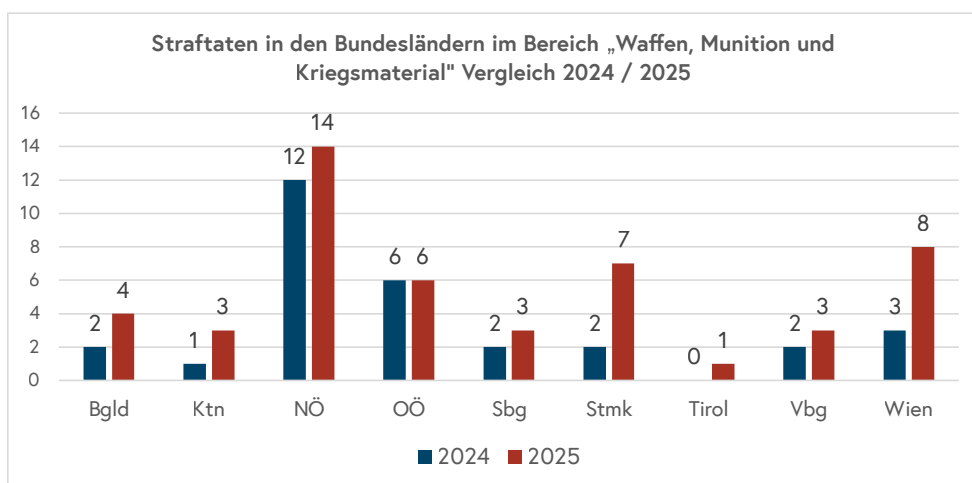


Anzeigen nach dem StGB	2024	2025
Diebstahl (§ 127 StGB)	0	1
Hehlerei (§ 164 StGB)	0	1
Vorbereitung eines Verbrechens durch Kernenergie, ionisierende Strahlen oder Sprengmittel (§ 175 StGB)	1	1
Ansammeln von Kampfmitteln (§ 280 StGB)	0	1
Sonstige StGB Delikte	4	0

Anzeigen nach anderen Gesetzen oder Verordnungen

§ 50 Waffengesetz (WaffG)	20	62
§ 51 Waffengesetz (WaffG)	11	6
§ 13 Waffengesetz (WaffG)	1	2
Sprengmittelgesetz (SprG)	0	5
Suchtmittelgesetz (SMG)	1	3
Pyrotechnikgesetz (PyroTG)	1	
Kriegsmaterialgesetz (KMG)	4	8
Chemikaliengesetz (ChemG)	1	10
Außenwirtschaftsgesetz (AußWG)	3	2
Verbotsgesetz (VbtG)	4	6
Summe	51	108

Im Phänomenbereich Waffen, Munition und Kriegsmaterial fanden 28,6 Prozent der Tathandlungen im Bundesland Niederösterreich statt, gefolgt von Wien (16,3 Prozent), der Steiermark (14,3 Prozent), Oberösterreich (12,3 Prozent), Burgenland (8,2 Prozent), Salzburg, Kärnten und Vorarlberg (jeweils 6,1 Prozent) und Tirol (2 Prozent).



2.8 Proliferation

„Proliferation“ bezeichnet die illegale Verbreitung chemischer, biologischer, radioaktiver oder nuklearer (CBRN) Massenvernichtungswaffen, der für ihren Einsatz notwendigen Trägersysteme sowie der zu ihrer Herstellung verwendeten Produkte, inklusive des dafür erforderlichen Know-how bzw. Fachwissens. Vordringlichste Aufgabe und Ziel der Proliferationsbekämpfung ist es, verdeckte Beschaffungsnetzwerke bzw. relevante (Schein-)Firmen zu identifizieren sowie verschleierte Zahlungsströme aufzudecken, um die Verbreitung von Massenvernichtungswaffen zu verhindern, da diese – insbesondere im Hinblick auf die aktuelle geopolitische Lage – ein unkalkulierbares Risiko bergen.

2.8.1 Überblick

Die Verhinderung und Bekämpfung von Proliferation spielt eine essenzielle Rolle für die internationale Sicherheit, da manche Staaten nicht davor zurückschrecken, zur Durchsetzung ihrer politischen Ziele Massenvernichtungswaffen einzusetzen oder dies zumindest anzudrohen. Aufgrund der Bestrebungen dieser Staaten, ihre bestehenden konventionellen Waffenarsenale durch Massenvernichtungswaffen zu ergänzen bzw. auszubauen, wurden sie von der internationalen Staatengemeinschaft mit teils umfassenden Sanktionen belegt. Das Sanktionsregime soll es diesen Staaten erschweren bzw. unmöglich machen, Proliferation zu betreiben.

„Massenvernichtungswaffen“ bzw. „weapons of mass destruction“ (WMD) sind Waffen, die das Potenzial haben, Zerstörungen in großem Ausmaß zu verursachen.



Im Bereich der Proliferationsbekämpfung liegt der Fokus des österreichischen Verfassungsschutzes auf Russland, Nordkorea und dem Iran.

Eine Sonderrolle in der Proliferation nimmt China ein, da es sich als Einkäufer proliferationsrelevanter Güter und Technologien am Weltmarkt für sanktionierte Staaten, allen voran Russland und Nordkorea, etabliert hat.

Für Pakistan, dessen vordringliches Ziel die (nukleare) Abschreckung seines „Erzfeindes“ Indien ist, scheint Österreich zwar kein primäres Zielland seiner Proliferationsversuche zu sein, allerdings gibt es einige österreichische Firmen im Hochtechnologiebereich, die hinsichtlich der Weiterentwicklung von Trägerraketensystemen für die pakistanische Führung von Interesse sind.

Zusammenwirken von Scheinfirmennetzwerken und Nachrichtendiensten

Weder Massenvernichtungswaffen noch Trägersysteme sind in der Regel als Gesamtprodukte am freien Markt erhältlich. Wenngleich Risikostaat wie Russland, Iran und Nordkorea zum Teil nicht unerhebliche technologische Fortschritte aufweisen, sind sie bei der Weiterentwicklung ihrer Waffenprogramme und der Beschaffung der dafür notwendigen Güter auch weiterhin auf den internationalen Markt angewiesen. Aufgrund der ihnen auferlegten Sanktionen können diese Staaten essenzielle proliferationsrelevante Produkte, insbesondere bestimmte Chemikalien, Rohstoffe oder Dual-Use-Güter, jedoch nicht direkt am freien Markt kaufen, sondern müssen auf entsprechende Umgehungsstrukturen zurückgreifen.



Der Begriff „Dual-Use-Güter“ definiert Waren und Produkte, die sowohl für zivile Anwendungen – beispielsweise in der Forschung oder der Medizin – als auch für militärische Zwecke verwendet werden können. Folglich spricht man von „doppelter Verwendbarkeit“.

Hierzu werden Beschaffungsnetzwerke etabliert und Scheinfirmen gegründet, oftmals unter Einbindung der jeweiligen staatlichen Nachrichten- und Geheimdienste, die diese Netzwerke mithilfe nachrichtendienstlicher Mitarbeiterinnen und Mitarbeiter oder Personen aus dem Umfeld der Nachrichtendienste als Strohmänner betreiben.

Ein weiterer gängiger Modus Operandi in der Proliferation ist die absichtliche Täuschung von Firmen durch Falschangaben des (de facto staatlich gesteuerten) Käufers hinsichtlich des Verwendungszwecks oder des vermeintlichen Endnutzers. Die Ziele solcher Proliferationsaktivitäten sind heimische Unternehmen, die proliferationsrelevante Technologien und Güter herstellen, oder Universitäten bzw. Forschungseinrichtungen, bei denen das notwendige proliferationsrelevante Fachwissen vorhanden ist.

Proliferationsbekämpfung durch nationale und internationale Kooperation

Der österreichische Verfassungsschutz arbeitet eng mit nationalen und internationalen Partnern und Institutionen zusammen, um den illegalen Handel und die Weitergabe sensibler Materialien und proliferationsrelevanter Güter und Technologien zu verhindern. Österreichs Rolle als Transitland und seine Position als internationaler Forschungs- und Wirtschaftsstandort erfordern besondere Vorsicht, um einen potenziellen Missbrauch zu verhindern. Insbesondere die Aufdeckung illegaler Aktivitäten und Scheinfirmennetzwerke bleibt eine der Schlüsselaufgaben des Verfassungsschutzes, um die Sicherheit der österreichischen Bevölkerung und der internationalen Gemeinschaft zu gewährleisten.

2.8.2 Aktuelle Lage

Im Berichtsjahr stellten sich der Proliferationsbekämpfung eine Vielzahl von Herausforderungen, die die internationale Sicherheit bedrohten, wobei die Entwicklungen in diesem Bereich maßgeblich vom sicherheitspolitischen Weltgeschehen beeinflusst werden. Die globalen geopolitischen Entwicklungen, insbesondere der russische Angriffskrieg gegen die Ukraine und der Nahostkonflikt, verdeutlichen die Notwendigkeit einer effektiven Proliferationsbekämpfung, um die internationale Sicherheit zu gewährleisten und die illegale Verbreitung von Massenvernichtungswaffen zu unterbinden.

Im Jahr 2025 war in Österreich kein Rückgang von Proliferationsaktivitäten zu verzeichnen, wobei insbesondere Dual-Use-Güter einen Schwerpunkt der Arbeit der österreichischen Proliferationsabwehr darstellten. Für heimische Firmen, die Dual-Use-Güter herstellen, ist es oftmals schwierig bis unmöglich zu erkennen, welche Absichten ein potenzieller Kunde tatsächlich hat. Für staatliche Akteure mit Proliferationsabsicht, die an Dual-Use-Gütern aus Österreich interessiert sind, gilt die Grundmaxime „Tarnen und Täuschen“.

Russland

Seit Beginn des russischen Angriffskrieges gegen die Ukraine hat die Europäische Union ihre Sanktionspakete immer wieder erweitert und angepasst. So wurden seit Februar 2022 nicht nur Finanzsanktionen und Einfuhrbeschränkungen gegen zahlreiche russische Güter beschlossen, sondern auch Einzelpersonen, Institutionen und eine Vielzahl russischer Unternehmen mit Sanktionen belegt. Ziel dieser EU-Sanktionen ist es unter anderem, die russische Rüstungsindustrie zu schwächen. Um die Sanktionen zu umgehen und die notwendigen Güter zu beschaffen, greift Russland auf seine Nachrichtendienste und ihre Proliferationsnetzwerke zurück.

Ein wesentliches Merkmal russischer Proliferationsnetzwerke ist die Präsenz der russischen Nachrichtendienste in den Scheinfirmen. Hier spielt vor allem der militärische Nachrichtendienst Russlands, GU, eine wesentliche Rolle. Ähnlich wie bei Illegalen-Netzwerken in der klassischen Spionage agieren auch hier die Bediensteten der russischen Nachrichtendienste unter falschem Namen. Ihr staatlicher Auftrag ist es, einerseits selbst Scheinfirmen im Ausland zu gründen und andererseits Strohmänner zu finden, die in den Firmennetzwerken tätig sind, um so diese Beschaffungsnetzwerke zu steuern und die Kontrolle über diese Firmengeflechte auszuüben. Sobald ein Beschaffungsauftrag für proliferationsrelevante Waren vorliegt, ist es Zweck dieser Firmennetzwerke, den Kauf unauffällig abzuwickeln. Bei Beschaffungsaufträgen gilt das Interesse Russlands einer breiten Produktpalette. Neben den klassischen Dual-Use-Gütern, wie Mikrochips oder CNC-Maschinen, sind oftmals Ersatzteile für die russische Rüstungsindustrie von größter Relevanz, um die Materialabnützungen im Kriegsgebiet kompensieren zu können.

Ein üblicher Modus Operandi bei russischen Proliferationsaktivitäten ist das Ausweichen auf Staaten, die selbst nicht mit Sanktionen belegt sind und auch Russland gegenüber nicht mit Sanktionen agieren, weshalb sie bei verdeckten Beschaffungsvorgängen einen „sicheren Hafen“ bieten. So laufen russische Beschaffungsnetzwerke und Scheinfirmer oftmals über die GUS-Staaten⁷⁹ oder über Länder des Nahen und Mittleren Osten.

Iran

Der Iran ist offiziell kein Atomwaffen-Staat, wird jedoch aufgrund seiner Proliferationsbestrebungen seit einigen Jahren von der EU und den USA mit umfangreichen Sanktionen belegt. Wenngleich der Iran die Existenz eines militärisch genutzten Atomprogramms verneint und sein Atomprogramm offiziellen Aussagen des iranischen Regimes zufolge ausschließlich für die zivile Nutzung betreibt, so gibt es dennoch immer wieder internationale Besorgnis über potenziell militärische Dimensionen des iranischen Atomprogramms. Die Unterscheidung eines zivilen Atomprogramms von einem militärischen Atomprogramm ist zudem dadurch erschwert, dass Nukleartechnologie von Natur aus Dual-Use-fähig ist.

Die internationalen Bemühungen zur Verhinderung von Proliferation durch den Iran waren jahrelang auf internationale Abkommen und Sanktionen gestützt. Österreich spielt dabei als Sitz der Internationalen Atomenergiebehörde (IAEA) eine wichtige Rolle.



Die „**Internationale Atomenergiebehörde**“ bzw. „**International Atomic Energy Agency**“ (IAEA) ist eine autonome Organisation, die den Beitrag der Kernenergie zu Frieden, Gesundheit und Wohlstand weltweit beschleunigen und vergrößern und den Missbrauch dieser Technologie – beispielsweise durch militärische Nutzung und Proliferation – mittels Überwachungsmaßnahmen verhindern soll.

Bei seinen Proliferationsaktivitäten greift der Iran auch auf seine Nachrichtendienste zurück, die mit der Errichtung von Umgehungsstrukturen zur verschleierte Beschaffung von Rüstungsgütern, proliferationsrelevanten Technologien und Materialien für Massenvernichtungswaffen betraut sind. Besonders das weit verzweigte Firmenimperium der Islamischen Revolutionsgarden (IRGC) soll vorrangig Proliferationszwecken dienen.

Iranisch gesteuerte Sanktionsumgehungsnetzwerke bedienen sich globalisierter und hochkomplexer Produktions-, Lieferketten-, Finanzierungs- und Logistikkanäle. Diese

⁷⁹ „GUS-Staaten“ sind die Nachfolgestaaten der Sowjetunion, die sich in der Gemeinschaft Unabhängiger Staaten (GUS) zusammengeschlossen haben. Im Jahr 2025 gehörten dazu Armenien, Aserbaidschan, Belarus, Kasachstan, Kirgisistan, Russland, Tadschikistan, Turkmenistan und Usbekistan. Georgien ist bereits 2008 aus der GUS ausgetreten; die Ukraine, die zwar Gründungsmitglied, aber formal nie Vollmitglied war, hat sich seit 2018 aus den meisten Abkommen zurückgezogen; Moldawien erklärte im Jänner 2026 seinen formellen Austritt.

ineinander verwobenen internationalen Netzwerke aus privaten Unternehmen, Lieferanten und Zwischenhändlern beschaffen und transferieren proliferationsrelevante Waren und tragen so – wissentlich oder unwissentlich – zur Bedarfsdeckung an sanktionierten Gütern, Technologie sowie Know-how für den Iran bei.

Nordkorea

Die in Form einer kommunistischen Diktatur geführte Demokratische Volksrepublik Korea (Nordkorea) verfügt über ein hoch entwickeltes Atomwaffenprogramm sowie über weitreichende Raketen, deren Existenz durch die erfolgten Raketentests bereits mehrfach nachgewiesen wurde. Aufgrund seiner teilweise durchaus offensiven Atomwaffenpolitik unterliegt Nordkorea umfassenden internationalen Sanktionen.

Wenngleich Nordkorea einer der politisch und wirtschaftlich isoliertesten Staaten der Welt ist, kann dennoch beobachtet werden, dass die Regierung nicht nur ihr eigenes Atomwaffenprogramm vorantreibt, sondern auch andere Proliferationsstaaten, insbesondere Russland, beim Aufbau und der Weiterentwicklung ihrer Rüstungsprogramme durch Waffenlieferungen und dergleichen unterstützt.

Proliferation stellt für Nordkorea einen essenziellen Bestandteil seiner Sicherheitspolitik nach außen und seiner Legitimation nach innen dar. Die vermeintliche Manifestierung externer Bedrohungen durch feindselige Mächte, allen voran Südkorea und die USA, ist ein Grundbaustein der nordkoreanischen Staatsideologie, der es für das Regime unumgänglich macht, das konventionelle sowie das Nuklearwaffenprogramm weiter auszubauen. Zudem erfüllt die Proliferationstätigkeit Nordkoreas zwei politische Ziele: Einerseits sollen dadurch die eigene Rüstungsindustrie und das Atomwaffenprogramm vorangetrieben werden, andererseits hat sich Nordkorea mittels Lieferung von Artillerie, Drohnen und Munition als Unterstützer Russlands im Angriffskrieg gegen die Ukraine positioniert.

Auf Grund der internationalen Sanktionierung ist es für das nordkoreanische Regime schwierig, im Ausland genügend personelle und finanzielle Ressourcen zu platzieren, um Proliferation, Regimefinanzierung, Sanktionsumgehungen und damit verbundene Aktivitäten zu betreiben. Auch die diplomatischen Einrichtungen Nordkoreas wurden von den meisten europäischen Ländern stark reduziert. In Österreich findet sich eine der letzten und personell stärksten nordkoreanischen Botschaften in Europa.

Trotz der massiven Sanktionierungen hat es Nordkorea über die letzten Jahrzehnte hinweg geschafft, sich auf die professionelle und zielgerichtete Durchführung von Proliferation und Sanktionsumgehung zu spezialisieren.

Sowohl zur Finanzierung seines Regimes als auch zur Weiterentwicklung seines Nuklearwaffenprogramms greift Nordkorea auf eine breite Palette illegaler Aktivitäten,

beispielsweise Waffen- und Suchtgifthandel, Luxusgüter-, Tabak- und Alkoholschmuggel sowie Geldwäsche und Cyberkriminalität, zurück. Diese Aktivitäten können teilweise auch in Österreich beobachtet werden.

Exkurs: Sonderrolle Chinas im Zusammenhang mit Proliferation

China nimmt in der Proliferation global gesehen eine Sonderstellung ein. Das Land, das selbst nicht von europäischen Sanktionen betroffen ist, agiert weltweit als Ein- und Verkäufer von Dual-Use-Gütern und hat sich auf diesem Weg zu einem Dreh- und Angelpunkt für die Proliferationsaktivitäten sanktionierter Staaten entwickelt.

Offiziell beteuert die chinesische Regierung ihre Unterstützung für internationale Non-Proliferationsbemühungen bzw. Rüstungskontrollreglementierungen und hat auch einige internationale Abkommen in diesem Zusammenhang unterzeichnet. In Kontrast dazu steht jedoch der Umstand, dass international sanktionierte Staaten zur Weiterentwicklung ihrer Rüstungsprogramme auf Hochtechnologie aus China setzen. Hierfür hat Chinas strategische Partnerschaft mit Russland und Nordkorea den Grundstein gelegt.

China selbst ist vor allem an der militärischen Nutzung der Quantentechnologie, insbesondere der Quantenkryptographie, interessiert. In diesem Segment findet aktuell ein Wettlauf zwischen den USA und China statt. Die Erkenntnisse der europäischen und auch der österreichischen Grundlagenforschung in diesem Bereich sind für China, insbesondere für das chinesische Militär, von großem Interesse.



2.8.3 Fälle 2025

Fall WERKZEUG

Im Rahmen der interministeriellen Zusammenarbeit wurde die DSN auf ein in Österreich etabliertes Unternehmen aufmerksam. Dieses war aufgrund einer verdächtigen Anfrage betreffend Lieferung spezieller Güter aufgefallen.

Das in Österreich ansässige Unternehmen stand im Verdacht, hochspezialisierte sanktionierte Waren über Umgehungsländer und damit unter Umgehung der geltenden EU-Sanktionen rechtswidrig nach Belarus bzw. an ein sanktioniertes belarussisches Unternehmen exportiert zu haben. Dieses wiederum soll die russische Armee mit Militärgütern beliefern, welche auf ukrainischem Hoheitsgebiet für militärische Handlungen eingesetzt werden.

Aufgrund dieses Hinweises wurden umfangreiche nationale und internationale Ermittlungen eingeleitet. Dabei stellte sich heraus, dass das in Österreich ansässige Unternehmen über mehrere Jahre hinweg Waren ausschließlich nach Belarus exportiert hatte. Mit dem Inkrafttreten der Sanktionen der Europäischen Union konnten jedoch keinerlei Exporte mehr nach Belarus festgestellt werden. Die hochspezialisierten Waren wurden ab diesen

Zeitpunkt ausschließlich in die Türkei und nach Hong Kong exportiert. Der Gesamtwert der Waren betrug seit Ende 2024 bis Dezember 2025 rund 600.000 Euro.

Derartige Exporte verstoßen gegen EU-Recht, weshalb der begründete Verdacht bestand, dass ein Verstoß gegen das Außenwirtschaftsgesetz vorlag. Der Sachverhalt wurde an die zuständige Staatsanwaltschaft berichtet. Diese ordnete mehrere Hausdurchsuchungen an, bei deren Durchführung es zur Sicherstellungen zahlreicher Datenträger kam. Das Ermittlungsverfahren war zum Zeitpunkt der Berichtslegung weiterhin laufend.

Fall LUXUSFAHRZEUGE

Die DSN wurde aufgrund der Sanktionierung eines Unternehmens in Hong Kong durch die US-amerikanische Behörde Office of Foreign Assets Control (OFAC)⁸⁰ auf einen in Österreich lebenden, russischen Staatsbürger aufmerksam. Grund für die Sanktionierung des Unternehmens durch die OFAC war dessen Verbindung zu einer russischen Firma, die als Zulieferer für das russische Militär im Angriffskrieg gegen die Ukraine fungiert.

Der russische Staatsbürger, der ebenfalls von den OFAC-Sanktionen betroffen ist, ist Geschäftsführer des sanktionierten Unternehmens in Hong Kong wie auch ehemaliger Gesellschafter und Geschäftsführer eines österreichischen Unternehmens. Aufgrund seines aufrechten österreichischen Wohnsitzes sowie seiner Rolle bei einem österreichischen Unternehmen wurden sowohl zur Person selbst als auch zum österreichischen Unternehmen entsprechende Erhebungen durchgeführt.

Dabei konnte in Erfahrung gebracht werden, dass das österreichische Unternehmen eine große Zahl hochpreisiger Kraftfahrzeuge nach Belarus exportiert hatte. Darin ist grundsätzlich kein Verstoß gegen EU-Sanktionen erkennbar, da Luxusfahrzeuge in der entsprechenden EU-Verordnung in Bezug auf Belarus nicht gelistet sind. Allerdings gilt Belarus durch sein Naheverhältnis zu Russland als eines jener Länder, das als Umgehungsland hinsichtlich der geltenden EU-Sanktionen bekannt ist.

Im Zeitraum zwischen Februar 2022 bis Dezember 2025 wurden durch das österreichische Unternehmen bzw. den russischen Geschäftsmann ca. 150 Fahrzeuge in einem Gesamtwert von rund 12 Millionen Euro exportiert.

Durch umfangreiche nationale und internationale Ermittlungen konnte festgestellt werden, dass ein Großteil jener exportierten Fahrzeuge, die zuvor nach Belarus bzw. Armenien exportiert wurden, mittlerweile in Russland zugelassen ist. In einem Zeitraum von ca. zwei Jahren wurden durch das österreichische Unternehmen Kraftfahrzeuge in einem Gesamtwert von rund drei Millionen Euro exportiert.

⁸⁰ Es muss jedoch erwähnt werden, dass eine OFAC-Listung per se keine rechtliche Bindung für Österreich hat.

Es besteht der dringende Verdacht, dass der russische Staatsbürger geltende Sanktionen der Europäischen Union gezielt umgangen hat und somit ein Verstoß gegen das Außenwirtschaftsgesetz vorliegt. Es wurde ein Anlassbericht an die zuständige Staatsanwaltschaft gelegt. Eine Hausdurchsuchung wurde durchgeführt, das Ermittlungsverfahren ist zum Zeitpunkt der Berichtslegung weiterhin laufend. Das Verfahren ist noch offen.

2.8.4 Trends und Entwicklungstendenzen

Russland

Aufgrund des andauernden russischen Angriffskrieges gegen die Ukraine ist ein Rückgang russischer Proliferationsaktivitäten in Österreich nicht zu erwarten – im Gegenteil: Russland scheint in seinen Drohgebärden gegen Europa und NATO immer offener und aggressiver zu agieren.

Zwar profitiert die russische Rüstungsindustrie von ihrer strategischen (und auch materiellen) Partnerschaft mit China und Nordkorea, dennoch ist die Nachfrage nach hochwertigen Werkzeugmaschinen, wie etwa CNC-Fräsen u. a., aus europäischer Produktion in Russland ungebrochen hoch. Vor allem die Beschaffung von Ersatzteilen für europäische Maschinen, die bereits vor Inkrafttreten der Sanktionen erworben wurden und in der russischen Rüstungsindustrie eingesetzt werden, wird weiterhin hohe Priorität bei russischen Proliferationsbestrebungen haben.

Die DSN kooperiert mit allen maßgeblichen Industriepartnern dieses Segments, um etwaige Proliferationsversuche und mögliche Sanktionsverstöße durch Russland frühzeitig zu erkennen und zu unterbinden.

Iran

Mit den Angriffen der israelischen und US-amerikanischen Streifkräfte auf die Uran-Anreicherungsanlagen und die militärische Infrastruktur des Iran im Juni 2025 sollte dem iranischen Atomprogramm ein Rückschlag versetzt werden. Wenngleich von unterschiedlichen Seiten das Ende des iranischen Atomprogramms verkündet wurde, kann zum aktuellen Zeitpunkt noch keine endgültige Aussage darüber getroffen werden, wie effektiv und nachhaltig diese Angriffe tatsächlich waren.

Mit Blick auf Österreich konnte keine Veränderung der Proliferationsaktivitäten des Iran festgestellt werden. Österreich stellt als bedeutende europäische Industrienation und Standort zahlreicher Unternehmen der Spitzentechnologie mit hoher Wahrscheinlichkeit auch weiterhin ein potenzielles Zielland iranischer Proliferationsaktivitäten dar.

Die weiteren Entwicklungen iranischer Proliferationsaktivitäten hängen allerdings maßgeblich von den Entscheidungen der iranischen Staatsführung in Bezug auf sein Atomprogramm ab, inwiefern der Iran in seinen Kapazitäten tatsächlich geschwächt wurde und ob diese wiederaufgebaut werden sollen. In weiterer Folge leitet sich daraus die

Aufgabe des Verfassungsschutzes ab, mögliche neue, verdeckte Beschaffungsnetzwerke in Österreich zu enttarnen.

Nordkorea

Der Wille einzelner internationaler Akteure zur Durchsetzung der Sanktionen gegen Nordkorea hat vor allem seit den zunehmenden internationalen Spannungen und Konflikten nachgelassen. So hat sich China inzwischen als zentrale Drehscheibe für sanktionierte Güter und Finanzmittel für das nordkoreanische Regime etabliert, und auch Russland ist nach Jahren konspirativ betriebener Sanktionsumgehungen nunmehr offiziell eine militärische und strategische Partnerschaft mit Nordkorea eingegangen.

Seitens des österreichischen Verfassungsschutzes wird der Fokus weiterhin auf die Aufklärung und Bekämpfung der nordkoreanischen Sanktionsumgehungsnetzwerke – allen voran ihrer in Österreich agierenden Abdeckorganisationen – gelegt, um deren Erstarken zu verhindern und einem Abfluss von Finanzmitteln zur Regimefinanzierung, dem Erwerb von Dual-Use-Gütern und der Gewinnung von technologischem Know-how entgegenzuwirken.

Neues Sanktionengesetz 2024

Im Zuge der Novellierung des Sanktionengesetzes 2024 wurde in § 3 SanktG die Möglichkeit normiert, Vorschläge zur Listung bzw. Entlistung sowohl juristischer als auch natürlicher Personen an die Vereinten Nationen oder die Europäische Union zu unterbreiten. Damit sind der Bundesminister für Finanzen und der Bundesminister für Inneres jeweils ermächtigt, im Einvernehmen mit der Bundesministerin für europäische und internationale Angelegenheiten, Vorschläge zur Listung (§ 1 Abs. 2 Z 1 SanktG) zu erstellen. Durch diese neue Gesetzesgrundlage eröffnen sich auch in der Proliferationsbekämpfung neue und verbesserte Möglichkeiten, den illegalen Aktivitäten ausländischer Proliferationsakteure in Österreich Einhalt zu gebieten.

Wie anhand der sanktionierten juristischen und natürlichen Personen mit Bezug zum russisch-militärischen Rüstungskomplex ersichtlich ist, wird dies auf EU-Ebene bereits seit Längerem erfolgreich praktiziert. Andere Länder nutzen ihre jeweilige nationale Gesetzgebung im Bereich Sanktionen, um enttarnte Scheinfirmen in Proliferationsnetzwerken davon abzuhalten, in Zukunft weitere Verstöße zu begehen. Hier bieten sich auch für die nationale Non-Proliferationsstrategie neue Handlungsspielräume, um auf die Gefahr von Scheinfirmennetzwerken aufmerksam zu machen und diesen präventiv und repressiv zu begegnen.

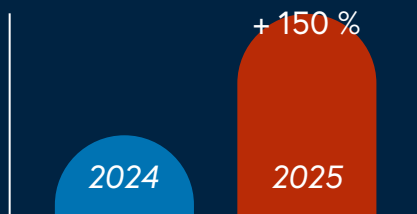
Proliferation



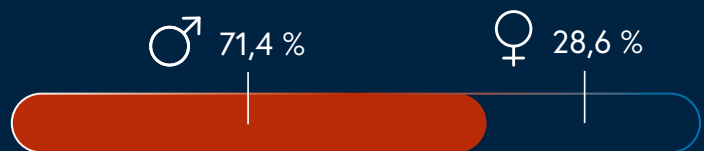
Aufklärungsquote



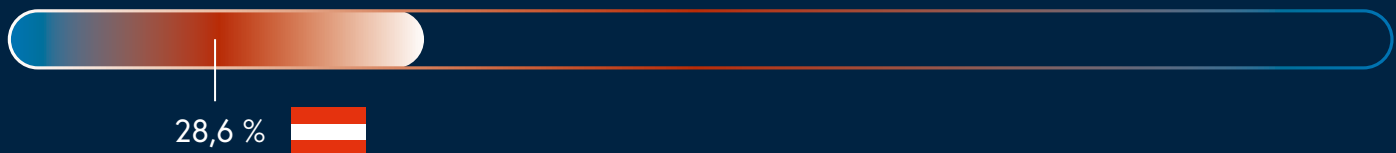
Anstieg zum Vorjahr



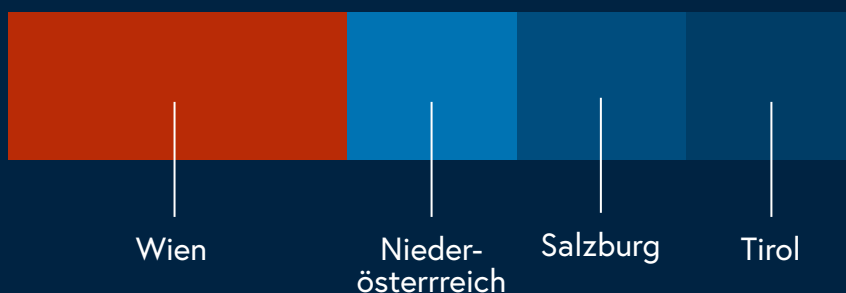
Täterinnen und Täter



Staatsbürgerschaft der Täterinnen und Täter



Bundesländeraufteilung



2.8.5 Zahlen/Daten/Fakten

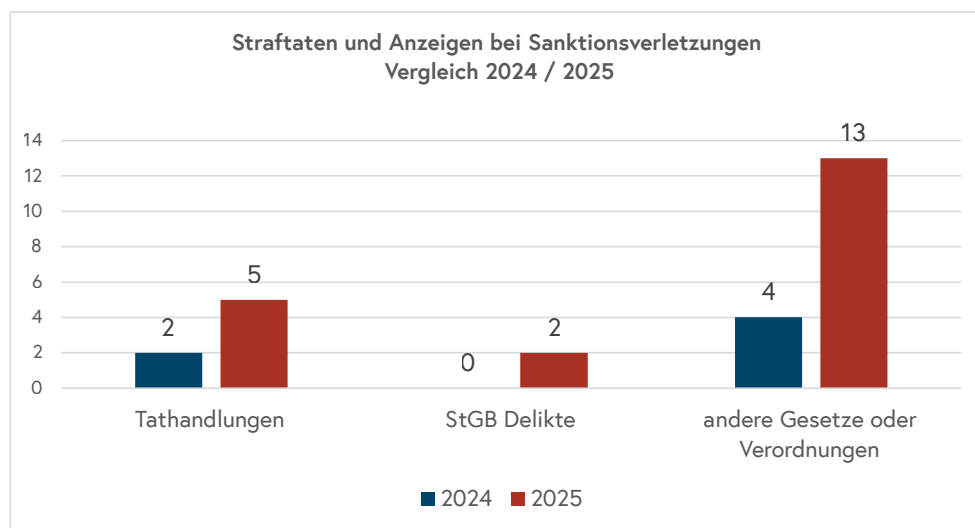
In der Kategorie **Sanktionsverletzungen** wurden den Sicherheitsbehörden im Berichtsjahr 2025 insgesamt **fünf Tathandlungen** bekannt (2024: 2). Gegenüber dem Jahr 2024 bedeutet dies einen **Anstieg um 150 Prozent**. Alle Tathandlungen wurden aufgeklärt; die **Aufklärungsquote** liegt somit bei **100 Prozent** (2024: 100 Prozent – 2 Tathandlungen).

Von den fünf Tathandlungen fanden zwei in Wien und jeweils eine in Niederösterreich, Salzburg und Tirol statt.

Insgesamt konnten **14 Tatverdächtige** (2024: 3) ausgeforscht und zur Anzeige gebracht werden. Dabei handelt es sich um zehn männliche Personen (71,4 Prozent) und vier weibliche Personen (28,6 Prozent; 2024: 2 männliche, 66,7 Prozent und eine weibliche, 33,3 Prozent). Vier (28,6 Prozent) der Tatverdächtigen besitzen die österreichische Staatsbürgerschaft (2024: 3, 100 Prozent).

Im Zusammenhang mit den gesetzten Tathandlungen gelangten insgesamt **15 Delikte** (2024: 4), zwei nach dem Strafgesetzbuch (StGB) sowie 13 nach anderen Gesetzen zur Anzeige.

Im Berichtsjahr 2025 erfolgten durch die Sicherheitsbehörden **drei Hausdurchsuchungen** (einschließlich freiwilliger Nachschauen) (2024: 0). Zu **Festnahmen** kam es nicht. (2024: 0).



Anzeigen nach dem StGB	2024	2025
Geldwäscherei (§ 165 StGB)	0	2
Anzeigen nach anderen Gesetzen oder Verordnungen		
§ 11 Sanktionengesetz	3	0
§ 16 Sanktionengesetz	0	3
§ 3 Verbandsverantwortlichkeitsgesetz (VbVG)	1	0
§ 79 Außenwirtschaftsgesetz (AußWG)	0	10
Summe	4	15

3

Schutz und Prävention

3.1 Schutz der Obersten Organe und verfassungsmäßigen Einrichtungen

3.1.1 Überblick

Um den kontinuierlichen Fortbestand der Handlungs- und Funktionsfähigkeit unserer demokratischen Grundordnung zu gewährleisten, obliegt der DSN im Zusammenwirken mit den LSE der besondere Schutz der Obersten Organe und verfassungsmäßigen Einrichtungen. Das erste Halbjahr 2025 stand anlässlich des Regierungswechsels ganz im Zeichen von initialen Sicherheitsberatungen mit den neu ernannten Regierungsgliedern, um diese einerseits für die mit ihrer Funktion verbundenen Sicherheitsrisiken zu sensibilisieren sowie ihnen andererseits die jeweils auf die individuell vorhandene Gefährdungslage angepassten Schutzmaßnahmen und Verhaltensempfehlungen zu erläutern.

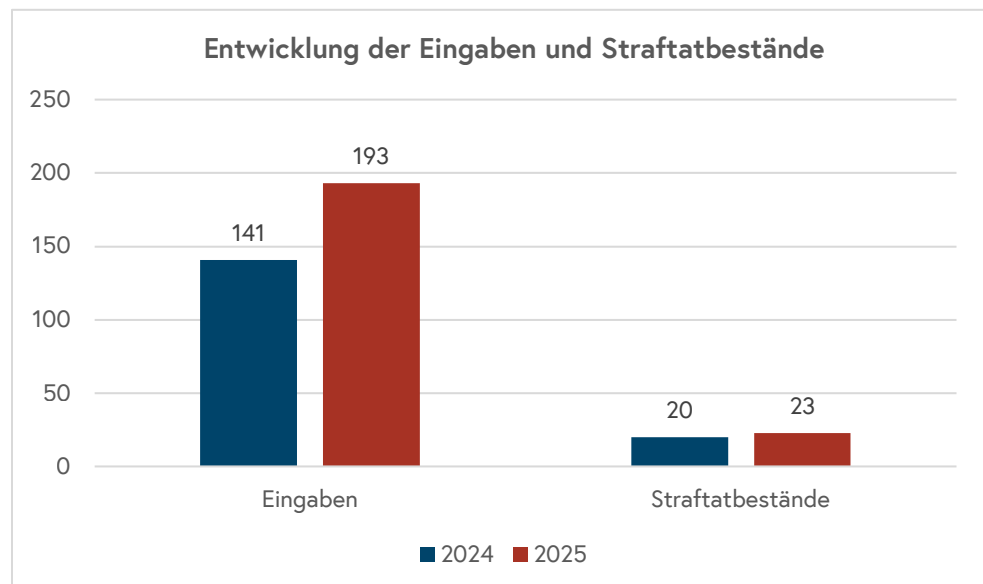
Zu den **Obersten Organen und verfassungsmäßigen Einrichtungen** zählen unter anderem: Nationalrat, Bundesrat, Bundespräsident, Bundeskanzler, Bundesminister und Staatssekretäre, Mitglieder der Landesregierungen, Oberster Gerichtshof, Verfassungsgerichtshof, Verwaltungsgerichtshof, Bundesverwaltungsgericht, Landesverwaltungsgerichte, Rechnungshof, Finanzmarktaufsicht, Volksanwaltschaft.

Im Berichtsjahr zeigte sich keine signifikante Steigerung des abstrakten Gefährdungspotenzials für Vertreterinnen und Vertreter der Bundesregierung und der verfassungsmäßigen Einrichtungen durch die extremistischen Szenen. Emotional aufgeladene und konfliktbehaftete Themen wie das Kopftuchverbot an Schulen, die Messenger-Überwachung durch Sicherheitsbehörden, die Verschärfung des Waffengesetzes oder die geplante Realisierung umstrittener Straßenbauprojekte riefen zwar vereinzelt Unmutsäußerungen hervor, führten jedoch nicht zu einer nachhaltigen Verschärfung der allgemeinen, abstrakten Gefährdungsexposition bestimmter Entscheidungsträgerinnen und Entscheidungsträger. Auch die für einige Bevölkerungsgruppen zum Teil merklich spürbaren, nachteiligen Maßnahmen zur Bekämpfung der angespannten Wirtschaftslage hatten im Jahr 2025 eher Auswirkungen auf die Zustimmungswerte als auf die Gefährdungsrelevanz. Auffallend mehr Resonanz in Form kritischer und diffamierender Replik in sozialen Medien oder direkten Zuschriften erzeugten hingegen jene Regierungsglieder, die sich zu geopolitischen Themen wie dem fortwährenden Nahostkonflikt oder der wachsenden Bedrohung der Sicherheitsinteressen Europas im Kontext des russischen Angriffskrieges gegen die Ukraine äußerten. In diesem Zusammenhang war festzustellen, dass Außenministerin Meinel-Reisinger im Beobachtungszeitraum mit den meisten inkriminierenden, verachtenden und bedrohlichen Zuschriften konfrontiert war. Generell ist zu beobachten, dass vor allem Alternativmedien immer stärker als Vehikel

für Polarisierung und Verstärkung von Aversion gegen demokratisch legitimierte und gewählte Repräsentantinnen und Repräsentanten genutzt werden.

3.1.2 Aktuelle Lage

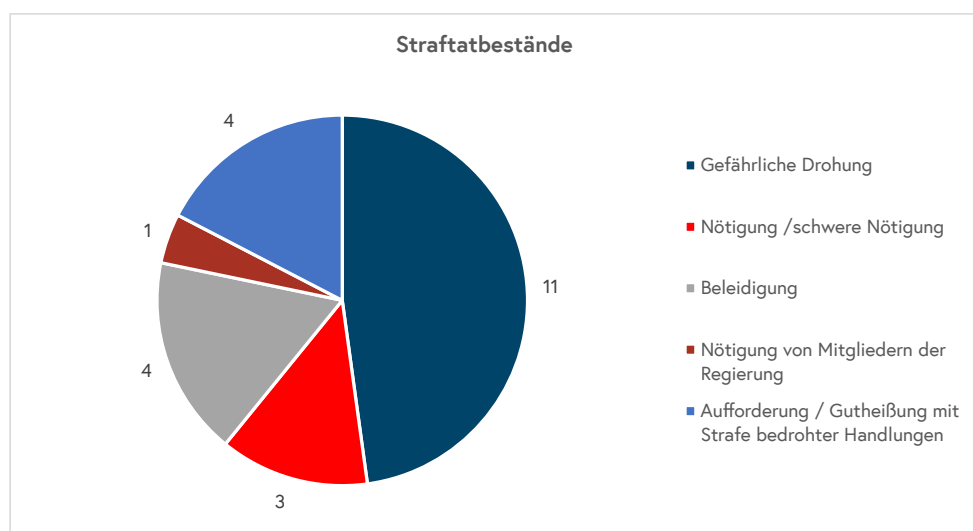
Ein wesentliches Werkzeug zur Beurteilung der individuellen Gefährdungslage österreichischer Politikerinnen und Politiker und der politischen Institutionen bildet das statistische Erfassen und die semantische Bewertung aller der DSN bekannt gemachten Zuschriften und Kommentare in den sozialen Medien. Entgegen einer angesichts zahlreicher innen- und außenpolitischer Konfliktthemen erwarteten Zunahme an ablehnender Agitation gegen die Vertreterinnen und Vertreter der Regierungsparteien vonseiten oppositioneller Akteurinnen und Akteure, ist die Gesamtanzahl von direkt an die Politikerinnen und Politiker und Institution gerichteten Hass- und Beschimpfungsschreiben wie auch die Zahl an Behördeneingaben mit kritischem, sicherheits- oder strafrechtlich relevantem Inhalt nur leicht gestiegen. Die Zahl der Straftatbestände stieg um 15 Prozent auf 23 Fälle.

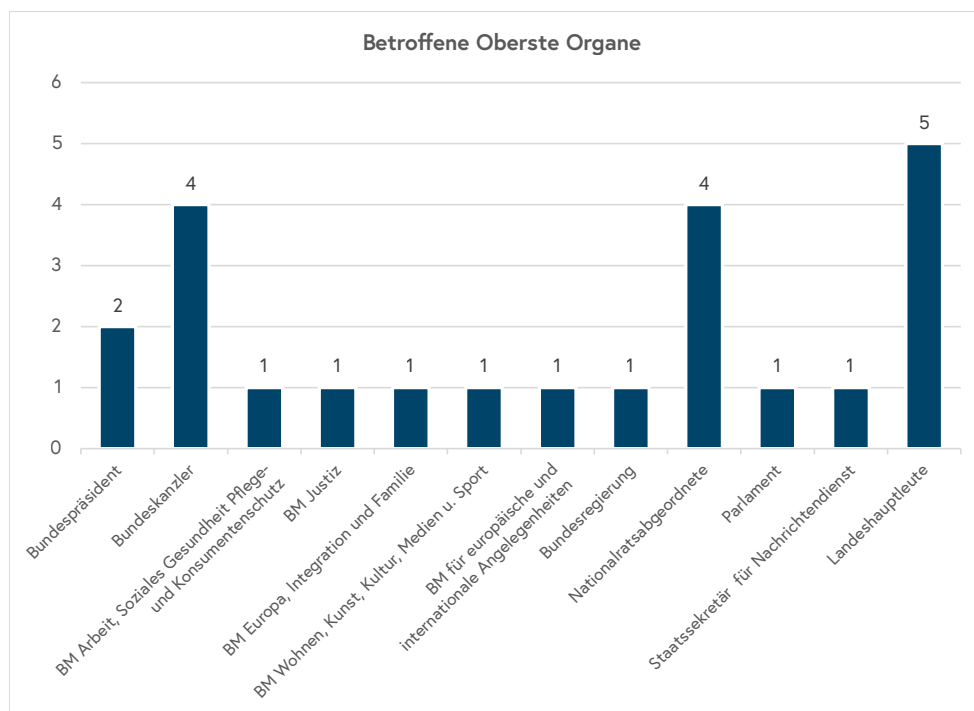


Im Jänner 2025 erfuhr Bundespräsident Alexander Van der Bellen infolge seines, aus Sicht politisch Andersgesinnter umstrittenen, Regierungsbildungsauftrages heftige Kritik, was sich im Rahmen schriftlicher Eingaben in einer deutlichen Häufung an Beschimpfungen gegen seine Person und seine Amtsführung widerspiegelte. Im restlichen Jahresverlauf bewegte sich die Zahl der an die Präsidentschaftskanzlei gerichteten Zuschriften jedoch auf demselben niedrigen Durchschnittsniveau wie in den vergangenen Jahren. Ungleich höher war phasenweise jedoch die Zahl kritischer Eingaben bei Österreichs Bundesministerin für europäische und internationale Angelegenheiten, deren Eingaben rund 30 Prozent aller registrierten Zuschriften des Jahres 2025 ausmachten. Der gemeinsame Anteil der gegen den Bundespräsidenten und die Außenministerin eingegangenen Eingaben belief sich auf rund 47 Prozent. Ein besonderes Merkmal bei einer Vielzahl der an

die Außenministerin gerichteten Schreiben oder Kommentare war der verwünschende oder beleidigende Inhalt ohne jegliche sachorientierte Kritik hinsichtlich der von ihr verfolgten Außenpolitik. Dies unterstreicht die anhaltende Tendenz stärkerer Betroffenheit vor allem weiblicher Politikerinnen von derartigen (unsachlichen) Hasskommentaren bzw. -schreiben. Ebenso außergewöhnlich war, dass das üblicherweise hohe Anfeindungs-geschehen gegen den in Hauptverantwortung für die Regierungsarbeit mit der höchsten Öffentlichkeits- und Medienpräsenz in Erscheinung tretenden Bundeskanzler bislang gering ausfiel.

Gesamt betrachtet ist festzustellen, dass die oftmals behauptete Zunahme an politischer und gesellschaftlicher Spaltung sowie die Abnahme des allgemeinen Vertrauens in die Politik und deren handelnde Verantwortungsträgerinnen und Verantwortungsträger nicht zwingend mit einer Intensivierung des Gefährdungspotenzials für Oberste Organe und die verfassungsmäßigen Institutionen einherzugehen scheint. Selbst bei jenen Regierungsmitgliedern, die in Verantwortung konfliktbehafteter Themenschwerpunkte (Familiennachzug, Kopftuchverbot für Mädchen an Schulen, Messenger-Überwachung, Abschiebungen in Konfliktregionen, Budgeteinsparungen etc.) stehen, waren keine stichhaltigen Indikatoren wahrzunehmen, die auf eine nennenswerte Erhöhung des jeweiligen Gefährdungspotenziales schließen lassen konnten.





3.1.3 Fälle 2025

Fall DROHNENSICHTUNG BEI REGIERUNGSGEBÄUDE

Während einer Besprechung von Kabinettsmitarbeiterinnen und Kabinettsmitarbeitern eines Regierungsmitglieds tauchte eine handelsübliche Drohne vor den Fenstern des Besprechungsraumes auf und verharrte dort für kurze Zeit bewegungslos in der Luft. Als die Besprechungsteilnehmerinnen und Besprechungsteilnehmer versuchten, die Drohne mit ihren Smartphones zu fotografieren, entfernte sich diese in unbekannte Richtung. Anlässlich dieses Zwischenfalles erfolgte eine zielgerichtete Beratung zur Reduzierung der mit Drohnen in Verbindung stehenden Risiken.⁸¹

Fall POLITISCH MOTIVIERTE SACHBESCHÄDIGUNG

Vier Personen wurden von Bediensteten der Objektschutzpolizei im Regierungsviertel über die dort befindliche Videoüberwachung dabei beobachtet, wie sie mit Lackfarbe-Spraydosen die Baustellenbepankung und das Türschild eines Regierungsgebäudes mit politischen Parolen im Zusammenhang mit dem Nahostkonflikt besprühten. Anhand der Schriftzüge war eine Pro-Palästina-Haltung als zugrundeliegendes Motiv auszumachen. Den unverzüglich alarmierten und am Tatort eintreffenden Polizeibeamtinnen und Polizeibeamten gelang es, im Zuge der Verfolgung der zu Fuß flüchtenden Verdächtigen eine

⁸¹ Beim Wiener Stadtgebiet handelt es sich um ein Flugbeschränkungsgebiet. Ohne spezielle Genehmigung ist das Fliegen nur mit sehr leichten Drohnen (<250g), nur bis maximal 30 Meter Flughöhe über dem Boden und nur unter bestimmten Auflagen erlaubt.

Person anzuhalten. Bei der auf frischer Tat betretenen Person konnte ein Rucksack mit Spraydosen vorgefunden und zu Beweis Zwecken sichergestellt werden.

Fall KRITIK WÄHREND FPÖ-ÖVP SONDIERUNGEN

Während der Sondierungsgespräche zwischen ÖVP und FPÖ Anfang des Jahres 2025 war eine Häufung sicherheitsrelevanter Vorfälle mit Bezug zu den beiden Parteien oder direkt im Umfeld von deren Parteizentralen festzustellen. Im gesamten Bundesgebiet häuften sich Meldungen über politische Schriftzüge im öffentlichen Raum, die auf Mauern, Straßen oder Gehwegen aufgefunden wurden. Ein Fenster und eine Schauvitrine der ÖVP-Landespartei zentrale Kärnten wurde mit den politisch motivierten Schriftzügen „IHR SEID ZUM KOTZEN“ sowie „WIR KOALIEREN NICHT MIT DER KICKL-FPÖ“ versehen. Bei der ÖVP-Bundespartei zentrale äußerte eine Person heftige Kritik an den Koalitionsverhandlungen mit der FPÖ und versuchte vorbeigehende Mitarbeiterinnen der ÖVP in Diskussionen zu verwickeln. Der Protest wurde von der Person live in den sozialen Medien gestreamt, zudem wurden Fotos von der Aktion angefertigt.

Fall PROTESTAKTIONEN GEGEN DAS MILITÄRISCHE VORGEHEN ISRAELS IM GAZASTREIFEN

Das Jahr 2025 war unter anderem von mehreren Protestaktionen gegen das militärische Vorgehen Israels im Gazastreifen geprägt. Beispielhaft dafür ist der Aktionismus bei zwei ORF-Standorten sowie bei der Eröffnung der Salzburger Festspiele während einer Ansprache eines Regierungsvertreters in der Felsenreitschule.

Fall PARLAMENTARIERDATEN IM DARKNET

Im Oktober 2025 wurde durch Analysen belegt, dass Zugangsdaten von privaten Profilen und Accounts österreichischer Parlamentarierinnen und Parlamentarier im Darknet kursieren. Die aufgefundenen Datensätze gerieten über verschiedene internationale Datenlecks in Umlauf und beinhalteten mitunter auch E-Mail-Adressen von Nationalratsabgeordneten.

Zwar konnte weder ein direkter Cyberangriff auf die IT-Systeme des Parlaments noch die konkrete Auswahl von Parlamentsabgeordneten als Zielobjekte festgestellt werden. Nichtsdestotrotz kann die Verfügbarkeit solcher Zugangsdaten auf Untergrund-Plattformen ein signifikantes Risiko sowohl für die persönliche Integrität, Reputation und körperliche Unversehrtheit der Betroffenen als auch für die nationale Sicherheitslage darstellen.

3.1.4 Trends und Entwicklungstendenzen

Die Analyse der aktuellen Entwicklungen, verfolgten Strategien und getätigten Statements der Obersten Organe im Beobachtungszeitraum weisen auch mit Blick auf die

nahe Zukunft auf unterschiedliche Gefahrenfelder hin, die sowohl mit abstrakten als auch konkreten Gefährdungspotenzialen einhergehen könnten.

In diesem Zusammenhang ist es absehbar, dass die Migrationspolitik neben der Inflation auch weiterhin eines der emotionalsten innenpolitischen Themen bleiben wird. Restriktive Maßnahmen wie der Stopp des Familiennachzugs oder die Arbeitspflicht für Asylwerberinnen und Asylwerber bieten einerseits Anlass für Proteste von NGOs, gesellschaftspolitisch linken Bewegungen oder Teilen der Zivilgesellschaft, könnten aber auch für entsprechend radikalisierte Einzeltäterinnen und Einzeltäter der Grund zur Begehung zielgerichteter Gewaltakte sein. Im Vergleich dazu werden allerdings Angriffe auf Symbole staatlicher Migrationspolitik (wie z. B. Regierungsgebäude, Parteizentralen etc.) als wahrscheinlicher erachtet.

Einschlägige Narrative rechtsextremistischer Gruppierungen können Regierungsmitglieder, die für die liberale Demokratie, Antidiskriminierung und EU-Integration eintreten, zur Zielscheibe extremistischer Feindbilder machen. Diverse Waffensicherstellungen bei dieser Szene zugehörigen Akteurinnen und Akteure weisen auf das damit verbundene, wachsende Bedrohungspotenzial hin.

Im linksextremistischen und klimaaktionistischen Spektrum wird bei ungenügend erscheinenden Klimaschutzmaßnahmen sowie während der Umsetzung von als klima- oder umweltschädlich wahrgenommenen Verkehrsinfrastrukturprojekten wie beispielsweise dem Lobau-Tunnel mit ernstzunehmender Gegenwehr zu rechnen sein. Dabei sind direkte Gewaltanwendungen gegen politisch Verantwortliche als weniger wahrscheinlich einzuschätzen als Blockaden, Besetzungen und Sabotageaktionen.

Der Ausbau staatlich bzw. gesetzmäßig gesteuerter KI-Strategien und die zunehmende Regulierung von Social-Media-Plattformen zur Bekämpfung von Fake-News und Hate-crime⁸² könnten insbesondere jene Regierungsmitglieder, die hier sichtbar befürwortend auftreten, in den Fokus koordinierter digitaler Hasskampagnen, Doxing⁸³-Versuche und Cyberangriffe rücken.

Vor allem der Beschluss der erweiterten Gefährderüberwachung verschlüsselter Kommunikationskanäle macht die dafür verantwortlichen Mitglieder der Bundesregierung zum Ziel für gegnerische Aktivistinnen und Aktivisten, um in zielgerichteten Kampagnen einen vermeintlich drohenden „Überwachungsstaat“ anzuprangern. Gezielte Störaktionen bei öffentlichen Auftritten oder digitale Angriffe wie Doxing oder Hacking erscheinen in

82 „Hatecrimes“ oder vorurteilsbedingte Straftaten sind gerichtlich strafbare Handlungen, die aufgrund der tatsächlichen oder vermeintlichen Zugehörigkeit geschädigter Personen zu Gruppen (Nationalität, sexuelle Orientierung usw.) begangen werden, die die Täterinnen oder Täter ablehnen.

83 Als „Doxing“ wird das internetbasierte Zusammentragen und anschließende Veröffentlichen personenbezogener Daten gegen den Willen des/der Betroffenen bezeichnet.

diesem Zusammenhang am wahrscheinlichsten. Die radikal-islamistische Szene könnte wegen dieser zielgerichteten, repressiven Ermittlungsmaßnahme, deren politische Beschlussfassung überwiegend mit der Abwehr terroristisch motivierter Anschläge argumentiert wurde, gerade deshalb eine gesteigerte Motivation entwickeln, Alternativen für konspirative Vernetzung und Kommunikation zu finden. Das ab September 2026 in Kraft tretende Kopftuchverbot für Schülerinnen und Schüler unter 14 Jahren birgt durchaus ein gewisses Risikopotenzial für die Beeinflussung von Radikalisierungsprozessen sowie Aktivitäten der islamistischen Szene gegen die hierfür politisch Verantwortlichen, wie es damals auch im Rahmen der Debatte um das sog. Burka-Verbot der Fall war, als die damalige Frauenministerin bedroht wurde.

Während politische Repräsentantinnen und Repräsentanten in einschlägiger Propaganda grundsätzlich zwar immer wieder als Ziel thematisiert werden, gelten nach wie vor neuralgische, symbolhafte oder personenfrequentierte Örtlichkeiten oder Objekte im öffentlichen Raum als Primärziel für terroristisch motivierte Straftaten.

Eine stetig zunehmende und länger andauernde Frustration der Bevölkerung bei damit einhergehendem Vertrauensverlust in die Fähigkeiten der Bundesregierung zur Bewältigung der angespannten Wirtschaftslage und Arbeitsmarktsituation könnte zu einer Zunahme kollektiver Proteste führen. Im Vergleich dazu erscheinen individuelle Bedrohungshandlungen aus momentaner Sicht unwahrscheinlicher zu sein. Jedoch kann im Umfeld entsprechend radikalisierter Einzeltäterinnen und Einzeltäter bei Vorliegen gewisser sozioökonomischer Rahmenbedingungen diese Frustration in zielgerichtete Gewaltfantasien gegen dafür verantwortlich gemachte Personen umschlagen.

Die Tendenz, durch kreativen und beharrlichen Aktionismus größtmögliche mediale Reichweite für bestimmte Anliegen zu erzielen, führt dazu, dass Oberste Organe aufgrund ihrer Bekanntheit und Präsenz zu attraktiven Zielen werden. Dies zeigen die angeführten Fälle beim ORF und bei den Salzburger Festspielen. Auch wenn diese Proteste primär nicht auf physische Gefährdung abzielen, muss die erhöhte Zielattraktivität bei der Gefährdungsbeurteilung künftig stärker berücksichtigt werden. Das Eintreten solcher aufsehenerregenden Vorfälle ist demnach jederzeit als wahrscheinlich anzunehmen. Pro-israelische Statements oder Besuche österreichischer Politikerinnen und Politiker in Israel könnten von islamistischen wie auch von pro-palästinensischen, radikalisierten Gruppen instrumentalisiert werden oder Anlass für dagegen gerichtete Gewalthandlungen sein. Insbesondere die Außenministerin, aber auch der Bundespräsident und der Bundeskanzler sind in diesem Zusammenhang aufgrund ihrer außenpolitischen Aktivitäten als besonders exponiert anzusehen.

Aus der gegenwärtigen Perspektive besteht zudem die Gefahr, dass aufgrund Österreichs humanitärer, wirtschaftlicher und diplomatischer Positionierung im Kontext des russischen Angriffskrieges gegen die Ukraine österreichische Regierungsmitglieder und/

oder verfassungsmäßige Einrichtungen ins Visier pro-russischer Akteurinnen und Akteure geraten und Ziel von Desinformationskampagnen und/oder Cyberangriffen werden.

3.1.5 Initiativen und Maßnahmen

Wissens- und Erfahrungsaustausch in Sicherheitsangelegenheiten unter den in den Ministerien damit betrauten Fachleuten kann dazu beitragen, die eigenen bisher ergriffenen Sicherheitsmaßnahmen kritisch auf Effektivität und Effizienz zu hinterfragen und somit die gesamtheitliche Resilienz verfassungsmäßiger Einrichtungen zu erhöhen. In diesem Sinne erfolgte auch im Berichtsjahr wieder die Ausrichtung einer Sicherheitsbeauftragten-Tagung, um den für die Sicherheit der verfassungsmäßigen Einrichtungen zuständigen Personen die Gelegenheit zum Austausch über neu entstandene Gefährdungspotenziale und die Möglichkeiten der Risikominimierung zu bieten. Darüber hinaus fanden im gesamten Berichtsjahr im Bedarfsfall bilaterale Gespräche mit den Sicherheitsverantwortlichen der Obersten Organe und Verfassungsmäßigen Einrichtungen statt, woraus mitunter schriftliche Sicherheitsempfehlungen in Bezug auf Personen- oder Objektschutzmaßnahmen resultierten.

Auf politischer Ebene tragen Maßnahmen wie der Beschluss der Bundesregierung zur Entwicklung einer ressortübergreifenden, gesamtstaatlichen Drohnenabwehrstrategie maßgeblich zur Bekämpfung rezenter, sich dynamisch entwickelnder Sicherheitsbedrohungen bei.

3.2 Schutz ausländischer Vertretungen, Vertreterinnen und Vertreter ausländischer Staaten und internationaler Organisationen

3.2.1 Überblick

Neben dem vorbeugenden Schutz verfassungsmäßiger Einrichtungen und ihrer Handlungsfähigkeit obliegt der DSN im Zusammenwirken mit den LSE auch der vorbeugende Schutz der Vertreterinnen und Vertreter ausländischer Staaten, der ausländischen Vertretungen sowie aller hier ansässigen internationalen Organisationen und anderer Völkerrechtssubjekte nach Maßgabe völkerrechtlicher Verpflichtungen. Dazu zählt auch der Schutz ausländischer Staatsoberhäupter und Regierungsmitglieder bei Besuchen in Österreich.

3.2.2 Aktuelle Lage

Gefährdungen bei Besuchen und Aufhalten von Vertreterinnen und Vertreter ausländischer Staaten, internationaler Organisationen oder anderer Völkerrechtssubjekte leiten sich primär aus internationalen, nationalen sowie regionalen Vorfällen und Geschehnissen ab.

Aktuelle Konflikte, wie beispielsweise der russische Angriffskrieg gegen die Ukraine oder der Nahostkonflikt, führen immer wieder zu Protestaktionen und Vorfällen bei Einrichtungen ausländischer Staaten oder internationaler Organisationen sowie bei Besuchen und Aufenthalten ausländischer Vertreterinnen und Vertretern in Österreich. Auslöser für Kundgebungen oder Aktionismus können auch entsprechende außenpolitische Haltungen des jeweiligen Staates im Zusammenhang mit aktuellen Konflikten oder innenpolitischen Entwicklungen sein.

Protestaktionen, Vorfälle und Drohungen gegenüber Vertreterinnen und Vertretern ausländischer Staaten, internationaler Organisationen und/oder anderen Völkerrechtssubjekten und die damit verbundenen Gefährdungen derselben haben ihren Ursprung oftmals in internationalen Konflikten oder nationalen bzw. regionalen Entwicklungen und Geschehnissen. Dazu zählen seit einigen Jahren vor allem der russische Angriffskrieg gegen die Ukraine und der Nahostkonflikt, insbesondere der Konflikt zwischen Israel und Hamas im Gazastreifen sowie die Geschehnisse im Zusammenhang mit den Atomanlagen im Iran und der Internationalen Atomenergie Organisation (IAEO) mit Sitz in Wien.

3.2.3 Trends und Entwicklungstendenzen

Internationale Geschehnisse wie zwischenstaatliche Kriege oder militärische Auseinandersetzungen, wie beispielsweise zwischen Russland und der Ukraine oder Israel und dem Iran, haben zumeist auch Auswirkungen auf die Gefährdung von Vertreterinnen und Vertretern ausländischer Staaten, internationaler Organisationen und anderer Völkerrechtssubjekte. Die Gefährdung ausländischer Vertreterinnen und Vertreter bei Besuchen wird maßgeblich durch den extremistischen Islamismus und die organisierte Kriminalität beeinflusst. Sonstige Extremismusformen tragen ebenfalls, jedoch in einer geringeren Größenordnung, zu diesem Gefährdungspotenzial bei.

Angetrieben durch die wachsende Intensität internationaler Konflikte, zeigte die Entwicklung der vergangenen Jahre eine deutliche Steigerung der Bedrohungslage für diplomatische Vertretungen in ganz Europa. Insbesondere die Eskalation im russischen Angriffskrieg gegen die Ukraine und die Instabilität im Nahen Osten verursachten einen signifikanten Anstieg sicherheitsrelevanter Vorfälle an den Botschaften und Konsulaten der in diese Konflikte involvierten Länder. Die damit verbundene erhöhte Gefährdungslage dürfte vorerst bestehen bleiben, ebenso wie die Möglichkeit eines gesteigerten Demonstrationsgeschehens im Zusammenhang mit nationalen Wahlen in russlandnahen Staaten oder autokratischen Tendenzen von Regierungen. Demgegenüber war bei türkischen Vertretungen in der jüngsten Vergangenheit ein Rückgang an Vorfällen zu verzeichnen, der mit den verringerten militärischen Aktivitäten und dem Friedensabkommen der türkischen Regierung und der PKK in Verbindung steht.

Die Sicherheitsarchitektur im Umfeld diplomatischer Vertretungen muss sich insgesamt weiterhin auf eine komplexer und dynamischer werdende Gefahrenlage einstellen, die sowohl von globalen Krisenherden als auch von transnationalisierten innenpolitischen Spannungen getrieben wird.



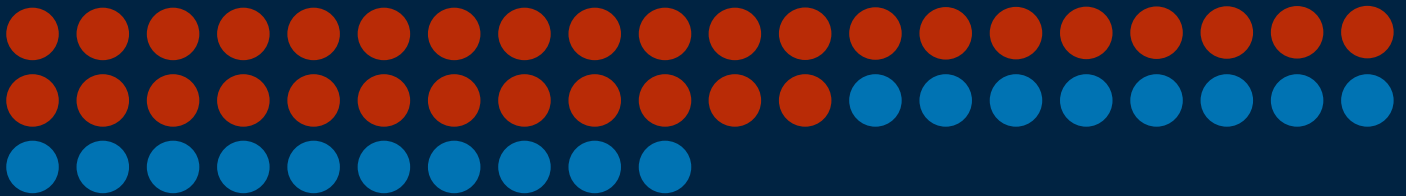
Schutz ausländischer Vertretungen, Vertreterinnen und Vertreter ausländischer Staaten und internationaler Organisationen

50

Vorfälle bei Vertretungen
ausländischer Staaten

18

unterschiedliche
Staaten betroffen



15

Vorfälle bei
internationalen Organisationen



286

Kundgebungen

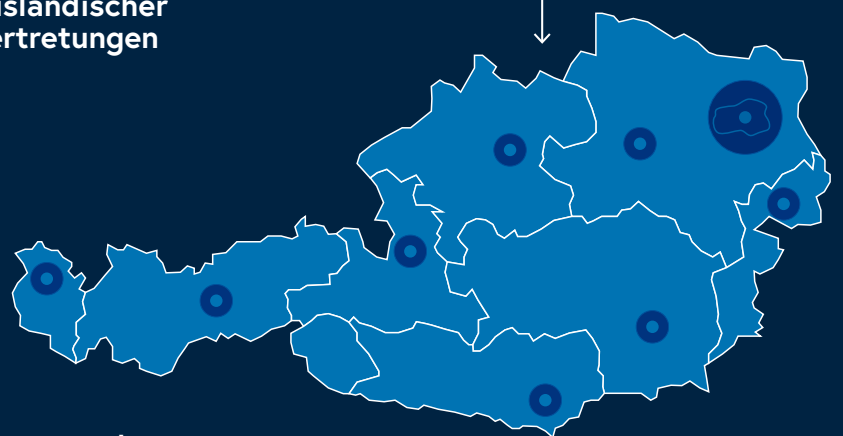
23
im Nahbereich
ausländischer
Vertretungen

Konzentration



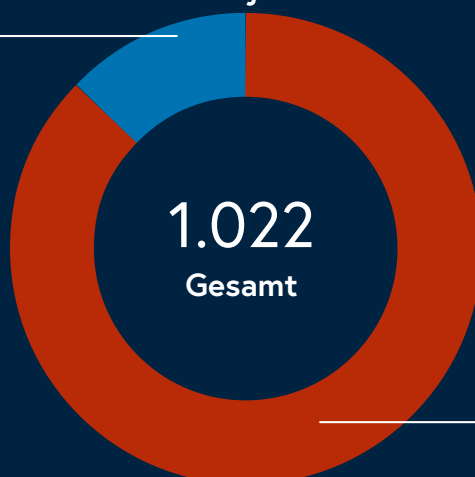
100

Teilnehmerinnen
und Teilnehmer
im Durchschnitt
pro Kundgebung



129

Besuche und Transite von Vertreterinnen und
Vertretern internationaler Organisationen
und anderer Völkerrechtssubjekte



893

Besuche und Transite von Vertreterinnen
und Vertretern ausländischer Staaten

3.2.4 Zahlen/Daten/Fakten

Die in Österreich ansässigen Vertretungen ausländischer Staaten verzeichneten im Jahr 2025 bundesweit 50 Vorfälle bzw. Drohungen, wovon 18 unterschiedliche Staaten betroffen waren.

Zusätzlich wurden bei internationalen Organisationen 15 Vorfälle oder Drohungen gegen Vertreterinnen und Vertreter und Einrichtungen registriert. Der Vergleich mit dem Jahr 2024 zeigt: 2024 wurden 35 Ereignisse bzw. Drohungen bei ausländischen Vertretungen vermerkt. Im Bereich der internationalen Organisationen gab es im Jahr 2024 keine Geschehnisse dieser Art.

Die Vorkommnisse bei ausländischen Vertretungen und internationalen Organisationen sind facettenreich. Im Berichtsjahr reichten sie von einer Blockade des Zugangs zu einer diplomatischen Vertretung durch Aktivistinnen und Aktivisten bis hin zum Wurf eines detonierenden pyrotechnischen Gegenstands auf ein Botschaftsgelände ohne Schaden.

Weiters gab es einen Drohnenüberflug – ohne Beeinträchtigung – bei einer Handelsvertretung und die Beschmierung der Fassade einer internationalen Organisation mit pro-palästinensischen Parolen, die Sachschaden verursachte. Zusätzlich wurden ab Juni 2025 bedenkliche Beiträge in sozialen Medien gegen einen Vertreter einer internationalen Organisation verzeichnet.

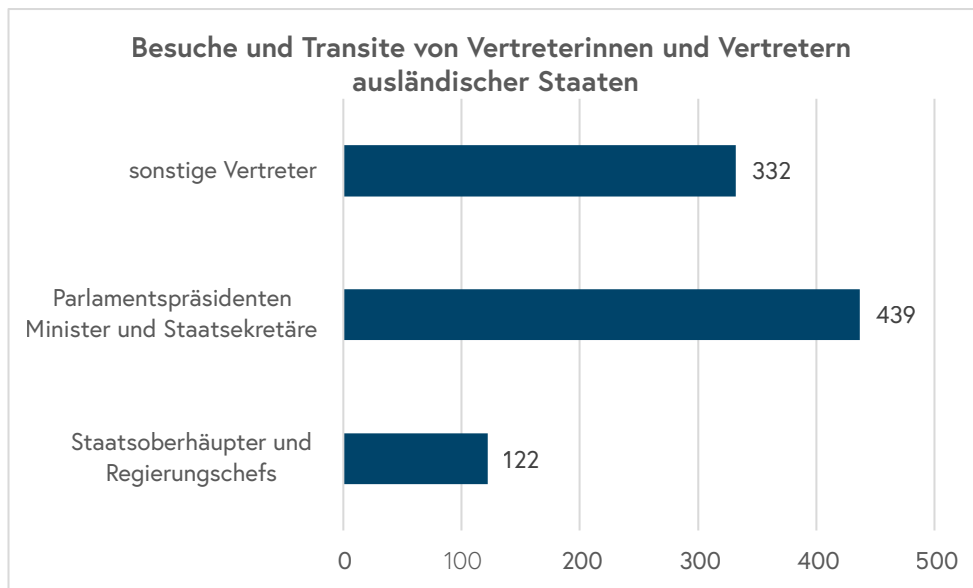
Im Jahr 2025 gab es bundesweit 286 Kundgebungen mit Bezug zu ausländischen Staaten. Nur 23 davon fanden im Nahbereich der jeweiligen ausländischen Vertretungen statt.

Die Versammlungen konzentrierten sich hauptsächlich auf Wien und in geringerem Maße auf die Landeshauptstädte. Die durchschnittliche Teilnehmerinnen- und Teilnehmerzahl pro Kundgebung lag bei rund 100 Personen. Wiederkehrende, thematisch gleiche Kundgebungen gegen denselben Staat sind hierbei nicht berücksichtigt.

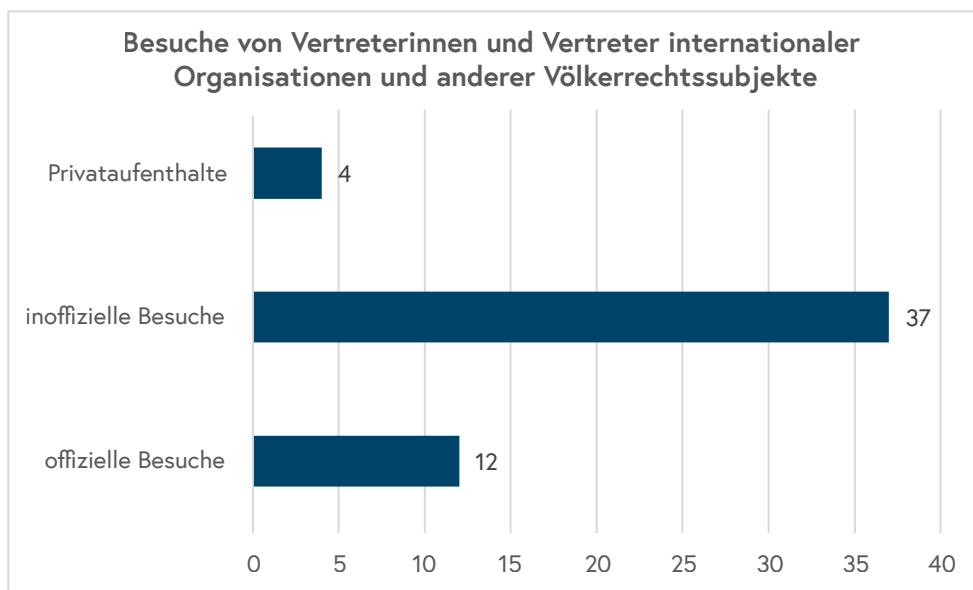
Zudem wurden vier Kundgebungen gegen internationale Organisationen gemeldet, die im unmittelbaren Nahbereich dieser Organisationen stattfanden und durchschnittlich etwa 60 Teilnehmerinnen und Teilnehmer zählten.

Die DSN registrierte im Jahr 2025 insgesamt 1.022 Besuche bzw. Aufenthalte und Transite von Vertreterinnen und Vertretern ausländischer Staaten (893), internationaler Organisationen und anderer Völkerrechtssubjekte (129) in Österreich. Im Vergleich zu 2024 (1.184) ist dies eine Reduktion um ca. 14 Prozent. Davon entfallen 467 auf Besuche bzw. Aufenthalte und 426 auf Transite von Vertreterinnen und Vertretern ausländischer Staaten (893). Bei den Besuchen bzw. Aufenthalten handelte es sich um 142 offizielle Besuche, 243 inoffizielle Besuche und 82 (467) Privataufenthalte in Österreich. Von den 893 Besuchen bzw. Aufenthalten und Transiten von Vertreterinnen und Vertretern

ausländischer Staaten entfielen 122 auf Staatsoberhäupter und Regierungschefs, 439 auf Parlamentspräsidentinnen und Parlamentspräsidenten, Ministerinnen und Minister, Staatssekretärinnen und Staatssekretäre sowie 332 auf sonstige Vertreterinnen und Vertreter ausländischer Staaten. Die Besuche erfolgten aus 101 verschiedenen Staaten. Diese unterteilten sich in 26 EU-Staaten sowie 75 Nicht-EU-Staaten.



Hinsichtlich der Vertreterinnen und Vertreter internationaler Organisationen und anderer Völkerrechtssubjekte können von den 129 Besuchen 53 einem Besuch bzw. Aufenthalt und 76 einem Transit zugeordnet werden. Von den 53 Besuchen waren es zwölf offizielle, 37 inoffizielle sowie vier Privataufenthalte. Die Vertreterinnen und Vertreter repräsentierten zwölf internationale Organisationen sowie acht Völkerrechtssubjekte (beispielsweise der EU).



Zur Gewährleistung der Sicherheit der in Österreich ansässigen Vertretungen ausländischer Staaten sowie deren Einrichtungen wurden im Jahr 2025 durch die DSN 20 objektschutzrelevante Maßnahmen zusätzlich zu den bestehenden angeordnet. 2024 waren es 19 objektschutzrelevante Maßnahmen. Im Kontext der in Österreich ansässigen Vertretungen internationaler Organisationen sowie deren Einrichtungen waren es drei Anordnungen. 2024 wurden keine Anordnungen erlassen.

3.3 Schutz kritischer Infrastruktur

3.3.1 Überblick

Während noch vor wenigen Jahren Cyberangriffe bzw. hybride Attacken wie Ransomware, Supply-Chain-Angriffe u. ä. abstrakte Bedrohungen waren, gehören diese und ähnliche Angriffe mittlerweile zum Alltag für viele Unternehmen, insbesondere auch im Bereich der kritischen Infrastruktur. Die kritische Infrastruktur ist aber nicht nur ein wirtschaftlicher Faktor, sondern auch die Lebensader unserer heutigen Gesellschaft und folglich unentbehrlich. Somit müssen bei solchen Ereignissen wie auch künftigen Entwicklungen gezielte Gegenmaßnahmen getroffen werden, um die betroffenen oder auch gefährdeten Unternehmen, Institutionen und Organisationen seitens staatlicher Sicherheitsbehörden zu unterstützen. Die DSN ist jene staatliche Stelle, welche die Unternehmen der sogenannten ACI-Liste⁸⁴ hinsichtlich aktueller Bedrohungen bei der Prävention unterstützt.

Für die Unternehmen der kritischen Infrastruktur wird die Vorbereitung auf mögliche Risiken und Bedrohungen immer komplexer. Einerseits sind die zur Verfügung stehenden Mittel beschränkt, andererseits werden die geopolitischen Verwerfungen mit ihren mittelbaren und unmittelbaren Auswirkungen immer spürbarer. Werden beispielsweise Drohnen in vielen Unternehmen mittlerweile zur Unterstützung bei verschiedenen Arbeiten verwendet, stellen sie gleichzeitig auch eine immense Bedrohung für viele Unternehmen dar. Spionage ist dabei nur ein mögliches Ziel der Nutzung.

Insgesamt verdeutlichen diese Entwicklungen, wie stark kritische Infrastrukturen durch unterschiedliche Risiken und Bedrohungen gefährdet sind. Die Kombination aus physischer Bedrohung und digitalen Gefahren erfordert verstärkte Sicherheitsmaßnahmen, eine verbesserte Koordination zwischen Behörden und Unternehmen sowie eine kontinuierliche Anpassung an sich wandelnde Bedrohungslagen, um die Sicherheit und Funktionsfähigkeit essenzieller Systeme langfristig zu gewährleisten.

Zusammenfassend kann festgestellt werden, dass für Unternehmen der kritischen Infrastruktur die geopolitische Lage derzeit sehr fordernd ist und staatliche Stellen Unternehmen bei der Bewältigung dieser Herausforderungen unterstützen müssen.

84 ACI: Austrian Critical Infrastructure

Das im Jahr 2025 beschlossene Gesetz „Resilienz kritischer Einrichtungen“ (RKEG) wird dazu einen wichtigen Beitrag leisten und dabei mit den Unternehmen auf eine immer wichtigere Resilienz hinarbeiten. Nur eine starke und resiliente Wirtschaft – hier vertreten durch die Unternehmen der kritischen Infrastruktur – kann die Versorgungssicherheit in Österreich sichern.

3.3.2 Aktuelle Lage

Hybride Angriffe

Im Jahr 2025 registrierte die DSN vor allem im Bereich der sogenannten hybriden Vorfälle einen Anstieg. Auch wenn in Österreich im Vergleich zu vielen anderen europäischen Staaten (noch) keine staatlich gesteuerten Sabotageakte festgestellt werden konnten, sind diese hybriden Bedrohungen doch allgegenwärtig. Sie zeigen sich in unterschiedlichsten Kombinationen, bestehen aus diversen Formen der Einflussnahme und der Aggression, die darauf abzielen, die Gesellschaft zu spalten und zu manipulieren. Es handelt sich dabei um komplexe, auf den ersten Blick oftmals nicht erkennbare militärische oder nicht-militärische Angriffe mit unterschiedlichsten Mitteln, um eine illegitime Einflussnahme auf den Staat oder auf Institutionen zu nehmen. Damit soll das Vertrauen in die Handlungsfähigkeit und die Stabilität der Institutionen untergraben werden. Dies kann nicht nur durch Informationsverfälschung, Einflussnahme auf Wahlen oder auch militärische Drohungen erfolgen, sondern bereits beim unerlaubten Überflug mittels Drohnen, der Störung von GNSS-Signalen⁸⁵ oder der Sabotage von Perimeter-Einrichtungen⁸⁶. Kritische Infrastrukturen können von derartigen Vorfällen betroffen sein.

Fachkräftemangel

Eine weitere Herausforderung ist der Fachkräftemangel. So kann eine unbesetzte Stelle in einem Unternehmen zu negativen Auswirkungen führen, wenn dadurch wesentliche Sicherheitsaufgaben nicht abgedeckt werden können. Aber auch eine Stellenbesetzung in sicherheitsrelevanten Bereichen mit Personal, das nicht sicherheitsüberprüft ist, stellt einen Risikofaktor im Sinne einer möglichen Innentäterschaft dar. Durch zunehmend internationales Personal-Recruiting heimischer Unternehmen wird es immer schwieriger, Personal in sensiblen Bereichen wirkungsvoll zu überprüfen. So wurde bekannt, dass IT-Mitarbeiterinnen und IT-Mitarbeiter aus Nordkorea in Europa mit gefälschten Identitäten Zugang zu einschlägigen Unternehmen suchten, um durch die Anstellungen Informationen an das Regime zu liefern.

85 GNSS-Signale sind schwache Funksignale im L-Band (1–1,5 GHz), die von Satelliten (GPS, Galileo, GLONASS, BeiDou) zur Erde gesendet werden. Sie übertragen präzise Zeitstempel und Satellitenpositionen (Ephemeriden), wodurch Empfänger mittels Laufzeitmessung (Trilateration) ihre Position zentimeter- bis metergenau bestimmen können. Die Signale bestehen aus Trägerwellen, Codes und Navigationsdaten.

86 Dies sind Schutzsysteme für die äußere Grenze eines Geländes oder Gebäudes, die unbefugten Zutritt verhindern sollen, indem sie eine erste Verteidigungslinie bilden. Sie kombinieren physische Barrieren (Zäune, Mauern), elektronische Überwachung (Kameras, Sensoren, Alarmanlagen) und organisatorische Maßnahmen (Zugangskontrollen, Personal).

Herausforderungen im Energiesektor

Im Sektor Energie bewirken vor allem das im aktuellen Regierungsübereinkommen festgeschriebene Ziel, Österreich bis zum Jahr 2040 klimaneutral zu machen, und die Auswirkungen des russischen Angriffskrieges gegen die Ukraine dynamische Entwicklungen. Die Energiewende wird vor allem in den Bereichen Verkehr, Wärmeversorgung und Industrie vorangetrieben. Dabei ist es erforderlich, die vertraglich vereinbarten, aber sanktionsbedingt nicht mehr zur Verfügung stehenden Gaslieferungen aus Russland durch Ersatzlieferungen aus anderen Ländern zu substituieren. Diese Ersatzlieferungen erfolgen nun über Importverbindungen, die keine Gebiete durchqueren, welche durch den russischen Angriffskrieg in Mitleidenschaft gezogen wurden. Die USA spielen mittlerweile eine dominierende Rolle beim LNG⁸⁷-Import in die Europäische Union. Der Anteil der von den USA gelieferten Mengen am gesamten LNG-Importvolumen in die Europäische Union ist seit Beginn des russischen Angriffskrieges auf über 50 Prozent angestiegen.

Die Versorgungssicherheit mit Strom und Gas ist in Österreich grundsätzlich als sehr hoch einzustufen. Der in den letzten Jahren erkennbare Trend zu privat installierten Photovoltaikanlagen ist ungebrochen. Zeitweise wurden in Österreich neue Photovoltaikflächen mit einem Nennleistungsäquivalent in der Größenordnung eines Donaukraftwerks errichtet. Dies stellt eine enorme Belastungsprobe für die öffentlichen Stromnetze dar, da es durch das volatile Stromerzeugungsverhalten der öffentlich angebundenen Photovoltaikanlagen zu Ungleichgewichten zwischen Stromerzeugung und Stromverbrauch kommt. Diese müssen durch die Regelungsmaßnahmen der Netzbetreiber, z. B. durch das Zuschalten von Gaskraftwerken, aktiv ausgeglichen werden.

Mit der Energiewende verfolgt Österreich das Ziel, ab dem Jahr 2040 keine Treibhausgasemissionen mehr zu produzieren und somit klimaneutral zu sein. Dies bedeutet, dass der Ausbau der Elektrizitätsinfrastruktur in den kommenden Jahren ambitioniert vorangetrieben werden muss. Ziel ist es daher, die notwendige Elektrifizierung der bisherigen Treibhausgas-Verursacher, d. h. insbesondere der Bereiche Transport, Verkehr und Wärme Gewinnung, sicherzustellen. Branchenverbände und Energieerzeuger prognostizieren die Notwendigkeit einer Verdreifachung der in Österreich installierten Kraftwerksleistung bis zum Jahr 2040. Essenziell bei der Ertüchtigung der österreichischen Strominfrastruktur ist die Einplanung steuerbarer Kraftwerkskapazitäten, die das Gleichgewicht zwischen der volatil verfügbaren Stromproduktion aus erneuerbaren Quellen und dem Stromverbrauch sicherstellen können.

87 „LNG“ oder „Liquefied Natural Gas“ ist flüssiges Erdgas. Erdgas wird durch extreme Abkühlung in flüssigen Zustand versetzt, um dadurch das Volumen zu verkleinern und den Transport zu vereinfachen.

Erhöhte Einsatzzahlen bei den Hilfs- und Einsatzkräften

Im Bereich der Hilfs- und Einsatzkräfte (z. B. Bergrettung, Feuerwehr, Flugrettung, Österreichisches Rotes Kreuz) wird in den letzten Jahren ein Anstieg an Einsätzen verzeichnet – mit weiterhin steigender Tendenz. Ein Großteil davon sind Einsätze aufgrund von Unwettern, Überflutungen oder Sturmereignissen, bei Unfällen oder als Versorgungseinsätze.

Die globale Erwärmung führt immer öfter zu Extremwetterereignissen wie beispielsweise der Hochwasserkatastrophe vom September 2024. Solche Einsätze stellen eine große Herausforderung und Belastung für die Einsatzkräfte dar und veranlassen sie zur Anpassung ihrer Einsatzpläne, da auch das Risikomanagement immer komplexer wird. Durch diese erhöhten Einsätze wird Personal gebunden, das oftmals anderweitig dringend benötigt wird.

Ein anderer Faktor, Einsatzkräfte kurzfristig verstärkt zu alarmieren, ist das sogenannte Swatting. Durch Drohmails oder -anrufe, z. B. mit Bombendrohungen, werden Einsatzkräfte, allen voran die Spezialeinheiten der Polizei, gebunden und sind für andere Einsätze nicht verfügbar. Diese Phänomene können fallweise auch als Teil bzw. Vorbereitungshandlungen hybrider Bedrohungen eingestuft werden.

Resilienz kritischer Einrichtungen

Die gestiegene Zahl an Vorfällen in kritischen Infrastrukturen auf internationaler Ebene verdeutlicht die Bedeutung eines einheitlichen europäischen Rahmens zur Steigerung der Resilienz. Im Fokus stehen dabei Einrichtungen, welche zur Aufrechterhaltung essenzieller gesellschaftlicher Funktionen notwendig sind.

Um den dafür notwendigen Rahmen zu schaffen, wurde am 24. September 2025 das Resilienz kritischer Einrichtungen-Gesetz im österreichischen Nationalrat beschlossen. Dieses Gesetz stellt die Umsetzung der Richtlinie (EU) 2022/2557 (RKE-Richtlinie) in nationales Recht dar. Das Gesetz richtet sich an kritische Einrichtungen, welche wiederum in elf Sektoren unterteilt sind.

Die Rolle der zuständigen Behörde und zentralen Anlaufstelle kommt laut RKEG dem BMI zu. In diesem Zusammenhang verantwortet die DSN als seit vielen Jahren zuständige Stelle für den Schutz kritischer Infrastruktur den Vollzug des RKEG.

Als zuständige RKE-Behörde hat das BMI unterschiedlichste Pflichten. So war der Bundesminister für Inneres verpflichtet, bis zum 17. Jänner 2026 eine nationale Strategie zu Stärkung der Resilienz und eine nationale Risikoanalyse zu erstellen. Diese Dokumente, die am 17. Jänner 2026 vom Ministerrat beschlossen wurden, unterstützen die kritischen Einrichtungen dabei, ihre Resilienz eigenständig zu stärken. Darüber hinaus hat der Bundesminister für Inneres die kritischen Einrichtungen bis zum 17. Juli 2026 per Be-

scheid zu ermitteln. Anschließend kommt dem BMI die Aufgabe zu, das Aufsichtsregime zu vollziehen.

Die zentralen Akteure des RKE-Regimes stellen die kritischen Einrichtungen dar. Aufgrund des regulativen Charakters des RKEG haben die jeweiligen Einrichtungen verschiedene Verpflichtungen, die sie stets mit Unterstützung des BMI erfüllen müssen. Auf Basis der nationalen Strategie und der Risikoanalyse des BMI ist von den kritischen Einrichtungen neun Monate nach Rechtskraft des Bescheids eine Risikoanalyse zu erstellen. Um die kritischen Einrichtungen zu unterstützen, wird die nationale Risikoanalyse derart aufgebaut sein, dass sie eine gute Grundlage für die Risikoanalysen der kritischen Einrichtungen darstellt. Um die Erkenntnisse der eigenen Risikoanalyse zu verarbeiten, werden die kritischen Einrichtungen in einem Resilienzplan geeignete Maßnahmen formulieren und diese in weiterer Folge umsetzen. In diesem Bereich sieht das RKEG Beratungen der kritischen Einrichtungen bei der Ergreifung der Resilienzmaßnahmen vor. Auf diese Weise sollen kritische Einrichtungen ihren Schutz eigenständig stärken, um Sicherheitsvorfälle, die die Erbringung eines wesentlichen Dienstes erheblich stören, zu verhindern. Sollte es trotzdem zu einem Sicherheitsvorfall kommen, haben kritische Einrichtungen den Vorfall dem BMI zu melden.

Abseits der angesprochenen Verpflichtungen des BMI sieht das RKEG verschiedene weitere Unterstützungs- und Vorsorgemaßnahmen gegenüber den kritischen Einrichtungen vor. So wird die RKE-Behörde Frühwarnungen an die kritischen Einrichtungen übermitteln oder kann für das Personal der kritischen Einrichtungen Schulungen anbieten.

Zur Durchsetzung der Verpflichtungen der kritischen Einrichtungen ist ein Aufsichtsregime vorgesehen. Dieses sieht in einem ersten Schritt vor, dass ab Juli 2027 die Dokumentation der kritischen Einrichtungen angefordert und überprüft wird. Bei Unstimmigkeiten können Audits bzw. Vor-Ort-Kontrollen folgen. Das RKEG sieht Verwaltungsstrafverfahren bei nicht- bzw. unzureichender Erfüllung der Verpflichtungen vor; diese sind allerdings Ultima Ratio. Der Dialog mit den Betreibern kritischer Einrichtungen steht hier klar im Vordergrund.



3.3.3 Vorfälle 2025

Der ORF als Ziel von pro-palästinensischem Aktionismus

Im Juni 2025 drangen neun verumumte pro-palästinensische Aktivistinnen und Aktivisten in das ORF-Landesstudio Tirol ein. Vier der Aktivistinnen und Aktivisten stiegen über ein Baugerüst auf das Gebäudedach, hissten auf einer Antennenplattform eine Palästinaflagge und zündeten bengalische Feuer. Die übrigen Aktivistinnen und Aktivisten kritisierten mittels Megafon im Inneren des Landesstudios die ORF-Berichterstattung über den Nahostkonflikt. Da der Versuch einer Deeskalierung mittels Kontaktaufnahme durch den diensthabenden Chefredakteur des Landesstudios nicht zur Beendigung der Kundgebung führte, wurde diese polizeilich aufgelöst. Aufgrund der im ORF-Landesstudio

Tirol etablierten Sicherheitsvorkehrungen konnten die Aktivistinnen und Aktivisten nicht in die Redaktions- und Senderäume vordringen und den Sendebetrieb unterbrechen.

Ein weiterer Vorfall ereignete sich im August 2025, als sich sechs als Besucherinnen und Besucher getarnte, pro-palästinensische Aktivistinnen und Aktivisten Zugang zum ORF-Sendezentrum am Küniglberg in Wien verschafften. Sie ver mummten sich während ihrer Teilnahme an einer Führung durch das Sendezentrum, versprühten rote Farbe aus Trinkflaschen und teilten lautstark ihren Unmut über die aktuelle Situation im Gazastreifen und die mediale Berichterstattung über den Nahostkonflikt mit. Die Aktivistinnen und Aktivisten drangen in den ORF-Newsroom ein und beeinträchtigten dort die redaktionellen Arbeitsabläufe. Der Regie- und Sendebetrieb war von der widerrechtlichen und nicht angemeldeten Kundgebung nicht betroffen. Aufgrund der mangelnden Kooperationsbereitschaft der Aktivistinnen und Aktivisten wurde die Kundgebung polizeilich aufgelöst; die betreffenden Personen wurden festgenommen. Der angerichtete Sachschaden belief sich auf mehrere tausend Euro.

Drohensymposium in Wien

Im September 2025 fand das internationale Symposium „DroneVation & Defence 2025“ in Wien statt. Bereits im Vorfeld wurde von einer internationalen Organisation eine Kundgebung angemeldet. Auch in den sozialen Medien gab es Aufrufe gegen die Veranstaltung. Diese Informationen wurden an den Veranstalter übermittelt. Schließlich kam es in der Nacht vor dem Symposium zu einem Einbruch in das Gelände und einem Buttersäureangriff auf den Veranstaltungsort. Zu Schaden kam dabei niemand, da das geworfene Behältnis letztendlich nicht zerbrach und der Buttersäureanschlag das volle Ausmaß seiner Wirkung nicht erreichen konnte.

Bombendrohungsserie gegen Bahnhöfe

Im Berichtsjahr kam es in Österreich erneut zu mehreren Bombendrohungen gegen Einrichtungen des Transportsektors. Betroffen waren vor allem Bahnhöfe und damit zentrale Knotenpunkte des öffentlichen Verkehrs. Durch anonyme Drohungen per E-Mail oder Telefon wurden wiederholt großflächige Sicherheitsmaßnahmen und Polizeieinsätze ausgelöst.

Bahnhöfe sind sowohl für die tägliche Mobilität unzähliger Menschen als auch für die Versorgung der Wirtschaft von zentraler Bedeutung. Angriffe oder Drohungen gegen diese Infrastrukturen können daher nicht nur das Sicherheitsgefühl der Bürgerinnen und Bürger beeinträchtigen, sondern auch den Ablauf des täglichen Personen- und Güterverkehrs erheblich stören.

Auch wenn sich die Drohungen im Nachhinein immer als substanzlos herausgestellt haben, hatten sie doch zu umfangreichen Ausfallszeiten der Bahnhöfe bzw. des Bahnbetriebes sowie zur Bindung von Einsatzkräften geführt. Dies verursachte insgesamt einen bedeu-

tenden wirtschaftlichen Schaden. Die Vorfälle zeigen zudem, dass kritische Transportinfrastrukturen nach wie vor ein attraktives Ziel für Drohungen und Störaktionen sind, da hier der Alltag der Bürgerinnen und Bürger mit einfachen Mitteln erschwert werden kann. Solche Handlungen erzeugen zudem großen Widerhall quer durch alle Medien.

3.3.4 Trends und Entwicklungstendenzen

Bombendrohungen und Cyberattacken gegen kritische Infrastrukturen

Im Vergleich zum Jahr 2024 stieg die Anzahl der Bombendrohungen im Berichtsjahr deutlich. Besonders betroffen war der Transportsektor, der aufgrund seiner zentralen Bedeutung für den Personen- und Güterverkehr besonders anfällig für derartige Störungen ist.

Aufgrund der Häufung von Bombendrohungen im Bundesgebiet und der damit einhergehenden starken medialen Präsenz hatte dies nebst der Gefahr von Trittbrettfahrerinnen und Trittbrettfahrern auch andere Auswirkungen. So wurden etwa die strafrechtlichen Konsequenzen und Erfolge durch den Staatsschutz und durch die polizeilichen Ermittlungen medial aufbereitet. Die Anpassung der Medienstrategie zur Berichterstattung, die klare Kommunikation der strafrechtlichen Folgen und die konsequente Verfolgung dieser Straftaten sind ebenso Maßnahmen, die zu einem Rückgang führen können.

Parallel zu dieser Entwicklung blieben auch Cyberangriffe im Jahr 2025 ein bedeutendes Problem. Besonders der Transportsektor war hier wieder stark betroffen. Hackerangriffe richteten sich gezielt gegen die IT-Infrastruktur kritischer Einrichtungen. Obwohl Österreich im Vergleich zu einigen anderen Ländern weniger stark von Cyberangriffen betroffen war, zeigen die Vorfälle die zunehmende Verwundbarkeit selbst hochentwickelter Systeme. Ein besonders auffälliger Fall war der Hackerangriff auf das Check-in-System der Flughäfen in Berlin, Brüssel, Dublin und London. Die daraus resultierenden Störungen führten zu erheblichen Verzögerungen im Flugverkehr, was zahlreiche Reisende beeinträchtigte und den Flughafenbetrieb stark belastete.

Hybride Angriffe auf kritische Infrastrukturen im Kontext der geopolitischen Situation

Hybride Bedrohungsformen wie Sabotage, Hacktivismus, Desinformation und Wirtschaftsspionage durch staatliche und nichtstaatliche Akteurinnen und Akteure gewinnen zunehmend an Bedeutung. Diese komplexen, koordinierten und oft schwer fassbaren Bedrohungen stellen nicht nur die Unternehmen der kritischen Infrastruktur vor neue, erhebliche Herausforderungen, sondern auch die Sicherheitsbehörden. Insbesondere in Europa haben die letzten Jahre gezeigt, dass russische Social Bots immer öfter systematisch zur Verbreitung von Desinformationen eingesetzt werden. Parallel dazu kam es auch vermehrt zu Distributed-Denial-of-Service-Angriffen, zahlreichen Cyber- und Sabotagevorfällen, Sichtungen nichtzuordenbarer Drohnen bei kritischen Einrichtungen sowie zu Drohungen, die das Sicherheitsgefühl und die Stabilität in vielen Bereichen

erheblich beeinträchtigten. Auch der anhaltende Nahostkonflikt hatte Auswirkungen auf Österreich: Industriebetriebe, die direkte oder indirekte Handelsbeziehungen zu Ländern in der Konfliktregion unterhalten, wurden mehrmals Ziel von Sabotageaktionen pro-palästinensischer Gruppen.

Die zunehmende Häufung von Cyberkriminalitätsvorfällen und die damit einhergehenden Risiken für betriebliche Abläufe haben die Betreiberinnen und Betreiber kritischer Infrastrukturen in den vergangenen Jahren dazu veranlasst, ihre Schutzmaßnahmen im Bereich der IT-Sicherheit deutlich zu verstärken. Die fortschreitende Digitalisierung und Vernetzung kritischer Systeme machen diese Maßnahmen unerlässlich, um den vielfältigen Gefahren, die von hybriden Bedrohungen ausgehen, wirksam begegnen zu können.

Sicherheitsbedarf im Bereich der Forschung

Österreichische Universitäten sind in den letzten Jahren immer wieder ins Visier von Cyberangriffen geraten. Das Interesse von Cyberkriminellen an Universitäten ist besonders groß, da diese Institutionen über eine Fülle hochsensibler Daten verfügen. Dazu zählen nicht nur personenbezogene Informationen, sondern auch wertvolle Forschungsdaten, die oftmals von internationaler Bedeutung sind. Zudem bergen die engen Projektkooperationen mit externen Partnerinnen und Partnern zusätzliche Sicherheitsrisiken, da durch diese Vernetzungen potenzielle Angriffspunkte entstehen können.

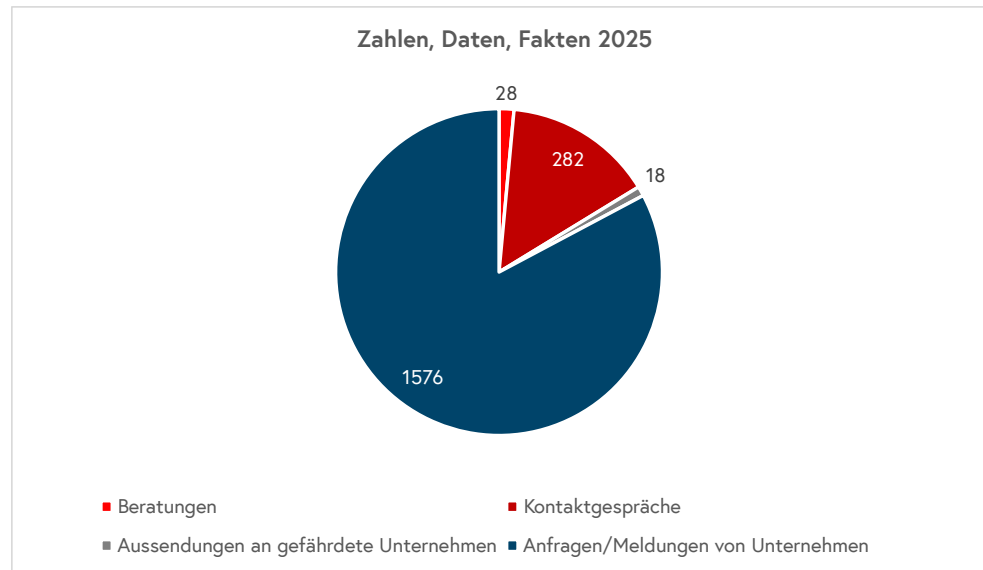
Mit einer Verstärkung dieses Trends ist zu rechnen. So wurde bekannt, dass im Herbst des Berichtsjahres eine Einrichtung aus dem medizinischen Bereich mit Malware infiltriert wurde. Das Besondere an diesem Fall war die hohe Professionalität sowohl auf technischer wie auch auf organisatorischer Ebene. Mittels Social Engineering wurde der eigentliche Cyberangriff vorbereitet. Die Ermittlungen diesbezüglich sind noch nicht abgeschlossen, daher können weitere Details nicht genannt werden.



3.3.5 Zahlen/Daten/Fakten

Der Schutz kritischer Infrastruktur kann nur in enger und vertrauensvoller Zusammenarbeit zwischen den Betreibern und den Sicherheitsbehörden erfolgreich erfüllt werden.

Die Basis dafür bieten gegenseitige Ansprechpartnerinnen und Ansprechpartner, persönliche Kontakte bei Erst- und Folgegesprächen, die bestmögliche Beratung und rasche Erledigung von Anfragen sowie eine Servicierung durch Weitergabe von relevanten sektorbezogenen oder betreiberspezifischen Informationen.



Die Tätigkeiten der DSN in diesem Aufgabenbereich zeigen, dass im Berichtsjahr 282 Kontaktgespräche und 28 Beratungen mit den Betreibern kritischer Infrastrukturen durchgeführt und 1.576 Unternehmensanfragen beantwortet und eingehende Meldungen bearbeitet wurden.

Das eingerichtete Frühwarn- und Informationssystem soll Betreiberinnen und Betreiber möglichst rasch über aktuell bestehende Gefahren sowie sonstige wichtige Informationen in Kenntnis setzen, sodass innerhalb der Unternehmen notwendige Sicherheitsmaßnahmen unmittelbar getroffen und dadurch Ausfälle verhindert werden können. Im Berichtsjahr wurden 18 Aussendungen an gefährdete Unternehmen durchgeführt.

Im Zuge von Amtshilfverfahren bei Genehmigungsanträgen nach dem Investitionskontroll-Gesetz wurden 366 Erhebungen und Bewertungen durchgeführt.

3.3.6 Initiativen und Maßnahmen der DSN

Schwachstellenanalysen

Auf Wunsch bzw. bei Bedarf können sich Unternehmen der kritischen Infrastruktur an die DSN wenden, um eine sogenannte Schwachstellenanalyse ihrer Objekte durchführen zu

lassen. Dabei werden diese in mehreren Schritten einem Penetrationstest⁸⁸ unterzogen, dessen Ergebnis anschließend in einem Bericht zusammengefasst wird. Neben der Auf-
findung möglicher Eintritts- und damit Schwachstellen werden Sicherheitsmaßnahmen empfohlen.

Sicherheits- und Zuverlässigkeitsüberprüfungen im Kontext mit dem Zonenkonzept

Gemeinsam mit sieben Unternehmen der kritischen Infrastruktur wurde im Juni 2025 ein Workshop zum Thema „Zonenkonzept und Zuverlässigkeitsüberprüfungen“ durchgeführt. Dabei wurden neben den Unterschieden zwischen einzelnen Überprüfungsformen – etwa bei den dafür notwendigen Voraussetzungen, dem Umfang, den Verpflichtungen, der Zuständigkeit und der Dauer – insbesondere auch die Herausforderungen im Zusammenhang mit dem Zutritt zu sicherheitsrelevanten Unternehmensbereichen diskutiert. Durch die unternehmensinterne Festlegung, welches Zonenkonzept für das Unternehmen passend ist und welche Überprüfungen in welcher Zone zielführend sind, wurde eine nachvollziehbare Indikation für die zu wählende Überprüfungsform in den jeweiligen Zonen erarbeitet. Daraus resultierend wurde in Kooperation mit einigen Betreiberinnen und Betreibern kritischer Infrastrukturen eine Broschüre mit Empfehlungen erstellt, die in der täglichen Unternehmenspraxis angewendet werden können. Diese Broschüre wurde am Tag der kritischen Infrastruktur präsentiert.

Veranstaltung Tag der kritischen Infrastruktur 2025

Im Rahmen des APCIP-Masterplans wird durch regelmäßige Veranstaltungen die Zusammenarbeit, Koordination und der Informationsfluss zwischen der Wirtschaft, Forschung und den Sicherheitsbehörden gezielt gefördert und intensiviert. Hierzu zählte auch der Tag der kritischen Infrastruktur 2025, der am 15. September 2025 stattfand. Die Veranstaltung verzeichnete insgesamt über 300 Teilnehmerinnen und Teilnehmer, was die große Relevanz und das breite Interesse an den behandelten Themen unterstreicht. Der Fokus der Veranstaltung lag auf dem Dialog und der Vernetzung zwischen Vertreterinnen und Vertretern von Behörden, Wissenschaft und Wirtschaft, um den Schutz kritischer Infrastrukturen weiter zu stärken. Dies soll den schnellen und effizienten Informationsaustausch im Anlass- oder Krisenfall sicherstellen und somit die Reaktionsfähigkeit aller Beteiligten deutlich erhöhen. Allgemein sollen im Rahmen der Veranstaltung Informationen hinsichtlich bewährter Praktiken und erfolgreicher Sicherheitsmaßnahmen auf zwei Ebenen geteilt werden: Einerseits in informellen Gesprächen zwischen den Teilnehmerinnen und Teilnehmern und andererseits durch Fachvorträge nationaler und internationaler Expertinnen und Experten.

88 Ein „Penetrationstest“ ist ein simulierter gezielter Angriff auf mögliche Schwachstellen, um zu bewerten, wie stark diese ausgenutzt werden können.

So wurden 2025 die Betreiber kritischer Infrastrukturen unter anderem über den aktuellen Stand der Verschlüsselung mittels Quantentechnologie, über Forschungsergebnisse im Bereich GNSS-Störungen⁸⁹ sowie über malevolente⁹⁰ Kreativität und deren Auswirkungen auf die Sicherheit von Unternehmen wie auch der Gesellschaft informiert.

Besonderes Augenmerk lag daher auf der Vorstellung neuester Forschungsergebnisse und Zukunftsthemen, die maßgeblich zur Sicherheit kritischer Infrastrukturen beitragen können. Die Beiträge reichten von innovativen Methoden im Bereich der Künstlichen Intelligenz über verbesserte Verfahren zur Risikobewertung bis hin zu fortschrittlicher Datenanalyse und Modellierung. Diese Technologien eröffnen die Möglichkeit, Bedrohungslagen noch präziser einzuschätzen und vorbeugende Maßnahmen effektiver zu gestalten. Die Verbindung von technologischem Fortschritt und praktischer Anwendung rückt damit immer stärker in den Mittelpunkt moderner Sicherheitsstrategien.

Evaluierung von Einsatzabläufen

Im Laufe des Jahres 2025 kam es bei den Landesleitzentralen (LLZ) im Bundesgebiet zu einer Evaluierung der Einsatzablaufsteuerung bei Objekten der kritischen Infrastruktur. Wesentliche Punkte der Einsatzvergaben, wie z. B. Verständigung der Sicherheitsverantwortlichen, Gefahrenhinweise, Sammelpunkte, Anzahl der zufahrenden Streifen usw., wurden thematisiert und evaluiert. Ziel ist es, diese relevanten Informationen in verbesserte Arbeitsabläufe zu integrieren und zu standardisieren, um künftige Einsätze bei Objekten der kritischen Infrastruktur effizient und sicher abarbeiten zu können.

Die Versorgungssituation im Teilssektor Gas

Aufgrund der veränderten österreichischen Versorgungssituation im Teilssektor Gas wurden Objekte der kritischen Infrastruktur von strategischer Bedeutung neu erfasst und mit Hilfe der betroffenen Unternehmen präzise bewertet. Zielführende sicherheitspolizeiliche Vorbereitungsmaßnahmen für eine mögliche polizeiliche Einsatzplanung können somit ab sofort effizienter zur Verfügung gestellt werden.

Drohnenaufnahmen zur verbesserten Objektdarstellung

Das im Jahr 2024 gestartete Projekt der 3D-Kartografie von Objekten der kritischen Infrastruktur durch Drohnenaufnahmen wurde auch im Berichtsjahr weitergeführt. Arbeitsprozesse von der Aufnahme der Objekte bis hin zur Einspielung in die jeweiligen Systeme wurden definiert und mit den betroffenen internen Organisationen abgestimmt. Ein Erfahrungsaustausch mit städtischen Magistraten und Einrichtungen, die bereits mit 3D-Modellen arbeiten, wurde durchgeführt und die daraus gewonnenen Erkenntnisse verwertet. Das Projekt wird im Jahr 2026 weiter forciert.

89 Globales-Navigationssatellitensystem

90 Bedeutung: bösartig, heimtückisch, gehässig

Erste Ergebnisse zu praxisorientierten Methoden im Zusammenhang mit dem RKE-Gesetz

Im Rahmen der RKE-Richtlinie wurde bereits im Jahr 2024 zusammen mit der Fachhochschule Campus Wien das KIRAS-Projekt „PUKE“⁹¹ gestartet. Ziel ist es, wissenschaftliche und praxisnahe Methoden für Unternehmen, die künftig unter das RKE-Gesetz fallen, zu entwickeln. Dazu wurde von Beginn an auf eine breite Einbindung relevanter Akteurinnen und Akteure gesetzt. Neben einer systematischen Auswertung der wissenschaftlichen Grundlagen führte das Projektteam der Fachhochschule zahlreiche Interviews mit Expertinnen und Experten sowie Vertreterinnen und Vertretern kritischer Infrastrukturunternehmen durch. Diese Gespräche lieferten wichtige Erkenntnisse über aktuelle Herausforderungen, bestehende Schutzmaßnahmen und mögliche Verbesserungen.

Ein wichtiger Meilenstein des bisherigen Projektverlaufs war die Präsentation der ersten Zwischenergebnisse am 12. Juni 2025. Im Rahmen dieser Veranstaltung fand ein Workshop statt, an dem zahlreiche Vertreterinnen und Vertreter aus Verwaltung, Forschung und Wirtschaft teilnahmen. Durch diese Kombination aus wissenschaftlicher Analyse, praktischer Erhebung und offenem Austausch soll sichergestellt werden, dass die Entwicklung der neuen Methoden praxisorientiert ist und diese auch den Erfordernissen des RKE-Gesetzes gerecht werden kann.

Krisenübungen

Die Unternehmen der kritischen Infrastruktur können bei ihren regelmäßigen Krisenübungen als zentraler Bestandteil des Krisenmanagements durch die DSN unterstützt werden. Die im Rahmen des Stabsverfahrens durchgeführten Übungsszenarien betreffen mehrere Sektoren und finden in einigen Fällen auch sektorenübergreifend statt.

Krisenübungen in den Unternehmen sind strukturierte Trainingsmaßnahmen, mit denen Organisationen ihre Vorbereitungen auf Notfälle, Störungen oder ernsthafte Krisenlagen testen und verbessern können. Ziel ist es, im Ernstfall handlungsfähig zu bleiben, Schäden zu minimieren und die Resilienz der Unternehmen zu stärken. Zudem ergibt sich ein Mehrwert durch das Erproben von Kommunikationswegen und Schnittstellen zwischen Behörden, Einsatzkräften und Organisationen. Zu den geübten möglichen Szenarien zählen beispielsweise Cyberangriffe auf Firmennetzwerke, Lieferkettenausfälle, Großbrände in Anlagenteilen oder allgemeine Bedrohungslagen.

Sicherheitsmonitor

Mit dem sogenannten Sicherheitsmonitor wird den Sicherheitsdienststellen eine täglich aktualisierte, kriminalpolizeiliche Information zur Verfügung gestellt, mit dessen Hilfe aktuelle Kriminalitätsschwerpunkte schneller und leichter erkannt werden können. Hierbei bewertet die DSN täglich die aktuellen Sicherheitsvorfälle im Nahbereich von Unter-

91 „PUKE“ steht für „Projekt zur Unterstützung kritischer Einrichtungen“.

nehmen der kritischen Infrastruktur und nimmt bei Bedarf mit betroffenen Unternehmen Kontakt auf. So können einerseits Entwicklungen präventiv bearbeitet und Unternehmen über ihnen noch unbekannt Vorfälle rasch informiert werden.

Broschüren

Die DSN stellt den Unternehmen der kritischen Infrastruktur verschiedene Broschüren, Folder und Checklisten zur Verfügung. Das Spektrum umfasst dabei allgemeine Sicherheitsempfehlungen genauso wie etwa Empfehlungen zum Verhalten bei Bombendrohungen oder zur Einordnung der Ergebnisse etwaiger Sicherheitsüberprüfungen von Personen im Personal-Aufnahmeprozess. Diese Broschüren und Folder werden in Zusammenarbeit mit unterschiedlichen Sicherheitsbehörden wie auch mit unterschiedlichen Unternehmen und Stakeholdern erarbeitet. 2025 wurde der Leitfaden „Sicherheits- und Zuverlässigkeitsüberprüfungen“ erarbeitet und erstmals zur Verfügung gestellt.

Workshop „Schützenswertes Krankenhaus“ in Vorarlberg 2025

Die Workshops „Schützenswertes Krankenhaus“ wurden auch im Jahr 2025 fortgesetzt. Anfang des Jahres fanden mit Unterstützung unterschiedlicher Organisationseinheiten des BMI Vorträge zu verschiedenen Sicherheitsthemen in Krankenhäusern statt. Die Spitäler des Bundeslandes Vorarlberg wurden in den Bereichen Bombendrohungen, Cybersicherheit, physischer Objektschutz und Social Engineering sowie zu CBRN-spezifischen Thematiken in ihren Einrichtungen sensibilisiert und geschult. Mit den Schwerpunkt-Krankenhäusern wurde zusätzlich eine Sicherheitsbegehung zur Schwachstellenanalyse durchgeführt, um anschließend eine Evaluierung und Verbesserung der sensiblen Bereiche zusammen mit den Verantwortungsträgerinnen und Verantwortungsträgern der Spitäler sicher zu stellen. Eine verbesserte Resilienz konnte vor allem auch dadurch erreicht werden, dass die örtlichen Behörden und Einsatzkräfte in den Workshop eingebunden waren.

3.4 Wirtschaftsschutz

Unter „**Wirtschaftsschutz**“ sind die präventiven Bemühungen zum Schutz der heimischen Wirtschaft vor Spionageangriffen zu verstehen. Dazu sensibilisiert die DSN österreichische Betriebe zu den Gefahren, die von Wirtschafts- und Industriespionage ausgehen.



„**Staatliche Wirtschaftsspionage**“ bezeichnet das gezielte und systematische Abschöpfen von wirtschaftlich oder technologisch bedeutsamen Informationen eines Unternehmens oder einer Forschungseinrichtung durch staatliche Nachrichtendienste oder von diesen beauftragten Akteuren.

Die österreichische Wirtschaft war 2025 in hohem Maß von komplexen internationalen Verflechtungen, technologischen Innovationszyklen und den geopolitischen Spannungen geprägt. Gleichzeitig stieg der Druck durch fremdstaatlich gesteuerte Wirtschaftsspionage, hybride Einflussoperationen und kriminelle Cyberangriffe. Unternehmen sämtlicher Branchen stehen damit zunehmend vor der Herausforderung, nicht nur wirtschaftlich erfolgreich zu agieren, sondern auch ihre Kernkompetenzen, Produktionsprozesse und Forschungsdaten proaktiv zu schützen. Wirtschaftsschutz hat sich daher zu einem zentralen Thema der nationalen Sicherheitsvorsorge entwickelt. In Übereinstimmung mit internationalen Erfahrungswerten zeigt sich, dass insbesondere Branchen mit hohem Innovationsgrad und langfristigen Investitionszyklen verstärkt Ziel wirtschaftsbezogener Ausspähungen sind. Für Österreich lässt sich diese Gefährdungslage in weiten Teilen bestätigen, insbesondere in den Bereichen Maschinen- und Anlagenbau, Halbleiterfertigung, Energietechnologie, Gesundheitstechnologie, Life Sciences⁹², Künstliche Intelligenz und Luftfahrt sowie im universitären und außeruniversitären Forschungssektor.

Angriffe auf Unternehmen erfolgen zunehmend digital und hybrid. Spionage tritt nicht mehr allein klassisch in Gestalt persönlicher Informationsabschöpfung auf, sondern wird ergänzt durch Cyberangriffe, Social Engineering-Methoden, gezielte Desinformationskampagnen und Versuche, Mitarbeiterinnen und Mitarbeiter durch subtile Kontaktanbahnungen einzubinden. Die professionalisierte Ausforschung von Schwachstellen in Lieferketten und Kooperationen gewinnt dabei an Bedeutung.

„**Social Engineering**“ bezeichnet im nachrichtendienstlichen Umfeld die gezielte Beeinflussung von Personen, um an vertrauliche Informationen, Zugänge oder Einschätzungen zu gelangen, ohne technische Mittel einsetzen zu müssen. Fremdstaatliche Akteure nutzen dabei psychologische Methoden und zwischenmenschliche Interaktionen, um Vertrauen aufzubauen und Informationsquellen zu erschließen. Dies kann über scheinbar harmlose Gespräche, berufliche Kontakte, gefälschte Identitäten, soziale Netzwerke oder offizielle Kooperationsanfragen erfolgen. Charakteristisch ist, dass die angegriffene Person in der Regel nicht erkennt, manipuliert zu werden. Ziel ist es, interne Kenntnisse, strategische Entscheidungsgrundlagen oder technologische Details zu gewinnen.



92 „Life Sciences“ bzw. „Biowissenschaften“ ist ein Sammelbegriff für Wissenschaften, die sich mit lebenden Organismen mit dem Ziel beschäftigen, von diesen den Aufbau, die Funktionen sowie Wechselwirkungen zu lernen, um dann die erlangten Erkenntnisse auf andere Bereiche, z. B. Medizin und Biotechnologie, anzuwenden.

3.4.1 Innentäterschaft im Kontext des Wirtschaftsschutzes

Mitarbeiterinnen und Mitarbeiter eines Unternehmens, insbesondere jene in wissensintensiven Funktionen, bilden das zentrale „Stammkapital“ jeder Organisation. Unzufriedenheit im Arbeitsumfeld, hohe Personalfluktuation oder die sogenannte „innere Kündigung“ können dabei zu unterschätzten Risikofaktoren für Unternehmen werden. In modernen Betrieben ist bekannt, dass auf dem neuesten Stand befindliche IT-Sicherheitsmaßnahmen, ein angemessenes Gebäudeschutzkonzept sowie ein klar geregeltes Zugriffsmanagement auf Unternehmensdaten unverzichtbar sind. Dennoch bleibt häufig unberücksichtigt, dass potenzielle Sicherheitsgefährdungen nicht nur von außen, sondern gerade auch aus dem Inneren des Unternehmens kommen können. Die Awareness, dass eine Insiderin oder ein Insider aufgrund ihres bzw. seines Zugangs und Wissens im schlimmsten Fall erheblichen Schaden verursachen kann, ist noch nicht überall ausreichend vorhanden.

Im Bereich Unternehmenssicherheit gibt es keine „One size fits all“-Lösung. Mitarbeiterinnen- und Mitarbeiterpflege sowie ehrliches Leadership sind die Hauptkriterien beim Schutz vor Innentäterinnen und Innentätern. Wichtig in diesem Konzept ist die Ergänzung der bestehenden Corporate Identity um eine neue Dimension: die Corporate Security. Diese dient dazu, dass Sicherheit bei den Mitarbeitenden nicht nur als Pflicht wahrgenommen wird, sondern Teil des Selbstbilds der Organisation wird. Sicherheitswerte sollten in die Leitlinien, Mission und Vision aufgenommen werden. „Wir schützen, was uns anvertraut wird“ könnte ein Beispiel sein. Somit wird Sicherheit unternehmensintern als Vertrauen und Verantwortung kommuniziert und von den Betroffenen nicht als Kontrolle wahrgenommen. Die intrinsische Motivation der Mitarbeiterinnen und Mitarbeiter, sich am Thema (pro-)aktiv zu beteiligen steigt exponentiell. Wiederkehrende klare Botschaften sind dabei von besonderer Bedeutung: „Sicherheit ist Teil unserer Professionalität“ könnte ein passender Claim⁹³ sein. Ein weiterer Aspekt in diesem Zusammenhang ist, dass die kommunizierten bzw. in Leitlinien, Mission und Vision festgeschriebenen Werte nicht nur dokumentiert, sondern auch aktiv gelebt und konsequent umgesetzt werden. Dabei kommt den Führungskräften eine besondere Vorbildfunktion zu, indem sie diese Werte glaubwürdig vorleben. Den schriftlichen Festlegungen müssen konkrete Handlungen folgen, um die Mitarbeitenden mitzunehmen und einzubinden. Nur auf diese Weise kann sichergestellt werden, dass Corporate Security als integraler Bestandteil der aktiv gelebten Unternehmenskultur verankert wird.

3.4.2 Mobiles Präventionsteam als Instrument zur Stärkung der betrieblichen Resilienz

Um der zunehmenden Komplexität der Bedrohungslagen und dem damit einhergehenden steigenden Sensibilisierungs- und Informationsbedarf proaktiv zu begegnen, setzte die DSN im Jahr 2025 verstärkt auf ein mobiles Präventionsteam. Ziel war es, Unternehmen und Forschungsinstitutionen in Form von Schulungen direkt vor Ort mit flexiblen, lage-

93 Ein „Claim“ ist ein kurzer, einprägsamer Satz, der ausdrückt, wofür eine Marke steht.

angepassten Präventionsformaten zu beraten. So wurde ein Beitrag dazu geleistet, dass Managerinnen und Manager sowie angehende Führungskräfte über zeitgemäße Sicherheits-Awareness im Zusammenhang mit staatlicher Spionage und Sabotage verfügen. Im Zuge dieser Schulungen wurde auf die Beweggründe und Vorgehensweisen staatlicher Akteure, die Spionage und/oder Sabotage betreiben, aufmerksam gemacht.

Das mobile Präventionsteam der DSN schulte im Berichtsjahr vor allem Führungskräfte von Kammern sowie Industrieunternehmen in Form von Sensibilisierungsvorträgen. Ein Schwerpunkt lag auf der Bewusstseinsbildung in Hinblick auf die Gefährdungslage des Managements selbst, da Führungskräfte oft unbewusst Angriffspunkte darstellen. Alltags- und praxisnahe Trainingsmodule zum Erkennen von Social Engineering, zur sicheren Kommunikation sowie zur Sensibilisierung im Umgang mit beruflich generierten Kontakten oder digitalen Plattformen bildeten die zentralen Bestandteile dieser präventiven Schulungsinhalte. Der Input wurde dabei so ausgewählt, dass das Auditorium im Anschluss in der Lage war, das erlangte Wissen „top-down“ innerhalb der eigenen Organisationen weiterzuvermitteln.

Weitere wesentliche Inhalte der Schulungen umfassten praxisnahe Tipps zur Erhöhung der Sicherheit bei Dienstreisen sowie zur Verbesserung der sicherheitsrelevanten Kriterien im Zuge der Auswahl-, Ausbildungs- und Fortbildungsmöglichkeiten. Veranschaulicht wurde dies anhand von Case Studies und tatsächlichen Fällen, die untermauerten, welche Phänomene 2025 von besonderer Sicherheitsrelevanz waren. Das mobile Präventionsteam ging dabei individuell, persönlich und praxisorientiert auf den Bedarf der jeweiligen Organisation ein. Zudem agierte die DSN in diesem Präventionsbereich multidisziplinär und vernetzt, indem sie bestehende Kooperationen mit der Wirtschaftskammer Österreich (WKO) sowie mit der Hochschule Campus Wien weiter stärkte. In der Folge konnte der Kontakt zur Wirtschaft und somit die Reichweite der Sensibilisierungen im Jahr 2025 weiter ausgebaut werden.

Darüber hinaus richtete sich das mobile Präventionsteam der DSN im Laufe des Jahres 2025 gezielt an Universitäten und Fachhochschulen. Österreichische Hochschulen sind Trägerinnen wesentlicher Forschungstätigkeiten und somit Hochrisiko-Ziele von fremden nachrichtendienstlichen Akteuren zur Informationsgewinnung. Besonders in offenen, international orientierten Arbeitsumgebungen besteht das Risiko, dass Schutzmechanismen als hinderlich oder schwer vereinbar mit wissenschaftlicher Kollaboration wahrgenommen werden. Das Präventionsteam vermittelte daher praxisorientierte Wege, wie exzellente Forschung und verantwortungsvoller Umgang mit sicherheitskritischem Wissen gleichermaßen gewährleistet werden können. Dazu zählten Schulungen zu sicheren Kooperationsmodellen, zur sorgfältigen Prüfung von Stipendien und Gastaufenthalten sowie zur Sensibilisierung im Austausch von Forschungsdaten mit internationalen Partnern.

3.4.3 Mehrwert für Unternehmen und Hochschulen

Der Nutzen dieser mobilen Präventionsarbeit ist vielfältig. Unternehmen gewinnen eine realistische Einschätzung ihres Gefährdungsprofils, das nicht allein auf technischen Aspekten basiert, sondern organisatorische und menschliche Faktoren gleichermaßen umfasst. Die Maßnahmen helfen, konkrete Risiken zu reduzieren und erhöhen zugleich die langfristige Widerstandsfähigkeit gegenüber Angriffen, Lieferkettenstörungen und unerwarteten Informationsabflüssen. Besonders in kleinen und mittleren Unternehmen (KMU), in denen oftmals nur wenige Schlüsselpersonen kritisches Wissen tragen, wirkt die Beratung dahingehend, Wissen systematisch abzusichern, ohne den betrieblichen Alltag unnötig zu belasten.

Hochschulen profitieren von bewusstseinsbildenden Informationen seitens des Verfassungsschutzes, die es ihnen ermöglichen, ihren wissenschaftlichen Auftrag mit Sicherheitsinteressen in Einklang zu bringen. Die Einführung angemessener Kontroll- und Dokumentationsprozesse schafft Transparenz und schützt Forschungsprojekte, ohne die internationale Zusammenarbeit einzuschränken. Bei Studentinnen und Studenten sowie Forscherinnen und Forschern entsteht ein stärkeres Bewusstsein dafür, dass Wissenschaft nicht im Widerspruch zu akademischer Freiheit steht, sondern diese langfristig erst gewährleistet.

3.4.4 Unternehmen mit erhöhtem Risikoprofil: Start-ups, KMU und innovationsgetriebene Betriebe im Fokus

Nicht alle Unternehmen sind gleichermaßen von Wirtschaftsspionage und unerwünschtem Technologietransfer betroffen. Ausschlaggebend ist weniger die Unternehmensgröße als vielmehr die Innovationskraft, die Tiefe des vorhandenen Wissens sowie die strategische Bedeutung bestimmter Technologien innerhalb globaler Wettbewerbsfelder. Gerade kleinere Unternehmen erleichtern den Angriff eines potenziellen Akteurs, da sie häufig aufgrund der begrenzten personellen und finanziellen Ressourcen nur über rudimentär ausgeprägte Sicherheitsstrukturen verfügen. In Österreich, wo wirtschaftlicher Erfolg traditionell stark auf spezialisierten Nischen, technischer Präzision und forschungsintensiven Branchen beruht, zeigt sich ein besonders sensibles Risikoprofil.

Start-ups gelten als besonders attraktiv für Informationsabschöpfung. Sie entwickeln oftmals neuartige Forschungsideen, Softwarearchitekturen oder Produktionsmethoden und sind damit wichtige Innovationsträger. Gleichzeitig stehen sie unter hohem wirtschaftlichen Druck: Finanzierung erfolgt in Zyklen, die Mitarbeiterinnen- und Mitarbeiterzahl wächst schnell, Prozesse sind flexibel, aber oft nicht sicherheitsorientiert strukturiert. Sensibles Know-how liegt häufig bei wenigen Schlüsselpersonen und auf Entwicklungsplattformen, die eher auf Effizienz als auf Sicherheitskontrolle ausgelegt sind. Hinzu kommt, dass Start-ups in hohem Maße von internationalen Kooperationen, externem Kapital und projektbasierter Zusammenarbeit abhängig sind. Diese Faktoren eröffnen potenzielle Angriffsvektoren, da sowohl der Personenkreis mit Zugang zu ver-

traulichen Informationen als auch der Einfluss externer Akteure schwerer zu kontrollieren sind. Nachrichtendienste und strategisch agierende Industriekonzerne beobachten daher gezielt Hochschulausgründungen, Förderprogramme und Patentanmeldungen, um frühzeitig Einblicke in zukünftige Schlüsseltechnologien zu gewinnen.

Wirtschaftsschutz in diesen Bereichen ist daher kein Mehraufwand, sondern eine Investition in die Zukunftsfähigkeit und Souveränität der Unternehmen, was die Beratungen der DSN vor Ort bestätigten.

3.4.5 Kleine und mittlere Unternehmen: Hidden Champions im Schatten des globalen Wettbewerbs

Kleine und mittlere Unternehmen (KMU) bilden besonders sensible Ziele. Viele dieser Betriebe nehmen in ihren Marktsegmenten international führende Positionen ein, ohne dass sie in der Öffentlichkeit große Sichtbarkeit besitzen. Gerade diese Hidden Champions⁹⁴ verfügen über spezialisiertes, schwer reproduzierbares Prozess- und Fertigungswissen. Solches Erfahrungswissen ist oftmals nicht umfassend dokumentiert, sondern innerhalb langjähriger Organisationsstrukturen gewachsen. Zugleich sind Lieferketten und Absatzmärkte häufig global vernetzt, was Abhängigkeiten und Sicherheitsrisiken erhöht. Schon ein vergleichsweise kleiner Informationsabfluss kann in diesen Fällen den über Jahrzehnte aufgebauten technologischen Vorsprung vernichten und so erhebliche ökonomische Schäden verursachen.

Wirtschaftsschutz ist daher kein punktueller Eingriff, sondern ein laufender Prozess, der nur durch enge Zusammenarbeit zwischen Staat, Wirtschaft und Wissenschaft erfolgreich sein kann. Der Verfassungsschutz leistet hierzu einen entscheidenden Beitrag: Er fördert Expertise in den Unternehmen, stärkt Bewusstsein, erhöht Handlungskompetenz und unterstützt eine Kultur der Sicherheitsverantwortung. Auf diese Weise wird ein wesentlicher Beitrag zum Schutz der Unternehmen, der Innovationskraft und der wirtschaftlichen Stabilität Österreichs geleistet.

3.4.6 Wirtschaftsschutz 2025: Risikoabschätzung im Kontext chinesischer Joint Ventures

China war auch im Jahr 2025 für die österreichische Wirtschaft ein bedeutender Markt und wichtiger Handelspartner. Zahlreiche Unternehmen profitierten von Absatzmöglichkeiten, Zuliefernetzwerken und technologischen Kooperationsprojekten. Gleichzeitig hat sich die sicherheitspolitische Bewertung wirtschaftlicher Zusammenarbeit in den vergangenen Jahren verändert. Im Bereich strategischer Industrien, Schlüsseltechnologien und Forschungsk Kooperationen lassen sich zunehmend Risiken erkennen, die sowohl wirtschaftliche als auch sicherheitspolitische Relevanz besitzen.

94 „Hidden Champions“ sind meist kleine oder mittelständische Unternehmen, die in ihrer Nische Marktführer, aber in der breiten Öffentlichkeit kaum bekannt sind.

Besonders im Fokus standen Joint Ventures, Beteiligungsmodelle und Forschungs-kooperationen mit Unternehmen, die direkt oder indirekt chinesischen staatlichen Einflusststrukturen unterliegen. Das chinesische Recht verpflichtet Unternehmen zur Zusammenarbeit mit staatlichen Stellen, wenn dies im Sinne der Interessen Chinas ist. In Kombination mit gezielten Industrie- und Technologieförderstrategien eröffnet dies die Möglichkeit, über Kooperationen Know-how, Fertigungsverfahren oder geistiges Eigentum langfristig zu übernehmen oder zu kontrollieren.

Für österreichische Unternehmen entsteht dadurch ein Risiko, das häufig erst zeitverzögert sichtbar wird. Technologische Kernkompetenzen, die zunächst gemeinsam entwickelt oder eingebracht werden, können nach einer Kooperationsphase von chinesischer Seite unabhängig weitergeführt oder in Konkurrenzmärkte übergeleitet werden. Besonders betroffen sind Bereiche mit Dual-Use-Potenzial, wie Halbleiterfertigung, Automatisierungstechnik, Robotik, Luft- und Raumfahrt, Medizintechnik oder KI-basierte Anwendungen. Hier besteht die Gefahr, dass Innovationsvorsprünge verloren gehen und strategische Abhängigkeiten entstehen.

Wirtschaftsschutz bedeutet in diesem Zusammenhang nicht, Kooperationen zu vermeiden, sondern sie souverän und unter klaren Rahmenbedingungen zu gestalten. Dazu gehören transparente Vertragsmodelle, klare Regelungen zum Umgang mit geistigem Eigentum, abgestufte Zugriffsrechte auf Entwicklungsdaten, ein strukturiertes Sicherheits- und Compliance-Management sowie laufende Risikoanalysen innerhalb des Unternehmens. Ebenso wichtig ist eine sorgfältige Partnerbewertung, die nicht nur wirtschaftliche, sondern auch sicherheitspolitische Einflussfaktoren berücksichtigt.

Die DSN unterstützte im Jahr 2025 Unternehmen dabei, solche Risiken frühzeitig zu erkennen und angemessene Maßnahmen zu setzen. Durch Sensibilisierung, vertrauliche Beratung und praxistaugliche Schutzkonzepte, die den Unternehmensführungen vom mobilen Präventionsteam der DSN erläutert werden, können österreichische Unternehmen weiterhin von internationalen Märkten profitieren, ohne ihre strategische Autonomie und Innovationskraft zu gefährden.

Ein verantwortungsvoller Umgang mit Joint Ventures ist folglich ein wichtiger Baustein zur Sicherung eines resilienten, technologisch souveränen und wettbewerbsfähigen Wirtschaftsstandortes Österreich.

3.4.7 Radikalisierung im öffentlichen Diskurs im Kontext des Wirtschaftsschutzes

Im Jahr 2025 hat die wachsende politische Sichtbarkeit einzelner einflussreicher Unternehmer im globalen Technologiesektor deutliche Auswirkungen auf gesellschaftliche und politische Diskurse gezeigt. Wenn Personen mit großer Medienreichweite und wirtschaftlicher Macht verstärkt Einfluss auf die Politik nehmen, kann dies sowohl unterstützende

als auch polarisierende Reaktionen hervorrufen. Besonders sichtbar wird dies, wenn ihre öffentlichen Aussagen in sozialen Netzwerken oder in Interviews von politischen Bewegungen interpretiert oder instrumentalisiert werden. In manchen Fällen entsteht daraus ein Klima, in dem sich extremistische Gruppierungen bestärkt fühlen, ihre eigenen Positionen radikaler und offensiver zu vertreten.

Dies kann sich unter anderem in gezielten Aktionen gegen Unternehmen äußern, die mit der betreffenden Person eng verbunden sind. Dazu zählen Vandalismusakte an Produktionsstätten, Fahrzeugen oder Ausstellungsräumen sowie öffentliche Aufrufe zu solchen Handlungen. Auch in Österreich gab es im Berichtsjahr vereinzelt Fälle, in denen Gruppierungen oder Einzelpersonen öffentlich zu Sabotageakten aufriefen, um ihrer Ablehnung Ausdruck zu verleihen. Die Motive reichten dabei von ideologischer Ablehnung wirtschaftlicher Machtkonzentrationen über Kritik an technologischen Zukunftsvisionen bis hin zu genereller Systemfeindlichkeit.

Solche Vorfälle zeigen, wie eng politische Kommunikation, mediale Aufmerksamkeit und gesellschaftliche Reaktionen miteinander verwoben sind. Die politische Haltung einflussreicher Wirtschaftsakteure kann weitreichende gesellschaftliche Resonanzen erzeugen, die letztlich über Diskussionen hinausgehen und konkrete Handlungen nach sich ziehen. Daher ist es für Politik, Zivilgesellschaft und Sicherheitsbehörden wichtig, Entwicklungen genau zu beobachten, um Eskalationen vorzubeugen und einen konstruktiven gesellschaftlichen Dialog zu ermöglichen.

Für den Wirtschaftsschutz hat das im Jahr 2025 bedeutet, nicht nur klassische Sicherheitsrisiken wie Spionage, Sabotage oder Cyberangriffe zu berücksichtigen, sondern auch die sozialen und politischen Dynamiken im öffentlichen Raum zu beobachten. Der Wirtschaftsschutz wird damit zu einer gesellschaftlichen Querschnittsaufgabe, in der Sicherheitsinteressen, politische Entwicklungen und soziale Verantwortung zusammenwirken müssen.

Der Verfassungsschutz hat auch in diesem Kontext wichtige Aufklärungs- und Sensibilisierungsarbeit geleistet. Den Betroffenen wurde adäquates Wissen vermittelt, um potenzielle Gefährdungen frühzeitig erkennen und Risiken einschätzen zu können, um in der Folge geeignete (Gegen-)Maßnahmen (auch im eigenen Verhalten) zu setzen.

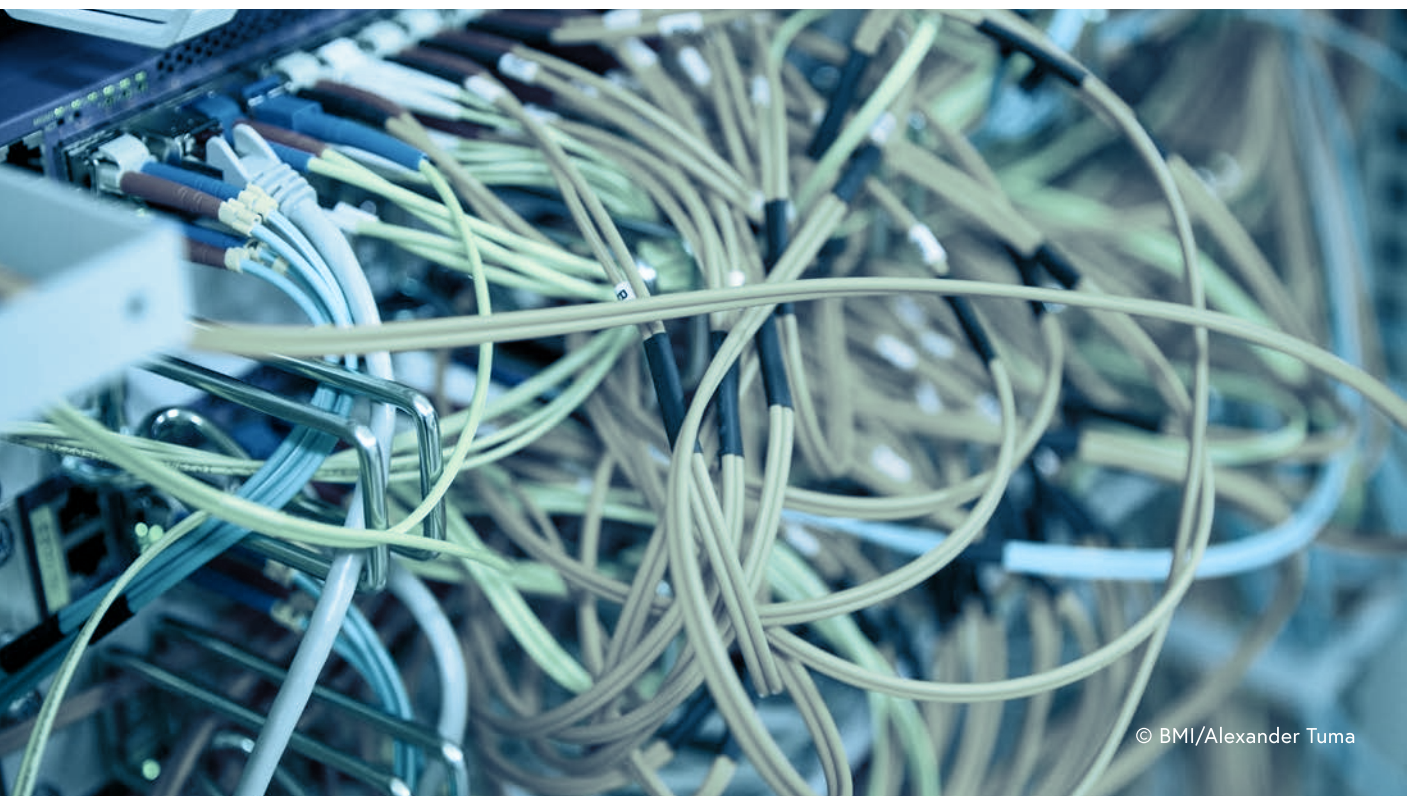
Wenn Sie für Ihre Organisation eine unverbindliche, anonyme und kostenlose Beratung durch den Wirtschaftsschutz der DSN wünschen, wenden Sie sich bitte an wis@dsn.gv.at.



3.5 Cyber Security Center

Unternehmen, zivilgesellschaftliche Einrichtungen, Ministerien und internationale Organisationen in Österreich sind einer Vielzahl an Bedrohungen im Cyberraum ausgesetzt. Es kommt dabei nicht nur zu Angriffen durch finanziell motivierte Cyberkriminelle, sondern auch durch Akteure, die im Auftrag eines Staates Cyberspionageoperationen durchführen. Diese Akteure verfolgen Ziele wie Wirtschaftsspionage, Unterwanderung von Aktivistengruppen und Sabotage internationaler Verhandlungen. Um diese Ziele zu erreichen, versenden sie auf ihre Opfer zugeschnittene Phishing-E-Mails, nutzen unbekannt Schwachstellen in IT-Systemen aus und setzen maßgeschneiderte Schadsoftware ein.

Das Cyber Security Center (CSC) der DSN kooperiert mit heimischen Unternehmen, der Zivilgesellschaft und internationalen Organisationen in Österreich, indem es Cyber Threat Intelligence für die von staatlichen Akteuren ausgehenden Bedrohungsszenarien liefert. Dies trägt zu einer Erweiterung der Sicherheitsmaßnahmen und damit zu einer verstärkten Cybersicherheit innerhalb Österreichs bei. Die Einbindung in die österreichische Cybersicherheitslandschaft sorgt für einen verstärkten fachspezifischen Austausch und eine damit verbundene Wissensverbreitung. Das CSC verfügt zudem über einen ausgeprägten Wissensschatz hinsichtlich Cyberbedrohungen durch staatliche Akteure, um Beratungen bei österreichischen Unternehmen und internationalen Organisationen durchzuführen. Im Jahr 2025 wurden durch das Cyber Security Center mehrere Beratungen im behördlichen Umfeld getätigt. In diesem Rahmen lag der inhaltliche Schwerpunkt auf der Sensibilisierung und Aufklärung zum Thema digitale Spionagemassnahmen sowie den dabei zu bedenkenden Faktoren – etwa die Mitnahme von Geräten bei Dienstreisen in kritische Länder. Zudem leistete das Cyber Security Center bei nationalen IT-Sicherheitskonferenzen Vorträge zu Cyberspionagefällen und den aktuellen Bedrohungslagen und auf diesem Weg einen Beitrag zur Bewusstseinsbildung von IT-Sicherheitsexpertinnen und IT-Sicherheitsexperten.



3.6 Extremismusprävention und Deradikalisierung

3.6.1 Strategische Prävention

Die Strategische Prävention der DSN hat die Aufgabe, die notwendigen Handlungsfelder der Prävention zu definieren und auf nationaler wie internationaler Ebene zu koordinieren. Die Umsetzung erfolgt im Rahmen des Bundesweiten Netzwerkes Extremismusprävention und Deradikalisierung (BNED), des Center for Security Analysis and Intelligence Research (CSAIR) und im Rahmen internationaler Organisationen bzw. der Gremien der Europäischen Union.

Bundesweites Netzwerk Extremismusprävention und Deradikalisierung

Das Bundesweite Netzwerk Extremismusprävention und Deradikalisierung setzt sich aus Expertinnen und Experten verschiedener Ministerien, aus den Landesregierungen aller Bundesländer, dem Städte- und Gemeindebund sowie aus Akteurinnen und Akteuren der Zivilgesellschaft zusammen. Seit der Gründung im Jahr 2017 trifft sich das BNED regelmäßig, um Fragen der Extremismusprävention und entsprechende Maßnahmen zu erörtern. Auch im Berichtsjahr 2025 fanden regelmäßige Koordinierungstreffen statt. Ergänzend zu den Plenumsveranstaltungen gab es Arbeitsgruppen (AG) zu den Themen „Active Clubs und Kampfsport“ und „Digitale Resilienz“.

- AG „Active Clubs und Kampfsport“
Die BNED-Arbeitsgruppe „Active Clubs und Kampfsport“ wurde Ende 2024 eingerichtet und widmete sich zu Beginn vor allem der Frage, ob und wie sich das Phänomen der Active Clubs von anderen Kampfsportbereichen analytisch trennen lässt, da es in der Kampfsportszene auch extremistische Gruppen gibt, die nicht Teil des Active Clubs-Netzwerkes sind. In der Folge wurde beschlossen, diese beiden Bereiche – die Active Clubs einerseits und die Kampfsportszene andererseits – getrennt zu untersuchen und in einem ersten Schritt den Status Quo bezüglich Active Clubs in Österreich zu erheben. Die 2020 in den USA entwickelte Strategie der Active Clubs zielt darauf ab, eine geheime, rechtsextreme Miliz aufzubauen, die für den sogenannten „Tag X“ bereitsteht. Das Active Clubs-Netzwerk hat inzwischen in vielen Ländern Europas Fuß gefasst, weshalb ein Übergreifen auf Österreich mittel- bis langfristig nicht ausgeschlossen werden kann.
- AG „Digitale Resilienz“
Extremistische und hassbezogene Inhalte verbreiten sich online in rasantem Tempo und erreichen eine große Reichweite. In vielen Bereichen des digitalen Raums, insbesondere in sozialen Netzwerken, kursieren radikale Ideologien, Desinformation (d. h. bewusst gestreute Falschinformationen), Verschwörungsnarrative, Hassreden und Aufrufe zu Gewalt. In der vernetzten Welt ist es daher unumgänglich, digitale Umgebungen in die Analyse von Radikalisierungsprozessen und der Verbreitung extremistischer Gedankengänge einzubeziehen. Um der Onlineradikalisierung pro-

aktiv entgegen zu treten, sollen in dieser AG Maßnahmen erarbeitet werden, die unter anderem die Medienkompetenz der Bevölkerung, vor allem die der Kinder und Jugendlichen, aber auch jene der Erwachsenen stärken.

Präventionsgipfel

Um das Thema der Arbeitsgruppe „Digitale Resilienz“ aufzugreifen und erste Ergebnisse einem breiteren Fachpublikum zugänglich zu machen, stand der 6. Präventionsgipfel am 13. November 2025 unter dem Generalthema „Digitale Resilienz“. Nach einer Keynote zum Thema „Desinformation im Wandel: Wie KI Öffentlichkeit verändert“ wurden in zwei Panels die Fragestellungen „Der virtuelle Raum: Lebenswelt unserer Jugend – zwischen Empowerment und (negativer) Beeinflussung?“ und „Wieviel Regulierung brauchen Soziale Medien und wie soll eine solche Regulierung ausgestaltet sein?“ unter Einbeziehung des Publikums diskutiert.

Nationaler Aktionsplan Rechtsextremismus (NAP REX)

Wie im aktuellen Regierungsprogramm⁹⁵ angekündigt, wurde das BNED unter der Koordination der DSN mit der Umsetzung eines Nationalen Aktionsplans Rechtsextremismus nach internationalem Vorbild beauftragt. Das Gremium wird unter Einbeziehung BNED-externer Institutionen in einem partizipativen Prozess den NAP REX erstellen.

Center for Security Analysis and Intelligence Research

Extremismus, Radikalisierung und Terrorismus sind fluide, sich mit den gesamtgesellschaftlichen Rahmenbedingungen bzw. unter dem Einfluss (geo-)politischer, ökonomischer und sozialer Entwicklungen verändernde soziale Phänomene. Als Folge davon stellen sich den Sicherheitsbehörden und damit auch dem Nachrichtendienst bei der (strategischen) Prävention von Extremismus, Radikalisierung und Terrorismus immer wieder neue Herausforderungen, deren frühzeitiges Erkennen wesentlich für den Erfolg des Verfassungsschutzes ist. Ein zentraler Punkt bei der Reform des Verfassungsschutzes war daher die Stärkung und Intensivierung des Austauschs mit der Wissenschaft. Zur Umsetzung dieser Zielsetzung wurde in der DSN das Center for Security Analysis and Intelligence Research eingerichtet, das sich insbesondere mit neuen Entwicklungen in allen Phänomenbereichen des Verfassungsschutzes beschäftigt.

Symposium zum Thema „Current and Future Drivers of Violent Extremism“ (27. und 28. Jänner 2025, Wien)

Am 27. und 28. Jänner 2025 fand das diesjährige CSAIR-Symposium statt. Das Generalthema lautete „Current and Future Drivers of Violent Extremism“ und versammelte

⁹⁵ Das im Jahr 2025 beschlossene Regierungsprogramm umfasst u. a. die Erstellung und Umsetzung eines Nationalen Aktionsplans Rechtsextremismus. Dies geschieht im Jahr 2026, unter der Koordination der DSN.

namhafte internationale Expertinnen und Experten aus den USA, Australien, Kanada, Nigeria, Großbritannien und Deutschland.

Den Auftakt machte Elizabeth Neumann, ausgewiesene Expertin im Bereich „Gewalttätiger Extremismus“ bzw. „Extremismusprävention“ und Chef-Strategin bei Moonshot, einer Organisation zur Bekämpfung von Bedrohungen im Online-Bereich. Davor war sie langjährige Mitarbeiterin im US-Department of Homeland Security und Beraterin des Director of National Intelligence (DNI) der USA. Unter dem Titel „Political Polarization, Targeted Violence, and Domestic Violent Extremism: Outlook for the USA in the Coming Years“ gab Elizabeth Neumann einen Einblick in die politische Polarisierung und die Gefahr von Extremismus in den USA. Beides stellt eine wachsende Bedrohung für das soziale und demokratische Gefüge der Vereinigten Staaten dar, vor allem aufgrund der damit verbundenen starken Zunahme gezielter Gewalt. Die in Teilen der US-amerikanischen Bevölkerung verbreitete Unzufriedenheit wird durch entsprechende Narrative und Desinformation angeheizt, wobei verschiedene soziale Medien für das schwindende Vertrauen in Institutionen und die Vereinnahmung des religiösen Glaubens der Evangelikalen für parteipolitische und extremistische Ziele eine große Rolle spielen. Als bisher oftmals vernachlässigte Faktoren im Rahmen einer Strategie zur Gewaltprävention nannte Elizabeth Neumann die Rolle der Regierungen und die herausragende Bedeutung der Zivilgesellschaft und der Glaubensorganisationen.

Anschließend präsentierte Fatima Akilu, geschäftsführende Direktorin der Neem Foundation und ehemals Sonderberaterin des Präsidenten von Nigeria, unter dem Titel „Current Developments in Sub-Saharan West Africa – and the Potential Threats for Europe“ eine Weltregion, die von einer Vielzahl an Problemen und Herausforderungen betroffen ist. Hierzu zählen unter anderem politische Instabilität, gewalttätiger Extremismus, Ressourcenkonflikte, ein rasantes Bevölkerungswachstum, der Klimawandel und die Zunahme der organisierten Kriminalität. Die Folgen sind humanitäre Krisen, massenhafte Vertreibungen und Fluchtbewegungen. In ihrem Vortrag benannte Fatima Akilu die aus diesen Entwicklungen möglicherweise resultierenden Implikationen für Europa. Erstens könnte der Druck auf die Grenzen und Einwanderungssysteme des Kontinents zunehmen, da die Menschen auf der Suche nach Sicherheit und besseren wirtschaftlichen (Überlebens-)Möglichkeiten vor der Instabilität ihrer Region fliehen. Zweitens könnte das Risiko extremistischer und organisierter krimineller Aktivitäten, vor allem des Menschenhandels – mit Westafrika als Basis und Europa als Drehscheibe – steigen. Außerdem könnte Europas Zugang zu geopolitischen und regionalen Wirtschaftsinteressen (Handelsrouten, Rohstoffe) gestört werden, wenn sich Konfliktsituationen verschärfen oder Lieferketten unterbrochen werden.

Brett Kubicek, strategischer und wissenschaftlicher Chefberater bei Public Safety Canada, thematisierte in seinem Vortrag die „Trajectories to Violent Extremism: Hybrid Grievances, Clusters of Risk and Vulnerability, and a Growing Focus on the Role of

Protective Factors“. Dazu stellte er vorab die Aktivitäten des 2017 installierten Canada Centre for Community Engagement and Prevention of Violence vor, dessen Themenfelder von der Primärprävention bis zur Deradikalisierung von Einzelpersonen reichen. In den letzten Jahren hat sich im Kontext eines zunehmend komplexen und polarisierten sozialen Umfelds der Schwerpunkt zunehmend auf die Stärkung der Online- und Offline-Prävention verlagert. Beispiele dafür sind laut Kubicek das gemeinsame Auftreten von ehemals getrennten Bewegungen des gewalttätigen Extremismus, die wiederholte Eskalation von Hass und Spannungen zwischen Gemeinschaften sowie die besorgniserregenden Trends bei nihilistischen Formen des Extremismus, in denen sich gewalttätiger Extremismus mit sexueller Ausbeutung und Missbrauch von Kindern überschneidet (z. B. 764⁹⁶).

Den Abschluss des ersten Veranstaltungstages machte Alexander Ritzmann, langjähriger Mitarbeiter des Counter Extremism Project (CEP). Mit seinem Vortrag „The Transnational Right-wing Extremist Active Club Network – Threat Potential and Strategies to Combat It“ gab er einen umfassenden Überblick über dieses schnell wachsende transnationale Netzwerk, das als dezentralisiertes Franchise-System arbeitet und das Ziel verfolgt, eine Schattenmiliz aufzubauen. Aktuell (Stand: März 2025) konnte Ritzmann 53 Active Clubs in Europa identifizieren, davon 12 in Frankreich, von denen einige als „Ausweichlösung“ entstanden, nachdem dort im Jahr 2021 die Identitäre Bewegung verboten wurde. Weiters hob Ritzmann den Offline-Fokus des Netzwerks hervor, der von den Mitgliedern verlangt, sich persönlich zu beteiligen, anstatt sich nur online zu engagieren. Zu den Aktivitäten gehören neben dem Kampfsporttraining vor allem ein illegaler politischer Aktivismus sowie logistische Übungen, die die Mitglieder auf koordinierte Milizoperationen vorbereiten sollen. Das Active Clubs-Netzwerk und seine Strategie stellen damit eine ausgeklügelte Weiterentwicklung früherer rechtsextremer Strategien dar:

Indem sich Active Clubs als harmlose Jugend(gegen)kultur-Bewegung präsentieren und ihre gewalttätigen Absichten unter dem Deckmantel von Fitness und Kameradschaft verbergen, zielen sie darauf ab, gefährdete Personen anzuziehen und sich der Kontrolle der Strafverfolgungsbehörden zu entziehen.

Den zweiten Tag des Symposiums eröffnete Jodie Wrigley mit der Frage „The Exploitation of Climate Chaos, Confusion and Change – A New Frontier for P/CVE Strategic Communication?“⁹⁷. Jodie Wrigley ist Leiterin der Abteilung Social Change bei der australischen Kommunikationsagentur SenateSHJ und Kommunikationsberaterin beim United Nations Office of Counter Terrorism und untersucht unter anderem die Überschneidung von Klimaereignissen, gewalttätigem Extremismus und strategischer Kommunikation. Wenngleich

96 Bei „764“ handelt es sich um ein Online-Netzwerk, das Kinder und Jugendliche sexuell nötigt bzw. erpresst („Sextortion“) und dabei zu unterschiedlichen Handlungen zwingt – von massiven Selbstverletzungen über Tierquälereien bis hin zum Suizid.

97 Die Abkürzung „P/CVE“ steht für „preventing/countering violent extremism“; dt.: Prävention/Bekämpfung von gewalttätigem Extremismus.

die wissenschaftliche Debatte über kausale Zusammenhänge zwischen Klimaereignissen und gewalttätigem Extremismus noch anhält, gibt es doch schon Hinweise darauf, dass solche Ereignisse die Anfälligkeit von Gemeinschaften für die Rekrutierung von Extremistinnen und Extremisten erhöhen, antidemokratische Ressentiments fördern und das Vertrauen in Institutionen und Regierungen untergraben. Diese Herausforderungen entfalten sich zunehmend sowohl in der Online- als auch in der Offline-Öffentlichkeit. Bei der Eindämmung dieser Risiken kann bzw. muss die strategische Kommunikation eine entscheidende Rolle spielen, indem sie als proaktives Instrument zur Prävention und zur Bekämpfung von gewalttätigem Extremismus im Kontext eskalierender, klimabezogener Herausforderungen eingesetzt wird.

Den letzten Vortrag hielt David Wells vom Cyber Threats Research Centre der Swansea University. Als Experte für die Schnittstelle zwischen neuen Technologien und internationaler Sicherheit befasste er sich mit dem Thema „The Misuse of Generative AI by Terrorists and Violent Extremists“ und gab einen Überblick, in welcher Form Terroristen und gewaltbereite Extremisten in den letzten zwei Jahren begonnen haben, mit Generativer KI (Gen-AI) zu experimentieren. Zwar sind diese Experimente bisher relativ begrenzt geblieben, jedoch legt eine Analyse aktueller oder bevorstehender Iterationen von Gen-AI-Tools nahe, dass sie Terroristen und gewalttätigen Extremisten das Potenzial bieten, einige ihrer bestehenden Fähigkeiten zu optimieren. So können mit Hilfe von Gen-AI Propagandamaßnahmen verbessert werden, insbesondere durch die Erstellung oder Veränderung von Bildern, Videos, Audios und Texten sowie durch die Verwendung von Übersetzungs- und Transkriptionstools. In anderen Bereichen der terroristischen Methodik – einschließlich der Erforschung terroristischer Ziele oder der Erstellung und Anpassung von Chatbots zur Radikalisierung und Rekrutierung – hängt der potenzielle Nutzen von Gen-AI von der Weiterentwicklung der Technologie selbst und den technologischen Fähigkeiten terroristischer Akteure ab. Wells verwies in seinem Vortrag auf die Notwendigkeit, diese Anwendungsfälle zu verstehen (und letztlich darauf zu reagieren). Darüber hinaus muss jede Analyse der potenziellen Auswirkungen von Gen-AI auf Terrorismus und gewalttätigen Extremismus auch die breiteren gesellschaftlichen Auswirkungen der Technologie berücksichtigen. Zu den potenziellen Auswirkungen zählen unter anderem ein deutlich verschlechtertes Informationsumfeld, die Stärkung autoritärer Regime und die Schaffung von Bedingungen, in denen extremistische Narrative gedeihen können.

Bevor es in eine abschließende Paneldiskussion ging, bei der mit Allison Curtis vom Strong Cities Network und Sian Hutchinson vom United Nations Office of Counter-Terrorism (UNOCT) zwei weitere hochrangige Expertinnen vertreten waren, gab es für die mehr als 100 Symposiumsteilnehmerinnen und Symposiumsteilnehmer im Rahmen von drei Breakout-Sessions die Möglichkeit, in kleinerem Rahmen aktuelle Herausforderungen zu diskutieren. Die Themen reichten von „Repressed Conflicts – Surpressed Dangers: From a Middle East in Transition to Sub-Sahara Africa in Turmoil“ über „Using Artificial

Intelligence and Machine Learning to Identify Terrorist Content Online“ bis zu „Effectively Combating Key Anti-Semitic Actors“.

CSAIR-Infobriefe

Im Jahr 2025 wurden im Rahmen des CSAIR erstmals zwei Infobriefe verfasst. Der erste widmet sich dem Thema „764 und O9A – Überschneidungen zwischen Okkultismus, rechtsextremem Akzelerationismus und sexueller Ausbeutung von Kindern“ und bietet eine kurze Darstellung des international operierenden Online-Netzwerkes 764. Kinder und Jugendliche werden von diesem Netzwerk über Gaming-Plattformen kontaktiert und anschließend sexuell genötigt und erpresst (Sextortion), wobei die Forderungen von Selbstverletzungen über das Quälen von Tieren und Drogenkonsum bis hin zu Amokläufen und Suiziden reichen. Zudem widmet sich der Infobrief den Verbindungen von 764 mit dem O9A – Order of 9 Angles (Orden der neun Winkel), einem rechtsextrem-akzelerationistischen Netzwerk, das esoterische bzw. satanische Rituale praktiziert. Die Aktualität dieses Themas und insbesondere die Dringlichkeit, sich diesem Thema auf politischer und gesellschaftlicher Ebene anzunehmen, wurden nur wenige Wochen nach Abfassung des Infobriefs durch den Fall „White Tiger“ unterstrichen. Bei der unter diesem User-Namen auftretenden männlichen Person handelt es sich um ein im Juni 2025 in Hamburg verhaftetes mutmaßliches 764-Mitglied, das unter anderem einen 13-Jährigen in den Suizid getrieben haben soll.

Der zweite CSAIR-Infobrief befasste sich unter dem Titel „Die westafrikanische Sahelzone – Herausforderung für die internationale Sicherheit und dennoch ein Krisenherd unter dem Radar“ mit der aktuellen Lage in den Ländern Mali, Burkina Faso und Niger. Diese Länder haben sich laut dem „Global Terrorism Index 2024“ in den letzten Jahren zum globalen Epizentrum des jihadistischen Terrorismus entwickelt. Diese Entwicklung liegt in einer Vielzahl an Ursachen begründet: von Regierungs- bzw. Staatsversagen über Korruption, ausgeprägter sozialer Ungleichheit und wirtschaftlicher Perspektivlosigkeit bis hin zu organisierter Kriminalität, einem oftmals gewaltsam ausgetragenen Kampf um natürliche Ressourcen und die gravierenden Folgen des Klimawandels. Diese Gemengelage ist Nährboden für die zahlreichen, sich gegenseitig verstärkenden Konflikte und auch Grund für die Vielzahl an Konfliktparteien, die von staatlichen Sicherheitskräften und ihren internationalen Verbündeten über separatistische Rebellengruppen und islamistische Terrorgruppen bis hin zu Selbstverteidigungsmilizen reichen. Besonders problematisch ist der Umstand, dass seit einiger Zeit sowohl die IS-Untergruppe Islamischer Staat Sahel Provinz als auch der al-Qaida-Ableger Jama'at Nusrat al-Islam wal-Muslimin (JNIM) immer größere Gebiete in Mali, Burkina Faso und Niger unter ihre Kontrolle bringen – eine Entwicklung, die auch durch die insgesamt fünf Militärcoups in diesen Ländern seit 2020 und den steigenden Einfluss russischer Söldner der Wagner-Gruppe bzw. des sogenannten Afrika-Korps bis dato nicht aufgehalten werden konnte.

Internationale Strategische Prävention

Im Zentrum der Bemühungen der internationalen strategischen Prävention steht die intensive europäische und internationale Kooperation – sowohl mit EU-Mitgliedsstaaten als auch Drittstaaten, deren Behörden und der Zivilgesellschaft, um eine kohärente und wissensbasierte Sicherheitsarchitektur zu gewährleisten.

Ein zentrales operatives Instrument auf europäischer Ebene ist der EU Knowledge Hub on Prevention of Radicalisation (EU-KH), der von der Europäischen Kommission betrieben wird und als Drehscheibe für Wissenstransfer, Trainings und strategische Kommunikation dient. Der EU-KH stellt eine Weiterentwicklung des 2024 ausgelaufenen Radicalisation Awareness Network (RAN) dar, wobei der Fokus nun verstärkt auf einem integrativen Ansatz liegt. Im Gegensatz zur früheren Trennung der Arbeitsgruppen vereinen die neuen Formate des EU-KH Vertreterinnen und Vertreter aus Politik, Praxis, Wissenschaft und Zivilgesellschaft in interdisziplinären Gruppen, um gemeinsam tiefergehende, praxisnahe Lösungen für die Prävention und Bekämpfung von gewaltbereitem Extremismus (P/CVE) zu entwickeln.

Die strategische Steuerung der europäischen P/CVE-Arbeit erfolgt über eine gestaffelte Governance-Struktur. Das Steering Board on Preventing and Countering Violent Extremism fungiert dabei als höchste strategische Instanz, dessen Mitglieder sich zweimal jährlich treffen und alle zwei Jahre die „Strategic Orientations“ verabschieden, welche die mittel- bis kurzfristige Schwerpunktsetzung der gesamten Präventionspolitik auf EU-Ebene festlegen. Auf operativer Arbeitsebene ist das Network of Prevent Policy Makers (NPPM) angesiedelt. Dieses Netzwerk bereitet die strategischen Entscheidungen inhaltlich vor, bündelt die nationalen Erfahrungen und trägt maßgeblich zur Formulierung der „Strategic Orientations“ bei.

Eine innovative Ergänzung dieser Struktur bilden die Thematic Panels (TPs) des EU-KH. Diese Panels bringen dauerhaft Fachleute aus verschiedenen Sektoren zu spezifischen Kernthemen wie Online-Radikalisierung oder psychische Gesundheit zusammen. Die gewonnenen Erkenntnisse und die erarbeiteten Handlungsempfehlungen fließen direkt in die Arbeit des NPPM und des Steering Boards ein. Durch diesen strukturierten Wissenstransfer-Kreislauf wird sichergestellt, dass die europäische Präventionsstrategie dynamisch bleibt und stets auf den neuesten wissenschaftlichen Erkenntnissen und praktischen Erfahrungen basiert.

3.6.2 Staatsschutzprävention

Die Prävention im Staatsschutz umfasst Maßnahmen, die darauf abzielen, extremistische Ideologien und potenzielle Gefahren für die öffentliche Sicherheit im Vorfeld zu erkennen, zu identifizieren und diesen entgegenzuwirken, bevor sie sich manifestieren. Dies ist besonders wichtig, da die Bedrohungen durch Radikalisierung, Extremismus und Terrorismus zunehmend komplexer und vielschichtiger werden.

Grundsätze der operativen Prävention im Staatsschutz – Universelle Prävention

Im Fokus der Staatsschutzprävention steht die universelle Präventionstätigkeit. Ziel ist es, in Österreich lebende Personen durch Informationsveranstaltungen und Workshops unmittelbar für menschenfeindliche Ideologien und extremistische Gruppierungen zu sensibilisieren. Zum einen soll dadurch eine erhöhte Wachsamkeit gegenüber extremistischen Einflüssen gefördert und zum anderen eine frühzeitige Erkennung solcher Tendenzen ermöglicht werden, um ihnen angemessen entgegenwirken zu können.

Dazu wurden mittlerweile österreichweit insgesamt 132 Bedienstete in den Landespolizeidirektionen ausgebildet, um durch Sensibilisierungsvorträge die Bevölkerung im Themenfeld der Radikalisierungs- und Extremismusprävention aufzuklären. Darüber hinaus richten sich eigens entwickelte Präventionsmaßnahmen an spezielle Zielgruppen. Im Jahr 2025 wurden von den ausgebildeten Präventionsbediensteten 1.461 Maßnahmen umgesetzt und 30.754 Personen erreicht.

Um den Schutz des demokratischen Rechtsstaates und unserer liberalen Werte als gesamtgesellschaftliche Aufgabe sicherzustellen, bindet der Staatsschutz im Rahmen seines ganzheitlichen Präventionskonzepts auch künftig wichtige Kooperationspartnerinnen und Kooperationspartner ein, die mit ihrer Nähe zu unterschiedlichen gesellschaftlichen Zielgruppen einen entscheidenden Beitrag zur Früherkennung, Aufklärung und Prävention leisten können.

Präventionsarbeit im Kontext internationaler Konflikte – Antisemitismus

Die Prävention im Staatsschutz hat in den letzten Jahren auch im Kontext internationaler Konflikte an Bedeutung gewonnen. Der deutliche Anstieg antisemitischer Tendenzen in den unterschiedlichsten Phänomenbereichen gefährdet nicht nur die jüdische Bevölkerung massiv, sondern auch den gesellschaftlichen Zusammenhalt und die politische Stabilität. Antisemitismus kann gesellschaftliche Spaltung und Polarisierung verstärken, Misstrauen zwischen Bevölkerungsgruppen fördern, Cliquenbildung intensivieren und dadurch ein inklusives Zusammenleben erschweren.

Antisemitismus bleibt eine persistente Ideologie, die inzwischen hauptsächlich über Online-Plattformen weitergetragen und normalisiert wird. Soziale Medien ermöglichen die schnelle Verbreitung, Reichweitensteigerung und einfache Verstärkung extremistischer Narrative durch Algorithmen, Gruppenbildung und virales Teilen.

Um diesen Tendenzen entgegen zu wirken, wurde die Ausbildung von Präventionsbediensteten in der Radikalisierungs- und Extremismusprävention erweitert. Neben historischen Hintergründen und Ursachen des Antisemitismus werden heutige Ausprägungen und Gruppierungen behandelt. Dieses Wissen schafft ein Bewusstsein für dieses Phänomen, ermöglicht ein frühzeitiges Erkennen von potenziell gefährlichen Entwicklungen und

trägt dazu bei, ein respektvolles Zusammenleben basierend auf Respekt und Toleranz zu sichern.

Zusammenarbeit mit dem Bundesministerium für Landesverteidigung (BMLV)

Ebenso wurde die Zusammenarbeit im Bereich der Präventionsarbeit mit dem BMLV intensiviert. In einem ersten Schritt konnte gemäß eines interministeriellen Knowledge-Sharings eine Vertreterin des BMLV an einer Ausbildung in der Radikalisierungs- und Extremismusprävention teilnehmen, um im Sinne des gesamtgesellschaftlichen Ansatzes die inhaltlichen Impulse der Ausbildung im dortigen Bereich einsetzen zu können.

Kooperation mit dem Bundesministerium für Bildung (BMB)

Schulen spielen eine zentrale Rolle bei der Sozialisation junger Menschen und sind zugleich potenzielle Räume, in denen radikale Ideologien aufgenommen, verstärkt, aber auch verlernt werden können. Bildungseinrichtungen prägen Werte, Identitäten und Zugehörigkeit. Gleichzeitig bieten sie Potenziale für die Prävention von Radikalisierung, da Bildung strukturiert Räume für Reflexion, Dialog und soziale Integration bereitstellt.

Aus diesen Gründen richtete sich im Berichtsjahr 2025 der Fokus der Präventionsmaßnahmen auf den Bildungsbereich. Gemeinsam mit der Abteilung Schulpsychologie des Bundesministeriums für Bildung wurde ein Leitfaden für Pädagoginnen und Pädagogen ausgearbeitet. Der Leitfaden soll Lehrpersonal für das Thema Radikalisierung sensibilisieren und anhand von Fallbeispielen Handlungssicherheit im Falle eines Radikalisierungsverdachts geben.

Präventionsangebot im schulischen und außerschulischen Setting

Im schulischen Setting finden die radikalierungs- und extremismuspräventiven Workshops „RE#work“ für die Zielgruppe der 13- bis 17-jährigen Schülerinnen und Schüler breiten Anklang. Gemeinsam mit den speziell ausgebildeten Jugendpräventionsbeamtinnen und Jugendpräventionsbeamten werden Themen wie Demokratie und Menschenrechte, Zivilcourage, Umgang mit sozialen Medien, Antidiskriminierung und Empathie in insgesamt fünf Modulen bzw. Workshops erarbeitet. Die Jugendlichen sollen durch die Lebenskompetenzorientierung dieser Maßnahme vor allem die eigene Resilienz stärken und zu den unterschiedlichen Themenbereichen informiert werden. Darüber hinaus stellen die Einbeziehung des Lehrkörpers sowie der Erziehungsberechtigten weitere Säulen im Sinne des Mehrebenen-Ansatzes innerhalb des Präventionsprogramms dar.

Vernetzung als zentrales Instrument gegen Radikalisierung und Extremismus

Ein gesamtgesellschaftlicher Ansatz in der Radikalisierungs- und Extremismusprävention bedeutet, dass die Verantwortung zur Vorbeugung und Bekämpfung von Radikalisierung nicht alleine bei staatlichen Stellen oder Sicherheitsbehörden liegt und liegen kann, sondern als gemeinsame Aufgabe der gesamten Gesellschaft verstanden wird. Radikalisierungs- und Extremismusprävention gelingt am besten, wenn alle gesellschaftlichen

Bereiche miteinander in einen Dialog treten, kooperieren und demokratische Werte aktiv gestärkt werden. Nur eine ganzheitliche, inklusive Strategie erhöht die Resilienz und die Bereitschaft der Gesellschaft, gemeinsam gegen extremistische Tendenzen vorzugehen. Vernetzung zwischen Behörden, Bildungseinrichtungen, zivilgesellschaftlichen Organisationen und lokalen Initiativen sind daher entscheidend, um Präventionsmaßnahmen effektiv zu gestalten und Radikalisierungsprozesse frühzeitig zu erkennen.

Innerhalb des BMI konnten mit dem Bundeskriminalamt (BK), mit der Bundespolizeidirektion (BPD) als auch mit der Sicherheitsakademie des Bundes (SIAK) Vernetzungspartner gewonnen werden. Vernetzungstreffen konnten sowohl mit dem Bundesamt für Fremdenwesen und Asyl (BFA) als auch dem Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung (BAK) abgehalten werden. Die Bundesagentur für Betreuungs- und Unterstützungsleistungen (BBU) und auch der Verein Saferinternet.at aus dem zivilgesellschaftlichen Bereich stehen als weitere Vernetzungspartner zum Thema der Radikalisierungs- und Extremismusprävention im stetigen Austausch mit der DSN.

Darüber hinaus konnten mit einem neugestalteten Ausbildungslehrgang zentrale Kompetenzen hinsichtlich Sensibilisierungsmaßnahmen zum Themenschwerpunkt Radikalisierung und Extremismus an die Mitglieder des Wiener Netzwerk für Demokratiekultur und Prävention sowie an Vertreterinnen und Vertreter aus den Bundesländern Niederösterreich und Burgenland, jeweils aus den Bereichen Bildung, Soziales, Asylwesen u. ä., weitergegeben werden.



3.6.3 Radikalisierungs- und Rückfallprävention

Aktuelle Entwicklungen im Bereich der Radikalisierung – Sekundärprävention

Nach wie vor lässt sich eine zunehmende Radikalisierung von Kindern und Jugendlichen, insbesondere im religiös-extremistischen Spektrum, feststellen. Die Radikalisierungsprozesse verlaufen mitunter sehr schnell, innerhalb weniger Monate, was unter anderem auf entsprechende Algorithmen in den sozialen Medien zurückzuführen ist, die die Jugendlichen in ein sogenanntes „Rabbit Hole“ ziehen und mit immer extremeren Inhalten konfrontieren. Auch agieren Radikalisierer im Internet sehr geschickt und fokussieren auf (vor allem psychisch) vulnerable, junge Menschen, die Anschluss oder einfache Antworten auf ihre Fragen suchen. In der Analyse der Biografien radikalierter Jugendlicher zeigen sich immer wieder mangelnde soziale Fertigkeiten, was es ihnen im realen Leben schwer macht, Anschluss und Anerkennung zu finden. Auch waren viele der radikalisierten Jugendlichen in ihrer schulischen Laufbahn Opfer von Mobbing oder klassische Außenseiter bzw. weisen sie eine geringe Resilienz auf, was es ihnen schwer macht, mit den mannigfaltigen Krisen der letzten Jahre umzugehen. Gemeinsam ist vielen radikalisierten Jugendlichen auch, dass sie in der Vergangenheit an Panikattacken, Depressionen oder Angststörungen litten, Erkrankungen aus dem schizophrenen Formenkreis aufweisen bzw. diese Erkrankungen nach wie vor virulent und unbehandelt sind. Auch das Phänomen von Konvertierungen autochthoner Jugendlicher, sowohl im urbanen als auch im ländlichen Raum, ist nach wie vor bemerkbar. Radikalisierung ist bei Weitem kein urbanes Phänomen mehr.

Bei jungen Menschen spielt eine spezielle Ideologie meist eine untergeordnete Rolle, vielmehr greifen sie oft Versatzstücke verschiedener Ideologien auf, um sich die Welt so zu konstruieren, wie es ihren Bedürfnissen entspricht. Die Radikalisierung dient ihnen dazu, Kontrolle in einer zunehmend unberechenbar erscheinenden Welt zu behalten, zudem stehen Bedürfnisse wie Zugehörigkeit, Selbstwirksamkeit und das Erhalten von Perspektiven bzw. einer Aufgabe im Vordergrund. In manchen Fällen stellt die Radikalisierung auch eine Rechtfertigung zur Ausübung unbewältigter Wut, von Gewaltfantasien oder Rachegefühlen dar.

Aufgrund dieser anhaltenden Radikalisierungsdynamik wurde ein Konzept für eine österreichweite Implementierung einer strukturierten Sekundärprävention im österreichischen Verfassungsschutz erarbeitet. Sekundärprävention adressiert Menschen, die bereits Radikalisierungstendenzen aufweisen, jedoch noch nicht einschlägig straffällig geworden oder noch nicht strafmündig sind. Durch rechtzeitige Interventionen in Kooperation mit der Zivilgesellschaft soll ein Fortschreiten der Radikalisierung aufgehalten oder eine Hinwendung zum Extremismus verhindert werden. So sollen problematische Entwicklungen unterbrochen werden, was einen wichtigen Beitrag für die Verhinderung künftiger Straftaten darstellt.

Im Jahr 2025 erfolgte die erste Repatriierung zweier österreichischer Frauen und ihrer Kinder, die zuvor jahrelang in syrischen Lagern inhaftiert waren, wobei eine Frau unmittelbar nach ihrer Ankunft in Österreich aufgrund eines vorliegenden Haftbefehls festgenommen wurde. Bereits Monate vor der Rückführung wurde die Prävention der DSN gemeinsam mit den betroffenen LSE aktiv, um in Kooperation mit relevanten Behörden und zivilgesellschaftlichen Vereinen die Wiedereingliederung dieser Frauen und Kinder in Österreich vorzubereiten. Es wurden Risikoanalysen vorgenommen, Fallkonferenzen abgehalten und Maßnahmenpläne entwickelt, die nach der Rückkehr auch laufend auf ihre Validität überprüft werden. So konnte dank der guten Kooperation aller Beteiligten ein engmaschiges Unterstützungs- und Kontrollnetzwerk etabliert werden, das es den Frauen und Kindern ermöglichen soll, sich gut in Österreich zu integrieren.

Kooperation mit dem Bundesministerium für Justiz – Tertiärprävention

Die intensive Kooperation zwischen der DSN und der Koordinationsstelle Extremismusprävention und Deradikalisierung (KED) in der Generaldirektion für den Strafvollzug im Bundesministerium für Justiz wurde auch im Jahr 2025 fortgeführt.

Die Gruppe der Strafvollzugsbediensteten bleibt eine zentrale Zielgruppe der Präventionsmaßnahmen. Haftanstalten stellen komplexe, milieubedingte Settings dar, in denen Radikalisierungspotenziale bestehen und sich Menschen aufgrund ihrer dort begünstigten kognitiven Öffnungen leichter radikalieren können. Daher ist es wichtig, Strafvollzugsbedienstete dahingehend zu sensibilisieren und zu stärken, Radikalisierungstendenzen rechtzeitig wahrnehmen zu können.

In einem gemeinsamen Arbeitsübereinkommen wurden neben der jährlichen Durchführung eines Ausbildungslehrganges in der Radikalisierungs- und Extremismusprävention für die Angehörigen des BMJ auch weitere Schritte zur gemeinsamen Konzeptionierung eines eigenen Präventionsprogrammes für die neu etablierte Strafvollzugsanstalt für Jugendliche gesetzt.

Ein weiterer Schwerpunkt der Zusammenarbeit liegt in der Risikoeinschätzung hinsichtlich jener Insassinnen und Insassen, die nach einem Delikt des Terrorbekämpfungsgesetzes (TeBG) inhaftiert sind, und der Ableitung notwendiger Maßnahmen sowohl für die Zeit der Inhaftierung als auch speziell für die Zeit nach der Haftentlassung. Der beidseitige Informationsaustausch ist hierbei von großer Bedeutung, da er einerseits dazu dient, die Sicherheit und Ordnung in den österreichischen Justizanstalten zu wahren sowie den Vollzug an die Bedürfnisse der Insassinnen und Insassen anzupassen, um ihre Deradikalisierung zu fördern. Andererseits dient er der optimalen Vorbereitung der Sicherheitsbehörden auf die Haftentlassung und gesellschaftliche Wiedereingliederung von einschlägig verurteilten Insassinnen und Insassen. Des Weiteren werden auf Anfrage der KED von der DSN Gefährlichkeitseinschätzungen anlässlich Gerichtsverhandlungen, Ausführungen und Überstellungen zwischen Justizanstalten erstellt.

Einmal im Quartal werden alle potenziellen Haftentlassungen einschlägiger Insassinnen und Insassen der nächsten Monate zwischen der DSN und der KED vorbesprochen, um frühzeitig geeignete Entlassungssettings und mögliche Gefahrenpotenziale auszuloten und – falls notwendig – eine Fallkonferenz Staatsschutz gem. § 6a SNG einzuberufen.

Im Berichtsjahr wurden durch die Vollzugsgerichte 60 Fallkonferenzen gemäß § 152 Abs. 2a StVG einberufen, an denen die Staatsschutzbehörden in Zusammenarbeit mit der KED teilnahmen. Der Schwerpunkt dieser Fallkonferenzen liegt auf der Evaluierung der Radikalisierung von Insassinnen und Insassen, die kurz vor einer bedingten Entlassung stehen und einschlägig verurteilt wurden. Im Rahmen dieser Fallkonferenzen wird ein individuell abgestimmter Maßnahmenplan entwickelt, der notwendige richterliche Weisungen für die Dauer der Probezeit beinhaltet. Darüber hinaus wurden durch die LSE 14 Fallkonferenzen Staatsschutz gemäß § 6a SNG abgehalten, im Rahmen derer Einzelfälle mit zuständigen Behörden und zivilgesellschaftlichen Einrichtungen zur Deradikalisierung besprochen und gemeinsame Maßnahmenpläne entwickelt werden. Ebenso fanden vier Fallkonferenzen gemäß § 6a SNG in Kooperation mit der KED sowie den betroffenen Justizanstalten statt, um Haftentlassungen besonders ideologischer Insassinnen und Insassen vorzubereiten.

Radikalisierungsverdachtsmeldungen aus Justizanstalten, die an die DSN und die LSE ergehen, werden in einem ersten Schritt analysiert. Nach stattgefundener Einschätzung ergeht eine Rückmeldung an die KED, damit entsprechende risikoreduzierende Maßnahmen implementiert werden können. Im Berichtsjahr 2025 zeigte sich ein deutlicher Anstieg von Radikalisierungsverdachtsmeldungen aus Justizanstalten (um 26 Prozent) im Vergleich zum Vorjahr.

3.7 Sicherheitsüberprüfungen im Rahmen des Sicherheitspolizeigesetzes

Die Sicherheitsüberprüfung gemäß § 55 Abs. 1 Sicherheitspolizeigesetz dient der Abklärung der Vertrauenswürdigkeit eines Menschen anhand personenbezogener Daten, die Aufschluss darüber geben, ob Anhaltspunkte vorliegen, dass diese Person gefährliche Angriffe begehen werde.

Dabei werden zwei Arten von Überprüfungen unterschieden.

Zum einen die Sicherheitsüberprüfung, die nur auf Grund der Einwilligung und einer Erklärung (Sicherheitserklärung) der oder des Betroffenen hinsichtlich ihres oder seines Vorlebens und der gegenwärtigen Lebensumstände durchgeführt werden darf. Diese Art der Sicherheitsüberprüfung stellt speziell für den öffentlichen Dienst, aber auch für Unternehmen der kritischen Infrastruktur eine Möglichkeit dar, das Risiko von schädigenden Handlungen durch Innentäterinnen und Innentäter zu minimieren. So können

Betreiberinnen und Betreiber kritischer Infrastrukturen für Personen, die eine Tätigkeit im Unternehmen wahrnehmen oder anstreben, bei der sie Zugang zu vertraulichen Informationen haben, deren unzulässige Verwertung eine nachhaltige Funktionsstörung oder Zerstörung der kritischen Infrastruktur bewirken würde, eine Sicherheitsüberprüfung beantragen.

In den unterschiedlichen Bereichen, in denen der Gesetzgeber gemäß den Bestimmungen des § 55 Abs. 2 SPG die Möglichkeit einer Sicherheitsüberprüfung normiert, wird diese im Rahmen eines verantwortungsvollen Human Risk Managements als ein probates Mittel zur Risikominimierung angesehen. Im Zuge einer laufenden Professionalisierung und Weiterentwicklung der Sicherheitsüberprüfungen wurden die dafür vorgesehenen Sicherheitserklärungsformulare überarbeitet und mit Verordnung⁹⁸ am 19. Dezember 2024 kundgemacht. Die Sicherheitserklärungs-Verordnung trat mit 1. Februar 2025 in Kraft. In dieser Verordnung wurden die Fragestellungen zu den unterschiedlichen Themenbereichen aktualisiert und den gültigen Rechtsvorschriften angepasst.

Die zweite Art betrifft die Sicherheitsüberprüfung gemäß § 55a Abs. 1 Z 2 SPG, die zum Zwecke des vorbeugenden Schutzes von Organwallerinnen und Organwaltern verfassungsmäßiger Einrichtungen und von Vertreterinnen und Vertretern ausländischer Staaten, internationaler Organisationen oder anderer Völkerrechtssubjekte hinsichtlich von Menschen, die sich im räumlichen Umfeld der zu schützenden Person aufhalten, durchgeführt wird. Diese darf ohne Einwilligung und Erklärung der betroffenen Person erfolgen.

Bei beiden Überprüfungsarten ist über Jahre hinweg ein vermehrter Bedarf wahrnehmbar, der sich auch in den Zahlen widerspiegelt. Dieser Anstieg ist zum einen auf eine zunehmende Bewusstseinsbildung, zum anderen auf ein stetig steigendes Sicherheitsbedürfnis, auch der geopolitischen Lage geschuldet, zurückzuführen.

	Sicherheitsüberprüfung (mit Zustimmung des Betroffenen) (gemäß § 55b Abs. 1 SPG)	Sicherheitsüberprüfung (ohne Zustimmung des Betroffenen) (gemäß § 55a Abs. 1 Z 2 SPG)
2021	6.716	4.774
2022	8.709	6.067
2023	10.371	11.451
2024	13.030	10.723
2025	10.267	11.943

98 Verordnung des Bundesministers für Inneres, mit der die Verordnung über Form und Inhalt der Sicherheitserklärung einschließlich der Zustimmungserklärung (Sicherheitserklärungs-Verordnung) geändert wird, BGBl II 2024/390.

3.8 Zuverlässigkeitsüberprüfungen im Kontext des Luftfahrtgesetzes

Die Sicherheitsbehörden haben gemäß § 134a (Sicherheitsmaßnahmen im Bereich der Zivilluftfahrt) i. V. m. § 140d (Mitwirkung der Sicherheitsbehörden) Luftfahrtgesetz (LFG) bei der Durchführung von Zuverlässigkeitsüberprüfungen (ZÜP) im Rahmen der Amtshilfe für das Bundesministerium für Innovation, Mobilität und Infrastruktur (BMIMI) mitzuwirken. Die DSN fungiert dabei als Schnittstelle für das BMI und überprüft sämtliche Personen, die zum unbegleiteten Zutritt in sicherheitssensible Bereiche von Flughäfen berechtigt werden sollen. Damit leistet die DSN einen wichtigen Beitrag zur Umsetzung der unionsrechtlichen Standards⁹⁹ für die Sicherheit in der Zivilluftfahrt.

Zu diesem Zweck ist die DSN gemäß § 140d LFG ermächtigt, personenbezogene Daten, die auf Grund von Bundes- oder Landesgesetzen ermittelt wurden, zu verarbeiten und das Ergebnis der Überprüfung dem BMIMI mitzuteilen.

Die abschließende Bewertung darüber, ob die notwendige Zuverlässigkeit einer Person gegeben ist, fällt ausschließlich in die Zuständigkeit des BMIMI als verfahrensführende Behörde.

Nach einem signifikanten Anstieg von ZÜP in den letzten fünf Jahren blieb die Anzahl auch im Jahr 2025 mit der Überprüfung von 34.532 Personen auf einem anhaltend hohen Niveau.

Um weiterhin eine professionelle Abarbeitung aller ZÜP in der gesetzlich vorgesehenen Frist von 28 Tagen sicherstellen zu können, wurde im Mai 2025 ein umfassendes Digitalisierungsprojekt realisiert. Moderne, automationsunterstützte Prozesse und einheitliche digitale Schnittstellen tragen seither zu einer ressourcenschonenden und effizienten Erledigung bei, weshalb die Durchführung der Überprüfungen erheblich beschleunigt werden konnte.

⁹⁹ Durchführungsverordnung (EU) 2019/103 der Kommission vom 23. Januar 2019 zur Änderung der Durchführungsverordnung (EU) 2015/1998 in Bezug auf Präzisierung, Harmonisierung und Vereinfachung sowie die Verstärkung bestimmter spezifischer Luftsicherheitsmaßnahmen.

Verfassung schützen,
Sicherheit gewährleisten.

