Bundesministerium
Inneres

Direktion Staatsschutz
und Nachrichtendienst

Verfassungsschutzbericht 2022

Verfassungsschutzbericht 2022

Impressum

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

Fotos:
Alle Fotos DSN,
außer Coverfoto und Foto Seite 107 - Adobe Stock,

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

Hersteller:
Digitalprintcenter des BMI
1010 Wien, Herrengasse 7

Inhalt

Vorwort

Sehr geehrte Leserinnen und Leser,

Bundesminister
Gerhard Karner

Generaldirektor für die
öffentliche Sicherheit
Franz Ruf

zur Bewältigung von Krisen ist ein starker, verlässlicher und handlungsfähiger Verfassungsschutz von großer Bedeutung. Das Jahr 2022 und somit das erste Jahr nach der Einrichtung der Direktion Staatsschutz und Nachrichtendienst (DSN) war geprägt von multiplen Krisen. Durch die Umsetzung der Verfassungsschutzreform konnte den aktuellen Gefahren umfassend begegnet werden.

Neben den zu beobachtenden Phänomenbereichen wie dem Extremismus und Terrorismus, der Spionage, dem internationalen Waffenhandel, der Proliferation und der Cybersicherheit hatte insbesondere der russische Angriffskrieg auf die Ukraine Auswirkungen auf die Gesamtsicherheitslage Österreichs. In diesem Kontext war die DSN mit daraus resultierenden Themen wie Sanktionen, Foreign Fighters, Spionage, Cyberbedrohungen und Schutz der kritischen Infrastruktur aufgrund der Energiekrise konfrontiert. Diese Herausforderungen werden in diesem Bericht im Kapitel „Akzente im Verfassungsschutz 2022“ thematisiert.

In Bezug auf die umfangreichen Aufgabengebiete des österreichischen Verfassungsschutzes wird im Bericht auch auf mögliche zukünftige Entwicklungen eingegangen. Dazu zählen die anhaltende Bedrohung durch radikalisierte Gefährderinnen und Gefährder, die zunehmenden Spionageaktivitäten im Hochtechnologiesektor sowie die bevorstehende Präsidentschaftswahl in der Türkei im Jahr 2023 mit den damit verbundenen Auswirkungen auf die Sicherheitslage in Österreich.

Dank des unermüdlichen Einsatzes der Mitarbeiterinnen und Mitarbeiter des Verfassungsschutzes begegnete dieser den Gefahren mit einem proaktiven Präventionsansatz, der in den nächsten Jahren weiter ausgebaut werden soll. Für einen stabilen Verfassungsschutz ist zudem das Vertrauen der Bevölkerung von essentieller Bedeutung. Dieses kann und soll durch Transparenz, professionales Arbeiten und Kooperationen mit Wirtschaft, Wissenschaft und Forschung weiter gestärkt werden.

Gerhard Karner
Bundesminister für Inneres

Franz Ruf
Generaldirektor für die
öffentliche Sicherheit

Ein moderner Verfassungsschutz für die Sicherheit Österreichs – Einleitende Worte des Direktors der Direktion Staatsschutz und Nachrichtendienst

Sehr geehrte Leserinnen und Leser,

Direktor der DSN
Omar Haijawi-Pirchner

am 1. Dezember 2021 nahm die Direktion Staatsschutz und Nachrichtendienst (DSN) ihre Arbeit mit dem Ziel auf, das Fundament des österreichischen Verfassungsschutzes zu festigen und die Organisation an internationale Standards anzupassen: Vernetzung, Transparenz und Vertrauenswürdigkeit stehen dabei im Mittelpunkt. Es entstand eine zukunftsorientierte Organisation, deren Kernaufgaben die Identifizierung, die Vorbeugung, die Ermittlung und das Abwehren von verfassungsgefährdenden Bedrohungen gegen die demokratische Freiheit und Sicherheit Österreichs sind. Nur der enorme Einsatz aller Mitarbeiterinnen und Mitarbeiter des Verfassungsschutzes machte es möglich, die Reformpläne konsequent umzusetzen und so den Ansprüchen einer modernen Sicherheitsbehörde gerecht zu werden.

Das Jahr 2022 war geprägt von Ungewissheit und gravierenden, langfristigen Veränderungen, die die Gesellschaft bewegten. Der russische Angriffskrieg auf die Ukraine, die daraus folgende Energiekrise mit der einhergehenden Teuerung, die Gefahr von Extremismus und Terrorismus, die Klimakrise, Cyber-Attacken und mögliche Angriffe auf die kritische Infrastruktur sind nur einige der Themen, die alle in Österreich lebenden Personen im letzten Jahr auf die eine oder andere Art beschäftigten. Die gesellschaftliche Verunsicherung führte zu herausfordernden Situationen und zeigte, wie wichtig schnelles Agieren und Resilienz für den österreichischen Verfassungsschutz sind.

Die DSN war im vergangenen Jahr aufgrund des Krieges in der Ukraine besonders beim Thema Sanktionen gefordert. Zudem wurde erneut die Problematik der Foreign Fighters und Foreign Volunteers transparent, nachdem Personen aus Österreich in die Ukraine ausgereist waren, um dort an Kampfhandlungen teilzunehmen. Auch im Bereich der Spionage ergaben sich im Kontext Russland-Ukraine besondere Herausforderungen, speziell im Bereich Cyberbedrohungen. Als Reaktion auf die Energiekrise wurde überdies der Schutz der kritischen Infrastruktur noch relevanter. Gleichzeitig stellen auch extremistische Bewegungen nach wie vor eine große Gefahr für die Bevölkerung dar, und die bevorstehende Präsidentschaftswahl in der Türkei im Jahr 2023 ließ bereits 2022 Auswirkungen auf die Sicherheitslage in Österreich erkennen.

Der vorliegende Bericht gibt einen Einblick in die umfangreichen Aufgabengebiete des österreichischen Verfassungsschutzes sowie aktuelle Herausforderungen und mögliche zukünftige Entwicklungen. Statistische Zahlen oder Kenngrößen im Bereich des Verfassungsschutzes werden im jährlich erscheinenden Sicherheitsbericht des Bundesministeriums für Inneres veröffentlicht.

Ein moderner Verfassungsschutz kann nur dann effizient arbeiten, wenn er die Möglichkeit bekommt, erforderliche Informationen zu sammeln und diese zu verwerten. Dafür sind auch die entsprechenden rechtlichen Befugnisse erforderlich, die es teilweise noch zu adaptieren beziehungsweise zu erwirken gilt. Die DSN konzentriert sich daher, neben der Gefahrenerforschung und Gefahrenabwehr, auch darauf, die Rahmenbedingungen der Arbeit des Verfassungsschutzes stetig zu verbessern.

> *„Der Verfassungsschutz ist das Fundament unserer Sicherheit. Die Direktion Staatsschutz und Nachrichtendienst gewährleistet, dass dieses Fundament stark und stabil bleibt und die Menschen in Österreich in Freiheit und Sicherheit leben können."*

Omar Haijawi-Pirchner
Direktor der DSN

1
Nach der Reform des Verfassungs-schutzes

Im ersten Jahr nach der Reform des Verfassungsschutzes hat sich nicht nur gezeigt, dass Österreich zur Bewältigung von Bedrohungen und Krisen vor allem einen starken Verfassungsschutz braucht, sondern auch, dass die richtigen Schritte gesetzt wurden, um das Vertrauen der Bevölkerung und Partnerdienste wiederzuerlangen. Speziell die gesetzlich vorgeschriebene Trennung von Staatsschutz und Nachrichtendienst mit einem Gemeinsamen Informations- und Lagezentrum als Schnittstelle wurde erfolgreich umgesetzt.

Durch zahlreiche bilaterale Arbeitstreffen mit nationalen und internationalen Partnern sowie durch nationale und internationale Kooperationen konnte die DSN entscheidende Maßnahmen für die Sicherheit Österreichs und den Vertrauensgewinn setzen.

Naturgemäß hat Sicherheit bei allen Tätigkeiten der DSN die oberste Priorität, weshalb auch die internen Sicherheitsmaßnahmen verstärkt wurden. Dazu zählen verpflichtende Vertrauenswürdigkeitsprüfungen für alle Verfassungsschutzbediensteten nach internationalem Standard und eine neue, mehrmonatige Grundausbildung. Begleitend soll ein Masterlehrgang für den Verfassungsschutz mit dem Ziel der Stärkung der strategischen und wissenschaftlichen Ausrichtung eingerichtet werden. Zudem wurden ein Prozess- und Qualitätsmanagement aufgebaut und durch Dienstanweisungen klare Regeln geschaffen, um Handlungssicherheit und Qualitätssicherung in der neuen Organisationsstruktur gewährleisten zu können.

Damit die DSN ihre Aufgaben in Zukunft noch effektiver erfüllen kann, verstärkte sie im Jahr 2022 die Suche nach neuen Mitarbeiterinnen und Mitarbeitern durch öffentliche und interne Ausschreibungen. Beim Personalausbau setzt die DSN auf Diversität bezüglich Ausbildung und Kompetenzen. Es werden daher nicht nur Polizistinnen und Polizisten, sondern auch Expertinnen und Experten aus unterschiedlichsten Bereichen gesucht. Zudem soll eine intensivere Kooperation mit Universitäten und Fachhochschulen Studierende frühzeitig für die spannenden Aufgabengebiete und eine Karriere beim Verfassungsschutz begeistern und folglich helfen, qualifiziertes Personal zu rekrutieren.

Einen neuen Weg zur Personalrekrutierung hat die DSN mit der Nutzung des Berufs- und Karriere-Netzwerks „LinkedIn“ eingeschlagen. Dieser Kanal wird seit April 2022 genutzt, um mögliche Bewerberinnen und Bewerber auf die DSN aufmerksam zu machen und Ausschreibungen zu veröffentlichen. Die ständig wachsende Follower-Zahl und die positiven Rückmeldungen vieler Bewerberinnen und Bewerber bestätigen den Nutzen dieses neuen Rekrutierungsweges.

Neben neuen Initiativen wurden im vergangenen Jahr auch Themen, die in der Vergangenheit in der Verfassungsschutzarbeit oft zu kurz gekommen sind, aktiv aufgenommen. So wurden eine Ansprechstelle und ein mobiles Präventionsteam für den Wirtschaftsschutz geschaffen. Das Präventionsteam unterstützt Unternehmen und wissenschaftliche Ins

titutionen individuell bei der Gefahrenerkennung sowie bei der Entwicklung wirkungsvoller Präventionsmaßnahmen gegen alle Erscheinungsformen der Wirtschafts- und Industriespionage.

Darüber hinaus wurde der Präventionsbereich im Verfassungsschutz insgesamt auf eine breitere Basis gestellt: Mit dem Wissen, dass Radikalisierung und Extremismus nur gesamtgesellschaftlich begegnet werden kann, wurde bereits vor einigen Jahren das Bundesweite Netzwerk zur Extremismusprävention und Deradikalisierung (BNED) gegründet, in dem sich Akteurinnen und Akteure aus unterschiedlichen Berufsgruppen und aus verschiedenen Blickwinkeln der Extremismusprävention und Deradikalisierung widmen. Im neuen Präventionsmodell ist die Prävention des Verfassungsschutzes in den Bereichen der Direktion, des Staatsschutzes und des Nachrichtendienstes verankert. In den Bundesländern erfolgte zudem der Ausbau der Extremismusprävention in den Landespolizeidirektionen.

Ein weiterer Baustein für die effektivere Arbeit des Verfassungsschutzes wurde durch die Verbesserung der Zusammenarbeit mit den Justizbehörden gelegt. Vor allem die durch das Staatsschutz- und Nachrichtendienstgesetz (SNG) neu eingerichteten „Fallkonferenzen Staatsschutz" stellen einen wichtigen Beitrag für die Vernetzung der Behörden dar. Sie ermöglichen ein frühzeitiges Erkennen von Radikalisierungstendenzen und dienen somit der Vorbeugung von verfassungsgefährdenden Angriffen. Je früher Radikalisierung erkannt wird, desto rascher und effektiver können Gegenmaßnahmen gesetzt werden.

Ein weiterer wichtiger Fokus der DSN liegt auf der Etablierung einer nachrichtendienstlichen Kultur in Österreich. Derzeit scheint vielerorts noch wenig Sensibilität für die Arbeit von Nachrichtendiensten vorhanden zu sein beziehungsweise fehlt oftmals das Bewusstsein, dass in gewissen Bereichen sensible Informationen nicht preisgeben werden dürfen. Auch wenn Transparenz in der Arbeit der DSN großgeschrieben wird und Medien sowie Öffentlichkeit wichtige Partner darstellen, dürfen nachrichtendienstliche Informationen nicht nach außen kommuniziert werden.

Insgesamt ist die Neuaufstellung des österreichischen Verfassungsschutzes auf einem vielversprechenden Weg. Im Jahr 2023 werden die Struktur und Aufgaben der für Staatsschutz zuständigen Organisationseinheiten der Landespolizeidirektionen – die bisherigen Landesämter für Verfassungsschutz und Terrorismusbekämpfung (LVT) – an die Verfassungsschutzreform angepasst. Weitere Ziele bleiben die Rekrutierung und Ausbildung von Fachpersonal sowie die Stärkung des Vertrauens wichtiger Stakeholder und der Bevölkerung in den Verfassungsschutz.

2 Verfassungs-schutzrelevante Phänomen-bereiche

2.1 Extremismus und staatsfeindliche Verbindungen

Allgemein werden unter **„Extremismus“** unterschiedliche politische Bestrebungen, die sich offen gegen die Normen und Regeln des Verfassungsstaates wenden, definiert. Extremisten und Extremistinnen sehen die Realität durch den ideologischen Filter einer bestimmten Weltanschauung, welche auf nicht überprüfbaren Aussagen beruht , aber dennoch mit dem Anspruch auf absolute Wahrheit behauptet wird. Für Extremistinnen und Extremisten ist die Anwendung von Gewalt ein legitimes Mittel zur Durchsetzung ihrer eigenen politischen Ziele. Jede Extremismusform für sich steht somit im Widerspruch zu den verfassungskonformen demokratischen Prinzipien einer auf Pluralität basierenden Gesellschaft und wird als Gefährdung der inneren Sicherheit auf Basis gesetzlicher Grundlagen bekämpft.

Im Gesamtkomplex Extremismus sind in Österreich – neben dem islamistischen Extremismus und Terrorismus – unter anderem folgende Teilphänomene besonders hervorzuheben: Rechtsextremismus und Linksextremismus sowie staatsfeindliche Verbindungen.

2.1.1 Rechtsextremismus

„Rechtsextremismus“ 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 modernen demokratischen Verfassungsstaates ablehnen und diesen mit Mitteln beziehungsweise unter Gutheißung oder Inkaufnahme von Gewalt bekämpfen.

2.1.1.1 Überblick

Der Terminus Rechtsextremismus ergibt sich aus unterschiedlichen gesellschaftlichen Verwendungskontexten und den damit korrespondierenden Interpretationen, mit denen er jeweils bezeichnet wird. Die Befürwortung einer Diktatur, Islam- und Fremdenfeindlichkeit, Antisemitismus, Chauvinismus, Sozialdarwinismus, Rassismus sowie die Verharmlosung und Relativierung des Nationalsozialismus (mit dem Ziel des Revisionismus) prägen das Weltbild rechtsextremer Ideologen und ideologisierter Gruppierungen/Bewegungen, Netzwerke, Szenen und Milieus. Charakteristisch für rechtsextremistische Einstellungs- und Handlungsmuster ist die Verherrlichung eines „völkischen Nationalismus“ auf Basis deutschnationaler beziehungsweise nationalistisch-konservativer Konzepte. Zentrale Wesensmerkmale rechtsextremistischer Ideologien sind antidemokratische und antiplu

ralistische Gesellschaftsauffassungen bei gleichzeitiger Ablehnung des vorherrschenden (das heißt demokratischen) politischen Systems. In seiner äußersten Form kann sich der Rechtsextremismus bis hin zum (Rechts-)Terrorismus steigern, mit dem Ziel, systematisch gegen politische Gegner, gegen Opfergruppen rechtsextremistischer Weltanschauungen und gegen staatliche Institutionen beziehungsweise gegen ihre Repräsentantinnen und Repräsentanten vorzugehen.

2.1.1.2 Aktuelle Lage

Die rechtsextreme Szene in Österreich wird seit rund einer Dekade durch zwei Hauptströmungen repräsentiert: einerseits durch den tradierten Neonazismus und andererseits durch die „Neuen Rechten". Beide haben Schnittstellen zur rechtsextremen Hooliganszene beziehungsweise in die einschlägige Musikszene und beide verfolgen das Ziel, durch nationalistische Narrative ein breiteres Gesellschaftsspektrum für sich zu gewinnen. Sowohl in der neonazistischen Strömung als auch in der „Neuen Rechten" haben sich führende Gruppen und Zirkel etabliert, die im Beobachtungszeitraum das definierte Ziel mit Hilfe unterschiedlicher Themen zu realisieren versuchten. Hier sind an erster Stelle die islam-, asyl- und fremdenfeindlichen Erklärungsmuster zu nennen, aber auch die deutlich erkennbare Ambition, mit radikal-fundamentaler Kritik an den behördlichen COVID-19-Maßnahmen bestehende Demokratiefeindlichkeit zu befeuern.

„NEUE RECHTE" – Die Hauptvertreterin der „Neue Rechten", die „Identitäre Bewegung Österreich" (IBÖ), präsentiert sich als patriotische Nichtregierungsorganisation (NGO), die sich über Parteigrenzen hinweg für den Erhalt einer vermeintlichen kulturellen Identität einsetzt. Sie geht dabei von einer geschlossenen, ethnisch homogenen „europäischen Kultur" aus, deren „Identität" vor allem von einer „Islamisierung" bedroht sei. Im Multikulturalismus sieht sie eine Bedrohung der Traditionen, Kulturen und Völker.

Ausgelöst durch einschlägige Ereignisse, wie beispielsweise der Spende des rechtsterroristischen Attentäters von Christchurch an den bekanntesten Vertreter der IBÖ, haben sich viele Funktionärinnen und Funktionäre sowie Exponentinnen und Exponenten der Identitären zu einer neuen Organisation namens „Die Österreicher – DO5" formiert. Mit teilweise denselben Akteurinnen und Akteuren, hierarchischen Strukturen, bekannten Zielsetzungen, verfassungsgefährdenden Argumentationslinien und Agitationen sollte durch einen anderen Namen ein neues Image aufgebaut werden, um möglichst unbelastet die eigene Reichweite wiederherzustellen beziehungsweise zu erhöhen und neue Attraktivitätsmomente für eine potenzielle Anhängerschaft zu generieren. Nach eigenen Aussagen war die Motivation für die Gründung der DO5, eine Bewegung ins Leben zu rufen, die für alle Bürgerinnen und Bürger, egal welcher Altersklasse oder aus welchem sozioökonomischen Milieu stammend, ansprechend ist. Die ideologischen Ziele der DO5 sind großteils kongruent mit jenen der IBÖ. Auffällig ist jedoch, dass sich „Die Österreicher" mit Beginn der COVID-19-Pandemie aktiv unter jene Bürgerinnen und Bürger mischten, die gegen die Maßnahmen zur Eindämmung der COVID-19-Pandemie demonstrierten, um deren Unmut für die eigenen Zwecke zu instrumentalisieren.

Die Argumentationslinien der „Neuen Rechten“ – subsumiert unter den Schlagworten „Bevölkerungsaustausch“, „Great Reset“ oder „Remigration“ – stellen einen Angriff auf bestehende liberal-demokratische und rechtsstaatliche Strukturen dar. Sie fokussieren gegenwärtig vor allem auf Tathandlungen von Asylwerberinnen und Asylwebern sowie Migrantinnen und Migranten, welche als unmittelbare und direkte Gefahr für alle Bürgerinnen und Bürger dargestellt werden. Mit Hilfe dieser Überzeichnung soll der liberale Rechtsstaat als die eigentliche Gefahr für die Bürgerin und den Bürger dargestellt und in weiterer Folge das Gefühl geschaffen werden, dass nur ein radikaler Systemwechsel im Sinne der „Neuen Rechten“ dem Schutzbedürfnis der Bevölkerung Rechnung tragen kann.

In diesem Zusammenhang ist festzuhalten, dass durch die bisherigen Aktivitäten der Gruppe – insbesondere während der stärksten Phase der COVID-19-Proteste – nicht nur eine offensive Unterstützung der IBÖ beziehungsweise der DO5 durch politisch weit rechts stehende antagonistische Strömungen besteht, sondern auch die Bereitschaft zur Kooperation – wie beispielsweise als „Demoschutz“ für die DO5 – mit rechtsextremen Hooligan-Gruppierungen, mit Vertreterinnen und Vertretern aus der rechtsradikalen Staatsverweigerer-Szene sowie mit Anhängerinnen und Anhängern der derzeit verbreiteten rechtsextremen Verschwörungsideologien gegeben ist. Somit manifestiert sich in diesen Netzwerken ein weites und tiefgehendes Problemfeld mit sicherheitsrelevanter Herausforderung.

NEONAZISMUS – Die Vertreterinnen und Vertreter der Gruppierungen unterstützen nationalsozialistisch geprägte Ideologien, einschließlich antisemitischer und ausländerfeindlicher Narrative, und sind weltanschaulich gegen die Prinzipien eines demokratischen Rechtsstaates eingestellt. Militanz und Gewaltbereitschaft zeigen sich bei den einzelnen

Verbindungen in unterschiedlichen Ausformungen – verbal und/oder physisch, versteckt und/oder offen. Zum Aktivistenumfeld der Neonazi-Szene ist festzuhalten, dass sich einschlägige Gruppen in Vereinen organisieren, welche der Rekrutierung beziehungsweise der Indoktrinierung potenzieller Sympathisantinnen und Sympathisanten, aber auch der Förderung rechtsextrem motivierter Aktivitäten dienen.

Seit Beginn der COVID-19-Pandemie 2020 machte diese Szene vor allem bei Demonstrationen der Corona-Maßnahmen-Gegner (CMG) auf sich aufmerksam und verstärkte ihre Aktivitäten im virtuellen Raum mit der Einrichtung der Website „Corona-Querfront". Ziel dieser Maßnahmen ist, Akzeptanz in der Gesellschaft zu erreichen, die weit über das inhärente Zielpublikum des rechtsextremen und rechtsradikalen Spektrums hinausgehen soll. Wie im Fall der „Neuen Rechten" wird auch von diesem Umfeld die Unterstützung von sowie die Kooperation mit rechtsextremen Hooligan-Gruppierungen, der rechtsradikal orientierten Staatsverweigerer-Szene und den Anhängerinnen und Anhängern rechtsextremer Verschwörungsideologien gesucht.

Ein weiterer Aspekt der Neonazi-Szene ist das breite Auftreten von nicht unmittelbar in Netzwerken eingebundenen Aktivistinnen und Aktivisten, die vor allem durch Internetauftritte die Verbreitung nationalsozialistischer Ideologieelemente vorantreiben. Als ein Beispiel kann die erfolgreiche Ausforschung eines Brüderpaars alias „Mr. Bond" und „Kikel Might" genannt werden. Sie waren als Rapper beziehungsweise als Betreiber der Homepage „Judas Watch" für Straftaten nach dem Verbotsgesetz und der Verhetzung verantwortlich und wurden zu zehn beziehungsweise vier Jahren unbedingter Haft verurteilt. Welche Bedrohung solche Individualaktivitäten der NS-Szene darstellen, zeigt die Tatsache, dass Mr. Bond das Online-Manifest des Attentäters von Christchurch (Neuseeland) ins Deutsche übersetzte und eines seiner Musikstücke während des rechtsterroristischen Anschlags in Hanau (Deutschland) als Untermalung für den Livestream des Angriffs verwendet wurde. „Kikel Might" wiederum verbreitete die Erzählung über die „Jüdische Weltverschwörung" und setzte jüdische Bürgerinnen und Bürger und die von ihm als „Unterstützer" definierten Personen durch Veröffentlichung auf der Seite „Judas Watch" der Gefahr von Angriffen fanatisierter Szenesympathisantinnen und -sympathisanten aus.

UKRAINE-KRIEG – Seit dem Frühjahr 2022 beeinflusst der Angriffskrieg Russlands gegen die Ukraine auch die rechtsextreme Szene in Österreich. In beiden Ländern finden sich relevante rechtsextreme, nationalistische Verbindungen, die bereits seit Längerem auch Kontakte in den deutschsprachigen Raum unterhalten. Daher wird in diesem Konflikt nicht für eine Seite ungeteilt oder eindeutig Partei ergriffen. Es gibt in diesem Zusammenhang geprüfte Hinweise zu Verdachtslagen, dass aus der heimischen REX-Szene individuelle und unorganisierte Ausreisen in das Kriegsgebiet erfolgten, um sich an Kampfhandlungen zu beteiligen. Jedoch erbrachten die bisherigen Ermittlungen noch keine ausreichend belastbaren Beweise für strafrechtliche Verfahren. Wie schon bei der

Rückkehr von Foreign Terrorist Fighters (FTF) aus den Konfliktgebieten des Nahen Ostens bilden auch die aufgrund traumatisierender oder verrohender Erfahrungen möglicherweise radikalisierten Rückkehrer aus der Ukraine ein potenziell hohes Gefahrenmoment, welches von den Sicherheitsbehörden im Allgemeinen und vom Verfassungsschutz im Besonderen zu beobachten ist.

2.1.1.3 Fälle 2022

Im März 2022 wurde ein rechtsextremer Intensivtäter nach einer mehrjährigen Haftstrafe entlassen. Der Grund für seine Verurteilung nach dem Verbotsgesetz war eine hohe Anzahl an begangenen Sachbeschädigungen mit dem dafür erforderlichen Wiederbetätigungsvorsatz sowie zuvor verübte Delikte wegen Volksverhetzung und Körperverletzung an Migrantinnen und Migranten in einem europäischen Staat.

Er konnte sich während seines gesamten Gefängnisaufenthalts nicht in den Arbeitsprozess integrieren, lehnte bis zum Ende sämtliche Resozialisierungsangebote ab und verbüßte letztendlich seine Haftstrafe zur Gänze ohne anschließende Bewährungsauflagen. Eine fachärztliche Untersuchung attestierte ihm eine Persönlichkeitsstörung bei voller Zurechnungsfähigkeit. Die Person wies außer der Anlassverurteilung in dem europäischen Land noch weitere überwiegend einschlägige Verurteilungen sowie in Österreich vorwiegend Eigentumsdelikte und politisch motivierte Tathandlungen und Gewaltdelikte auf. Mehrere Delikte davon setzte er während des Strafvollzuges.

Aufgrund der wiederkehrend erfolgten emotionalen Entgleisungen und Sachbeschädigungen im Vollzug und insbesondere aufgrund der geäußerten Gewaltfantasien gegen politisch anders Denkende war konkret zu befürchten, dass der Mann erneut verfassungsgefährdende Angriffe begehen wird. Diese Tatsache bewog die Verfassungsschutzbehörden dazu, vor Haftentlassung eine Gefährderansprache durchzuführen und ihn nach seiner Entlassung weiterhin zu beobachten. Bald war offensichtlich, dass er eine extreme und konspirative Lebensweise an den Tag legt. Im Alltag mied er bewusst öffentliche Verkehrsmittel, verzichtete gänzlich auf die Verwendung eines Mobiltelefons und wohnte in einer Obdachloseneinrichtung einer Stadtgemeinde. Der rechtsextreme Delinquent fuhr regelmäßig in grenznahe Städte in ein Nachbarland Österreichs, wo er von öffentlich zugänglichen Computern seine rechtsgerichtete Ideologie vor allem im virtuellen Raum verbreitete. Die verwendeten Accounts wurden gesichert und der Sachverhalt bei der zuständigen Staatsanwaltschaft angezeigt.

In einem weiteren Fall verurteilte das LG Eisenstadt einen Rechtextremisten am 31. März 2022 wegen Verstoßes gegen die § 3g Verbotsgesetz (Wiederbetätigung im nationalistischen Sinn), § 283 StGB (Verhetzung), § 50 Waffengesetz (Unbefugter Besitz von Waffen der Kategorie B) und § 28a Abs. 1 Suchtmittelgesetz (Suchtgifthandel) zu einer unbedingten Freiheitsstrafe von drei Jahren und sechs Monaten.

Bereits im Jahr 2021 hatten intensive (Internet-)Recherchen auf die Spur dieses österreichischen Staatsbürgers geführt, der im Verdacht stand, Tatbestände nach dem Verbotsgesetz und der Verhetzung begangen zu haben. Zudem gab es Hinweise auf unbefugten Waffenbesitz. Im Zuge einer daraufhin angeordneten Hausdurchsuchung konnten zahlreiche Waffen, NS-Devotionalien sowie Sprengmittel sichergestellt werden. Der Verdächtige wurde noch am Tag der Hausdurchsuchung festgenommen. Er ist langjähriger Anhänger der rechtsextremen „Identitären Bewegung Österreich" (IBÖ) und führte mehrere Zahlungen auf das Konto der IBÖ sowie IBÖ-naher Vereine durch. Ebenso konnten diverse Demo- und Werbeutensilien bei dem Verdächtigen sichergestellt werden. Durch die Ermittlungen wurden zahlreiche Kontakte zu Mitgliedern der IBÖ festgestellt. Auch in Chatgruppen (WhatsApp und Telegram) der IBÖ war der Verdächtige sehr aktiv.

Bei der Sichtung eines sichergestellten USB-Sticks konnte ein Ordner mit der Bezeichnung „Nationale Wehrkraft" vorgefunden werden. Der Ordner beinhaltete detaillierte Anleitungen zum Bomben- und Waffenbau sowie eine Datei mit dem Namen „Freundes- und Feindesliste". Ebenso wurden Listen mit mehreren politisch links gerichteten Organisationen vorgefunden, die als Feinde beziehungsweise potenzielle Ziele geführt wurden. Außerdem ergab sich der Hinweis auf einen geplanten Anschlag auf das Volksstimmefest in Wien, ein traditionelles Pressefest der kommunistischen Wiener Monatszeitschrift. Auch wurden auf den USB-Sticks diverse islamfeindliche sowie rechtsextreme beziehungsweise neonazistische Bilder entdeckt.

Aufgrund der gewonnenen Erkenntnisse und der bei der Hausdurchsuchung vorgefundenen Waffen und Sprengmittel erhärtete sich der Verdacht der Vorbereitung einer nationalsozialistisch motivierten, rechtsterroristischen Straftat. Zudem wurde ein selbst angefertigtes Video vorgefunden, auf welchem bereits erfolgreiche Sprengübungen mit selbstgebauten Sprengkörpern durchführt wurden.

Aufgrund der Auffindung des im Haus vorgefundenen Lehr-/Handbuchs für Aktivisten, Extremisten und Terroristen des rechten Spektrums sowie der im Zuge der Hausdurchsuchung aufgefundenen Waffen und waffenähnlichen Gegenstände wurde die Schlussfolgerung gezogen, dass der Verdächtige alle Mittel zur Umsetzung eines rechtsextrem motivierten Anschlags hatte, sich gedanklich auch damit auseinandersetzte und lediglich durch die rechtzeitig erfolgte Festnahme an der Umsetzung des Vorhabens behindert wurde.

Nach der Verurteilung legte die Staatsanwaltschaft gegen das Urteil Berufung ein, da der von ihr angeregten Einstufung der besonderen Gefährlichkeit nicht gefolgt wurde. Das Oberlandesgericht Wien stellte nach neuerlicher Verhandlung mit Urteil vom

20. Oktober 2022 fest, dass beim Beschuldigten eine besondere Gefährlichkeit vorliegt und erhöhte die Verurteilung/Strafe auf fünf Jahre unbedingte Freiheitsstrafe.

2.1.1.4 Trends und Entwicklungstendenzen

Das Risiko rechtsextremistisch motivierter Tathandlungen und nachhaltiger Radikalisierung von Akteurinnen und Akteuren sowie Gruppierungen bleibt konstant erhöht. Eine besondere Gefährdung kann zudem von Mobilisierungen und Protestaktionen ausgehen, die durch gewaltbereite (rechtsextremistische) Personen initiiert, organisiert und getragen werden und die direkte Konfrontation mit dem ideologischen Gegner (zum Beispiel aus dem linken bis linksextremistischen Spektrum) suchen. Einen wesentlichen Einflussfaktor auf diesen Trend bildete das Corona-Demonstrationsgeschehen, welches Ende 2021 und Anfang 2022 in Österreich seinen zahlenmäßigen Höhepunkt zu verzeichnen hatte. Durch systematische Vereinnahmungsversuche des Protests seitens rechtsextremistischer Propagandisten konnten diese bislang kaum erreichbare Gesellschaftsschichten an ihr verfassungsgefährdendes Gedankengut heranführen. Vernetzungsstrukturen rund um einen bereits herauskristallisierten harten Kern dieser heterogenen Protestbewegung wurden ausgebaut, wodurch sowohl ein neues Mobilisierungspotenzial als auch ein erweitertes Publikum für rechtsextremistische, antisemitische und rassistische Narrative geschaffen werden konnten. Grundsätzlich ist festzustellen, dass die COVID-19-Pandemie Radikalisierungsprozesse, gekennzeichnet durch zunehmende Enthemmung zur Aggression, ausgeprägten Vertrauensverlust in Kerninstitutionen der Demokratie sowie durch Hinwendung zu extremistischen und staats- beziehungsweise demokratiefeindlichen Netzwerken in einer Weise förderte, welche diese Entwicklungen vermutlich langfristig nachwirken lassen.

Im Bereich des nationalsozialistisch inspirierten und gewaltbereiten Extremismus in Österreich zeigt sich teilweise die diskursive Einbettung in internationale Phänomene und Bestrebungen, die von der Absicht gekennzeichnet sind, den demokratischen Verfassungsstaat zu überwinden beziehungsweise dessen Niedergang revolutionär zu beschleunigen (Akzelerationismus). Charakteristisch für dieses Phänomen ist die propagandistische Verklärung rechtsextremer Terroranschläge im Ausland sowie – neben gruppenbezogener Menschenfeindlichkeit – das Propagieren der „white supremacy". Projektionsfläche dieser von rassistischen, antisemitischen oder minderheitenfeindlichen Narrativen geprägten Form extremistischer Agitation sind dabei der Staat beziehungsweise seine Vertreterinnen und Vertreter, das politische Gegenüber sowie Minderheiten. Online-Inhalte, die sich auf die Phänomen-Ausprägung „Siege Culture" berufen, bieten Echokammern, die zur Radikalisierung von Einzeltäterinnen und Einzeltätern führen können.

Die **„Siege Culture“** dient als ideologische Grundlage für neonazistische, zumeist rechtsterroristische Gruppierungen. Die „Siege-Ideologie“ hat ihre Ausgangslage im gleichnamigen Werk „Siege“ („Belagerung“) des rechtsextremen Autors James Mason, das mit seinen NS-verherrlichenden Ideologiefragmenten unter anderem die US-amerikanische rechtsterroristische Gruppierung „Atomwaffen Division“ und deren europäische Ableger maßgeblich beeinflusste. Das Werk besteht aus einer Textsammlung, welche Mason in Vertretung der Neo-Nazi-Organisation „National Socialist Liberation Front (NSLF)“ zunächst in Form eines Newsletters namens „Siege“ veröffentlichte. In den gebündelten Publikationen propagiert Mason politisch motivierte Gewalt bis hin zu terroristischen Akten als einzig legitimes Mittel zum Aufstand der weißen Bevölkerung gegen liberale, multikulturelle Gesellschaften, um den Zusammenbruch des vorherrschenden „Systems“ zu beschleunigen (=Akzelerationismus). Seine Ideen umfassen antisemitische, rassistische und antifeministische Grundansichten und zeugen vom Bestreben einer neuen, von der „weißen Rasse“ dominierten „Universal Ordner“. Sein schließlich veröffentlichtes Sammelwerk und dessen Aufruf zur Terrorgewalt für die ideologische Zielerreichung inspirieren bis heute den transnationalen militanten Neonazismus und Rechtsterrorismus, und werden von ihnen in einer Weise fetischisiert, dass sie gar zu einer „Kultur“ erhoben wurde.

Rechtsextremer Musik aus Österreich kommt weiterhin die Funktion als Rekrutierungs- und Ideologisierungsansatz zu. Sie bleibt ein ernstzunehmender Faktor der Bildung von Vernetzungsstrukturen und der Positionierung von Rechtsextremismus als „Lifestyle“.

Neben der Holocaustleugnung oder -relativierung bleiben auch die Kontaktpflege mit rechtsextremen Strukturen und Gruppierungen im Ausland und die daraus resultierenden Vernetzungsaktivitäten ein Aktionsfeld. Sich verstetigende Kooperationen können dabei auch zu einem Professionalisierungsschub der heimischen Szene führen. Weiters waren Ideologisierungs- und Rekrutierungsversuche, auch im Zuge ideologie-externer Diskurse (zum Beispiel COVID-19- oder Wissenschaftsskepsis) zu beobachten.

Seit dem weitgehenden Schwinden des gesellschaftlichen Interesses an der Pandemie erfolgt seitens der „Neuen Rechten“ eine Sondierung neuer Mobilisierungsmöglichkeiten. Nach der Wiederaufnahme von aktionistischen Protesten und Vernetzungsinitiativen auf nationaler und internationaler Ebene sowie dem erneuten Fokus auf altbekannte Kernbotschaften (zum Beispiel „Bevölkerungsaustausch“, „Remigration“) werden vorrangig die Migrations- und Asylpolitik, die Energiepolitik und vereinzelt auch noch die Gesundheitspolitik diskursiv besetzt. Insbesondere migrations- und asylfeindliche Inhalte werden verstärkt für potenzielle Mobilisierungsmomente verbreitet und darauf aufbauend propagandistische Aktionsformen umgesetzt und gerechtfertigt. Mit der Grunderzählung,

die „Massenmigration“ sei der Ursprung aller anderen Krisen (zum Beispiel Gesundheitskrise, Energiekrise), werden gezielte Versuche unternommen, gegenwärtige Proteste unter anderem gegen die Preissteigerungen auf den eigenen thematischen Schwerpunkt zu verlagern. Dadurch soll eine neue Plattform zur Generierung von maximaler Aufmerksamkeit geschaffen und der öffentlichkeitswirksame Diskurs zu eigenen Gunsten politisch beeinflusst werden.

Zur etwaigen Verschärfung der Lage können demnach gesellschaftliche Entwicklungen wegen der prekären Situation im Energie- und Wirtschaftssektor beitragen. Nachdem die Anti-Corona-Demonstrationen als Mobilisierungs- und Rekrutierungspool ausgeschöpft sind, ist eine Fokussierung auf die Energiekrise als neues Thema mit Protestpotenzial evident. Je nach weiterer Entwicklung der Lage um die Energieversorgung und die sozialen Auswirkungen der Teuerungen ist ein Trend zu verhältnismäßig größeren Protesten möglich. Angesichts der vermehrten Agitationen von neurechten Proponenten, die ebendieses Potenzial aufgreifen, ist davon auszugehen, dass diese mit dem Ziel verbunden sind, für eine „politische Wende“ ein Protestaufkommen in der Größenordnung wie zu Zeiten der Pandemie zu erreichen und für eigene Zwecke zu unterwandern. Eine vorrangig materielle Lageverschärfung durch die Energiekrise kann Verbreitung und Wirkungsgrad rechtsextremistischer Rhetorik in der Zivilgesellschaft verstärken. Wie schon in der Gesundheitskrise können – auf Basis von verschwörungsideologischen Deutungsmustern – die Bundesregierung, staatliche Organe und demokratische Institutionen zu alleinigen Verantwortungsträgern für die prekären Verhältnisse und somit zum Feindbild erklärt werden. Daher bergen mögliche Entwicklungen (etwa im Zusammenhang mit dem Kriegsgeschehen in Europa oder möglicherweise wieder notwendigen Pandemie-Schutzmaßnahmen) und deren Auswirkungen auf das öffentliche Leben, vor allem aber ihre Vereinnahmung durch rechtsextremistische Akteurinnen und Akteure und Gruppierungen, ein schwer kalkulierbares Risiko für die Sicherheitslage Österreichs.

Hinsichtlich des Krieges in der Ukraine lässt sich bei rechtsextremistischen Gruppierungen keine in sich geschlossene, einheitliche Positionierung für eine der beiden Kriegsparteien feststellen. Eindeutige Haltungen zugunsten einer Kriegspartei sind bei einzelnen Personen erkennbar und dürften auf mannigfaltigen, individuellen Motiven beruhen, die sich jedoch nicht in eine gemeinsame Position eines Gruppengefüges übersetzen lassen. Es gibt keine erkennbaren organisatorischen Vorgaben, wie sich die Anhängerschaft auszurichten oder wie sie zu agieren habe. Das individuelle Interesse an einer Ausreise in die Ukraine wird im Rechtsextremismus daher mit an Sicherheit grenzender Wahrscheinlichkeit auch künftig sehr gering ausfallen. Neben diesen Ambivalenzen wurde im Laufe des Geschehens der Ukraine-Krieg an sich in der Außenkommunikation auch nicht mehr thematisiert – bei neurechten Gruppierungen jedoch umso mehr dessen geopolitische Auswirkungen. Gegenwärtige Diskurse um erhöhte Energie- und Treibstoffpreise, Gaslieferungen, Ressourcenknappheit und die österreichische Neutralität werden narrativ

aufgenommen, aktionistisch verwertet und mit Migrations- und Asylthemen verknüpft. Auf diese Weise sollen sowohl das neue Mobilisierungspotenzial entsprechend genützt als auch gesellschaftliche Ressentiments verstärkt auf die Migrations- und Asylpolitik gelenkt und dahingehend geschürt werden.

2.1.2 Staatsfeindliche Verbindungen

Unter **„staatsfeindlichen Verbindungen"** versteht man jegliche Arten von Gruppierungen, die die Existenz der Republik Österreich, deren Institutionen sowie das System des Rechtsstaates nicht anerkennen. Das hoheitsrechtliche Handeln des Staates wird abgelehnt und zudem wird versucht, die in der Verfassung festgelegte Staatsform oder eine verfassungsmäßige Einrichtung der Republik Österreich oder eines ihrer Bundesländer zu erschüttern.

Im Zuge der COVID-19 Pandemie hat sich in Österreich eine **neuartige demokratieablehnende Szene** aus den heterogenen Protestgruppierungen der „Corona-Maßnahmen Gegner" und einigen Akteurinnen und Akteuren aus dem Milieu der Staatsfeindlichen Verbindungen entwickelt. Diskursiver und aktionistischer Ausgangspunkt für die Entstehung dieser Szene war der Protest gegen die Maßnahmen zur Eindämmung der COVID-19 Pandemie, wobei sich seit dem Frühjahr 2022 ein allmählicher Szenewandel abzeichnet. Dieser lässt sich vorrangig anhand einer themenmäßigen Entgrenzung sowie eines verstetigten Demonstrationsgeschehens erkennen. Ferner ist eine zunehmende nationale und internationale Vernetzung mit sogenannten „alternativen Medien" und Gruppierungen aus dem Spektrum des organisierten Rechtsextremismus und der Staatsfeindlichen Verbindungen für diesen Entwicklungstrend wesentlich.

2.1.2.1 Überblick

Die ideologische Haltung staatsfeindlicher Verbindungen, welche einerseits der Reichsbürgerideologie oder Naturrechtsableitungen entspringt, hat zum Ziel, staatsähnliche Parallelstrukturen zu errichten und diese Strukturen durch eine steigende Anhängerschaft wachsen zu lassen. Dazu wird versucht, ein eigenes Gewaltmonopol aufzubauen, um ebenjene eigenen Verwaltungs-, Rechts- und Hoheitskonstrukte durchsetzungsfähig zu machen. Schlussendlich wird der Zusammenbruch des derzeit bestehenden Systems herbeigesehnt, um die errichtete eigene Ordnung flächendeckend installieren zu können.

Anhängerinnen und Anhänger der **„Reichsbürger“** vertreten die Ansicht, dass das Deutsche Reich fortbestehe, da die Weimarer Verfassung von 1919 niemals abgeschafft worden sei. Gruppierungen, die den **Naturrechtsableitungen** folgen, erkennen ausschließlich das „Naturrecht“ beziehungsweise „Common Law“ als rechtswirksam an und lehnen die durch parlamentarische Abstimmungen erlassenen Gesetze des Rechtsstaates ab.

Einige der Gruppierungen, die in Österreich vor allem seit Beginn und Mitte der 2010er-Jahre versuchten beziehungsweise versuchen Fuß zu fassen, sind: „Staatenbund Österreich“, „International Common Law Court of Justice Vienna“ (ICCJV), „Global Common Law Court“ (GCLC), „Freeman Movement“ und „One People Public Trust“ (OPPT).

In ideologischer Hinsicht ist eine demokratieablehnende und anti-pluralistische Gesinnung in der Szene vorherrschend. Diese rekurriert auf rechtsesoterische bis rechtsextremistische Weltanschauungen und manifestiert sich prozesshaft in Form von Agitationen gegen das (gesellschaftliche) „System“. Gleichwohl lassen sich in der Szene verbreitete politische Grundeinstellungen und Wertevorstellungen nicht im Sinne eindimensionaler Klassifikationssysteme präzise zuordnen. Dies führt zu einer großflächigen Anschluss- und Anpassungsfähigkeit disponibler Ideologeme, die sich in äußerst heterogenen Mobilisierungs- und Rekrutierungsfeldern widerspiegelt. Folglich finden sich ideologische Berührungspunkte und inhaltliche Überschneidungen mit radikalen bis extremistischen Gruppierungen und Strömungen über das gesamte politische Spektrum hinweg.

2.1.2.2 Aktuelle Lage

Obwohl die Maßnahmen zur Bekämpfung der COVID-19-Pandemie im Jahr 2022 weitgehend beendet wurden, ergaben die Folgen des Ukraine-Krieges (unter anderem Teuerung, Energiekrise) ab Februar 2022 neue Herausforderungen für große Teile der österreichischen Bevölkerung. Insbesondere Sympathisantinnen und Sympathisanten der staatsfeindlichen Verbindungen konnten mit ihrer vornehmlich auf Verschwörungsideologien basierenden Kritik an politischen Institutionen ihre Ansichten einer breiteren Öffentlichkeit zugänglich machen.

Wie der unten beschriebene Fall („Wir das Volk“) zeigt, konnte seit dem Jahr 2020 – dem Beginn der Maßnahmensetzung der österreichischen Bundesregierung zur Bekämpfung der COVID-19-Pandemie – wieder ein Anstieg von Eingaben, Drohschreiben und Unterlassungsbefehlen an die österreichischen Behörden und Institutionen beobachtet werden. Im Berichtsjahr kam es verstärkt zu szenetypischen Behördeneingaben: Durch diesen sogenannten „Papierterrorismus“ versuchten Sympathisantinnen und Sympathisanten ihre

Abkehr vom „System“ zu bekunden und dem öffentlichen Verwaltungsapparat zu schaden. Auch die auf Aktivistinnen und Aktivisten der Szene zurückzuführende Verbreitung von Beiträgen mit gängigen staatsfeindlichen Narrativen, antisemitischen Verschwörungsideologien und gewaltaffinen Inhalten in sozialen Medien und Netzwerken konnte im Jahr 2022 vermehrt beobachtet werden.

Allerdings sind bis auf die unten beschriebene Ausnahme derzeit keine Anzeichen bemerkbar, dass sich mehrere Anhängerinnen und Anhänger der staatsfeindlichen Verbindungen organisieren und strukturierte Verbindungen gründen, wie sie in der zweiten Hälfte des letzten Jahrzehnts in Österreich in Form des „Staatenbundes Österreich“ und des „International Common Law Court of Justice Vienna“ in Erscheinung traten. Es scheint, dass die zum Teil mehrjährigen Haftstrafen für die Führungspersönlichkeiten dieser Verbindungen für das derzeitige Ausbleiben von Strukturen in der Szene ausschlaggebend waren. Zum einen fehlen nun die Führungspersönlichkeiten, die die staatsfeindliche Ideologie in die Bevölkerung transportieren und Menschen für ihre Gruppierungen rekrutieren und zum anderen erzielen die strafrechtlichen Verurteilungen eine generalpräventive Wirkung in der österreichischen Bevölkerung.

Eine weitere durch die Anti-Corona-Maßnahmen indizierte Veränderung war die Verlagerung der Szene ins Internet. Die diversen Theorien und pseudojuristischen Botschaften

wurden hauptsächlich via Telegram großflächig artikuliert. Auch die bis Anfang 2020 physisch stattfindenden Treffen und Stammtische wurden in der Folge online via Zoom abgehalten.

UKRAINE-KRIEG – Mit dem Beginn des Angriffskrieges Russlands gegen die Ukraine konnte vom Verfassungsschutz eindeutig eine Themenänderung innerhalb der demokratieablehnenden Szene in Österreich festgestellt werden. Das bis dahin vorherrschende Thema COVID-19 – mit all seinen Facetten von Verschwörungsideologien rund um das Virus bis hin zur Impfung und den von der Regierung gesetzten Maßnahmen zur Bekämpfung der Pandemie – wurde von der Kriegsthematik in Osteuropa abgelöst. Anders als in der Rechtsextremismus-Szene ist allerdings in der demokratieablehnenden Szene eine mehrheitlich pro-russische Meinungshaltung beziehungsweise eine Billigung der kriegerischen Handlungen durch Russland erkennbar. Der russische Präsident Wladimir Putin beziehungsweise der russische Staat an sich gelten seit langer Zeit als Vorbilder in der Szene. Somit ist es wenig verwunderlich, dass die internationalen Sanktionen gegen Russland von den Aktivistinnen und Aktivisten abgelehnt werden und die Problematik der Teuerung und der Energiekrise einen wichtigen Anteil in ihrer Argumentation einnimmt.

2.1.2.3 Fälle 2022

Bereits im August 2021 trat die staatsfeindliche Verbindung „Wir das Volk“ mit dem Verfassen und Übermitteln von typischen staatsfeindlichen Eingaben an Behörden erstmals in Erscheinung. Die Mitglieder der Gruppierung verfassten in den Folgemonaten 166 Drohschreiben, Unterlassungsbefehle und Anordnungen und versandten diese per Post und via E-Mail an österreichische Institutionen (konkret an Oberste Organe des Bundes und der Bundesländer). In diesen Schreiben wurden von der österreichischen Bundesregierung unter anderem die sofortige Beendigung der Anti-Corona-Maßnahmen und der Impfpflicht sowie die Öffnung der Grenzen zu den österreichischen Nachbarländern gefordert. Außerdem wurde suggeriert, dass der „Internationale Gerichtshof“ 75 führende Persönlichkeiten der sogenannten „COVID-Konzernherrschaft“ – unter anderem den CEO von Pfizer, die britische Monarchin Elizabeth II. und den kanadischen Premierminister Justin Trudeau – verurteilt und Enteignungsbefehle für diese Personen unterzeichnet hätte. Ebenfalls wurde in den Schreiben festgehalten, dass US-Präsident Joe Biden am 14. Jänner 2021 nicht angelobt worden sei und das US-Militär die Kontrolle über die Vereinigten Staaten hätte. Des Weiteren nahmen die Schreiben Bezug auf die selbsternannte „Königin von Kanada“, Romana Didulo, die eine führende Figur der kanadischen QAnon-Bewegung und der kanadischen Anti-Corona-Maßnahmen-Gegner ist. Diese trat auch öffentlich während der „Trucker-Proteste“ in Ottawa in Erscheinung. Die Verbreitung der Nachrichten an diverse Behörden wurde via dem Online-Messenger Telegram forciert: Dazu veröffentlichte die „Königin“ ihre Botschaften auf ihrem Hauptkanal, anschließend teilten Administratorinnen und Administratoren diese in den jeweiligen landeseigenen Kanälen, um sie an die dortigen Regierungen und Behörden zu übermitteln.

Nach einer Sachverhaltsdarstellung des Verfassungsschutzes in der Causa „Wir das Volk“ wurde die Einleitung eines Ermittlungsverfahrens gemäß § 246 Abs. 2 StGB (Staatsfeindliche Verbindungen) durch die Staatsanwaltschaft Klagenfurt angeordnet. Durch intensive Ermittlungshandlungen wurden die Täterinnen und Täter (Verfasserinnen und Verfasser der Eingaben) ausgeforscht. Insgesamt wurden sieben Täterinnen und ein Täter im Alter zwischen 55 und 62 Jahren von der DSN und den für Staatsschutz zuständigen Organisationseinheiten der Landespolizeidirektionen ermittelt. Die acht Beschuldigten wurden im Februar und März 2022 von den Staatsschutzbehörden zum Tathergang einvernommen. Des Weiteren wurden am 7. Juli 2022 – im Zuge des Joint-Action-Days der österreichischen Staatsschutzbehörden – bei den zwei Hauptbeschuldigten Hausdurchsuchungen an ihrer Heimatadresse durchgeführt. Nach diesen polizeilichen Maßnahmen wurde die Auswertung der sichergestellten Gegenstände, insbesondere elektronischer Datenträger, die das Verfassen und Versenden der Schreiben bestätigten, vorgenommen. Im zweiten Halbjahr 2022 wurden die Abschlussberichte an die Staatsanwaltschaft Klagenfurt übermittelt. Die acht Personen werden strafbarer Handlungen gemäß § 246 Abs. 2 StGB (Staatsfeindliche Verbindungen), §§ 15, 12, 302 StGB (versuchte Anstiftung zum Missbrauch der Amtsgewalt) sowie § 282 StGB (Aufforderung zu mit Strafe bedrohter Handlungen und Gutheißung mit Strafe bedrohter Handlungen) beschuldigt.

2.1.2.4 Trends und Entwicklungstendenzen

Die mehrjährigen Haftstrafen gegen führende Aktivistinnen und Aktivisten und das dadurch entstandene Machtvakuum haben die Szene in Österreich in den vergangenen Jahren nachhaltig geschwächt. Dennoch ist seit dem erneuten Aufkommen von staatsfeindlichen Verbindungen während der Corona-Pandemie ein kontinuierlicher Anstieg gruppenspezifischer Aktivitäten festzustellen.

Hinsichtlich der am 7. Dezember 2022 in Österreich, Deutschland und Italien durchgeführten Hausdurchsuchungen und Festnahmen im Milieu der „Reichsbürgerszene“ kam es in einschlägigen sozialen Medien und Netzwerken vereinzelt zu ablehnenden Reaktionen gegen das behördliche Vorgehen. Diese Reaktionen waren vorrangig von gezielten Verharmlosungen staatsfeindlicher Strukturen und Aktivitäten getragen. Nachhaltige Auswirkungen auf die heimische Szene zeichnen sich in diesem Kontext bislang nicht ab.

Ferner kann als Entwicklungstrend eine „Ökonomisierung“ der Szene angeführt werden. Diese manifestiert sich unter anderem in einem wachsenden Angebot einschlägiger Veranstaltungen. Derartige „Indoktrinationsveranstaltungen“ – die meist als kostenpflichtige Seminare beworben werden – dienen zur Rekrutierung neuer Mitglieder sowie zur Vermarktung von Scheindokumenten (beispielsweise „Delegiertenpässe“). In diesem Kontext wird das Propagieren der Thematik „Souveränität gegenüber dem Staat“ und eine damit verbundene Anstiftung zur Gründung von Initiativen, Vereinen und Plattformen mit staatsfeindlichen Agenden aktuell relevanter.

Aufgrund des Bedeutungsverlustes pandemiebedingter Diskurse ist davon auszugehen, dass staatsfeindliche Verbindungen künftig versuchen werden, ihre Argumentationslinien an tagespolitische Geschehnisse und gesellschaftliche Entwicklungen fortlaufend anzupassen, um neue Agitationsfelder zu erschließen und Mobilisierungspotenziale auszubauen. Dabei könnten bereits vorhandene Ressentiments gegenüber dem Staat und die in der Szene vorherrschende Ablehnung von demokratischen Einrichtungen, Institutionen und deren Repräsentantinnen und Repräsentanten weiter vertieft werden. In diesem Kontext zeichnet sich bereits ein Fortbestehen des „harten Kerns" der Szene sowie die Formierung neuer Radikalisierungs- und Rekrutierungsräume ab, die sich aufgrund von evidenten inhaltlichen Schnittmengen zu anderen (rechts)extremistischen Akteurinnen und Akteuren sowie Gruppierungen zunehmend etablieren.

Darüber hinaus könnten vorhandene Sympathien und ideologische Naheverhältnisse zu anderen staatsfeindlichen Akteurinnen und Akteuren – beispielsweise zur militanten „QAnon"-Bewegung in den USA – hiesige Aktivistinnen und Aktivsten zu gewalttätigem Aktionismus inspirieren. Allerdings lassen die im Beobachtungszeitraum festgestellten Entwicklungen nicht auf die Entstehung von bewaffneten, strukturiert operierenden Gruppen aus dem Milieu der staatsfeindlichen Verbindungen in Österreich schließen. Entsprechend ergibt sich aus der gegenwärtigen Gesamtbetrachtung ein moderates Gefahrenpotenzial für die Funktions- und Handlungsfähigkeit des Staates. Störungen der öffentlichen Ruhe, Ordnung und Sicherheit durch gewaltbereite Aktivistinnen und Aktivisten aus dem Spektrum der staatsfeindlichen Verbindungen sind jedoch weiterhin als Risiko zu bewerten.

2.1.3 Linksextremismus

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

2.1.3.1 Überblick

In Österreich umfasst der Linksextremismus mehrere Strömungen, die aufgrund ihrer Gewaltbefürwortung zur Durchsetzung ihrer ideologischen Wertvorstellungen Beobachtungsgegenstand des Verfassungsschutzes sind. Innerhalb der linksextremen Szene Österreichs gibt es zwar ideologische Differenzen, gemeinsame Kernthematik der politischen Agenda ist jedoch die Ablehnung des bürgerlich-kapitalistischen Systems, das von einer sozialistischen Staatsform oder einer herrschaftsfreien Gesellschaft abgelöst werden soll. Ebenso ist den Strömungen gemein, dass der demokratische (Rechts-)Staat

abgelehnt und dessen Demontage angestrebt wird. Die Gegenhaltung zum Faschismus ist ebenfalls eine gruppierungsübergreifende Verbindungslinie, die sich durch das gesamte Szene-Spektrum zieht.

Neben den marxistisch-leninistischen und trotzkistischen Gruppierungen sind in Österreich autonom-anarchistische Gruppierungen zu finden, die sich in losen Verbindungen sowie in der Regel kleinen Bezugsgruppen organisieren.

„Marxistisch-leninistische/trotzkistische Gruppierungen“ streben die politische Umgestaltung des vorherrschenden demokratischen Systems auf Basis eines Gedankengerüsts an, das dem Marxismus-Leninismus entspringt beziehungsweise folgen 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 jeglicher Freiräume, die der Selbstbestimmung dienlich sind. Dabei baut man ideologisch auf dem Anarchismus auf, der die Abschaffung jeglicher Herrschaft von Menschen über Menschen (insbesondere in Gestalt des Staates) beschreibt. Inhärent ist dabei, dass Gewalt befürwortet und aktiv gegen gegnerische politische Gruppen und staatliche Institutionen angewendet wird.

Hauptaktionsfelder des Linksextremismus sind Antifaschismus, Antikapitalismus, Antirassismus, Antimilitarismus, Antirepression sowie die Erlangung von „Freiräumen“. In jüngerer Zeit haben neben den „traditionellen“ Aktionsfeldern neue Agitations- und Handlungsbereiche (beispielsweise die Klima- und Umweltthematik, der Krieg in der Ukraine und sozioökonomische Krisen) Aktualität erlangt. Überdies sind Militanz und Gewaltakzeptanz der Aktivistinnen und Aktivisten als ein identitätsstiftendes, zentrales Element anzusehen. Hinsichtlich der in diesem Umfeld auftretenden Gruppierungen ist festzustellen, dass es sich überwiegend um auf kurz- und mittelfristige Dauer ausgerichtete Verbindungen handelt, die sich häufig mit dem Ziel der Umsetzung gewalttätiger Aktionen und Proteste vereinigen.

2.1.3.2 Aktuelle Lage

Im Vergleich zu den vergangenen Jahren lässt sich die Lage in Österreich im Berichtsjahr 2022 als konstant beschreiben. Im linksextremistischen Spektrum treten weiterhin autonom-anarchistische Gruppierungen am stärksten in den Vordergrund und sind maßgeblich an der Meinungsführung innerhalb der Szene beteiligt. Evident ist, dass es einen gewaltbefürwortenden Kern gibt, der jede Eskalation gutheißt oder gar herbeisehnt. Aktionen, die unter Umständen auch in der Begehung von Straftaten, wie etwa (schwere) Sachbeschädigungen, Widerstand gegen die Staatsgewalt oder Körperverletzungen, enden, richten sich gemäß der eigenen ideologischen Agenda gegen (staatliche) Repression, Faschismus, Kapitalismus und politische Gegnerinnen und Gegner.

Dementsprechend werden nicht nur Repräsentantinnen und Repräsentanten staatlicher Institutionen und (Sicherheits-)Behörden, wie beispielsweise Polizistinnen und Polizisten – die von linksextremen Agitatorinnen und Agitatoren als ausübender Arm des Rechtsstaates und damit als unterdrückende Staatsorgane wahrgenommen werden – zum diametral-positionierten Gegenpart erklärt. Auch deutschnationale Burschenschaften oder „Neue Rechte" zählen zu politischen Antipoden der Linksextremen. Unter der Prämisse, den Faschismus zu bekämpfen, wird den Szene-Exponentinnen und -Exponenten des rechtsextremen Spektrums unter anderem bei Kundgebungen und Demonstrationen und nicht zuletzt unter Anwendung von Gewalt entgegengetreten. Das Bestreben der Sicherheitsbehörden, die öffentliche Sicherheit bei derart gelagerten Zusammentreffen zu gewährleisten, wird vom linksextremen Spektrum als Repressionsversuch verstanden.

Auffallende Belege der hohen Gewaltbereitschaft des linksextremen Szene-Kerns in Österreich im Jahr 2022 waren einerseits ein Angriff gegen österreichische Sicherheitsbehörden durch einen schadens- und symbolträchtigen Brandanschlag auf sechs Dienstfahrzeuge sowie Sachbeschädigungen an Objekten der Sicherheitsbehörden; andererseits fanden gewaltsame Zusammentreffen zwischen linksextremen Szene-Angehörigen und neurechten Gruppierungen sowie mit deutschnationalen Burschenschaften statt, die schwere Sachbeschädigungen, Raufhandel und andere Gewalttaten nach sich zogen.

Markante Eckpfeiler des Vorgehens der österreichischen Exekutive und Justiz gegen das Gewaltpotential linksextremer Aktivistinnen und Aktivisten waren die Verurteilungen von sechs linksextremen Aktivisten wegen (schwerer) Körperverletzung.

UKRAINE-KRIEG – Besonders sozialpolitische und wirtschaftliche Ereignisse, die tiefgreifende Folgewirkungen auf das Alltagsleben haben, bergen hohes Mobilisierungs- und Aktionspotential für Extremistinnen und Extremisten. Deshalb bieten sozioökonomische Veränderungen wie jene, die durch den Angriffskrieg Russlands gegen die Ukraine ausgelöst wurden, neuen Nährboden für linksextreme Radikalisierung. Vorranging verschärft die zunehmende Teuerung, die sich mittlerweile durch alle Lebensbereiche zieht, die Argumentationsgrundlage gegen den Kapitalismus und für soziale Gleichheit. Aber auch

die durch den Konflikt entstandenen Flüchtlingsbewegungen, deren Einschätzungen seitens rechtsextremer Akteurinnen und Akteuren sowie der Umgang der Politik mit dem Thema, bringen vermehrt Diskurspunkte auf. So wird von der linksextremen Szene dazu aufgerufen, sich mit Flüchtlingen aus dem Kriegsgebiet zu solidarisieren, den Krieg zu verurteilen und Bewegungsfreiheit über jegliche (Staats-)Grenzen hinweg für alle, unabhängig von der Herkunft, zu fordern.

MILITANTE UMWELTGRUPPIERUNGEN – Die aktuell hoch polarisierenden Aktionen seitens militanter Umweltgruppierungen, die sich medienwirksam für den Klimaschutz einsetzen, finden in der linksextremen Szene Zuspruch. Aufgrund des Umstandes, dass ein erheblicher Teil der Aktionen durch Umweltgruppierungen in Gesetzesübertretungen münden, wird innerszenisch bei Linksextremen von „repressiver Kriminalisierung" der Klima-Aktivistinnen und Klima-Aktivisten durch die Sicherheitsbehörden gesprochen. Der Umfang der personellen Überschneidungen zwischen den militanten Umweltgruppierungen und der linksextremen Szene kann derzeit nicht belastbar verifiziert werden.

Militante Umweltgruppen traten im Jahr 2022 nicht nur in Österreich, sondern auch international mit aufsehenerregenden Aktionen stärker als in den Jahren zuvor in den Vordergrund. Ihren Ursprung haben diese Gruppierungen in den frühen 2010er-Jahren in Großbritannien. Thematischer Schwerpunkt sind der Klimawandel sowie umweltorientierte politische, soziale und wirtschaftliche Maßnahmen zur Eindämmung desselbigen.

Gruppierungen, die im Berichtszeitraum 2022 in Österreich in Erscheinung traten und mitunter das größte Personenpotential aufweisen, sind „Last Generation“ und „Extinction Rebellion“, zwei Organisationen, die Klimaschutz-Aktivismus betreiben, jedoch aktuell nicht als linksextrem eingestuft werden. Breit angelegte Verkehrsblockaden von Verkehrshauptachsen sowie Sachbeschädigungen durch Beschütten mit Farbe oder sich Festkleben von und an (Kunst-)Objekten oder Gebäuden stellen einen großen Teil der aktivistischen Aktionen in Österreich dar. Das Rekrutierungspotential ist aufgrund inhaltlicher Überschneidungen mit anderen Umweltgruppen und der starken medialen Präsenz als hoch einzustufen und wird durch die Möglichkeit, sich über das Internet in Echtzeit und grenzüberschreitend zu verbinden, erweitert.

2.1.3.3 Fälle 2022

Im Mai 2020 fand in der Wiener Innenstadt eine durch die IBÖ angemeldete Kundgebung zum Thema „Information über die Masseneinwanderung und Bevölkerungsaustausch“ statt. Beim Verlassen der Veranstaltung wurden vier Teilnehmer von mehreren vermummten und dunkel gekleideten Personen angegriffen, wodurch drei der vier angeführten Personen verletzt wurden. Ermittlungen führten zu einem einschlägig bekannten Linksextremisten. Aufgrund dieses Angriffs und eines weiteren Vorfalls im März 2020 – bei welchem der Verdächtige ebenfalls als einer der Täter eruiert und angezeigt wurde – wurde bei der Staatsanwaltschaft Wien eine Hausdurchsuchung sowie die sofortige Vernehmung beantragt. Bei der Hausdurchsuchung konnten szenetypische Kleidungsstücke und Poster sowie eine Jacke, die der Verdächtige beim Angriff im März 2020 mit an Sicherheit grenzender Wahrscheinlichkeit getragen hatte, vorgefunden werden.

Am 20. Oktober 2022 fand nach insgesamt vier Verhandlungstagen im Landesgericht für Strafsachen Wien die Urteilsverkündung statt. Sechs linke Aktivisten wurden wegen §§ 83 StGB (Körperverletzung), 84 StGB (Schwere Körperverletzung) sowie § 284 StGB (Sprengung einer Versammlung) in unterschiedlichen Konstellationen schuldig gesprochen und zu vier bzw. fünf Monaten bedingter Haftstrafe verurteilt. Ein Angeklagter wurde in allen Anklagepunkten freigesprochen.

Im Oktober 2022 wurde im Nahbereich einer Wiener Polizeiinspektion ein beißend übler Geruch wahrgenommen. Dieser konnte sowohl im Innenraum der Polizeiinspektion, in den davor geparkten Polizeifahrzeugen sowie im Gehsteigbereich bemerkt werden. Durch Polizeikräfte wurde festgestellt, dass eine übelriechende Flüssigkeit, vermutlich Buttersäure, gezielt durch einen oder mehrere unbekannte Täterinnen und/oder Täter verschüttet worden war. Die vor der Polizeiinspektion geparkten Streifenwagen waren aufgrund des Gestanks im Fahrzeuginneren für eine weitere Benutzung unbrauchbar. In weiterer Folge erfolgte die Spurensicherung vor Ort und die Kontaktaufnahme mit ortsansässigen Personen, um diese zu möglichen Wahrnehmungen vor Ort zu befragen. Im Zuge einer Bestreifung im Nahbereich konnten einige Standpunkte, die über genehmigte Videokameras verfügen, ausfindig gemacht und deren Aufzeichnungen sichergestellt

und ausgewertet werden. Relativ schnell lag der Verdacht nahe, dass es sich bei dem Vorfall um einen Vergeltungsschlag der linksextremen Szene handeln könnte: Zum einen aufgrund der zeitlichen Nähe zu der Verurteilung von sechs linksextremistischen Protagonisten und zum anderen aufgrund der Tatsache, dass Buttersäureanschläge schon in der Vergangenheit ein typischer Modus Operandi dieser Szene waren.

Nach Abschluss der kriminalpolizeilichen Ermittlungen wurde eine Anzeige gegen unbekannte Täter wegen §§ 105, 125, 126 StGB (Verdacht der Nötigung und der schweren Sachbeschädigung) an die Staatsanwaltschaft Wien erstattet.

2.1.3.4 Trends und Entwicklungstendenzen

Nach dem pandemiebedingten Abflauen der einschlägigen Aktivitäten der linksextremen Szene kam es im Jahr 2022 wieder zu teils aufsehenerregenden, dem linksextremen Spektrum zuordenbaren Tathandlungen. Die Aktivitäten und Mobilisierungspotenziale dieser Szene wurden im Berichtsjahr wieder stark von aktuellen politischen, wirtschaftlichen und gesellschaftlichen Entwicklungen und Ereignissen beeinflusst.

Szenetypisch ist weiterhin davon auszugehen, dass vom primären Aktionsfeld „Antifaschismus“ ein umfassendes Mobilisierungspotenzial im linksextremen Spektrum ausgehen wird. Neben den in den letzten Jahren evidenten Mobilisierungsschwerpunkten (beispielsweise dem Wiener Akademikerball) sind Aktivitäten, Veranstaltungen und Vereinsörtlichkeiten der „Neuen Rechten“ attraktive Angriffsziele einzelner Szeneproponenten. Ein weiterer Entwicklungstrend zeichnet sich im Zusammenhang mit den multiplen und längerfristigen Krisensymptomen in der Gesellschaft ab. Dazu zählen einerseits der russische Angriffskrieg auf die Ukraine sowie die inflationsgetriebenen Teuerungen der Lebenserhaltungskosten. Neben der Asylthematik rückt zudem auch das Thema Umweltschutz und Klimawandel immer mehr in den Agitationsfokus linksextremer Kräfte.

Es ist zu beobachten, dass aufgrund des nachhaltigen Rekrutierungsproblems in der linksextremen Szene die Klima-Protestbewegung und ihre teils heterogenen Splittergruppen als ein mögliches Reservoir zur Infiltrierung mit linksextremer Ideologie in Betracht kommen könnte. Hierbei kommen nicht selten weltanschauliche Formeln zum Tragen, die sich unter dem Begriff des „Klassenkampfes“ zusammenfassen lassen. Durch die Energiekrise und den russischen Angriffskrieg in der Ukraine geraten kritische Infrastrukturen als potenzielles Aggressionsziel linksextremer Aktivistinnen und Aktivisten in den Fokus, da diese für höhere Energiekosten und in weiterer Folge für die Steigerung der Lebenserhaltungskosten mitverantwortlich gemacht werden. Dies könnte auch zu einer Verstärkung der internationalen Vernetzung europäischer Linksextremistinnen und Linksextremisten führen.

In einer Gesamtbetrachtung stellt der Linksextremismus gegenwärtig keine ernsthafte Gefahr für die Funktions- und Handlungsfähigkeit des Staates dar. Für die öffentliche Ruhe, Ordnung und Sicherheit sind Teilbereiche des linksextremen Spektrums jedoch weiterhin als Risiko zu bewerten.

2.2 Islamistischer Extremismus und Terrorismus

„Islamismus“ ist ein Sammelbegriff für unterschiedliche politische Ideologien, die sich vorgeblich auf Ideen oder eine spezifische Interpretation des Islam stützen. All diesen Strömungen liegt die Ansicht zu Grunde, dass der Islam nicht nur als Religion, sondern als ganzheitliches System, das sowohl soziale, juristische, politische und wissenschaftliche Dimensionen beinhaltet, betrachtet werden muss und in dieser Form die einzige Quelle für eine politische Ordnung sein kann und sogar sein muss. Der islamistische Extremismus und Terrorismus ist stets von der Ideologie des „Islamismus“ getrieben, wodurch er sich von anderen Formen extremistischer und terroristischer Kriminalität unterscheidet.

Der Begriff **„Terrorismus“** ist nicht einheitlich wissenschaftlich definiert. Allgemein kann festgehalten werden, dass Terrorismus die bewusste Gewaltanwendung von nicht-staatlichen Akteuren gegenüber einer oder mehrerer Personen, einer Gruppe oder der Bevölkerung zur Erreichung politischer, ideologischer und religiöser Ziele ist.

„Islamistischer Extremismus“ bezeichnet eine religiös motivierte Form des politischen Extremismus, die danach strebt, jedes Individuum, die Gesellschaft und die bestehende Herrschaftsordnung nach islamistischen Idealen umzugestalten. Islamistischer Extremismus setzt im Gegensatz zum Terrorismus nicht notwendiger Weise die Bereitschaft zu extremistischer Gewalt voraus. Allerdings finden sich in islamistischem Denken Grundannahmen, die einer Gewaltbereitschaft förderlich sind: Hierzu gehört insbesondere eine rigorose Ablehnung bestehender Gesellschaftsordnungen. Islamisten und Islamistinnen wollen die Alternative einer islamisch legitimierten Diktatur unbedingt durchsetzen. Fehlt ihnen die politische und soziale Unterstützung, greifen Islamisten und Islamistinnen unter Umständen ebenso zu Mitteln der Gewalt. Der islamistische Extremismus tritt in Form von jihadistischen, salafistischen und legalistisch, radikal islamistischen Bewegungen auf.

2.2.1 Überblick

Dem islamistischen Extremismus liegt die (politische) Ideologisierung des Islam als allumfassendes Lebens-, Gesellschafts- und Herrschaftssystem zugrunde. Islamistischer Extremismus setzt nicht notwendiger Weise die Bereitschaft zu extremistischer Gewalt (Terrorismus) voraus; allerdings finden sich im islamistischen Denken Grundannahmen, die der Gewaltbereitschaft förderlich sein können. Hierzu gehört eine rigorose Ablehnung bestehender Gesellschaftsordnungen in der muslimischen wie auch der westlichen Welt. Diese sollen durch eine auf islamistischen Idealen basierende Herrschaftsordnung ersetzt werden. Auch das Konzept eines „wahren" Islams, der sich von anderen derzeit vertretenen Interpretationen des Islams abhebt, spielt eine wichtige Rolle. Je nach Ausrichtung innerhalb des Spektrums des islamistischen Extremismus unterscheiden sich die bevorzugten primären Methoden der unterschiedlichen Bewegungen, insbesondere in Hinblick auf die Ablehnung oder Akzeptanz bzw. Befürwortung von Gewalt unter gewissen Bedingungen bis hin zu terroristischer Gewalt als zentrales Mittel zur Durchsetzung der eigenen Ziele. Terroristische Attentate finden zumeist in der Öffentlichkeit statt und zielen bewusst auf willkürliche zivile Opfer ab, wodurch die Bevölkerung in Angst und Schrecken versetzt werden soll. Terrorismus kann somit als eine Form von politisch motivierter Gewaltanwendung in systematischer Form mit dem Ziel des psychologischen Einwirkens auf die Bevölkerung betrachtet werden.

2.2.2 Aktuelle Lage

Die Bedrohung durch das islamistisch-extremistische Spektrum in Österreich geht wie in den letzten Jahren primär von radikalisierten Einzeltäterinnen und Einzeltätern aus, welche interpersonelle Vernetzungen innerhalb der radikalisierten Szene im deutschsprachigen Raum aufweisen können. Trotz der territorialen Zurückdrängung der Terrororganisation Islamischer Staat (IS) in Syrien beziehungsweise im Irak im Jahr 2019 verfügt das Terrornetzwerk – im Vergleich zu anderen islamistisch-extremistischen Organisationen – immer noch über die höchste Strahlkraft auf radikalisierte Jugendliche und junge Erwachsene in Österreich.

TERRORORGANISATION IS – Die enorme Attraktivität des IS, die zu den Hochzeiten der Organisation im Jahr 2014/2015 unter anderem auf die Kontrolle weiter Teile Syriens und des Irak sowie auf die vermeintliche Wiedererrichtung des Kalifats zurückzuführen war, basiert zum gegenwärtigen Zeitpunkt vor allem auf der ideologischen Kompromisslosigkeit gegenüber allen Andersdenkenden außerhalb des eigenen ideologischen Zirkels. Teile der österreichischen islamistisch-extremistischen Szene zeichnen sich durch einen „takfiristischen" Ansatz aus, deren Anhängerinnen und Anhänger der festen Überzeugung sind, dass alle anderen Musliminnen und Muslime sowie Nicht-Musliminnen und Nicht-Muslime vom wahren Glauben abgefallen sind.

Der arabische Begriff **„takfir“** kann mit „für ungläubig erklären“ übersetzt werden und bezeichnet den Ausschluss aus der muslimischen Gemeinschaft (umma). Durch diesen Schritt wird die Person zum Apostaten und folglich zum Ungläubigen (kafir) erklärt. Im extremistischen Islamverständnis der Takfiristen kann als Konsequenz der bewaffnete Kampf gegen die vom Glauben abgefallenen Personen erlaubt oder sogar gefordert werden.

Unter der geistigen Führung des von März bis Oktober 2022 eingesetzten Kalifen Abu Hassan Al-Hashemi Al-Quraishi war der IS vor allem in Form seiner regionalen Ableger in Teilen West- und Zentralafrikas, dem Maghreb, der Arabischen Halbinsel und dem Nordkaukasus bis nach Südost-Asien aktiv.

Die **„Terrororganisation IS (Islamischer Staat)“** hat sich im Jahr 2003 im Kontext der US-Invasion im Irak aus der Gruppierung Tauhid wa-l-Dschihad unter der Führung des Jordaniers Abu Musab Az-Zarqawi entwickelt. In den ersten Jahren noch Teil des Al-Qaida Netzwerkes, spaltete sich die Gruppierung später von dem prominenten Ideologen Aiman Az-Zawahiri und der Al-Qaida ab. 2014 rief der damalige IS-Anführer Abu Bakr Al-Baghdadi über weite Teile Syriens und den Irak ein Kalifat aus.

FOREIGN TERRORIST FIGHTER (FTF) – Trotz der territorialen Zurückdrängung des IS in Syrien und im Irak im Jahr 2018 hat das Phänomen der sogenannten FTF – deren Ausreisebestrebungen die österreichische Sicherheitslage vor allem in den Jahren 2012 bis 2018 maßgeblich mitbestimmt hat – nach wie vor Auswirkungen auf die Bedrohungslage in Österreich. Personen mit jihadistischer Gesinnung, die von einer Ausreise abgehalten wurden, aus den Konfliktgebieten nach Österreich zurückgekehrt sind oder aus Haftanstalten entlassen werden, stellen ein anhaltendes Sicherheitsrisiko dar. Von diesen Personen kann aufgrund ihrer militärischen Ausbildung, ideologischen Indoktrinierung, möglicher Frustration, Traumatisierung und/oder Verrohung durch Gewalterfahrungen ein Gefährdungspotential ausgehen. Personen, die eine Haftstraße verbüßt haben, können darüber hinaus innerhalb ihrer Peer-Group mit einem besonderen Status versehen werden und in der Folge – insofern sie in die militante Szene zurückkehren –erheblich an Einfluss gewinnen. Auch wenn seit 2019 keine geglückten Ausreisen und seit 2021 keine Ausreisebestrebungen in die Konfliktgebiete Syrien und Irak vermerkt werden konnten,

sind lose ideologische Affiliationen zu internationalen Terrororganisationen – allen voran dem IS – nach wie vor ungebrochen.

Unter dem Beriff des **„Foreign Terrorist Fighter“** (FTF) werden Personen subsumiert, die in ein anderes Land reisen, um dort terroristische Aktivitäten in unterschiedlicher Form, wie zum Beispiel durch Teilnahme an Kampfhandlungen, Ausbildungen beziehungsweise Trainings oder Planungen, zu unterstützen.

INTERNET UND PROPAGANDA – Internationale und nationale Akteurinnen und Akteure sowie Gruppierungen aus dem islamistisch-extremistischen Spektrum haben über diverse YouTube-Kanäle, Messaging-Plattformen und soziale Medien eine umfassende Online-Präsenz entwickelt. So können für Extremismus empfängliche Personen kontaktiert, Finanzmittel akquiriert, Propaganda verbreitet und strategisch mit der eigenen Anhängerschaft kommuniziert werden. Der Erfolg der Terrororganisation IS liegt mitunter darin begründet, dass diese ihre Propaganda zielgerichtet auf Jugendliche beziehungsweise junge Erwachsene – unter Berücksichtigung von Sprache, Trends und Stil der Jugendkultur – ausgerichtet hat. Auch wenn seit der territorialen Zurückdrängung des IS ein Rückgang bezüglich der Propagandaaktivitäten zu verzeichnen ist, sind Jugendliche und junge Erwachsene – männliche wie auch weibliche – nach wie vor sowohl Empfängerinnen und Empfänger als auch selbst aktive Mitgestalterinnen und Mitgestalter jihadistischer Propaganda, indem sie Audio- und Videomaterial erstellen und verschicken. Hervorzuheben ist, dass salafistische Netzwerke – einschließlich gewaltbefürwortender Jihadistinnen und Jihadisten und Prediger ohne politischer Agenda – gleichsam ein Monopol auf Suchergebnisse und YouTube-Videos zum Thema Islam halten.[1] Salafistische Prediger, die ihre religiösen Abhandlungen in deutscher Sprache vortragen, vermitteln Authentizität und bieten Identifikationsmöglichkeiten für Jugendliche, da sie ihr dualistisches Islamverständnis in einer leicht verständlichen und Jugend-adäquaten Sprache wiedergeben und den gegenwärtigen Lebenskontext im deutschsprachigen Raum berücksichtigen. Da die Jugendlichen oft ein oberflächliches beziehungsweise gar kein religiöses Basiswissen aufweisen, können sie die teilweise sektiererischen und polarisierenden Abhandlungen der Prediger nicht (religions-)kritisch beurteilen. Im virtuellen Raum agierende Prediger und Muftis, sogenannte „Influencer Preacher“, verfügen daher gegenwärtig über eine ausgesprochen starke Anziehungskraft und ersetzen teilweise die Notwendigkeit der Konsultation von Predigern in Moscheen oder der Zugehörigkeit zu Islamverbänden.

Darüber hinaus vermögen die sozialen Medien die Vernetzung von ideologisch Gleichgesinnten zu begünstigen und zu beschleunigen. Dies führt dazu, dass sich Chatteilneh

1 Comerford, Milo; Ayad, Moustafa, Guhl, Jakob. Generation Z & Das Salafistische Online-Ökosystem: Executive Summary. 2021.

merinnen und -teilnehmer meist nur bei ihrem (oftmals schnell wechselnden) Usernamen kennen und sich die Beziehung zunächst auf den virtuellen Raum beschränkt. Aufgrund der Anonymität und der Kurzlebigkeit ihrer Accounts wird oft durch bestimmte religiös-ideologische Kurzformeln beziehungsweise Fragen zu Beginn eines Chats die ideologische Ausrichtung des Gegenübers abgefragt, um sicher zu gehen, dass man sich mit einem/einer wahren „Glaubensbruder/-schwester" austauscht.

BIOGRAFISCHE ASPEKTE UND MOTIVLAGEN – Das islamistisch-extremistische Milieu in Österreich, das seit vielen Jahren eher in wirtschaftlich schwächeren Schichten zu finden ist, wird im gegenwärtigen Kontext vor allem von relativ jungen Anhängerinnen und Anhängern extremistischer Glaubensauslegungen geprägt. Angehörige der sogenannten Generation Z – geboren zwischen 1995 und 2010 – treten verstärkt als Rezipientinnen und Rezipienten und/oder aktive Mitgestalterinnen und Mitgestalter extremistischer und terroristischer Online-Propaganda hervor. Auch wenn Anhängerinnen extremistischer Ideologien das Extremismusgeschehen in Österreich mitbestimmen – fast ein Drittel aller Foreign Terrorist Fighter sind Frauen – ist die Szene gegenwärtig stark von männlichen, jungen Erwachsenen geprägt. Hervorzuheben ist, dass – dem Zeitgeist dieser Generation entsprechend – vor allem junge Konvertitinnen und Konvertiten sowie Personen, die sich tiefergreifend mit der eigenen Religion befassen wollen, zur Beantwortung von Glaubens- und Identitätsfragen vermehrt das Internet als Medium zur Sinnsuche heranziehen. Die normierte Darstellung religiöser Sichtweisen, in Kombination mit dem fehlenden Kontakt zu Vergleichsgruppen oder -personen in der realen Welt, kann eine relativ zügig voranschreitende Radikalisierung initiieren.

Die Motivlagen, die bei der Radikalisierung von jungen Personen eine Rolle spielen, sind meist nicht monokausal erklärbar, sondern eng verwoben mit der persönlichen Lebenssituation der/des Einzelnen. Extremistische Akteurinnen und Akteure verstehen es, Entfremdungserfahrungen von Menschen zu instrumentalisieren, indem sie Halt, Wertschätzung und Zusammengehörigkeit vermitteln sowie Kanalisationsmöglichkeiten für Protest gegen soziales Unrecht, Provokation und Gewalt bieten. Diverse Push-Faktoren (wie Lebenskrisen, gefühlte oder tatsächliche Diskriminierungserfahrungen, prekäre Lebensverhältnisse) und Pull-Faktoren (wie Kanalisierung von Gewalt, Zugehörigkeit, Statusgewinn) können das Abgleiten in den religiösen Extremismus begünstigen.[2]

UKRAINE-KRIEG – Auf einschlägigen Webseiten jihadistischer Akteurinnen und Akteure sowie Gruppierungen wurden Appelle zur Ausreise an die Kriegsschauplätze der Ukraine wahrgenommen – unter der Voraussetzung, von der militärischen Ausbildung zu profitieren sowie Waffen für Attentate gegen die westliche Bevölkerung und Einrichtungen zu lukrieren. Eben jene Versuche der ideologischen Instrumentalisierung des Krieges blieben bislang in Österreich allerdings wenig erfolgreich. Bis zum gegenwärtigen Zeitpunkt

2 Hofinger, Veronika; Schmidinger, Thomas. Wege in die Radikalisierung. Wien: 2017.

können keine systematischen Ausreisebestrebungen von Personen des islamistisch-extremistischen Spektrums aus dem Bundesgebiet in die Ukraine wahrgenommen werden.

2.2.3 Fälle 2022

Wie sehr das Internet Radikalisierungsverläufe beeinflussen und verstärken kann, zeigt der Fall einer Gruppe junger Salafisten, die sich im Verlauf der Jahre 2021 und 2022 derart radikalisierten, dass sie Tathandlungen setzten, die von der Verbreitung islamistischer Propaganda und gefährlicher Drohung über ideologisch motivierte Sachbeschädigungen und Körperverletzungen bis hin zur Mitgliedschaft in einer terroristischen Vereinigung reichten. Das Internet und hier vor allem die sozialen Medien fungierten als Informationsquelle, da der überwiegende Teil der Jugendlichen nur über ein rudimentäres religiöses Wissen verfügte. Besonders beliebt sind in diesem Zusammenhang radikale, als Influencer agierende Prediger, die etwa mit TikTok- oder Youtube-Videos radikal islamistische Inhalte vermitteln, welche aufgrund ihrer Kürze leicht verständlich und dementsprechend einprägsam sind. Zudem werden die sozialen Plattformen als Kommunikationsmittel verwendet, wobei der Fokus einerseits auf dem Austausch von propagandistischen Inhalten zum Zwecke der Radikalisierung und andererseits bis zu einem gewissen Grad auch auf einem gegenseitigen „Imponieren“ liegt. Häufig werden der Besitz und das Versenden von Videos des IS als Ausdruck von „Mut“ und „Coolness“ verstanden und zur Erhöhung des eigenen Ansehens innerhalb der Freundesgruppe genutzt, ohne sich der strafrechtlichen Folgen bewusst zu sein.

Die Gruppe dieser jungen Salafisten war im Hinblick auf die ethnische Herkunft, das religiöse Bekenntnis, die Beziehungen untereinander und das Geschlecht als heterogen zu charakterisieren. So weisen die Personen zum Teil Migrationshintergrund auf, waren bereits muslimischen Glaubens oder sind konvertiert und neben langjährigen Freundschaften gibt es auch oberflächliche Bekanntschaften als Folge gemeinsamer Moscheebesuche. Demgegenüber sind die verbindenden Elemente das durchwegs junge Alter von 16 bis maximal 20 Jahren und die deutsche Sprache – zwei Komponenten, die sowohl die Ermittlungen als auch mögliche Präventionsansätze beeinflussen. Darüber hinaus ist die gemeinsame sprachliche Grundausrichtung für die starke Vernetzung innerhalb des deutschsprachigen Raums ausschlaggebend, der folglich zu einem gemeinsamen kriminalgeographischen Raum im Bereich des islamistischen Extremismus und Terrorismus wird.

Der Radikalisierungsprozess der angesprochenen Jugendlichen verlief in groben Zügen sehr ähnlich, wobei der Terroranschlag vom 2. November 2020 in Wien und die damit einhergehende Verarbeitung in der Gesellschaft in vielerlei Hinsicht eine Rolle gespielt haben dürfte: Sei es als Motivationsgrund, sich mit der eigenen religiösen Identität verstärkt auseinander zu setzen, sei es als Bestärkung eines bereits schwelenden Opfernarrativs oder auch einfach als Vorbild für die eigene persönliche Selbsterhöhung aufgrund bisher empfundener Diskriminierungs- beziehungsweise Außenseitererfahrungen. Auffallend ist,

dass bei all diesen Radikalisierungsverläufen online abrufbare Predigten von zum Teil seit Jahren inhaftierten Predigern immer noch konsumiert und besonders einprägsame Zitate graphisch neu aufbereitet weitergegeben werden.

Der vorliegende Fall weist mehrere Phasen auf, die eine fortgesetzte negative Steigerung im delinquenten Verhalten der Jugendlichen zeigen. Erste staatsschutzrelevante Handlungen beziehungsweise Verhaltensweisen wurden sowohl in der Öffentlichkeit als auch im Internet im Herbst 2021 evident – angefangen mit provokantem Verhalten kurz vor dem ersten Jahrestag des Terroranschlags von Wien. Hier wurde das Auftreten an sensiblen Örtlichkeiten im ersten Bezirk mit einem der islamistischen Szene angepassten äußeren Erscheinungsbild dazu benutzt, Leute vor Ort in Unruhe und Angst zu versetzen. Diese erwünschte Reaktion wurde auch später durch bestimmte Verhaltensweisen immer wieder absichtlich herbeigeführt. Ebenso weisen die Auftritte in den sozialen Medien dieses Muster auf, indem Propaganda der Terrororganisation IS offen geteilt wurde und Personen, die augenscheinlich nicht dem eigenen Wertekanon entsprechend handeln, (mit dem Tod) bedroht wurden.

Unbeeindruckt von kriminalpolizeilichen Interventionen im Rahmen der Strafprozessordnung (StPO) setzten die jungen Salafisten ihr Verhalten nicht nur fort, sondern schienen die Aufmerksamkeit der Sicherheitsbehörden für die Anhebung ihres Ansehens innerhalb der Gruppe zu nutzen. So wurde dem Verfassungsschutz auch bekannt, dass einzelne Personen dieser Gruppierung mit der ihnen geltenden Aufmerksamkeit der DSN beziehungsweise der Landespolizeidirektionen prahlten und dies als weitere Motivation sahen, ihr inkriminiertes Verhalten sogar zu steigern. In weiterer Folge kam es zu Verhaltensweisen, die den Straftatbestand der Verhetzung verwirklichten, sowie zu ideologisch motivierten Sachbeschädigungen, die zum Teil gefilmt und als Zerstörung von „Götzen“ einer salafistischen Argumentation unterworfen werden.

Der **demokratische Rechtsstaat** wird von Salafisten als **„Götzentum“** angesehen, weil er durch Akzeptieren und Anerkennen und/oder die Teilnahme an Wahlen „angebetet“ werden kann. Diese Götzenanbetung widerspricht im Verständnis der Salafistinnen und Salafisten ihrem strengen Monotheismus und ist für sie ein Ausdruck des „Unglaubens“. Gegenstände oder Gebäude, die als Teil oder Ausdruck einer als ideologisches Feindbild verstandenen, aufgeklärten, demokratischen Gesellschaft gelten, werden als Götzen wahrgenommen, deren Zerstörung folglich als legitim gilt.

Nachdem sich Hinweise auf ein mögliches Interesse an einer Nachahmungstat des Terroranschlags vom 2. November 2020 verdichtet hatten und die Gefährdung durch einzelne Personen aus der Gruppe – aufgrund ihres Manipulationsvermögens und ihrer führenden

Stellung oder ihrer Beeinflussbarkeit und psychischen Verfassung – gestiegen war, kam es zur Umsetzung weiterer strafprozessualer Maßnahmen wie Hausdurchsuchungen, Sicherstellungen und der Verhängung von Untersuchungshaft. In mehreren Fällen führten diese Maßnahmen und die damit verbundenen weiteren Ermittlungen schließlich zu Anklagen, unter anderem nach §§ 278b ff StGB.

Obwohl strafprozessuale Maßnahmen in diesem Fall kurz- bis mittelfristig zu einer Minimierung des Risikos beitragen konnten, ist die meist kurze Inhaftierung eines Teils dieser jungen Salafisten langfristig keine zufriedenstellende Lösung. Das junge Alter der betroffenen Personen eröffnet eine größere Bandbreite an deradikalisierenden und stabilisierenden Möglichkeiten, die mit dem Abschluss einer Ausbildung und dem Nachgehen einer geregelten Arbeit ihren Anfang nehmen könnten. Dies bedarf jedoch eines gesamtgesellschaftlichen Ansatzes und kann nicht ausschließlich im Verantwortungsbereich der Sicherheitsbehörden liegen.

2.2.4 Trends und Entwicklungstendenzen

Die vornehmlich regionale Ausrichtung der terroristischen Organisationen IS und al-Qaida sowie der mit ihnen affiliierten Gruppierungen bestand im Jahr 2022 fort. Der geografische Fokus terroristischer Aktionen lag insbesondere auf der Westafrikaregion, dem Irak, Syrien sowie Afghanistan. Im Jahr 2022 fanden folgende Führungswechsel statt: Im Februar verstarb der IS-Anführer Abu Ibrahim al-Hashimi al-Qurashi in Syrien im Zuge einer Operation von US-Spezialkräften. Sein Nachfolger, Abu Hassan al-Hashimi al-Qurashi, kam im Oktober ebenfalls in Syrien ums Leben und wurde von Abu Hussein

al-Husseini al-Qurashi beerbt. Im Juli wurde der Anführer der al-Qaida, Ayman al-Zawahiri, durch eine US-Drohne in Afghanistan getötet. Im Jahr 2022 wurde kein Nachfolger bekannt gegeben. Die besagten Führungspersönlichkeiten zeigen sich für die strategische Ausrichtung der Gesamtorganisationen verantwortlich, auch wenn die Zielsetzungen der zentralen Führungsriegen bisweilen wenig ausschlaggebend für regionale Entscheidungen sind. Das Jahr 2023 wird zeigen, welche strategischen Schwerpunkte die neuen Anführer setzen werden und ob eine Adaptierung in Richtung zentral organisierter Gruppierungen gelingen wird. Kurz- bis mittelfristig wird die regionale Ausrichtung der terroristischen Organisationen IS und al-Qaida jedoch mit hoher Wahrscheinlichkeit andauern.

Das Ziel, zukünftig erneut komplexe Terroranschläge in Europa anzuleiten, verfolgen sowohl der IS als auch al-Qaida. Die Gruppierungen priorisieren derzeit jedoch regionale Strategien und verfügen nicht über die nötigen operativen Kapazitäten. Eine baldige Verstärkung der gewaltaffinen Ausrichtung der Organisationen in Europa liegt jedoch im Bereich des Möglichen und könnte den Verfassungsschutz in Österreich schon bald vermehrt beschäftigen. Der Verfassungsschutz konnte im Jahr 2022 national und international beobachten, dass im Besonderen der IS erneut organisatorisch erstarkte, woraus sich auch Potenzial für zukünftige Terrorattentate entwickeln kann. Die strategische und operative Ausrichtung der genannten transnationalen, terroristischen Organisationen wirkt sich auch auf die Gefährdungslage in Österreich aus. Das größte Gefahrenpotenzial ging 2022 in Österreich weiterhin von radikalisierten Einzeltäterinnen und Einzeltätern sowie autonom agierenden Kleinstgruppen aus, die Anschläge ohne direkten Auftrag beziehungsweise Anleitung einer terroristischen Organisation ausführen. In den vergangenen Jahren wurden in Europa vermehrt Anschläge verübt, deren Täter keiner terroristischen Gruppierung zugeordnet werden konnten. Zugleich konnten jedoch auch Organisationsversuche in Österreich, die durch im Ausland aufhältige Islamisten angeleitet oder unterstützt wurden, beobachtet werden. Als Tatmittel werden auch künftig insbesondere Alltagsgegenstände mit hinreichender Schadenswirkung (hierzu zählen beispielsweise Messer und Fahrzeuge) Verwendung finden. Jüngste Tatvorgänge zeigen jedoch, dass auch Anschläge, die mit Schusswaffen begangen werden, weiterhin ein unverändert hohes Gefahrenpotenzial darstellen. Attraktive Örtlichkeiten für terroristische Aktionen werden auch im Jahr 2023 leicht zugängliche Menschenansammlungen mit hoher Öffentlichkeitswirkung darstellen. Terroristische Angriffe richteten sich in den letzten Jahren jedoch auch vereinzelt gegen Vertreterinnen und Vertreter staatlicher Institutionen.

Österreich zählt im Vergleich zu anderen europäischen Staaten zu jenen mit einer an der Einwohnerzahl gemessen überproportional hohen Anzahl an FTF. Diese Zahl ist zuletzt jedoch nicht weiter gestiegen. Im Jahr 2022 wurden dem österreichischen Verfassungsschutz keine Ausreisen in die ehemalige syrisch-irakische Konfliktregion aus Österreich bekannt. Da der IS das verlorene Gebiet auch im vergangenen Jahr nicht rückerobern konnte, werden auch im Jahr 2023 mit hoher Wahrscheinlichkeit weder Syrien noch der

Irak an Attraktivität für ausreisewillige Kämpferinnen und Kämpfer aus Europa gewinnen. Andere Regionen wie die Sahel-Zone oder Afghanistan könnten sich in Zukunft jedoch in interessante Jihad-Schauplätze für Europäerinnen und Europäer verwandeln. Eine solche Entwicklung scheint allerdings in naher Zukunft nicht wahrscheinlich, da die vor Ort aktiven Gruppierungen meist lokale Agenden verfolgen, die vorherrschenden Lebensbedingungen nicht dem europäischen Standard entsprechen und Reisen in die genannten Konfliktregionen aus Europa vergleichsweise schwierig sind. Höchstwahrscheinlich wird es im nächsten Jahr demnach zu keinen großen Ausreisebewegungen aus Europa kommen, sollte nicht eine neue Konfliktregion in einem Land, in welchem die Mehrheitsbevölkerung muslimischen Glaubens ist, entstehen. Nicht außer Acht zu lassen ist in diesem Zusammenhang der Umstand, dass derzeit zahlreiche österreichische Frauen und Kinder der FTF seit mehreren Jahren in Lagern für IS-Gefangene (beispielsweise Al-Hol in Syrien) leben. Diese Lager liegen einerseits in poltisch-militärischen Konfliktzonen, andererseits konnten Befreiungsversuche und Angriffe des IS auf diese Lager verzeichnet werden. Aus beiden Umständen ergibt sich die Gefahr eines Ausbruchs und einer damit verbunden unkontrollierten Rückkehr von IS-affinen österreichischen Staatsbürgerinnen und Staatsbürgern nach Österreich.

Eine bedeutende Rolle im Jahr 2023 wird zudem die Provinz Khorassan – eine Grenzregion zu Afghanistan – einnehmen. Der gleichnamige Arm des IS – ISKP („Islamic State – Khorasan Province“) – steht im Kampf gegen die Taliban in Afghanistan und ist seit spätestens 2018 aufgrund seiner letalen Anschläge gegen die Zivilbevölkerung bekannt. Im Zuge der US-Evakuierung in Kabul im Jahr 2021 töteten Anhänger des ISKP über 180 Personen. Seit 2022 kann ein Anstieg an Terrorattacken auf westliche Ziele im Ausland und auf den Westen selbst verzeichnet werden. Der ISKP fokussiert dabei zum einen auf higher-profile Targets, um internationale Aufmerksamkeit zu erhalten und das Taliban-Regime zu blamieren. Zum anderen hat die Organisation 2022 aktiv begonnen, Beziehungen mit der Diaspora in Europa aufzubauen. Aus Sicht des ISKP sind dabei bereits Messer-Angriffe (Lone-Wolf-Attacks) in Europa als Erfolg anzusehen.

Der Beginn des russischen Angriffskrieges gegen die Ukraine im Februar 2022 schürte Befürchtungen, dass dieser sich unmittelbar auf die terroristische Bedrohung in Europa auswirken könnte. Die ursprüngliche Hypothese bestand darin, dass der Krieg durch jihadistische Gruppierungen instrumentalisiert werden könnte, indem sich islamistisch-extremistisch eingestellte Personen den ukrainischen Freiwilligen-Bataillonen anschließen, dort eine Kampfausbildung und Schusswaffen erhalten, sich weiter radikalisieren und danach in ihre Heimatregionen zurückkehren, um terroristische Anschläge zu begehen. Obwohl es diesbezüglich Aufrufe gab, haben sich diese Befürchtungen für Österreich bisher nicht bestätigt. Auch aktuell sind keine Anzeichen ersichtlich, dass es diesbezüglich im nächsten Jahr große Änderungen geben und zu massiven, systematischen Ausreiseversuchen in das Kriegsgebiet kommen wird.

Die Inhaftierung bedeutender Führungspersönlichkeiten islamistisch-extremistischer Gruppierungen Österreichs in den vergangenen Jahren führte zum Entstehen eines Machtvakuums, das auch im Jahr 2022 nicht vollständig wieder gefüllt werden konnte. Allerdings konnten insbesondere Prediger, die primär Social-Media-Plattformen nutzen, um konservativ-islamisches beziehungsweise salafistisches Gedankengut zu verbreiten, in den vergangenen Jahren erfolgreich in dieses Vakuum vordringen und stellen damit ein vergleichsweise neues Phänomen im deutschsprachigen Raum dar. Die Videos dieser „Influencer Preacher" unterscheiden sich von herkömmlichen Aufzeichnungen von Predigten in zwei wesentlichen Aspekten: Zum einen nutzen diese Prediger die neuesten Technologien, um sich der Social-Media-Trends bestmöglich zu bedienen; zum anderen sind die veröffentlichten Online-Inhalte stark komprimiert. Hier folgt man dem Trend zu kurzen Videos, sogenannten Shorts beziehungsweise Reels, mit einer Abspiellänge von meist unter einer Minute. Die veröffentlichten Inhalte werden dadurch stark vereinfacht dargestellt. Die Hauptzielgruppe der Influencer Preacher ist die junge, internetaffine „Generation Z", die überdurchschnittlich viel Zeit auf Social-Media-Plattformen verbringt. Die Erstellung, der Konsum und die Verbreitung konservativ-islamischer und/oder salafistischer Online-Inhalte werden mit hoher Wahrscheinlichkeit auch im Jahr 2023 ein hohes Maß erreichen beziehungsweise weiter zunehmen. Durch den Konsum dieser verzerrten und vereinfachten Auslegung des Islam werden religiös und ideologisch nicht gefestigte Jugendliche und junge Erwachsene zu extremistisch und terroristisch motivierten Straftaten verleitet. Der Verfassungsschutz konnte dahingehend mehrere Personen im Jahr 2022 beobachten und beabsichtigte Gewalttaten verhindern.

In Verbindung damit konnte der Verfassungsschutz zudem beobachten, dass das Internet – vorwiegend Online-Plattformen und verschlüsselte Chatgruppen – als bevorzugter und nur schwer zu überwachender Raum für den Austausch islamistischer Gedanken (insbesondere von IS-Propaganda) und für die Organisationen islamistischer Aktionen verstärkt genutzt wird. Die gehäufte Nutzung kann dabei auch auf die COVID-19-Restriktionen zurückgeführt werden. Innerhalb dieses Raumes findet auch ein Großteil des Radikalisierungsprozesses statt, noch bevor die Personen im realen Leben in Erscheinung treten. Das Internet bietet dabei überdies die Möglichkeit einer einfachen und raschen bundesländer- und länderübergreifenden Vernetzung der Szene, womit ein zusätzliches Gefährdungspotenzial einhergeht. Haftanstalten gelten ebenso als Orte der Radikalisierung, an welchen Inhaftierte für jedwede Radikalisierung und Rekrutierung besonders anfällig sind. Der Prozess der Inhaftierung kann soziale und psychologische Mechanismen auslösen, die bei einzelnen Individuen eine ideologische Entwicklung hin zu einer radikal-islamistischen Weltanschauung begünstigen. Darüber hinaus verfügen Personen des islamistisch-extremistischen Spektrums, die eine Haftstrafe in Zusammenhang mit einem Terrorismusdelikt (§§ 278 ff StGB) verbüßt haben, über Prestige und können innerhalb ihrer Peer-Group bei Rückkehr in die militante Szene eine führende Rolle bei der Radikalisierung weiterer Personen einnehmen. Haftentlassungen, insbesondere von

Personen, die nach §§ 278 ff StGB verurteilt wurden, stellen daher weiterhin ein Risiko für die Sicherheit Österreichs dar.

Der Verfassungsschutz konnte im Jahr 2022 – wie bereits in der Vergangenheit – eine nicht unerhebliche Anzahl an Personen des islamistisch-extremistischen Spektrums in Österreich beobachten, die zu Studien- und Fortbildungszwecken insbesondere nach Saudi-Arabien und Ägypten gereist sind, um eine international anerkannte konservativ-islamische Ausbildung zu erhalten. Im letzten Jahr entwickelte sich – zusätzlich zu den bereits bekannten Studienorten – Mauretanien aufgrund der tendenziell konservativen Auslegung des Islam sowie der vergleichsweise geringen Lebenshaltungskosten zu einer bedeutenden Destination für die europäische islamistisch-extremistische Klientel. In naher Zukunft muss daher auch mit Ausreisen aus dem österreichischen Bundesgebiet nach Mauretanien gerechnet werden. Mit diesen „Studien-Reisen" geht insofern eine Gefahr für die österreichische Sicherheit einher, als über die Gelehrten eine konservativ- bis radikal-islamistische Ansicht des Islam in Österreich verbreitet und damit ein Nährboden für islamistische Aktionen geschaffen wird.

Das Gefahrenpotenzial, das von islamistisch-extremistischen Akteurinnen und Akteuren beziehungsweise Gruppierungen ausgeht, ist aufgrund der oben beschriebenen Tendenzen und Entwicklungen in Österreich als konstant erhöht zu bezeichnen, wenngleich jüngste Entwicklungen wie der Ukraine-Krieg bislang kaum unmittelbare Auswirkungen auf die Gefährdungslage hatten. Das erhöhte Risiko islamistisch-motivierter Aktionen wird somit auch im Jahr 2023 bestehen bleiben und ist insgesamt – auch mit Blick auf internationale Entwicklungen – im Zunehmen begriffen. Zudem können geopolitische Entwicklungen wie etwa die Entstehung neuer Konfliktregionen oder erstarkende terroristische Gruppierungen mit transnationaler Agenda mittel- bis langfristig sogar zu einem Anstieg des Gefahrenpotenzials führen.

2.3 Spionageabwehr und Cybersicherheit

2.3.1 Spionageabwehr

Unter „**Spionageabwehr**" wird im Wesentlichen die Bekämpfung und Aufklärung von staatlichen Handlungen verstanden, die einen Nachteil für das ausspionierte Land beziehungsweise einen Vorteil für die Auftragsnation zur Folge haben könnten. Mit gezielten Maßnahmen im Bereich der Spionageabwehr sollen mögliche Spionageangriffe rechtzeitig erkannt und der Schutz von staatlichen Geheimnissen sowie die Wahrung der eigenen Interessen ermöglicht werden.

2.3.1.1 Überblick

Im Vergleich zu anderen Phänomenbereichen ist die Bedrohungslage im Bereich der Spionageabwehr hinsichtlich Zielsetzung, Methodik oder Dimension nicht eingrenzbar. Abhängig von den staatlichen Interessen können demnach enorme Mittel für umfangreiche Methoden eingesetzt werden, die das Ziel verfolgen, verdeckt Informationen zu beschaffen oder die eigenen staatlichen Interessen durchzusetzen. Österreich ist als eine der führenden europäischen Industrienationen und Standort zahlreicher Unternehmen der Spitzentechnologie ein Zielgebiet für entsprechende Bemühungen durch Risikostaaten. Konkret erweisen sich – aus Sicht fremder Nachrichtendienste – dabei die günstige geografische Lage des Landes, seine Mitgliedschaft in der Europäischen Union sowie seine wissenschaftliche und wirtschaftliche Stärke als wesentliche Faktoren. Des Weiteren sind auf österreichischem Staatsgebiet eine Vielzahl an internationalen Organisationen und ausländischen Vertretungen eingerichtet, weshalb zahlreiche fremde Nachrichtendienste in Österreich sogenannte „Legalresidenturen" unterhalten. Diese Legalresidenturen weisen entweder einen offiziellen Charakter – beispielsweise in Form von Botschaften oder Generalkonsulaten – auf, spiegeln sich in halboffiziellen Vertretungen wie etwa Presseagenturen oder Fluggesellschaften wider oder können unter Umständen als getarnte beziehungsweise konspirative Residenturen eingerichtet sein. Auch die geltende Rechtslage in Österreich, hier konkret die zur Spionageabwehr sehr eingeschränkten rechtlichen Möglichkeiten des Verfassungsschutzes, aber auch die strafrechtlich geforderten Tatbestandsmerkmale, führen zu einem sehr hohen Aufkommen fremder Nachrichten- und Geheimdienste in unserer Republik.

Für den österreichischen Verfassungsschutz sind vor allem Staaten wie die Russische Föderation oder der Iran sowie türkische und chinesische Geheim- und Nachrichtendienste von Relevanz. Die Intensität der Operationen ist heutzutage gleichbleibend hoch. HUMINT, verdeckte Einflussnahmen, Desinformation, Wirtschaftsspionage sowie das Durchführen von Cyberangriffen zählen zu den methodischen Vorgehensweisen der Dienste. Auch der Einsatz von sogenannten „Illegalen" ist ein weiterhin gängiges Mittel.

Als **„Human Intelligence" (HUMINT)** wird die klassische Spionage bezeichnet, welche sich der Gewinnung von Erkenntnissen durch menschliche Quellen bedient.

Als **„Illegale"** bezeichnet man im nachrichtendienstlichen Sprachgebrauch Personen, die mit fremden Identitäten ausgestattet werden. Deren Einsatz stellt eine gezielte nachrichtendienstliche Methode dar, welche eine Vorbereitung und Durchführung über längere Zeiträume erfordert. Mittels Illegalen werden in weiterer Folge nachrichtendienstliche Operationen und Aufklärung unter bestmöglicher Verdeckung betrieben.

2.3.1.2 Aktuelle Lage

Die gegenwärtige Lage im Zusammenhang mit Spionageaktivitäten hat sich im Vergleich zu den Vorjahren nicht signifikant verändert und ist konstant hoch. Sowohl die Intentionen und Zielverfolgungen fremder Nachrichtendienste als auch einzelne Modi Operandi zeichnen sich durch lange Kontinuitäten aus und blieben deshalb weitestgehend konstant. Lediglich der Ukraine-Krieg stellt die Verfassungsschutzbehörden auf internationaler Ebene aktuell vor mehrdimensionale Aufgaben und Problemstellungen, die vereinzelt mit Aktivitäten der Nachrichtendienste Russlands verstrickt wirken.

Die unerlaubte und verdeckte Beschaffung und Aneignung von nur eingeschränkt zugänglichen Informationen und Wissen ist nach wie vor ein wesentliches und wichtiges Instrument einzelner Länder, um die eigenen Interessen verfolgen und Ziele erreichen zu können. Nationale Intentionen divergieren oftmals deutlich zwischen den verschiedenen Staaten, wenngleich die Hintergründe für Spionageaktivitäten in der Regel der Aufklärung innenpolitischer, außenpolitischer, wirtschaftspolitischer und/oder verteidigungspolitischer, und aufgrund der Kriegssituation in der Ukraine, auch sicherheitspolitischer Themen dienen und hinsichtlich strategischer Zielsetzungen in jedem Fall eine Übervorteilung anderer Parteien und Interessenslagen zum Ziel haben. Nachrichtendienstliche Aufklärung und geheimdienstliche Operationen können dabei wichtige Bestandteile langfristiger staatlicher Strategien sein, deren Wirkung meist eine deutlich größere Tragweite aufweist, als dies ein erster Blick vermuten lässt. Dabei ist auch ein Vorrücken in verschiedene gesellschaftliche Bereiche denkbar; so können einer Ausspähung der im Ausland befindlichen Diaspora ebenso längerfristige Intentionen zugrunde liegen wie einer vorausschauenden Errichtung und Installation von Illegalen.

Zusätzlich bietet Österreich aufgrund seiner exponierten Stellung in den Bereichen Industrie und (Hoch-)Technologie sowie eines entsprechend breiten Forschungssektors ein denkbar lohnendes Aufklärungsziel für fremde Nachrichtendienste. Dabei ist eine enge Verbindung zu anderen Phänomenbereichen wie Proliferation und Waffenhandel festzustellen, zumal mehrere Staaten durchaus ihre Dienste dazu nutzen, gezielt Aufklärungsarbeit und Informationsabschöpfung zu betreiben, um relevante Güter für die eigenen Rüstungsbestrebungen unrechtmäßig und verdeckt zu beschaffen.

Es ist davon auszugehen, dass sämtliche Staaten nachrichtendienstliche Aufklärung im Ausland betreiben. Im Fokus des Verfassungsschutzes stehen aufgrund ihrer Aktivitäten jedoch insbesondere die verschiedenen Nachrichtendienste Chinas, des Irans, der Türkei und – vor allem aufgrund derzeitiger geopolitischer Entwicklungen besonders in den Fokus der Staatengemeinschaft gerückt – der Russischen Föderation.

UKRAINE-KRIEG – Der nach wie vor anhaltende Angriffskrieg Russlands gegen die Ukraine birgt mehrere Bedrohungslagen für die westliche Welt und damit auch für Österreich, die eine nachrichtendienstliche Einwirkung Russlands annehmen lässt. Vor

allem im Zusammenhang mit Ausweisungen von russischem diplomatischem Personal aus Europa - auch aus Österreich - sowie mit Sanktionierungen als Antwort auf Russlands Handeln sind mögliche Entwicklungen und Auswirkungen noch nicht gänzlich abschätzbar. Zumindest ist aufgrund der Sanktionen von einem Anstieg an Wirtschaftsspionage in Europa und auch Österreich auszugehen, um die Auswirkungen verschlossener legaler Kanäle am Weltmarkt abfedern und notwendige Güter für die eigenen Rüstungsbestrebungen trotz Exportkontrollen weiterhin beschaffen zu können.

Neben einer fordernden Rolle russischer Nachrichtendienste zur militärisch-strategischen und außenpolitischen Informationsbeschaffung im unmittelbaren Krisengeschehen ist die russische Nomenklatur seit Ausbruch des Konflikts um gelenkte und deutlich einseitige Berichterstattung im eigenen Interesse bemüht. Dabei war nicht nur die Außenwirkung Russlands im internationalen Kontext von Bedeutung, sondern vorrangig auch die kanalisierte Information beziehungsweise Beeinflussung der eigenen Bevölkerung. Eine direkte Einwirkung russischer Nachrichtendienste in Desinformationskampagnen, Steuerung russischer Medien und von russischen Medienportalen sowie eine Diffamation von Gegnern – damit sind sowohl die Feinde im direkten Kriegsgeschehen selbst gemeint, als auch die NATO als Sinnbild der westlichen Welt – ist damit anzunehmen.

Ebenso ist nicht auszuschließen, dass russische Nachrichtendienste die anhaltenden Flüchtlingsbewegungen für eigene Interessenslagen verwenden. Wenngleich die gezielte Schleusung von Personen durchaus zu den Praktiken von Nachrichtendiensten zählt, sind

im Zusammenhang mit dem Ukraine-Krieg und den daraus resultierenden Flüchtlingsbewegungen bislang keine entsprechenden Fälle bekannt.

Abseits des Krieges zeichnet sich im Zusammenhang mit anderen ausländischen Nachrichtendiensten wenig Änderung hinsichtlich Zielverfolgung und Agieren ab, wenngleich sich die eingesetzten nachrichtendienstlichen Methoden dem technischen Fortschritt angepasst haben und weiter anpassen. Daraus ergibt sich eine Verschränkung mit dem Bereich der Cyberkriminalität. Generell kann gesagt werden, dass Intentionen und Bestrebungen einzelner Länder zum eigenen Machterhalt und Machtausbau beziehungsweise zum Machtabbau anderer durch nachrichtendienstliche Aktivitäten vorangetrieben oder zumindest befeuert werden. Plakativ ersichtlich wird dies anhand von Wahlbeeinflussungen im Ausland. Besonders gesellschaftlich herausfordernde Zeiten, geprägt von Krieg, Krisen, Rezession und Unzufriedenheit der Bevölkerung, bieten Nachrichtendiensten zudem eine größtmögliche und bestmögliche Angriffsfläche, um direkt oder indirekt auf gesellschaftliche Themen einzuwirken, die diesbezügliche Entwicklung durch gezielte Einflussnahme im Sinne der eigenen strategischen Staatsinteressen zu beeinflussen und mittels Spionage, Abklärung und Infiltration einen nicht unwesentlichen Teil zum Machtausbau beziehungsweise zu einer Machtverschiebung zu leisten.

2.3.1.3 Fälle 2022

Die DSN führte im Jahr 2022 in enger Zusammenarbeit mit internationalen Partnerdiensten und der Justiz ein Ermittlungsverfahren gegen einen Beschuldigten wegen des Verdachts der Unterstützung eines geheimen Nachrichtendienstes zum Nachteil Österreichs gemäß § 256 StGB durch. Der Beschuldigte stand im Verdacht, Informationen an den russischen militärischen Geheimdienst GRU (Glawnoje Raswedywatelnoje Uprawlenije) weitergegeben zu haben. Es konnten zahlreiche Kontakte zu in Europa stationierten russischen Diplomaten im Aktiv- als auch im Ruhestand, die an Botschaften, Konsulaten oder an zwischenstaatlichen Organisationen tätig sind oder tätig gewesen waren, nachgewiesen werden. Für den Austausch von Informationen wurden konspirative Örtlichkeiten im Stadtgebiet von Wien genutzt, wobei auch diplomatisches Personal der Russischen Föderation im engen zeitlichen und örtlichen Zusammenhang identifiziert werden konnte.

Die **Übergabeorte** sind durch Vereinbarungen oder meist unscheinbare Markierungen nur dem Absender und dem Empfänger bekannt beziehungsweise erkennbar und dadurch vor der Entdeckung durch Nichteingeweihte geschützt.

Bei dem russischstämmigen Beschuldigten handelt es sich um den Sohn eines ehemaligen Nachrichtendienstmitarbeiters des russischen Militärgeheimdienstes GRU, der zu seiner aktiven Dienstzeit als Diplomat in Deutschland und in Österreich stationiert war. Der Beschuldigte soll eine militärische Spezialausbildung in Russland absolviert haben. Durch den Besitz des russischen wie auch griechischen Reisepasses wurde ihm die uneingeschränkte Reisefreiheit innerhalb der Europäischen Union sowie nach Russland und Belarus ermöglicht. Diese Reisefreiheit nutzte er, um im Zeitraum von 2018 bis Anfang 2022 in Summe 65 Reisen ins innereuropäische Ausland sowie nach Russland, Belarus, Georgien und in die Türkei anzutreten. Besondere Bedeutung kommt hierbei der Reise nach Moskau von Mitte Februar bis Anfang März 2022 zu, da am 24. Februar 2022 die militärische Invasion der regulären russischen Streitkräfte in die Ukraine begann. Hieraus leitet sich aus nachrichtendienstlicher Sicht der Verdacht ab, dass der Verdächtige als geführte Quelle seinen Verbindungspersonen in Moskau möglicherweise Informationen aus Österreich und dem zentraleuropäischen Raum überbrachte.

Es wird davon ausgegangen, dass derartige Rückholungen von im Ausland geführten Quellen zur Informationssammlung betreffend außenpolitische, gesamtgesellschaftliche und/oder sicherheitspolitische Diskurse innerhalb der Bevölkerung, der Politik und der Medien genutzt werden. Derartige Informationen erscheinen notwendig, um im Vorfeld von geplanten militärischen Operationen mögliche Reaktionen des Auslands besser abschätzen zu können.

In einer Gesamtschau betrachtet und insbesondere aufgrund seiner Kontakte, Reisebewegungen und mutmaßlich verwendeter Kommunikationsmittel besteht der begründete Verdacht, dass der Beschuldigte an den russischen Militärgeheimdienst Informationen übermittelte, durch deren Kenntnis vitale Interessen der Republik Österreich gefährdet wurden. Das Ergebnis des kriminalpolizeilichen Ermittlungsverfahrens wurde in einem Abschlussbericht an die Staatsanwaltschaft Wien übermittelt, welche derzeit prüft, ob Anklage zu erheben sein wird. Die Erfahrungen des Verfassungsschutzes der letzten Jahre zeigen, dass einzelne nachrichtendienstliche Verhaltensweisen sehr oft auf eine Weise passieren, die auf den ersten Blick nicht per se auf ein inkriminiertes Verhalten hindeuten und dieses nur in der Gesamtschau erkennen lassen. Die macht die strafprozessuale Ermittlung in der Spionageabwehr zur Königsklasse der nachrichtendienstlichen und kriminalpolizeilichen Arbeit.

2.3.1.4 Trends und Entwicklungstendenzen

Auf globaler Ebene äußert sich die nachrichtendienstliche Bedrohung dadurch, dass revisionistische Akteurinnen und Akteure versuchen, die unipolare Weltordnung („Pax Americana“) durch eine multipolare Weltordnung gleichrangiger Mächte zu ersetzen.

Auf regionaler Ebene sollen dabei die innereuropäische Kohäsion sowie die NATO- beziehungsweise EU-Verteidigungsstruktur geschwächt und die transatlantischen Sonderbeziehungen diskreditiert werden.

Auch der Ukraine-Krieg zieht weitreichende Folgen nach sich – nicht zuletzt auf nachrichtendienstlicher Ebene. Es wird von einer allgemeinen Bedeutungszunahme der Thematik für Europa ausgegangen. Ein auch für Österreich relevantes Gefährdungspotenzial wird sich durch die potenzielle Zunahme verdeckter nachrichtendienstlicher Aktivitäten ergeben – mit der Einschränkung der operativen Handlungsfähigkeit von Nachrichtendiensten im Ausland aufgrund der erfolgten Ausweisung von diplomatischem Personal.

Die Bedeutung der Republik Österreich im nachrichtendienstlichen Kontext ist aufgrund ihrer geografischen Lage, als Sitz multilateraler Organisationen, ihrer Rolle als EU-Mitglied und NATO-Partnerland sowie ihrer Funktion als Wirtschafts- und Forschungszentrum evident und wird aufgrund dessen als operativer Standort künftig an Bedeutung gewinnen. Es muss daher mit einer Zunahme an diplomatischem Personal in multilateralen Organisationen gerechnet werden, das jedoch auch nur mit größerem Aufwand ausgewiesen werden kann.

Als größte Herausforderung können Anwerbungsversuche von Informationsbeschaffungsquellen sowie Versuche der Einflussnahme zur Manipulation der westlichen Gesellschaften und Schwächung beziehungsweise Destabilisierung der politischen Situation des Ziellandes durch ausländische Nachrichtendienste sowie der Einsatz sogenannter „Illegaler“ erachtet werden. HUMINT-Methoden (wie etwa die Rekrutierung), Cyber-Operationen, Desinformationskampagnen oder wirtschaftliche Einflussnahme werden zudem zum Beziehungsaufbau genutzt, der in weiterer Folge der Sammlung vertraulicher Informationen dient.

In der Gesamtbetrachtung ist davon auszugehen, dass Österreich aufgrund der beschriebenen Faktoren auch weiterhin als Zentrum für nachrichten- und geheimdienstliche Tätigkeiten fremder Mächte dienen wird und der Einfluss auf Österreich im diesem Kontext steigen wird.

Die relevanten Akteure bleiben grundsätzlich gleich. Neben Russland sind auch Länder wie der Iran, China und die Türkei in Österreich aktiv. Im Jahr 2023 können sich die Bedrohungen wie folgt konkretisieren:

Russland ist durch die europaweite Ausweisung von Diplomatinnen und Diplomaten geschwächt und wird in den kommenden Jahren wieder operative Schlagkraft aufbauen müssen, wobei von einem größeren Gebrauch sogenannter „Non Official Cover“ ausgegangen werden muss. Dies bedeutet, dass nachrichtendienstliches Personal nicht unter dem Schutzmantel der Diplomatie in Österreich aktiv sein wird.

Der Iran und China werden ihre geopolitischen Machtansprüche und vor allem ihre Kontrolle über die Diaspora in Österreich weiterführen. Der Iran ist aufgrund der Unruhen und Proteste im eigenen Land verstärkt bemüht, die im Ausland lebenden Dissidentinnen und Dissidenten sowie Regimekritikerinnen und Regimekritiker aufzuklären. China hingegen hat zusätzlich zur Kontrolle der Diaspora noch einen starken Fokus auf Wirtschaftsspionage im Hochtechnologiebereich.

In der Türkei stehen richtungsweisende Wahlen an. Der Wahlkampf wird aus der Türkei nach Europa getragen und auch in Österreich stattfinden. Türkische Nachrichtendienste agieren in diesem Kontext einerseits als Verbinder von Personen in Österreich und der Türkei, andererseits können sie auch eingesetzt werden, um kritische Stimmen im Ausland zu erkennen und aufzuklären.

2.3.2 Cybersicherheit

Unter dem Begriff **„Cybersicherheit“** werden im Wesentlichen alle Maßnahmen verstanden, mit denen der Schutz von Netz- und Informationssystemen, der Schutz von Bedarfsträgerinnen und Bedarfsträgern solcher Systeme sowie der generelle Schutz der Bevölkerung vor Cyberbedrohungen gewährleistet werden soll.

2.3.2.1 Überblick

Der technische Fortschritt und der sich beschleunigende digitale Wandel prägen so gut wie alle Bereiche des gesellschaftlichen Zusammenlebens. Neben den zahlreichen Möglichkeiten und Vorteilen, die diese Entwicklungen schaffen, stellt die voranschreitende Digitalisierung insbesondere die Sicherheit vor große Herausforderungen. Die sichere Abwicklung sämtlicher Handlungen im Cyberraum gewinnt daher immer mehr an Bedeutung.

Cyberangriffe sind kriminelle Handlungen, bei der Täterinnen und Täter verhältnismäßig kostengünstig agieren können und sich in größtmöglicher Anonymität und somit in Sicherheit wiegen.

Im Cyberbereich fallen in erster Linie die Bearbeitung von Cyberbedrohungen durch fremde Nachrichtendienste sowie die Aufklärung von Cyberangriffen gegen verfassungsmäßige Einrichtungen, kritische Infrastrukturen oder internationale Organisationen in das Zuständigkeitsgebiet des Verfassungsschutzes.

2.3.2.2 Aktuelle Lage

Die Cybersicherheit ist eng mit dem weltweiten Phänomen der rasch voranschreitenden Digitalisierung verbunden. Durch die zunehmende Nutzung der Computertechnologie

und die sich ständig erweiternde digitale Vernetzung sämtlicher Bereiche des täglichen Lebens nehmen auch die Gefahren in diesem Bereich ständig zu.

Aktuell bestehen **verschiedene Arten von Cyberbedrohungen**, gegen die es sich zu schützen gilt. Zu den häufigsten zählen **Ransomwareangriffe**, die Systeme verschlüsseln und für den Zugriff auf Daten eine Lösegeldzahlung verlangen. Ferner der **Phishing-Betrug**, bei dem gefälschte E-Mails oder Websites verwendet werden, um Menschen dazu zu bringen, vertrauliche Informationen preiszugeben, sowie **„Distributed Denial-of-Service" (DDoS)-Angriffe**, bei denen eine Website oder ein Netzwerk mit Datenverkehr überflutet wird, um diese für Benutzerinnen und Benutzer unzugänglich zu machen.

Andere Bedrohungen umfassen Netzwerkangriffe, bei denen Angreiferinnen oder Angreifer unbefugten Zugriff auf ein Netzwerk erlangen, Spionageangriffe, bei denen vertrauliche Informationen gestohlen oder offengelegt werden sowie Insider-Bedrohungen, bei denen aktuelle oder ehemalige Mitarbeiterinnen oder Mitarbeiter einer Organisation ihre Zugänge nutzen, um Schaden anzurichten.

Ransomware entwickelte sich in den letzten Jahren zu einer zunehmend verbreiteten und für die Täterschaft lukrativen Bedrohung. Ein dieses Wachstum fördernder Faktor ist die steigende Komplexität der Angriffe: Die Tragweite von Ransomwareangriffen hat sich von der einfachen Verschlüsselung einiger weniger Dateien zu komplexen und gezielten Angriffen entwickelt, die gesamte Netzwerke und Systeme verschlüsseln können. Die zunehmende Bedeutung der Kryptowährungen vereinfachte für Angreiferinnen und Angreifer den anonymen Erhalt von Zahlungen. Neben den technischen Fortschritten entwickelten sich die dahinterstehenden kriminellen Gruppen zu professionellen Unternehmen, die Dritten eine „Software as a Service" (SaaS) anbieten, um damit Netzwerke anzugreifen und die Daten bis zur Zahlung erfolgreich als „Geisel" zu halten.

UKRAINE-KRIEG – Schon vorher, aber vor allem seit Beginn des russischen Angriffskrieges auf die Ukraine kam es zu Cyberangriffen auf ukrainische Einrichtungen. Wie schon bei NotPetya im Jahr 2017 wurde auf europäischer Ebene befürchtet, dass die gegen die Ukraine gerichteten Cyberattacken in der einen oder anderen Form auch über die Grenzen hinauswirken könnten und folglich verstärkt Cyberabwehr-Maßnahmen in den EU-Staaten ergriffen werden müssen.

Bei „**NotPetya**“ handelt es sich um eine Sabotage-Schadsoftware, die unter dem Mantel einer Ransomware im Juni 2017 aktiv war. Durch einen Supplychain-Angriff in einer ukrainischen Buchhaltungssoftware verschlüsselte dieses Schadprogramm hunderte IT-Infrastrukturen in der Ukraine und machte diese unbrauchbar. Im Gegensatz zu „üblicher“ Ransomware wurden jedoch die Daten gegen Lösegeld nicht mehr entschlüsselt. NotPetya gelangte über in der Ukraine präsente internationale Firmen und IT-Netze auch ins Ausland und richtete Schaden in Milliardenhöhe an. Die USA machten Russland für diesen Angriff verantwortlich.

In Österreich wurden die Einschätzung der Bedrohungslage und die sich daraus abzuleitenden Vorbereitungen in Abstimmung mit den im IKDOK („Innerer Kreis der Operativen Koordinierungsstruktur“) vertretenen staatlichen Organisationen vorgenommen. Noch vor der Invasion wurde ein Sonderlagebild an die IT-Sicherheitsbeauftragten der kritischen Infrastrukturen und verfassungsmäßigen Einrichtungen übermittelt, um vor den potenziellen Szenarien im Falle eines Angriffs Russlands zu warnen. Die in Europa feststellbaren Auswirkungen in der Cyberdomäne entsprachen den erwarteten Szenarien, wobei Österreich von den Auswirkungen fast gänzlich verschont blieb. Einzige Ausnahme waren mehrere DDoS-Angriffe einer oder mehrerer prorussischer Hackergruppierungen im Dezember 2022, die IT-Netzwerkkomponenten von kritischen Infrastrukturen und verfassungsmäßigen Einrichtungen für je ein bis zwei Tage überlasteten, und die in weiterer Folge als „Erfolge“ auf Telegram-Kanälen veröffentlicht wurden. Diese Attacken verursachten keine oder nur eingeschränkt bleibenden Schäden und wurden dazu genutzt, bereits vorbereitete Prozesse und Vorgänge im Bereich der Cybersicherheit umzusetzen und zu verbessern.

Neben den genannten Phänomenen bestehen weitere Herausforderungen, die aus Perspektive der nationalen Abwehr von Cyberangriffen Hindernisse oder Schwachpunkte darstellen. Viele Organisationen, insbesondere kleine und mittlere Unternehmen, verfügen nur über begrenzte Ressourcen und Fachkenntnisse, um sich ausreichend mit dem Thema Cybersicherheit zu befassen. Dieser Umstand kann den wirksamen Schutz vor Bedrohungen erschweren. So tragen etwa Handlungen wie die Verwendung schwacher Passwörter durch einzelne Personen oft zum Erfolg von Cyberangriffen bei.

Tätergruppen können bei Cyberangriffen nicht immer sofort identifiziert werden, zumal sie nicht nur von außen, sondern auch von innen (Innentäterinnen oder Innentäter) agieren können oder die Angriffe über geografische Grenzen hinweg umgesetzt werden. Diese Faktoren, noch mehr aber die weitreichende Anonymität im Internet, gepaart mit einer ständig von technischen Neuerungen getragenen Dynamik, erschweren sowohl die präventive als auch repressive Tätigkeit der Verfassungsschutzbehörden.

2.3.2.3 Fälle 2022

Die DSN führte aufgrund eines Cyberangriffes gegen eine weltweit tätige internationale Organisation mit Hauptsitz in Österreich seit Mitte des Jahres 2022 Ermittlungen gegen die Ransomware-Gruppierung „Karakurt". Der initiale Angriffsvektor war – wie auch bei etlichen anderen Cyberangriffen – eine an einen Mitarbeiter gerichtete Phishing-Mail. In dieser Phishing-Mail war eine infizierte Zip-Datei enthalten, die nach dem Öffnen das Endgerät und in weiterer Folge die Infrastruktur der Organisation infizierte.

Bei der Hackergruppe „**The Karakurt Team**" (auch „Karakurt Lair" oder „Karakurt Data Extortion Group" genannt) handelt es sich um eine Gruppe, die sich auf Datendiebstahl und Erpressung spezialisiert hat. Diese Gruppierung trat erstmals mit Cyberangriffen im September 2021 in Erscheinung. Der geografische Fokus der Angriffe liegt primär auf den USA, mit zunehmender Häufigkeit finden diese auch in Europa statt.

Im Zuge der Malware-Analyse konnte in der betreffenden E-Mail sowie der infizierten Zip-Datei die entsprechende Schadsoftware aufgefunden und genauer analysiert werden. Die weitere Ausbreitung der Schadsoftware in der IT-Infrastruktur der Organisation erfolgte via Remote Desktop-Zugängen. So konnte sich die Täterschaft mittels „Lateral Movement" und „Privilege Escalation" auf den Servern ausbreiten und diese infizieren.

Unter „**Lateral Movement**" wird die horizontale Ausbreitung der Angreiferinnen und Angreifer in der angegriffenen IT-Infrastruktur verstanden, also das Übernehmen immer weiterer Rechnersysteme. Im Zuge dessen beziehungsweise um „Lateral Movement" zu ermöglichen, trachten Angreiferinnen und Angreifer danach, ihre Rechte im System auszubauen. Diesen Vorgang nennt man „**Privilege Escalation**".

Kurz nach der Infektion und Ausbreitung konnten durch das IT-Personal der betroffenen Organisation bereits verdächtige Vorgänge am eigenen Mailserver festgestellt werden. So wurde unter anderem eine verdächtige Session[3] aufgefunden und als fremde Aktivität klassifiziert. Als unmittelbare Folge zog die internationale Organisation ein Incident

3 Eine Session beziehungsweise eine Sitzung ist im Grunde eine Art „Zeitraum", in dem eine Benutzerin oder ein Benutzer mit einem IT-System (zum Beispiel einer Webplattform) interagiert und alle notwendigen Informationen gespeichert werden, um die Interaktion der Benutzerin beziehungsweise des Benutzers zu verwalten und zu verfolgen.

Response Team hinzu, wobei in einer ersten Auswertung Logdaten[4] gesichert werden konnten, die einen Fremdzugriff bestätigten.

Zudem stellte man fest, dass zu diesem Zeitpunkt bereits circa 500 Gigabyte an Daten aus dem Netzwerk des Opfers exfiltriert worden waren. Am Tag der Entdeckung der Infektion erfolgte seitens der Täterschaft eine Kontaktaufnahme mit der betroffenen Organisation via E-Mail. In dieser war ein Link zu einem gesicherten Tor[5]-Chatraum enthalten, der vom Opfer für die anonymisierte Kommunikation mit der Täterschaft verwendet werden sollte. Die Tätergruppierung „The Karakurt Team" wies in der Kommunikation auf den Datendiebstahl hin, gab die Lösegeldforderung bekannt und setzte ein Ultimatum für die gewünschte Transaktion – die Lösegeldforderung belief sich auf einen einstelligen Millionenbetrag in Euro. Als Nachweis über den erfolgten Datendiebstahl sowie zur Erhöhung des Drucks auf das Opfer wurden Teile der abgezogenen Daten in der Kommunikation vorgewiesen. Die DSN wurde durch die betroffene Organisation in die erwähnten Vorgänge eingebunden und führte die Ermittlungen. Im Zuge des

4 Logdaten sind eine Art elektronisches Protokoll, das Informationen über die Aktivitäten eines Computersystems oder einer Anwendung aufzeichnet.

5 Tor ist eine kostenlose Software, die verwendet wird, um das Internet anonym zu durchsuchen und die Privatsphäre der Benutzerinnen und Benutzer zu schützen. Es funktioniert durch das Routing des Datenverkehrs über ein Netzwerk von zufällig ausgewählten Servern, um die Identität der Benutzerin oder des Benutzers zu verschleiern und ihre oder seine Online-Aktivitäten zu verschlüsseln.

Ermittlungsverfahrens übernahm die DSN die Kommunikation mit der Täterschaft. Ein besonderes Augenmerk wurde dabei auf die Gewinnung von neuen Erkenntnissen und Ermittlungsansätzen gelegt. Dadurch konnten nicht nur mehrere IP-Adressen der Hackergruppe ermittelt werden, sondern auch die Bitcoin[6]-Adresse der Wallet[7] der Täterschaft. Diese sollte dazu dienen, das Lösegeld an die Täter zu transferieren.

In Absprache mit dem Opfer wurde von einer Bezahlung des Lösegeldes Abstand genommen – das Opfer wurde darauf vorbereitet, dass wahrscheinlich eine Veröffentlichung der Daten durch die Täterschaft erfolgen werde. Da die Lösegeldforderung nicht erfüllt wurde, erhöhte die Täterschaft durch Androhung der Veröffentlichung von Daten der Organisation, aber auch privater Datensätze von Mitarbeiterinnen und Mitarbeitern den Druck. Die Drohanrufe erfolgten mit gefälschten Rufnummern (Caller-ID-Spoofing), um keine Hinweise oder Rückschlüsse auf die Identität der Täterinnen oder Täter zu ermöglichen.

Das sogenannte **„Caller-ID-Spoofing“** dient dazu, die Identität der Anruferin oder des Anrufers zu verschleiern. Dabei werden unter Verwendung von Softwarelösungen und ohne das Wissen der eigentlichen Inhaberinnen und Inhaber der Rufnummern fremde oder erfundene Rufnummern benutzt.

In solchen Fällen gestaltet sich die Ermittlungsarbeit aufgrund der Hintereinanderschaltung der IP-Adressen zur Verschleierung des Herkunftsorts der Angreiferin oder des Angreifers schwierig: Die Rückverfolgung von IP-Adressen erfordert den internationalen Rechtsweg sowie die Kooperation mit anderen Staaten und Providern. Zum Teil verwendeten die Täter bewusst Dienste und Provider, die nicht mit Behörden kooperieren und/oder deren Firmensitz in Staaten liegt, die sich dem Zugriff der Strafverfolgungsbehörden entziehen. Dennoch erfolgt auf internationaler Ebene ein Datenaustausch, um im Wege der Zusammenarbeit einen Erkenntnisgewinn zu ermöglichen.

In derartigen Fällen wird verstärkt auf internationale Kooperationen und Austausch gesetzt, da bei Cyberangriffen aufgrund ihrer grenzüberschreitenden Natur eine enge Zusammenarbeit und Abstimmung erforderlich ist.

---

6 Bitcoin ist eine Art digitale Währung, die auf einer Technologie namens Blockchain basiert. Es ermöglicht Peer-to-Peer-Transaktionen ohne die Notwendigkeit einer zentralen Autorität, wie zum Beispiel einer Bank. Bitcoin wird oft als „Kryptowährung“ bezeichnet, da es auf kryptographischen Technologien basiert, die es sicher und unveränderlich machen.

7 Ein Bitcoin Wallet ist eine digitale Brieftasche, die verwendet wird, um Bitcoins aufzubewahren, zu senden und zu empfangen.

Im Frühjahr 2022 konnte ein weiterer Cyberangriff auf eine in Österreich ansässige Organisation aufgedeckt werden, der die Merkmale eines APT-Akteurs aufwies. Bei der Analyse von organisationsinternen IT-Systemen wurde dabei die Infektion mehrerer Rechner mit der Schadsoftware „Babyshark" festgestellt, durch welche die Angreifenden über einen längeren Zeitraum Zugriff auf die entsprechenden Systeme hatten.

„**Advanced Persistent Threats**" (APT) sind zielgerichtete Angriffe, die typischerweise unter Einsatz großer personeller und technischer Ressourcen eine andauernde Bedrohung für das Opfer darstellen. APT kommen oft im Bereich von staatlich gesteuerter Spionage zum Einsatz.

Nach einer Bereinigung der betroffenen Systeme konnte die Schadsoftware zwar beseitigt werden, es zeigte sich aber das typische Merkmal einer APT-Kampagne – die dauerhafte Bedrohung. Denn auch nach Entfernung der Schadsoftware können erneut zielgerichtete Angriffe erfolgen. So wurde die Organisation etwas später von einem vermeintlichen Journalisten kontaktiert und um ein Interview beziehungsweise eine Analyse zu einem aktuellen geopolitischen Thema gebeten. Dem Opfer sollte so ein infiziertes Dokument übermittelt werden. Durch das Öffnen des Dokuments wurde erneut eine Schadsoftware aktiv, die sich im aktuellen System persistierte, dieses analysierte, die gewonnenen Informationen an die Angreiferin oder den Angreifer schickte und regelmäßig versuchte, weitere Befehle der Angreiferin oder des Angreifers zu empfangen und auszuführen. Um dabei unentdeckt zu bleiben, überprüfte die Schadsoftware die im System vorhandenen Sicherheitslösungen (Antivirensoftware) sehr genau, um dann Angriffsvektoren zu wählen, die vom jeweiligen Produkt nicht erkannt wurden. Auch nach diesem abgewehrten Angriff versuchte die Täterschaft wiederholt, Mitarbeiterinnen und Mitarbeiter der Opferorganisation zu kontaktieren, was jedoch frühzeitig erkannt und wodurch weiterer Schaden abgewendet wurde.

Als Angreifer konnte die APT-Gruppe „Kimsuky" identifiziert werden, hinter der sich ein nordkoreanischer Akteur verbirgt. Dieser ist seit zumindest zehn Jahren für die Durchführung von Spionageangriffen bekannt. Während zunächst südkoreanische Einrichtungen Ziel von „Kimsuky" waren, erweiterte die Gruppe ihr Zielspektrum nach und nach auf westliche Staaten und internationale Einrichtungen. Durch die Angriffe sollen Informationen zur unmittelbaren Sicherheitslage auf der koreanischen Halbinsel, zu nuklearen und außenpolitischen Strategien sowie zu Sanktionen westlicher Staaten in Bezug auf Nordkorea beschafft werden. „Kimsuky" arbeitet dabei eng mit anderen nordkoreanischen APT-Gruppierungen zusammen und wird der berüchtigten „Lazarus Group" zugerechnet, die laut US-Justizministerium für den nordkoreanischen Nachrichtendienst „Reconnaissance General Bureau" arbeitet.

2.3.2.4 Trends und Entwicklungstendenzen

Ransomware wird auch in naher Zukunft die größte Cyberbedrohung darstellen. Aufgrund der Lukrativität des Ransomware-Marktes konnte in den letzten Jahren eine Professionalisierung beobachtet werden, wodurch die Angreifergruppen mittlerweile Klein- und Mittelunternehmen ähneln: Mehrere interne Hierarchieebenen dienen zur Umsetzung und Koordination von Entwicklung, Zahlungsabwicklung und Support. Dadurch sollen den „Affiliates" (Partnern) die zur Verfügung gestellten Services möglichst professionell aufbereitet werden, um die Kundschaft nicht an andere „Ransomware as a Service"-Hersteller zu verlieren.

„**Ransomware as a Service**" (RaaS) lehnt sich an den in der IT-Branche üblichen Businessansatz „Software as a Service" (SaaS) an. Hierbei wird ein Softwareprodukt vollumfänglich und bereit zur sofortigen Ausführung zur Verfügung gestellt. Ein „RaaS"-Ansatz inkludiert, dass neben der Bereitstellung der Schadsoftware durch den Hersteller auch die Serverinfrastruktur, die Zahlungsabwicklung und das Veröffentlichen von zahlungsunwilligen Opfern im „Servicepaket" inkludiert ist.

Derzeit einzig erfolgversprechender ermittlungstechnischer Ansatz bei der Bekämpfung von Ransomwareangriffen ist das gezielte Abschalten („Takedowns") der RaaS-Infrastruktur außerhalb Russlands.

Der Angriffskrieg Russlands gegen die Ukraine wurde durch staatliche Cyberangriffe auf ukrainische IT-Systeme begleitet, was mehrfach auch zu Kollateralschäden in EU-Staaten führte. Außerhalb der Ukraine wurden primär durch pro-russische und staatlich geförderte Hackergruppen einfach umsetzbare, öffentlichkeitswirksame DDoS-Angriffe oder Informationsveröffentlichungen durchgeführt. Sollte der Krieg in der Ukraine längere Zeit andauern, ist es wahrscheinlich, dass in Ukraine-Unterstützungsländern verstärkt Cyberangriffe gegen die jeweiligen IT-Systeme geführt werden. Diese Länder waren im letzten Jahr nicht demselben Bedrohungslevel wie die IT-Systeme der Ukraine ausgesetzt und weisen daher nicht denselben Sicherheitsreifegrad auf.

APT-Gruppierungen werden auch weiterhin den geopolitischen und eigenen Interessen entsprechend sowohl kurzfristige als auch längerfristige Akzente setzen. Ferner werden chinesische APT-Gruppierungen zur Unterstützung der Umsetzung des Fünf-Jahresplans der Kommunistischen Partei herangezogen. Innerhalb der Industrie sind in Österreich daher „Hidden Champions" durchaus lohnende Ziele. Diese sind mit einem Nischenprodukt internationaler Marktführer, weisen aber oftmals keine hohen IT-Sicherheitsvorkehrungen auf.

„ChatGPT“ ist eine auf Basis eines neuronalen Netzwerks programmierte und trainierte Künstliche Intelligenz (KI), mit der im Format eines Chats interagiert werden kann, wodurch sie auch aktiv laufend dazu lernt. Diese KI kann sowohl Fragen in längeren Texten beantworten, Programmcodes generieren und interpretieren sowie Fehler erkennen.

Im November 2022 sorgte die US Firma OpenAI mit der Veröffentlichung von ChatGPT für große Aufmerksamkeit. Nach ersten Erkenntnissen kann diese Künstliche Intelligenz (KI) sowohl zur Verteidigung bei Analysen von Schadcodes genützt werden, aber auch bei Angriffen Unterstützung bieten. Für Phishing-Angriffe können etwa zu einem vorgegebenen Thema Textvorlagen, aber auch Quellcodeteile von Hilfswerkzeugen, die für den Angriff auf Computersysteme relevant sind, generiert werden. Dies könnte eine Vereinfachung der Arbeitsschritte bei der Umsetzung von Cyberangriffen bedeuten und zeugt von einer neuen Generation von Angriffswerkzeugen. Die Umsetzung von praktikablen, vollautomatisierten Cyberangriffen wird jedoch vermutlich noch Jahre dauern. Instrumente wie ChatGPT werden IT-Administratorinnen und –Administratoren dennoch vor neue Herausforderungen stellen und in den kommenden Jahren immens an Bedeutung gewinnen.

Cyberangriffe werden im Jahr 2023 ein probates Mittel für die Tätigkeiten von Nachrichten- und Geheimdiensten in Europa und Österreich darstellen. Insbesondere die Russische Föderation, die Volksrepublik China, der Iran, aber auch Nordkorea werden ihre Fähigkeiten und Kapazitäten in dem Bereich ausbauen und verstärken. Die Einflussnahme türkischer Akteure auf deren Diaspora in Österreich im Zusammenhang mit der Wahl in der Türkei 2023 unter dem Einsatz von Cybermitteln bleibt abzuwarten.

2.4 Internationaler Waffenhandel und Proliferation

2.4.1 Internationaler Waffenhandel

Der Begriff des **„internationalen illegalen Waffenhandels“** bezeichnet die Weitergabe von und den Handel mit konventionellen Waffen (in ihrer Gesamtheit oder auch in Teilen), entsprechender Ausrüstungsgüter, Software und Technologie entgegen den gesetzlichen Bestimmungen über nationale Grenzen hinweg.

2.4.1.1 Überblick

Auf Ebene der Europäischen Union spielt die Bekämpfung des internationalen illegalen Waffenhandels eine immer wichtigere Rolle, da dieses Kriminalitätsfeld im Zusammenhang mit terroristischen Straftaten und der Organisierten Kriminalität steht. Kriminelle

Aktivitäten im Bereich des illegalen Handels mit Waffen, Kriegsmaterial und Explosivstoffen sind von Relevanz für den Verfassungsschutz, da diese Materialien bei regionalen und überregionalen Konflikten zum Einsatz kommen und deren illegale Lieferung und Verwendung verhindert werden soll. Die EU-Kommission hat mit der Aktualisierung des EU-Aktionsplans gegen den unerlaubten Handel mit Feuerwaffen für die Jahre 2020 bis 2025 ihren Fokus verstärkt auf die Bekämpfung des internationalen illegalen Waffenhandels beziehungsweise der internationalen Waffenkriminalität gelegt. Des Weiteren hat sie Durchführungsrichtlinien zur Eindämmung der illegalen Verbreitung von Schusswaffen erlassen, deren Umsetzung in nationales Recht letztlich entscheidend für die EU-weite Harmonisierung der Kontrolle des Waffenerwerbs und Waffenbesitzes sein wird.

2.4.1.2 Aktuelle Lage

Der illegale Waffenhandel ist ein internationales Problem, betrifft alle Regionen der Welt und wirkt sich auf vielfältige Art und Weise negativ auf die dortigen Gesellschaften aus. Er findet dabei sowohl auf nationaler als auch auf internationaler Ebene statt – beide Ebenen stehen in der Regel miteinander in Beziehung.

Auf Ebene der Europäischen Union ist man sich der Gefahr, die vom illegalen Handel mit Waffen ausgeht, und der destabilisierenden Wirkung, die dieser auf die Nachbarschaft der Europäischen Union haben kann, bewusst. Daher wird auf europäischer Ebene durch Forcierung der Zusammenarbeit und den verstärkten Informationsaustausch versucht, rechtliche Lücken zu schließen, durch transparente Verfahren mit den Entwicklungen Schritt zu halten und so die Gefahr für die innere Sicherheit zu verringern.

Kleine und leichte Waffen, im internationalen Sprachgebrauch oft als **„Small Arms and Light Weapons“** bezeichnet, fordern weltweit mehr Opfer als alle anderen Waffengattungen. Oft werden sie daher als die wahren Massenvernichtungswaffen bezeichnet.

Für den legalen Markt werden konventionelle Waffen durch berechtigte Hersteller erzeugt. Dabei besteht jedoch zu jedem Zeitpunkt die Gefahr, dass diese auf den Schwarzmarkt umgeleitet werden. Anders als bei anderen Gütern handelt es sich bei konventionellen Waffen um sehr langlebige Produkte, die bei entsprechender Lagerung Jahrzehnte überdauern und in dieser Zeit immer wieder weiterverbreitet werden können. Illegal gänzlich selbstangefertigte Waffen bilden die Ausnahme.

Im Bereich des internationalen illegalen Waffenhandels sind in der Republik Österreich hauptsächlich kurzzeitig aktive Gruppierungen mit losen Strukturen tätig. Dabei handelt es sich meist um Personen, die anlassbezogen im Bereich des illegalen Waffenhandels aktiv werden, wenn sich die entsprechende Gelegenheit ergibt. Dabei wird das aus ver

wandten Kriminalitätsfeldern erworbene Wissen zur Anwendung gebracht. In der Regel sind im internationalen illegalen Waffenhandel tätige Personen durch finanzielle Motive gesteuert, da es sich bei einer illegalen Schusswaffe um ein lang lagerbares Produkt handelt, nach dem konstante Nachfrage besteht und dessen Preis sich am Schwarzmarkt je nach Angebot und Nachfrage vervielfachen kann. Unter den Käuferinnen und Käufern illegaler Waffen finden sich auch gewaltbereite Extremistinnen und Extremisten, bei denen immer wieder illegale Schusswaffen sichergestellt werden. Bei der Beschaffung solcher Schusswaffen sind auch sie auf den Schwarzmarkt beziehungsweise entsprechende Kontakte dorthin angewiesen.

Die Republik Österreich ist im Bereich des internationalen illegalen Waffenhandels aufgrund ihrer geografischen Lage vor allem Transitland für Waffen aus den Ländern des Westbalkans, die in den Westen und Norden Europas geschmuggelt werden. Gleichzeitig dient Österreich aber auch als Zielland für illegale Waffen und wird bei bestimmten Modi Operandi als Beschaffungsland genutzt. Dasselbe gilt für den illegalen internationalen Handel mit Explosivstoffen, dessen Bekämpfung ebenso in die Zuständigkeit des Verfassungsschutzes fällt.

Neben dem internationalen illegalen Waffenhandel aus kriminellen Motiven versuchen vor allem staatliche Akteure, an konventionelle Waffen, entsprechende Ausrüstungsgüter, Software und Technologie zu gelangen, um die eigenen Rüstungsbestrebungen voranzubringen. Dabei sind sie auf den Weltmarkt angewiesen, um die angestrebten Rüstungsziele zu erreichen. Dieser unterliegt jedoch Exportkontrollmaßnahmen, um die unkontrollierte Weiterverbreitung solcher Waffen und Güter zu verhindern.

Die Republik **Österreich** ist Teilnehmerstaat des **„Wassenaar Abkommens“ (WA)**, ein Exportkontrollregime, das geschaffen wurde, um einen Beitrag zur regionalen und internationalen Sicherheit und Stabilität zu leisten, indem Transparenz und ein verantwortungsvolleres Handeln bei Exporten von konventionellen Rüstungsgütern und Dual-Use-Gütern gefördert und auf diese Weise destabilisierende Waffenanhäufungen verhindert werden. Ziel dieses Abkommens ist es auch, den Erwerb dieser Güter durch Terroristen und Terroristinnen zu verhindern.

Um diese Exportkontrollmaßnahmen zu umgehen, bedienen sich die genannten Akteure verdeckter Beschaffungsmethoden. Damit soll der eigentliche Verwendungszweck der Güter gegenüber involvierten Unternehmen, aber auch gegenüber den in die Exportkontrolle involvierten Behörden verschleiert werden.

Eine besondere Problematik stellen hier Güter mit doppeltem Verwendungszweck, meist als „Dual-Use-Güter“ bezeichnet, dar – also Materialien oder Produkte, die sowohl für

den zivilen Bereich verwendet, aber auch für den militärischen Bereich zweckentfremdet werden können. Dasselbe gilt für hochwertige Freiwaren, das heißt Güter, deren Ausfuhr eigentlich keiner Beschränkung unterliegt.

Generell haben auch im Bereich des illegalen Waffenhandels unerlaubte Exporte von exportbeschränkten Rüstungsgütern das Potential, Österreichs politische Glaubwürdigkeit und die auswärtigen Beziehungen nachhaltig zu schädigen.

Auch für in solche Vorgänge wissentlich oder unwissentlich eingebundene Personen oder Unternehmen können sich über eine Strafbarkeit hinausgehend Nachteile ergeben. Diese reichen von finanziellen Einbußen über Reputationsverlust bis hin zu Sanktionierungen.

UKRAINE-KRIEG – Der Angriffskrieg Russlands gegen die Ukraine erwies sich 2022 noch nicht als neuer Faktor im Bereich des illegalen Waffenhandels in Österreich. Derartige Konflikte im geographischen Nahebereich Österreichs bergen jedoch immer die Gefahr, sich zu einer Herkunftsquelle für illegale Waffen am heimischen Markt zu entwickeln, aber auch als Zielgebiet für illegal in Österreich beschaffte Waffen und Güter zu dienen.

2.4.1.3 Fälle 2022

Auf Grundlage des Verdachts des illegalen Waffenhandels konnte im März 2022 in der Steiermark durch die Verfassungsschutzbehörden eine staatsanwaltschaftliche Durchsuchungsanordnung erwirkt werden. Im Zuge der Hausdurchsuchung wurden Gegenstände, die im Zusammenhang mit illegalem Waffenhandel stehen könnten, sichergestellt. Dabei

handelte es sich um eine Kalaschnikow, eine Maschinenpistole, eine Pistole, leere und mit Munition gefüllte Magazine, diverse Munition, eine Pistolentasche sowie fünf Handgranaten. Bei der Einvernahme zeigte sich der Verdächtige nicht geständig und bestritt vorerst jeden Zusammenhang mit Besitz oder Handel von Waffen oder Kriegsmaterial. Über die Herkunft der bei der Hausdurchsuchung sichergestellten Gegenstände tätigte er widersprüchliche Aussagen. Der Beschuldigte wurde im Juli 2022 vom Landesgericht für Strafsachen zu einer unbedingten Geldstrafe von 3.600 Euro verurteilt.

Aufgrund eines Hinweises wurden Ermittlungen gegen ein im Westen Österreichs etabliertes Waffengeschäft geführt. Es bestand der Verdacht, dieses verkaufe illegal und gewinnbringend nicht ordnungsgemäß registrierte Schusswaffen der Kategorie B sowie Munition für Faustfeuerwaffen in Österreich und ins benachbarte Ausland. Im Zuge der Ermittlungen erhärtete sich der Verdacht, dass Waffen- und Munitionsbestellungen über Dritte aus dem Ausland getätigt wurden, wobei der potenzielle Käufer über keine waffenrechtlichen Dokumente (Waffenbesitzkarte beziehungsweise Waffenpass), die zum Erwerb, Besitz oder Führen von Schusswaffen der Kategorie B notwendig sind, verfügte. In Kooperation mit einer ausländischen Sicherheitsbehörde konnten bei einer in diesem Land durchgeführten Hausdurchsuchung vier Faustfeuerwaffen der Kategorie B, eine Schrotflinte der Kategorie C sowie circa 15.000 Schuss scharfe Munition sichergestellt werden. Laut Angaben des beschuldigten Käufers wurden die oben angeführten Gegenstände im österreichischen Waffengeschäft erworben. Bei der in Österreich durchgeführten Hausdurchsuchung wurden insgesamt zehn Faustfeuerwaffen vorgefunden und sichergestellt. Erhebungen ergaben, dass acht der zehn Waffen zu keinem Zeitpunkt in Österreich registriert gewesen waren. Bei zwei Waffen konnte ein Verkauf nach Österreich festgestellt werden. Wie diese Waffen in den Besitz der Waffenhändlerin übergingen, konnte jedoch nicht geklärt werden, wodurch ein Verkauf am Schwarzmarkt wahrscheinlich erscheint.

Neben der Waffenhändlerin konnte zusätzlich ein österreichischer Staatsbürger ausgeforscht werden, der diese bei ihren Tathandlungen unterstützte, indem er den Verkauf nicht registrierter Schusswaffen vermittelte oder diese reparierte und in weiterer Folge Personen überließ, die nicht zum Erwerb, Besitz oder Führen derartiger Schusswaffen berechtigt waren. Die beiden Beschuldigten in Österreich wurden nach einer Verhandlung Ende August 2022 schlussendlich vom Oberlandesgericht zu einer unbedingten Geldstrafe von 1.920 Euro beziehungsweise 2.160 Euro verurteilt.

2.4.1.4 Trends und Entwicklungstendenzen

Während sich die Weltwirtschaft aufgrund steigender Energiekosten nach den Jahren der Pandemie vor neuen Herausforderungen sieht, verzeichnen Rüstungs- und Waffenproduzenten nach wie vor Umsatzzuwächse. Dies hat vor allem mit dem Krieg in der Ukraine, aber auch mit Entwicklungen auf dem afrikanischen Kontinent zu tun.

Dass Waffen, die für die Ukraine bestimmt waren, letztendlich über den illegalen Waffenhandel wieder in Österreich landen, war im Berichtsjahr ein medial diskutiertes Thema. Erfahrungen aus dem Bürgerkrieg im ehemaligen Jugoslawien werden vielfach als Argument für das Eintreten dieses Szenarios angeführt. Im aktuellen Berichtsjahr wurden der DSN keine Hinweise bekannt, wonach illegaler Waffenhandel aus der Ukraine nach Österreich beziehungsweise Europa bereits strukturiert und geplant durchgeführt wurde. Für Strukturen der Organisierten Kriminalität, die es auch in der Ukraine gibt, ist der illegale Waffenhandel seit jeher ein lukratives Geschäft. Die Verbreitung dieser ist jedoch auch zu einem Narrativ in russischen Desinformationskampagnen geworden, um Europa einzuschüchtern beziehungsweise davon abzuhalten, die Ukraine weiter mit Waffenlieferungen im Kampf gegen Russland zu unterstützen. Gleichwohl bleibt dieses Szenario, die sogenannte „Battlefield Collection" – also das Sammeln und in Umlauf bringen im Kriegsgebiet vorgefundener Waffen – eine Gefahr, welcher von Seiten der DSN große Bedeutung zugemessen wird und deren Entwicklungen in der Europäischen Union genau beobachtet werden.

Für das Jahr 2023 wird der Fokus auf der Beobachtung der Auswirkungen des Krieges in der Ukraine liegen, insbesondere auf Kooperation der Verfassungsschutzbehörden mit internationalen, europäischen und nationalen Gremien und Stakeholdern.

Österreich ist insbesondere Quellland hinsichtlich Waffen- und Munitionsbestandteilen, die in anderen Staaten strengeren Beschränkungen unterliegen. Hierbei werden gezielt unterschiedliche gesetzliche Vorgaben ausgenützt, entsprechende Güter in Österreich erworben und in der Regel rechtswidrig aus Österreich ausgeführt. Waffenteile, welche nicht gasdruckbelastet sind und nicht gesondert als registrierungspflichtige Waffenteile gelten, sind vom österreichischen Waffengesetz nicht erfasst und somit in Österreich frei und ohne Registrierung erhältlich. Diese Waffenteile, insbesondere Griffstücke für Pistolen, sind international von erheblicher Relevanz und werden weltweit weiterhin bei Sicherstellungen im Bereich der organisierten Kriminalität und bei verfassungsschutzrelevanten Gruppierungen auftreten.

2.4.2 Proliferation

Unter dem Begriff **„Proliferation"** wird die Weitergabe von atomaren, biologischen und chemischen Massenvernichtungswaffen, für deren Einsatz notwendiger Trägersysteme sowie der zu deren Herstellung verwendeten Produkte inklusive des dafür erforderlichen Know-hows verstanden. Wesentliche Aufgaben der Proliferationsbekämpfung sind das Feststellen von relevanten Firmen und Beschaffungsnetzwerken, der Verschleierung von Zahlungsströmen sowie die Abklärung, ob und in welcher Form fremde Nachrichtendienste in entsprechende Aktivitäten involviert sind.

2.4.2.1 Überblick

In Anbetracht der Vielzahl an internationalen oder innerstaatlichen Konflikten und des Missbrauchs von Waffen jeglicher Art durch substaatliche Akteure, die in den Besitz chemischer, biologischer, radioaktiver oder nuklearer Stoffe gelangen können, erhöht sich das Risiko für den Bereich der Proliferation. Die Bekämpfung der Proliferation zählt daher weiterhin zu den zentralen Sicherheitsaufgaben Österreichs. Die Gefahr, dass Massenvernichtungswaffen, Trägersysteme, Dual-Use-Güter und entsprechendes Know-how in den Besitz sogenannter „Risikostaaten", sanktionierter Regime oder terroristischer Organisationen gelangen oder bestimmte Güter entgegen offizieller Angaben für eine proliferationsrelevante Verwendung missbräuchlich herangezogen werden, stellt eine wesentliche proliferationsbezogene Gefährdung dar.

Als „**Massenvernichtungswaffen**" gelten dabei Waffen, die das Potential haben, Zerstörungen in großem Ausmaß anzurichten, wie atomare, biologische und chemische Massenvernichtungswaffen.

2.4.2.2 Aktuelle Lage

Neben der Bekämpfung der unkontrollierten Weiterverbreitung konventioneller Waffen obliegt dem Verfassungsschutz auch die Bekämpfung von Massenvernichtungswaffen, der Proliferation. Relevante Vorgänge beschränken sich dabei nicht nur auf die Weiterverbreitung der Massenvernichtungswaffen selbst, sondern umfassen auch Vorhaben, die darauf abzielen, bestehende Arsenale von Massenvernichtungswaffen zu komplettieren, sie in Belangen der Lagerfähigkeit, Einsetzbarkeit und Wirkung zu verbessern oder aber gänzlich neue Systeme zu entwickeln.

Verschiedene Staaten gelten aufgrund ihrer Bestrebungen, in den Besitz von Massenvernichtungswaffen und entsprechende Trägersysteme zu gelangen, diese weiterzuentwickeln oder ihre Bestände zu erweitern, als sogenannte „Risikostaaten". Sie sind bemüht, Güter und Knowhow zur Herstellung von Massenvernichtungswaffen und Trägertechnologien weltweit zu beschaffen. Aus Sicht dieser Staaten stellt der Erwerb oder die Entwicklung von Massenvernichtungswaffen eine Möglichkeit dar, sich durch Abschreckung präventiv gegen militärische Bedrohungen zu wappnen und die eigene internationale Stellung durch politische Druckausübung zu verbessern. Auch bieten solche Massenvernichtungswaffen und entsprechende Technologien durch den Weiterverkauf für ansonsten exportschwache Staaten die Möglichkeit, finanzielle Quellen zu erschließen und dringend benötigte Devisen zu beschaffen.

Für den Rest der Welt stellt die Verbreitung von Massenvernichtungswaffen eines der größten aktuellen Sicherheitsrisiken dar. Die Vorhaben verschiedener Risikostaaten, in den Besitz von Massenvernichtungswaffen und entsprechender Trägertechnologie zu ge

langen, birgt die Gefahr, dass diese künftig in Konflikten oder als politisches Druckmittel Verwendung finden und damit die sicherheitspolitische Weltlage in ihrer Gesamtheit nachteilig verändern. Die unkontrollierte Verbreitung von Massenvernichtungswaffen bedroht somit auf unkalkulierbare Art und Weise den Weltfrieden, erhöht die Gefahr eines regionalen Wettrüstens und birgt die Gefahr eines nicht mehr zu kontrollierenden Flächenbrandes.

Die Republik Österreich ist sich der Gefahr bewusst, die von der unkontrollierten Verbreitung von Massenvernichtungswaffen ausgeht. Um dieser zu begegnen, ist sie verschiedene, gegen die Proliferation von Massenvernichtungswaffen gerichtete Verpflichtungen eingegangen. Als wichtigste ist hier für den Bereich der atomaren Waffen der **„Vertrag über die Nichtweiterverbreitung von Atomwaffen" (NPT)** zu nennen. Im Bereich der biologischen und chemischen Waffen ist die Republik Österreich Vertragsstaat des **„Übereinkommens über das Verbot der Entwicklung, Herstellung und Lagerung von biologischen Waffen und Toxinwaffen" (BWTC)** sowie der **„Chemiewaffenkonvention" (CWC)**.

Um die erforderlichen Güter, aber auch einschlägiges Know-how für ihre Rüstungsvorhaben zu beschaffen, sind Risikostaaten auf den Weltmarkt angewiesen, der jedoch Exportkontrollmaßnahmen unterliegt. Um diese zu umgehen, setzen Risikostaaten verschiedene, sich ständig weiterentwickelnde verdeckte Beschaffungsmethoden ein. Dabei werden Güter und Know-how für die Massenvernichtungswaffenprogramme über Umwege für einen angeblich zivilen Zweck beschafft. Langfristiges Ziel der Risikostaaten ist es jedoch stets, die bestehenden Abhängigkeiten von Produkten und Knowhow aus dem Ausland zu verringern und schlussendlich Autarkie in den relevanten Bereichen zu erlangen.

Die Republik Österreich ist **Teilnehmerstaat verschiedener Exportkontrollregime**, welche die Verhinderung der Proliferation von Massenvernichtungswaffen und entsprechender Trägertechnologie gewährleisten sollen. Ziel der Gruppe der **Nuklearlieferländer (NSG)** ist es, nicht zur Verbreitung atomarer Waffen beizutragen. Die **„Australische Gruppe" (AG)** ist das Exportkontrollregime für bestimmte Chemikalien und biologische Agenzien sowie Dual-Use-Güter, die zur Herstellung biologischer oder chemischer Waffen missbraucht werden können. Das **„Trägertechnologie-Kontrollregime" (MTCR)** kontrolliert die Weitergabe von Gütern, die zur Herstellung von Trägersystemen von Massenvernichtungswaffen beitragen können. Dazu zählen etwa ballistische Raketen, Marschflugkörper oder unbemannte Luftfahrzeuge.

Der langjährige Trend der Beschaffung von Gütern mit doppeltem Verwendungszweck sowie hochwertiger Freiwaren setzt sich nach wie vor fort.

Neben der klassischen Beschaffung solcher proliferationsrelevanten Güter streben Risikostaaten auch im Bereich der Wissenschaft und Forschung danach, sich im Zuge des Austausches zwischen Institutionen der Wissenschaft und Forschung proliferationsrelevantes Know-how anzueignen. Solche Vorgänge können Universitäten und Fachhochschulen, aber auch außeruniversitäre Forschungseinrichtungen sowie Forschungs- und Schulungsabteilungen der Industrie betreffen. Besonders gefährdet sind hierbei Fachbereiche, deren Inhalt auch in den Programmen zur Entwicklung von Massenvernichtungswaffen genutzt werden kann.

Österreich weist im internationalen Vergleich eher kleine, aber hochspezialisierte Unternehmen und Forschungseinrichtungen auf. Gerade Österreichs klein- und mittelbetriebliche Unternehmen entwickeln, produzieren und vertreiben in diversen Branchen Güter und Know-how, mit denen sie am Weltmarkt führend sind. Dieser Umstand macht solche Unternehmen interessant für entsprechende Beschaffungsvorhaben von Risikostaaten und Österreich damit zum Zielgebiet.

Erfolgreiche Beschaffungsvorgänge von proliferationsrelevanten Gütern in Österreich können dazu führen, dass österreichische Unternehmen in letzter Konsequenz den Massenvernichtungswaffenprogrammen von Risikostaaten Vortrieb leisten. Eine solche unkontrollierte Weiterverbreitung von Massenvernichtungswaffen wirkt sich negativ auf die internationale Sicherheitslage aus, wie die mediale Berichterstattung täglich vor Augen führt.

Auch proliferationsrelevante Vorgänge unter Einbindung Österreichs haben das Potential, Österreichs politische Glaubwürdigkeit und die auswärtigen Beziehungen zu schädigen. Für in solche Vorgänge eingebundene Personen und Firmen können sich, wie bei der unkontrollierten Weiterverbreitung konventioneller Waffen, neben allfälligen Strafbarkeiten anderwärtige Nachteile wie vor allem finanzielle Einbußen, Reputationsverlust oder Sanktionierungen ergeben.

Im Zusammenhang mit der Bekämpfung des internationalen illegalen Waffenhandels und der Proliferation von Massenvernichtungswaffen werden zudem Sachverhalte mit chemischen, biologischen, radiologischen und nuklearen Waffen (CBRN) bearbeitet, die durch nichtstaatliche Akteure beschafft werden.

Nicht nur die Bekämpfung des illegalen Handels mit konventionellen Waffen ist eine Aufgabenstellung der DSN in diesem Phänomenbereich. In der Proliferation zeichnen sich Zukunftstechnologien, wie etwa Halbleiterindustrie, Quantenforschung und Künstliche Intelligenz, als künftige Brennpunkte für die Interessen ausländischer Nachrichtendienste ab.

Als Gegenstrategie hat die DSN über den DSN-Wirtschaftsschutz Kontakte zu betroffenen Unternehmen und Forschungsstellen aufgenommen und bietet präventive Sensibilisierungs- und Schutzmaßnahmen für diese Technologiefelder an.

2.4.2.3 Fälle 2022

Im Berichtsjahr beschäftigte die DSN die Abwehr von Proliferationsversuchen staatlich gelenkter Akteure aus dem Ausland. Vor allem der Hochtechnologiebereich in Österreich war Ziel der Gefährdung durch Proliferationsversuche fremder Staaten.

Ein ausländisches Proliferationsnetzwerk gründete mehrere Scheinfirmen, mit denen Geschäfte in Österreich angebahnt wurden. Als Einkäufer fungierte eine Scheinfirma aus dem arabischen Raum. Die Endabnehmer konnten jedoch in einem von Embargos betroffenen Land identifiziert werden. Die Geschäftsanbahnung sollte mittels einer Täuschung über den eigentlichen Endverbraucher stattfinden. Dazu besuchte eine Delegation unter Vortäuschung falscher Tatsachen die betroffene Firma, um durch den persönlichen Kontakt den Kauf der Hochtechnologie zu ermöglichen.

Das Ziel war die Beschaffung von Hochtechnologiewaren aus dem Produktportfolio einer österreichischen Firma. Die Hochtechnologieprodukte sollten genutzt werden, um die Streitkräfte im Herkunftsland des Proliferationsnetzwerkes mit moderner Waffentechnologie auszurüsten. Die militärischen Mittel beziehungsweise Waffen, die durch den Einsatz dieser Technologie hergestellt werden können, dienen im militärischen Bereich zu Angriffs- und nicht zu Verteidigungszwecken.

Die DSN konnte den Proliferationsversuch verhindern und ist nach wie vor mit der Abwehr verschiedener Proliferationsnetzwerke in Österreich beschäftigt, welche nach einem ähnlichen Modus Operandi vorgehen.

2.4.2.4 Trends und Entwicklungstendenzen

Der Beschuss der kritischen Infrastruktur in der Ukraine mit Raketen und Drohnen durch Russland hat der Weltöffentlichkeit im letzten Jahr vor Augen geführt, welche Bedeutung ballistische Raketen für die Austragung von Kriegshandlungen weiterhin besitzen. 2022 haben auch nichtstaatliche Akteure wieder stark auf den Einsatz ballistischer Raketen gesetzt. Vor allem islamistisch-terroristische Gruppierungen im Nahen und Mittleren Osten setzen zunehmend auf die Beschaffung von Marschflugkörpern bei ihren Bestrebungen, Konflikte mit Waffengewalt auszutragen. Im Bereich der Proliferation ballistischer Raketen durch staatliche Akteure bleiben der Iran, Pakistan, Syrien und Nordkorea zentrale Akteure in der Beschaffung, der Herstellung und dem Weiterverkauf dieser Waffensysteme für Konfliktherde in unterschiedlichsten Regionen der Welt.

Ab Herbst 2022 wurde der Einsatz von sogenannten „Kamikaze“-Drohnen im Angriffskrieg Russlands gegen die Ukraine ein Thema. Die aus iranischer Produktion stammen

den Drohnen sind im Vergleich zu ballistischen Raketen vergleichsweise günstig in der Produktion. Für die Proliferationsabwehr der DSN ist die Verhinderung, dass Bauteile aus Österreich in Drohnen eingesetzt werden, die schließlich keine zivile, sondern eine militärische Endverwendung finden, eine aktuelle Herausforderung. Hier stellt zum einen die gesamtstaatliche Kooperation in Österreich zwischen Exportkontrolle, Zoll und Sicherheitsbehörden ein wichtiges Mittel bei der Verhinderung solcher Entwicklungen dar. Über den DSN-Wirtschaftsschutz wird auch direkt mit Herstellern und Zwischenhändlern Kontakt aufgenommen und über die Gefahren von solchen Dual-Use-Beschaffungsvorgängen sensibilisiert.

Internationale Militärbeobachter und Militärbeobachterinnen beschreiben den Krieg in der Ukraine als vor allem vom Einsatz von Artillerie, ballistischen Raketen und Kampfdrohnen geprägt. Die Verhinderung der Wiederbeschaffung von Kriegsmaterial wird für 2023 ein Trend in der internationalen Proliferationsabwehr sein. Vor allem Bauteile für Kampfdrohnen, die nicht als Dual-Use-Güter deklariert werden, sind ein Thema in den Sensibilisierungs- und Präventionsmaßnahmen der DSN.

3
Schutz und Prävention

3.1 Schutz der Obersten Organe und verfassungsmäßigen Einrichtungen

3.1.1 Überblick

Der DSN obliegt im Zusammenwirken mit den für Staatsschutz zuständigen Organisationseinheiten der Landespolizeidirektionen der besondere Schutz der durch Verfassungsgesetze eingerichteten Institutionen und Organe des Bundes und der Länder (Oberste Organe und verfassungsmäßige Einrichtungen). Dazu zählen unter anderem der Nationalrat, der Bundesrat, der Bundespräsident, der Bundeskanzler, die Bundesministerinnen und Bundesminister, die Mitglieder der Landesregierungen sowie die Höchstgerichte. Die Schutzmaßnahmen sichern den kontinuierlichen Fortbestand der Handlungs- und Funktionsfähigkeit der demokratischen und rechtsstaatlichen Grundordnung. Vorbeugende Schutzmaßnahmen sind als „Immunsystem der Handlungsfähigkeit" von politischen Funktionsträgerinnen und Funktionsträgern zu verstehen. Die Schutzmaßnahmen werden fortwährend auf Plausibilität und Effektivität geprüft, um entsprechend auf wechselnde Bedrohungsarten und Gefährdungsintensitäten reagieren zu können.

Neben der Veranlassung gefährdungsbezogener Personen- und Objektschutzmaßnahmen und der Evaluierung des Sicherheitsniveaus von Amts- und Wohnsitzen führt die DSN weitere sicherheitsbezogene Beratungen durch. Durch Sensibilisierung und Information wird präventiv gegen Bedrohungen der inneren und äußeren Sicherheit vorgegangen.

Unmittelbar nach Amtsantritt eines Obersten Organs finden routinemäßig Sicherheitsberatungen statt, bei denen sicherheitsorientierte Verhaltensweisen besprochen und wichtige Kontaktdaten ausgetauscht werden. Im Berichtszeitraum erfolgten auch anlassbezogene Sicherheitsberatungen aufgrund kurzfristig eingetretener, gefährdungsrelevanter Umstände, beispielsweise infolge von Drohschreiben, bedrohlichen Kommentaren in sozialen Medien oder anderer verfassungsschutzrelevanter Bedrohungen, die das jeweilige Oberste Organ in der Wahrnehmung seiner gesetzlich definierten Aufgaben beeinträchtigen hätten können.

3.1.2 Aktuelle Lage

Öffentliche Aussagen und Handlungen von politischen Entscheidungsträgerinnen und Entscheidungsträgern führen oftmals zu kontroversiellen Diskursen, zu diffamierender und inkriminierender Agitation bis hin zu strafrechtlich relevanten Beleidigungen, Nötigungen und Drohungen. Themenfelder wie Österreichs Haltung zur Frage der Neutralität, Asyl- und Migrationspolitik, Gesundheitspolitik, Korruption und der Umgang mit Transparenz in der Politik, Inflation und Teuerung, Energieversorgungssicherheit und Energiekosten sowie Klimapolitik hatten im Jahr 2022 immense Polarisierungskraft und waren essentielle Einflussfaktoren bei der Beurteilung der Gefährdungsexposition einzelner Mitglieder der Bundesregierung.

Eine Grundlage zur Feststellung des Gefährdungsgrades von Obersten Organen ist ein strukturiertes Monitoring der an politische Funktionsträgerinnen und Funktionsträger gerichteten Schreiben, bei denen 2022 gesamtbetrachtet ein Rückgang um 85 % im Vergleich zum Vorjahr zu verzeichnen war. Ein Großteil aller „bedenklichen" Schreiben hatte ähnliche Beweggründe: Das Anprangern persönlicher oder fachlicher Inkompetenz, Inkriminieren im Zusammenhang mit persönlichen, politischen Skandalen oder Machtmissbrauch sowie die Bezichtigung korrupten Verhaltens. Dies sind nur einige Beispiele, wie Unmut und Protestverhalten in schriftlicher Form zum Ausdruck gebracht werden.

Zu Jahresbeginn 2022 sank die hohe Anzahl an schriftlichen Eingaben sukzessive und rasant. Im Verlauf des Frühjahrs gab es durchschnittlich nur noch circa 15 bedenkliche Schreiben pro Monat, die Anzahl blieb bis zum Jahresende auf diesem Niveau.

Gleichzeitig aber war bei öffentlich einsehbaren Kommentaren in sozialen Medien eine niedrige Hemmschwelle in Sachen delegitimierender Agitation zu erkennen. Auf diese Weise wurden demokratische Entscheidungsprozesse und damit in Zusammenhang stehende politische Repräsentantinnen und Repräsentanten verächtlich gemacht oder ihnen öffentlich die Legitimität abgesprochen. Damit einhergehend ist ein Vertrauensverlust in staatliche Institutionen und deren Funktionsfähigkeit eine gesamtgesellschaftliche und sicherheitsbehördliche Herausforderung.

Im Berichtsjahr 2022 wiesen rund ein Zehntel aller in der DSN erfassten Eingaben den strafrechtlich relevanten Tatbestand einer gefährlichen Drohung, Nötigung oder schweren Nötigung auf. Im Vergleich zum Vorjahr stellt dies eine Verringerung um circa 65 % dar. Die Motivlage bei etwa der Hälfte der Drohschreiben, die überwiegend in der ersten Jahreshälfte versendet wurden, war Kritik an den von gesetzten Maßnahmen gegen die COVID-19-Pandemie. Rund ein Drittel der strafrechtlich relevanten Eingaben wurde über Social-Media-Plattformen in Form von öffentlich einsehbaren Kommentaren oder persönlichen Nachrichten, fast ein Drittel per E-Mail und circa ein Viertel analog in Briefform verfasst. Die restlichen strafrechtlich relevanten Eingaben erfolgten mittels Telefonanruf.

3.1.3 Fälle 2022

Im Vergleich zum Jahr 2021, in dem nahezu die Hälfte aller sicherheitsrelevanten Ereignisse den Tatbestand einer Sachbeschädigung an Objekten verfassungsmäßiger oder öffentlicher Einrichtungen erfüllten, war im Berichtsjahr 2022 ein deutlich spürbarer Anstieg an Aktionismus im Umfeld von verfassungsmäßigen Einrichtungen sowie direkt-konfrontativen Ereignissen in Bezug auf politische Funktionsträgerinnen und Funktionsträger zu erkennen.

Zu Jahresbeginn 2022 – dem zahlenmäßigen Höhepunkt des COVID-19-Protestgeschehens in Österreich – marschierte eine der Querdenkerszene zurechenbare Personengruppe aus Protest zum Privatwohnsitz des Landeshauptmannes von Vorarlberg.

Durch die ebenfalls vor Ort befindliche Exekutive konnte ein unbefugtes Betreten der Liegenschaft unterbunden werden.

Im Frühjahr 2022 wurde eine Nationalratsabgeordnete in einem Gastronomiebetrieb im Zuge eines Streitgesprächs über die Politik der Bundesregierung von einem Bürger tätlich angegriffen, indem er ihr ein Trinkglas ins Gesicht schleuderte. Die Politikerin blieb dabei zwar unverletzt, die attackierende Person wurde wegen versuchter Körperverletzung auf freiem Fuß angezeigt.

Im Sommer 2022 äußerte eine anfangs noch unbekannte Person auf der Social-Media-Seite eines Regierungsmitgliedes in mehreren bedenklichen Postings und in „Stalking-ähnlicher" Manier die Absicht, das Regierungsmitglied bei einigen öffentlichen Veranstaltungen aufsuchen zu wollen. Bis zum Zeitpunkt der definitiven Identifizierung des tatsächlichen Verfassers dieser beunruhigenden Postings wurden für die besagten Veranstaltungen personenbezogene Schutzmaßnahmen gesetzt. Bei diesen Veranstaltungen wurden in weiterer Folge weder der vermeintliche Verfasser selbst noch sicherheitsrelevante Vorkommnisse durch andere Personen wahrgenommen.

Während des zweiten Halbjahres 2022 wurden im Umfeld einiger Landtage und während Landtagssitzungen häufiger unangekündigte Kundgebungen abgehalten. Das Ziel einer friedlichen Blockade bei der Garageneinfahrt des Landhauses Vorarlberg, bei der sich Klimaaktivistinnen und Klimaaktivisten an einem mitgebrachten Tisch festklebten, war, Aufmerksamkeit für die aktuelle Klimaproblematik zu generieren und die Landtagsabgeordneten zu einem „Umdenken" zu bewegen. Nach freiwilligem Verlassen der Örtlichkeit wurden die Teilnehmerinnen und Teilnehmer verwaltungsrechtlich angezeigt.

Eine unangemeldete Demonstration vor dem Bundeskanzleramt im Sommer 2022, bei der sich zwei Klimaaktivisten mit ölartiger Flüssigkeit übergossen und anschließend sitzend vor dem Haupteingang verweilten, endete mit einer behördlichen Auflösung der Demonstration und der Festnahme beider Versammlungsteilnehmer.

Gegen Jahresende gelang es zwei Klimaaktivisten, die Fassade des Landhauses St. Pölten zu beschmieren – wie sich herausstellte lediglich mit Farbe und nicht wie zunächst angenommen mit Öl. Sie wurden nach geltendem Recht angezeigt.

Im Herbst 2022 versuchten mehrere Personen an einer höher gelegenen Stelle der Fassade des Innenministeriums ein Transparent anzubringen. Nachdem ein Aktivist bereits an einer Leiter emporgeklettert war, konnte dieser vom intervenierenden Objektschutzpersonal an der weiteren Ausführung des Aktionismus gehindert und die dafür bestimmten Utensilien sichergestellt werden. Die Personen waren der rechtsextremen Szene in Österreich zuzuordnen.

Die Vielfalt der geschilderten Vorfälle verdeutlicht die große Bandbreite an Gefährdungspotenzialen für Oberste Organe und verfassungsmäßige Einrichtungen in Abhängigkeit verschiedenster Beweggründe und Tatausführungsvarianten, denen nur durch effektives Zusammenwirken von präventiven und reaktiven Schutzmaßnahmen adäquat begegnet werden kann.

3.1.4 Trends und Entwicklungstendenzen

Das durch die Energie- und Wirtschaftskrise verursachte gesellschaftliche Spannungsfeld stellt in absehbarer Zeit einen wachsenden Nährboden für erhöhtes Protestpotenzial gegenüber Obersten Organen sowie verfassungsmäßigen Einrichtungen dar. Besonderes Augenmerk wird dabei auf die Entwicklung der sozioökonomischen Herausforderungen für die Bevölkerung als maßgeblichen Einflussfaktor zu legen sein. Sollte der laut Umfragen bereits vorhandene Vertrauensverlust in staatliche Strukturen größer werden, ist mit einer Zunahme an zielgerichteten Protesthandlungen unterschiedlichster Ausprägung – Drohschreiben, Aktionismus, tätliche Übergriffe – gegen Oberste Organe und verfassungsmäßige Einrichtungen zu rechnen.

Eine ähnliche Entwicklung ist in Bezug auf die Klimakrise zu erwarten. Aufgrund von Protesthandlungen im Nahbereich von verfassungsmäßigen Einrichtungen ist eine Verlagerung von klimaaktivistischen Aktionen vom öffentlichen Raum hin zu staatlichen Institutionen festzustellen. Bleiben klimapolitische Forderungen von Klimaaktivistinnen und Klimaaktivisten unerfüllt, so könnte die dadurch induzierte Frustration in radikaler werdende Formen des zivilen Ungehorsams münden, um den Druck auf politische Entscheidungsträgerinnen und Entscheidungsträger sukzessive zu erhöhen.

Die systematische Analyse der bereits zu beobachtenden und sich allmählich verschärfenden Heterogenität und Interdependenz von sowohl innen- als auch außenpolitischen Themen wird in Zukunft bei Gefährdungseinschätzungen von Obersten Organen und verfassungsmäßigen Einrichtungen eine noch gewichtigere Rolle einnehmen. Das daraus resultierende frühzeitige Erkennen relevanter Gefährdungspotenziale ist die Basis zur proaktiven Etablierung vorbeugender Schutzmaßnahmen.

Das vom Ministerrat bereits beschlossene und vermutlich 2023 in Kraft tretende Krisensicherheitsgesetz beinhaltet die wesentlichen Regelungen für ein gesamtheitliches Vorgehen aller verfassungsmäßigen Einrichtungen in Krisensituationen. Die darin geregelten Prozesse werden sowohl für die Verbesserung der ressortübergreifenden Interaktion als auch für die individuellen Krisenvorsorgebestrebungen – insbesondere bei der Erstellung von Blackout-Vorsorgeplänen – einen wesentlichen Mehrwert darstellen, zusätzliche Handlungssicherheit bieten und so insgesamt zur Erhöhung der Resilienz von verfassungsmäßigen Einrichtungen beitragen.

3.2 Schutz kritischer Infrastruktur

3.2.1 Überblick

Das „Österreichische Programm zum Schutz kritischer Infrastrukturen“ (Austrian Programme for Critical Infrastructure Protection – APCIP 2014) regelt die staatlichen Schutzmechanismen, um die Resilienz strategisch wichtiger Unternehmen stärken zu können. Die Umsetzung zur Erhöhung der Sicherheit kritischer Infrastruktureinrichtungen obliegt im strategischen Bereich dem Bundeskanzleramt und dem Bundesministerium für Inneres. Die DSN und die für Staatsschutz zuständigen Organisationseinheiten der Landespolizeidirektionen setzen das Programm operativ um und sind für konkrete Maßnahmen zum vorbeugenden Schutz gefährdeter Unternehmen und Objekte zuständig.

Die Versorgung der Bevölkerung und der Wirtschaft fußt auf einer komplexen und sehr vernetzten Infrastruktur. Um den Schutz dieser hochkomplexen Versorgungswege umfassend gewährleisten zu können, bedarf es einer funktionierenden Kooperation zwischen staatlichen Stellen und Betreibern kritischer Infrastrukturen. Eine intensive Kommunikation, Beratungen zu sicherheitsrelevanten Themen, gemeinsame Workshops und Objektschutzmaßnahmen zielen auf eine vertrauensvolle Zusammenarbeit ab. Seit Beginn der COVID-19-Pandemie haben sich die Unterstützungsleistungen der DSN für die Betreiber stetig erhöht. Nicht zuletzt hat der Ukraine-Krieg und die damit einhergehende massive Reduktion von Energielieferungen die Zusammenarbeit mit den für kritische Infrastrukturunternehmen Verantwortlichen nachhaltig vertieft.

3.2.2 Aktuelle Lage

Der Stellenwert des Schutzes kritischer Infrastrukturen stieg in der Wahrnehmung der österreichischen Bevölkerung im Jahr 2022 merklich an. Bereits seit Beginn der COVID-19-Pandemie nahm die mediale Aufmerksamkeit gegenüber dem damit einhergehenden Protestgeschehen gegen kritische Infrastruktureinrichtungen (etwa im Gesundheitssektor) sukzessive zu. Seit Beginn des Ukraine-Kriegs ist der mediale Fokus nun vermehrt auf den Energiesektor gerichtet.

Sicherheitsrelevante Bedrohungsszenarien wie Sabotageakte und Störungen beziehungsweise Zerstörungen im Energiesektor nahmen im Berichtszeitraum zu. Aber auch Klebe-, Beschmierungs- und Besetzungsaktionen durch Klimaaktivistinnen und Klimaaktivisten prägten das Jahr 2022.

Drohungen gegen Gesundheitspersonal, Sicherheitspersonal oder gegen das Personal öffentlicher Verkehrsmittel erzeugten nicht nur in den genannten Branchen ein Klima der Unsicherheit. Zwar gingen Demonstrationen und Kundgebungen vor Krankenhäusern und Gesundheitseinrichtungen durch Corona-Maßnahmen-Gegner und die „Demokratie ablehnende Szene“ (DAS) im Berichtszeitraum zahlenmäßig zurück, nichtsdestotrotz stellen

Agitationen aus dem Kreis weltanschaulich motivierter DAS-Aktivistinnen und -Aktivisten auch weiterhin ein realistisches Gefährdungspotential für kritische Infrastrukturen dar.

Im Gesundheits- und Pflegebereich kam es zudem zu Protestveranstaltungen durch Mitarbeiterinnen und Mitarbeiter, die auf den akuten Personalmangel und die Missstände in ihren Bereichen hinweisen wollten. Die generell angespannte Personalsituation wurde durch die Auswirkungen der COVID-19-Pandemie verstärkt und führte in vielen Krankenhäusern und Kliniken zu einem Personalnotstand aufgrund von Kündigungen und Langzeitkrankenständen. Diese Personalnotstände könnten in weiterer Folge die Aufrechterhaltung des Betriebes einzelner, aber auch mehrerer Krankenhäuser gefährden und dadurch das Gesundheitssystem überlasten.

Einen weiteren Risikofaktor stellen die seit Beginn des russischen Angriffskrieges sprunghaft angestiegenen Energiepreise und die Abhängigkeit Europas von russischen Brennstoffen dar. Österreichs Wirtschaft und Energieendverbraucher waren oder sind zum Teil immer noch auf Erdgas aus Russland angewiesen. Aufgrund des Krieges wurden von der Europäischen Union mehrere Sanktionspakete gegen Russland verhängt. Als Reaktion darauf wurden die Mengen der vereinbarten Gaslieferungen durch die russischen Vertragspartner an den Gasübernahmestationen und Verteilknoten der europäischen Gasinfrastruktur verringert. Die Minderlieferungen russischen Erdgases wurden durch unübliche und technisch nicht begründbare Wartungs- beziehungsweise Revisionsarbeiten an den russischen Förder- und Transportanlagen für Erdgas flankiert, was die notwendige Gasbevorratung für die Wintersaison 2022/2023 in Europa zusätzlich erschwerte. Ersatzlieferungen für das fehlende russische Erdgas erfolgten in der zweiten Jahreshälfte 2022 neben anderen Quellen hauptsächlich durch Norwegen, wobei der österreichischen Speicher- und Verteilinfrastruktur für Erdgas eine tragende Rolle in der Versorgung und Weiterleitung innerhalb Europas zukam. Österreichs Ziel, die heimischen Erdgasspeicher für den Winter 2022 zu füllen, wurde erreicht.

Im September des Berichtsjahres wurden die von Russland durch die Ostsee nach Europa führenden Gaspipelines Nordstream 1 und Nordstream 2 durch einen offensichtlichen Sabotageakt stark beschädigt, wodurch diese als Transportinfrastruktur für Erdgasimporte auf unbestimmte Zeit ausfielen. Ein Problem bei der Suche nach Ersatzlieferanten stellen jedoch die langfristigen Lieferverträge da, die die Produktionsländer wünschen, was wiederum der österreichischen Zukunftsperspektive in der Stromerzeugung widerspricht. Zudem besteht Konkurrenz mit anderen Staaten, die ihrerseits längerfristige Abnahmen zusichern.

Gerade die derzeitigen Bestrebungen Österreichs, die Stromproduktion zu dekarbonisieren (Ausstieg aus fossilen Brennstoffen), erfordern eine ausreichende Gasbevorratung zur Regelenergieerzeugung. Die stark von Umweltparametern abhängigen volatilen erneuerbaren Energieformen wie Photovoltaik und Windkraft setzen eine oft kurzfristig

verfügbare Regelreserve durch Wärmekraftwerke zur Stabilisierung des Stromnetzes voraus, um eine ausfallsichere Versorgung der heimischen Stromkunden sicherzustellen.

Durch die rudimentären Energiealternativen ergibt sich in der Folge eine herausfordernde Situation, da es bei Ausfall der herkömmlichen Strom- und Gaslieferungen zu schwerwiegenden Auswirkungen für die Versorgungssicherheit der österreichischen Bevölkerung kommen kann. Die Sensibilisierung der Verantwortlichen von kritischen Infrastrukturen und damit einhergehend die Bereitschaft, alternative Energiequellen einzusetzen, hat insgesamt seit Beginn des Ukraine-Krieges zugenommen.

Der Angriffskrieg Russlands gegen die Ukraine wirkt sich dabei nicht nur auf die Energiewirtschaft aus, sondern beeinflusst auch die Lebensmittelmärkte. Die Abhängigkeit Österreichs von Lebensmittelimporten ist jedoch als gering einzustufen. Die österreichischen Exporte im Lebensmittelsektor überwiegen deutlich, wodurch eine grundlegende Versorgungsicherheit mit Lebensmitteln in Österreich als gewährleistet angesehen werden kann. Gleichzeitig sind die Wirtschaftlichkeit und die Wettbewerbsfähigkeit in der gesamten Wertschöpfungskette eine Herausforderung. Die Situation im Lebensmittelhandel in Bezug auf die Lieferketten ist in Teilbereichen weiterhin angespannt, beispielsweise aufgrund von Lieferausfällen in einigen Branchen, durch Probleme bei Verpackungsmaterial sowie Engpässen im Transport- und Logistiksektor auf Grund fehlender Kapazitäten und fehlendem Kraftfahrpersonal.

Weiters stehen die Betreiber kritischer Infrastrukturen unter besonders hohem Digitalisierungsdruck. Neue Technologien werden zügig eingeführt, um den Anforderungen des Marktes gerecht zu werden – gleichzeitig vergrößert jede neue Komponente in Unternehmensnetzwerken und jede zusätzliche Zugriffsmöglichkeit auf ein System die Angriffsfläche, die von Cyberkriminellen ausgenützt werden könnte. Darüber hinaus setzen die Energieversorger zunehmend auf intelligente Stromnetze und Messsysteme. Industrielle Kontrollsysteme werden aus der Distanz nicht nur bedient, sondern auch gewartet. Im Gesundheitswesen wiederum nimmt die Zahl und die Weiterentwicklung medizinischer Geräte zu, bis hin zu Analysegeräten, die die Patientinnen und Patienten tragen und bedienen. Der Ausbau von Fernwartung und Fernbedienung stellt daher ein nicht zu unterschätzendes Sicherheitsrisiko dar.

Zudem lassen sich vermehrt hybride Angriffe auf die Energieinfrastruktur durch staatliche oder nichtstaatliche Akteurinnen und Akteure beobachten. Beispiele dafür sind Sabotageangriffe auf die Bahn in Deutschland im Oktober 2022 und Angriffe auf Gaspipelines in der Nordsee im September 2022. Auch sogenannte Supply Chain Attacks, das heißt Angriffe auf Lieferketten, werden zunehmend beobachtet. Dabei stehen Unternehmen, die spezielle Ausrüstungen und Dienstleistungen für kritische Infrastrukturunternehmen anbieten, im Fokus der Angreiferinnen und Angreifer.

3.2.3 Fälle 2022

Unternehmen mit geschäftlichem Bezug zu Russland befanden sich aufgrund des russischen Angriffskrieges gegen die Ukraine besonders im Fokus der Öffentlichkeit. So war ein Unternehmen aus dem Finanzsektor Ziel von Demonstrationen, bei denen der Rückzug des Institutes aus Russland gefordert wurde, gleichzeitig stand es im Visier des Hacker-Kollektivs „Anonymus“. Das Unternehmen wurde mittels Ultimatums in offenen Social-Media-Kanälen aufgefordert, sich aus Russland zurückzuziehen.

Im Jahr 2022 kam es vor allem in Wien zu mehreren Straßenblockaden durch die Aktivistinnen- und Aktivistengruppe „Letzte Generation“, die durch Blockaden an wichtigen neuralgischen Punkten des Wiener Straßenverkehrs niedrigere Tempolimits als Sofortmaßnahmen gegen die Klimakrise fordert. Durch Festkleben der Aktivistinnen und Aktivisten an den Straßen wurde eine rasche Räumung der Blockade verhindert und es kam zu zeitweiligen Behinderungen im Straßenverkehr. Störungen im Verkehr treffen auch Rettungseinsätze und Transportunternehmen der kritischen Infrastruktur, die dadurch möglicherweise behindert werden könnten.

In der ersten Jahreshälfte 2022 fanden an der für die heimische Treibstoffproduktion notwendigen Hauptdestillationsanlage der Raffinerie Schwechat Wartungsarbeiten statt. Bei den abschließenden Überprüfungen der Anlage kam es infolge einer Druckprobe zu einem technischen Gebrechen, bei dem ein Druckbehälter zerstört wurde und die gesamte Destillationsanlage außer Betrieb genommen werden musste. Die Folge waren

zeitweise Engpässe in der Versorgungssicherheit der österreichweiten Treibstoffversorgung. Diese wurden durch den Einsatz einer kleineren Destillationsanlage sowie die mehrfache Freigabe der staatlichen Ölreserve ausgeglichen. Die Hauptdestillationsanlage konnte nach umfangreichen Reparaturarbeiten im Oktober 2022 wieder in Betrieb genommen werden. Die Wiederauffüllung der zwischenzeitlich freigegebenen staatlichen Ölreserve wird bis Ende des ersten Quartals 2023 abgeschlossen sein.

Der Gesundheitssektor war wie schon im Vorjahr von den Auswirkungen der COVID-19-Pandemie massiv betroffen. Maßnahmen wie die Maskenpflicht, die Vorlage eines negativen COVID-Tests und limitierte Patientinnen- und Patienten-Besuche führten vor allem im ersten Halbjahr 2022 zu Ordnungsstörungen und aggressiven Handlungen gegenüber dem Krankenhaus- und Sicherheitspersonal. Bezogen sich im Berichtsjahr 2021 Kundgebungen und Demonstrationen vor Krankenhäusern und Gesundheitseinrichtungen überwiegend auf Corona-Schutzmaßnahmen, Verordnungen und Gesetze, war ein Großteil dieser im Berichtsjahr 2022 auf die angespannte Lage aufgrund des fehlenden beziehungsweise abwandernden Personals und die Unzufriedenheit über die Gehälter zurückzuführen. Protestaktionen des Personals sollten auch auf fehlendes Personal und damit verbunden auf eine eingeschränkte Versorgung im Gesundheitssystem hinweisen.

Demonstrationen gegen Corona-Schutzmaßnahmen, wie sie in den vergangenen Jahren oftmals stattgefunden haben, führten 2022 zu einer Gesetzesänderung. Da als Folge von Kundgebungen der Betrieb von Gesundheitseinrichtungen und damit auch die Versorgung von Patientinnen und Patienten gefährdet werden kann, wurde mit § 36a Abs. 1a iVm Abs. 3a SPG (Schutzzone) für Sicherheitsbehörden die Möglichkeit geschaffen, Schutzzonen rund um Krankenhäuser und Gesundheitseinrichtungen zu verordnen, sofern es zu einer möglichen Störung beziehungsweise Gefährdung dieser Einrichtungen kommen kann. Durch diese Maßnahmen sollen vor allem vorab angekündigte Aktionen entschärft und verhindert werden.

Auch Aktivismus von protestierenden Klimaschützerinnen und Klimaschützern sorgte für Störungen im Transportsektor. So klebten sich beispielsweise Klimaaktivistinnen und Klimaaktivisten der Gruppierung „Letzte Generation“ auf dem Rollfeld des Berliner Flughafens fest und legten den Flugverkehr lahm. Auch in Österreich wurde versucht, im Bereich des Flughafens Schwechat klimabezogenen Aktivismus umzusetzen.

3.2.4 Trends und Entwicklungstendenzen

Die Beeinträchtigung der Versorgungssicherheit der österreichischen Bevölkerung, verursacht durch den Ukraine-Krieg, wird im Bereich der Energieversorgung weiterhin eine nicht unerhebliche Rolle spielen. Es bleibt abzuwarten, in welchem Ausmaß russisches Gas und Öl dauerhaft substituiert werden kann. Durch das aus den EU-Sanktionen gegen Russland resultierende Ölembargo ergibt sich die Notwendigkeit, Ersatzlieferungen aus anderen Ländern zuzukaufen oder bestehende Liefervereinbarungen auszuweiten.

Der wichtigste Rohöllieferant der heimischen Ölindustrie ist Kasachstan mit einem Anteil von knapp 40 % der österreichischen Ölimporte. Die Lieferkette des kasachischen Rohöls erfolgt teilweise über russisches Territorium und erfordert die Nutzung örtlicher Pipelines und Hafenterminals, wodurch weiterhin Abhängigkeiten von Russland in Bezug auf die heimische Versorgung mit Rohöl bestehen. Um die Abhängigkeit von russischem Gas kompensieren zu können, wird erwogen, die Importform des Energieträgers zu diversifizieren und sich an europäischen Initiativen für den Import von „Liquefied Natural Gas" (LNG) zu beteiligen. Ein Vorteil von LNG-Importen liegt im raschen Aufbau von Handelsbeziehungen, da der zeitintensive Bau von Pipelines entfällt und zum Transport teils auf bestehende Infrastruktur zurückgegriffen werden kann. Dabei muss jedoch der Wettbewerb bezüglich der Verfügbarkeit am Weltmarkt mitbedacht werden. Die bereits beschriebene Langfristigkeit der Verträge stellt eine weitere nicht zu unterschätzende Hürde dar.

Im Teilsektor Strom wird durch das „Gesetz über den Ausbau erneuerbarer Energien" (Erneuerbaren-Ausbau-Gesetz) geregelt, wie die Rahmenbedingungen für den Ausbau des zukünftigen österreichischen Stromsystems zu gestalten sind. Es ist vorgesehen, die gesamte Menge des in Österreich benötigten Stroms aus erneuerbaren Energien zu generieren. Fundament für eine stabile und sichere Stromversorgung ist ein funktionierendes und ausfallsicheres Übertragungsnetz, welches durch den Einsatz neuer Übertragungstechnologien auf bereits bestehenden Freileitungen und die Installation besonders leistungsfähiger Transformatoren optimiert wird. Um das Ziel der Strombedarfsdeckung zur Gänze aus erneuerbaren Energien zu erreichen, ist die Errichtung neuer Infrastrukturen und die damit verbundene Durchführung von Umweltverträglichkeitsprüfungen unumgänglich, die allerdings mit langen Verfahrensdauern verbunden sind.

Angriffe auf die Verkehrsinfrastrukturen in der Ukraine sowie Blockaden an den ukrainischen Häfen führten im Berichtszeitraum zu Lieferschwierigkeiten und Rückgängen bei den Ausfuhren von Getreide und Ölfrüchten aus der Ukraine. Dadurch verschoben sich nicht nur die Lieferländer und folglich auch die Lieferketten, sondern sanken auch die österreichischen Importe. Aufgrund neuer Importquellen ist die österreichische Versorgungslage derzeit jedoch gut und wird auch für das Jahr 2023 als stabil angesehen.

Wie bei vielen anderen Produkten sind Lieferengpässe auch bei Medikamenten ein ernst zu nehmendes Problem. Aufgrund der Tatsache, dass ein Großteil der Arzneimittelproduktion beziehungsweise der Wirkstoffproduktion aus Europa ausgelagert wurde und nun vorwiegend in Asien stattfindet, besteht in Europa eine große Abhängigkeit von diesen Staaten. Von Seiten der Europäischen Union gibt es deshalb Anstrengungen zur Bevorratung von Medikamenten in den einzelnen Mitgliedsländern. Langfristig sollte jedoch intendiert sein, die Produktion wieder in Europa zu etablieren, um bei der Medikamentenproduktion und -lieferung auch nachhaltig unabhängig zu werden.

Die Sicherheitslage wird im Kontext der aktuell erhöhten Lebenserhaltungskosten angespannt bleiben. Auch die erheblichen Personalengpässe in vielen Bereichen wie Gesundheit, Handel, Tourismus oder im Facharbeitsbereich können zu einem vermehrten Protestgeschehen führen. Strafbare Handlungen gegen Objekte der kritischen Infrastrukturen können daher nicht ausgeschlossen werden. Bei Straßenblockaden und anderen Formen des Aktionismus durch Klimaaktivistinnen und Klimaaktivisten ist ebenso ein Anstieg festzustellen.

3.2.5 Schutz kritischer Infrastrukturen und die Bedeutung der Resilienz dieser Einrichtungen

Eine ordnungsgemäß funktionierende Infrastruktur ist essentieller Bestandteil einer modernen Gesellschaft. Die steigende Abhängigkeit von funktionierenden Infrastrukturen zeigt sich nicht nur im täglichen Leben, sondern besonders in Krisensituationen. Die Versorgung mit Wasser, Lebensmittel, Energie oder Informationen, aber auch eine funktionierende Gesundheitsversorgung sowie die Funktionsfähigkeit des Staates an sich werden als selbstverständlich vorausgesetzt. Die hohe Versorgungssicherheit, wie sie Österreich in der Stromversorgung mit einem aktuellen Spitzenwert von 99 % aufweist, reduziert gleichzeitig das Bewusstsein für die Vulnerabilität selbiger. Die Nichtbeachtung der Verwundbarkeit kritischer Infrastruktur wird in der Literatur auch als „Verwundbarkeitsparadoxon“ bezeichnet. Gerade aufgrund der hohen Versorgungssicherheit sind bei tatsächlichen Vorfällen die Auswirkungen umso größer, da eine alternative Vorsorge kaum vorhanden ist. Diese mangelnde Vorsorge betrifft nicht nur private Haushalte, sondern die gesamte Wirtschaft. Die lange Zeit als sicher geltenden Lieferketten führten zu einem Verzicht des Auf- oder Ausbaus von Lagerkapazitäten und zu einer Just-in-time-Produktion. Sowohl die COVID-19-Pandemie als auch der Vorfall des Containerschiffs „Ever Given“, das im Suezkanal feststeckte und somit eine wichtige Handelsroute blockierte, machten die damit verbundenen volkswirtschaftlichen Auswirkungen solcher Lieferkettenunterbrechungen deutlich.

Wie fragil die Versorgung der Bevölkerung und der Wirtschaft mit notwendigen Gütern sein kann, wurde spätestens mit dem Sabotageakt an den Nord-Stream-Pipelines nahe der dänischen Insel Bornholm im September 2022 offensichtlich. Ein weiterer Sabotageakt am 8. Oktober 2022 hatte den Ausfall des Zugverkehrs in Teilen Norddeutschlands zur Folge. Bei beiden Sabotageakten wurde einschlägiges technisches Wissen eingesetzt, um größtmöglichen Schaden anzurichten.

Die Versorgung mit Gas, Strom, Erdöl, Wasser, Daten und weiteren notwendigen Gütern fußt letztendlich auf einfachen mechanischen Verteilungssystemen, die mit krimineller Energie störbar und schlussendlich auch zerstörbar sind. Physische Schwachstellen finden sich in beinahe jedem System. Zusätzlich zur relativ einfachen Möglichkeit einer Störung beziehungsweise Zerstörung kommt der Umstand hinzu, dass derartige Handlungen an Versorgungssystemen kaskadenartige Auswirkungen nach sich ziehen können: Fällt ein

grundlegendes System wie die Stromversorgung aus, beeinflusst dies auch alle anderen Versorgungssysteme. Aus diesem Grund sind Anlagen der kritischen Infrastruktur als potenzielle Ziele für Angriffe jeglicher Art anzusehen, sei es im Umfeld des Klimaaktivismus, als Mittel der hybriden Kriegsführung oder als Ziel für terroristische Anschläge.

In Deutschland zeigten im Frühjahr/Sommer 2022 Aktivitäten im Bereich des Klimaaktivismus bei Energieversorgungseinrichtungen sehr deutlich, dass neben dem Ziel, Aufmerksamkeit zu erlangen, seitens der Klimaaktivistinnen und Klimaaktivisten sowohl Schäden im Bereich der Versorgungssicherheit als auch Kollateralschäden im Zusammenhang mit ihren Aktionen zunehmend akzeptiert werden.

Im Berichtsjahr 2022 wurden im Umfeld kritischer Infrastrukturen auch Handlungen bekannt, die als Spionagetätigkeiten einzuordnen waren. So wurden beispielsweise im Ausland bei mehreren Atomkraftwerken, aber auch bei anderen Objekten der kritischen Infrastruktur, vermehrt Drohnen gesichtet, die möglicherweise der Aufklärung zur Vorbereitung für etwaige spätere Aktionen dienten.

Da kein System vollständig und absolut lückenlos gesichert werden kann, findet derzeit ein Paradigmenwechsel statt. Dabei verlagert sich der Fokus immer mehr von der Gefahrenabwehr in Richtung Resilienz. Organisationen sollen folglich nach einem Vorfall möglichst schnell wieder handlungsfähig sein und eingetretene Schäden möglichst rasch behoben werden können. Die Umsetzung zielführender Schutzmaßnahmen sowie die Bildung von Resilienz sind ein komplexes Unterfangen. Im Berichtsjahr setzte der Verfassungsschutz verschiedene präventive und situationsgebundene Schutzmaßnahmen für kritische Infrastruktureinrichtungen. Auch präventive Konzepte und Maßnahmenkataloge für den Eintritt eines Ernstfalles werden laufend und gemeinsam mit den Unternehmen der kritischen Infrastruktur erarbeitet.

Ein Zeichen für die steigende Bedeutung des Schutzes kritischer Infrastruktur setzte die Europäische Union. Mit der Umsetzung der Richtlinie „Resilienz kritischer Einrichtungen“ (RKE-Richtlinie) wird der koordinierte Schutz digitaler und physischer Entitäten angestrebt. Aufgrund der aktuellen Bedrohungslage wurde durch die Europäische Kommission die Umsetzung in nationales Recht nicht abgewartet, sondern vorab ein 5-Punkte-Plan verabschiedet, der die wichtigsten Maßnahmen herausstreicht und die Mitgliedsstaaten dazu anregt, dem Schutz kritischer Einrichtungen einen besonderen Stellenwert zukommen zu lassen und diesbezügliche Maßnahmen umzusetzen.

In Anbetracht der steigenden Bedrohung durch die genannten unterschiedlichen Protagonistinnen und Protagonisten wird dem Schutz der kritischen Infrastruktur in Zukunft eine noch höhere Bedeutung zukommen müssen, da der Wegfall der Versorgungssicherheit von Gesellschaft und Wirtschaft ein Nährboden für gesellschaftliche Verwerfungen und damit zum sozialen Unfrieden werden kann.

3.3 Staatsschutzprävention

3.3.1 Konzeptionierung der österreichischen Staatsschutzprävention – Erschaffung neuer Präventionsstrukturen

Das Kernelement der **Staatsschutzprävention** als Teil eines kooperativen gesamtstaatlichen und gesamtgesellschaftlichen Sicherheitsansatzes eines zukunftsorientierten Staatsschutzes ist die Wissensvermittlung. Als zentrale Anlaufstelle für Aus-und Fortbildungen innerhalb des gesamten Bundesministeriums für Inneres zum Themenkomplex Extremismusprävention spielt sie eine tragende Rolle zur Vorbeugung und Verhinderung aller Formen des Extremismus.

Im Mittelpunkt der ersten dreizehn Monate DSN stand für den neu geschaffenen Bereich der Staatsschutzprävention die Konzeptionierung einer klaren fachlichen und standardisierten Struktur, um zukünftig zielgruppenorientiert, schnell, effizient und effektiv Präventionsmaßnahmen umsetzen zu können. Angelehnt an die Struktur der Kriminalprävention im Bundeskriminalamt wurde auch die Präventionsstruktur im Staatsschutz festgelegt, wobei die DSN für die Staatsschutzprävention national und international als Ansprechpartnerin und fachlich verantwortliche Stelle agiert. Die Koordination und Umsetzung der operativen Präventionsarbeit im Staatsschutz in den Bundesländern fällt in die Verantwortung der für Staatsschutz zuständigen Organisationseinheiten der Landespolizeidirektionen. Der flächendeckende Ausbau der Präventionsstrukturen ist und bleibt dabei eine Prämisse für erfolgreiche Präventionsarbeit und stellt die strategische Ausrichtung der Staatsschutzprävention dar.

3.3.2 Standardisierte Ausbildungsstruktur für Präventionsbedienstete

Die operative Staatsschutzprävention fungiert als zentrale Anlaufstelle für Aus- und Fortbildungen innerhalb des Bundesministeriums für Inneres im Themenschwerpunkt Extremismusprävention. Die Einbindung neuester Erkenntnisse aus Wissenschaft und Forschung aus dem Bereich Extremismusprävention in die Wissensvermittlung setzt stetigen nationalen und internationalen Austausch mit Expertinnen und Experten und Gremien voraus. Um dem Ziel eines breiten Ansatzes der Staatsschutzprävention gerecht zu werden sowie effiziente, schnelle und effektive Wirkung der staatspolizeilichen Präventionsarbeit zu gewährleisten, wurde eine standardisierte Ausbildung für Präventionsbedienstete erarbeitet, die 2023 in Umsetzung geht. Die ausgebildeten Präventionsbeamtinnen und Präventionsbeamten werden nicht mehr nur im formellen schulischen Kontext, sondern auch für Organisationen, Institutionen und staatliche Einrichtungen auf Ebene der Gemeinden und Bezirke als Ansprechpartnerinnen und Ansprechpartner fungieren. Im Sinne des gesamtgesellschaftlichen Ansatzes, wonach

Extremismusprävention auch in der Verantwortung jeder Bürgerin und jedes Bürgers liegt, soll die Zusammenarbeit und Kommunikation mit der Bevölkerung durch diese speziell geschulten Präventionsbeamtinnen und Präventionsbeamten gestärkt werden. Denn nur durch ein gemeinschaftliches Handeln kann Tendenzen der Polarisierung und Radikalisierung rechtzeitig entgegengewirkt werden.

3.3.3 Zielgruppenorientierte Präventionsarbeit – Jugendliche und Erwachsene

Die Grundlage für den Schutz unserer Demokratie sind aufgeklärte und wachsame Bürgerinnen und Bürger, die in der Lage sind, extremistische Bestrebungen als solche zu erkennen und wissen, was sie tun können, wenn sie derartige Tendenzen in ihrem Umfeld bemerken. Dennoch ist es notwendig, wesentliche Zielgruppen im Vorfeld zu identifizieren, um Präventionsmaßnahmen zur Wissensvermittlung zielgerichtet planen und umsetzen zu können.

In der Radikalisierungsforschung gelten Jugendliche in schwierigen und als krisenhaft empfundenen Lebensumständen in Kombination mit der für die Altersphase typischen Sinn- und Orientierungssuche als besonders empfänglich für extremistische Weltbilder. Junge Menschen sind in besonderem Maß auf der Suche nach Sinn, nach ihrer öffentlichen und auch privaten Rolle und Stellung in der Gesellschaft sowie nach Orientierung. Sie befinden sich in teilweise konfliktbeladenen Abnabelungsprozessen von ihren Eltern und müssen vielfältige Entwicklungsaufgaben meistern. In einer zunehmend komplexen und teils als unsicher empfundenen Welt können einfache Erklärungen und eindimensionale Identitätskonstruktionen daher erhebliche Anziehungskraft haben. Extremistische Akteurinnen und Akteure nutzen diese Lebenssituation, indem sie mit speziell auf Jugendliche zugeschnittenen Angebote auf diese zugehen, um sie für ihre Ideologien und Organisationen zu gewinnen.

Als besonders vulnerable Zielgruppe stehen daher Jugendliche im Alter von 13 bis 17 Jahren im Fokus der Maßnahmen der Staatsschutzprävention. So wurde die Staatsschutzprävention mit Jugendlichen im Gesamtkonzept der polizeilichen Präventionsarbeit „UNDER 18“ als zusätzliches Programm etabliert, um den Ansatz der lebenskompetenzorientierten Präventionsarbeit auch im Staatsschutz zu etablieren. Die Umsetzung des Programms ist im Schuljahr 2023/2024 geplant.

Der „**lebenskompetenzorientierte Präventionsansatz**“ charakterisiert den aktuellen Zeitgeist in der Präventionsarbeit mit Jugendlichen. Seine Methoden sind an die notwendigen, Resilienz steigernden Lebenskompetenzen wie Konfliktfähigkeit, Kommunikation, Beziehungsaufbau und Gewaltfreiheit angelehnt.

Um einen möglichst breiten Präventionsansatz zu gewährleisten, wird neben der Zielgruppe der Jugendlichen auch die Zielgruppe der Erwachsenen in die Präventionsarbeit aufgenommen. Diese Zielgruppe wird mit Sensibilisierungsmaßnahmen und Informationen zu aktuellen Staatsschutzthemen erreicht. Der Fokus dieser Präventionsmaßnahme liegt darauf, Erwachsenen Radikalisierungsprozesse zu veranschaulichen, um Radikalisierungsanzeichen rechtzeitig erkennen zu können. Dabei ist es auch wichtig, Risikofaktoren in den Blick zu nehmen und zu hinterfragen, worin die Anziehungskraft von extremistischen Gruppen liegt und welche Angebote diese ihren Anhängerinnen und Anhängern machen. Nur dann kann man Radikalisierungsprozesse verstehen und ihnen gesamtgesellschaftlich entgegentreten.

3.4 Strategische Prävention im Aufgabenbereich Nachrichtendienst

Die strategische Prävention ist im nachrichtendienstlichen Bereich des Verfassungsschutzes angesiedelt und gliedert sich in zwei Einsatzbereiche: den strategischen Sensor und die Primärprävention. Die gesetzliche Ermächtigung nach § 8 SNG ermöglicht die Gewinnung und Analyse von Informationen zur Beurteilung von verfassungsschutzrelevanten Bedrohungslagen, welche in der Folge Grundlage für den Einsatz als strategischer Sensor sind. Die Primärprävention spricht ein möglichst breites Feld an Rezipientinnen und Rezipienten an und dient der grundsätzlichen Sensibilisierung der Bevölkerung zu Themen der Extremismusprävention.

3.4.1 Strategischer Sensor

Der Nachrichtendienst wurde als Frühwarnsystem zum Schutz der Bevölkerung vor verfassungsschutzrelevanten Bedrohungen eingerichtet. Die strategische Prävention steht bezüglich aller Aufgabenbereiche der DSN im engen Austausch mit der Wissenschaft, zivilgesellschaftlichen Organisationen und anderen Ministerien. Ziel ist es, sich auf dem aktuellen Stand des wissenschaftlichen Diskurses zu befinden und neue sowie bereits bestehende Phänomene aufgrund eines breiten Basisverständnisses in einer auf strategischer Ebene durchgeführten Analyse einordnen und bewerten zu können. Die Vernetzung und der Austausch mit Expertinnen und Experten aus der Wissenschaft stellt einen zusätzlichen Mehrwert im Bereich des Wissensaufbaus dar und unterstützt die Analyse von Phänomenen mit zusätzlicher Fachexpertise. Die verschiedenen Sichtweisen von Sicherheitsbehörden wie der DSN einerseits und Expertinnen und Experten aus Wissenschaft und Forschung andererseits sind eine Bereicherung für beide Seiten und auch auf internationaler Ebene ein weitverbreitetes Modell.

3.4.2 Primärprävention

Das durch die DSN koordinierte „Bundesweite Netzwerk Extremismusprävention und Deradikalisierung“ (BNED) feierte 2022 sein fünfjähriges Bestehen. Das BNED ist das zentrale Gremium zum Informationsaustausch und zur Koordination zwischen Stakeholdern der österreichischen Präventionslandschaft und damit von österreichweiten Maßnahmen der Extremismusprävention und Deradikalisierung. Die Aktivitäten im Berichtsjahr standen im Zeichen des Wiederauflebens der Strukturen nach pandemiebedingten Einschränkungen der Netzwerktätigkeiten. Der für ein strategisches Gremium zur Maßnahmensetzung unabdingbare Austausch zwischen Ministeriums- und Behördenvertreterinnen und -vertretern sowie Praktikerinnen und Praktikern aus der Zivilgesellschaft wird verstärkt fortgesetzt und wird weiterhin einen hohen Stellenwert in der Präventionsarbeit der DSN einnehmen.

„Primärprävention“: Bei der primären oder universellen Radikalisierungsprävention geht es darum, möglichst viele gesellschaftliche Gruppen zu erreichen.

„Sekundärprävention“: Bei der sekundären Prävention ist die Zielgruppe genauer definiert und bietet Hilfe in herausfordernden Lebenssituationen.

„Tertiärprävention“: Tertiäre Prävention richtet sich an Personen, die strafrechtlich relevante Handlungen gesetzt haben und bei denen ein Rückfall in extremistische Handlungsmuster verhindert werden soll.

3.4.3 Initiativen 2022

Erstmals seit 2018 konnte im Jahr 2022 wieder ein durch die DSN veranstalteter Präventionsgipfel stattfinden. Der Präventionsgipfel ist das zentrale jährliche Zusammenkommen der Präventionseinrichtungen in Österreich und dient der Vernetzung und dem Austausch zwischen der Zivilgesellschaft und behördlichen Vertreterinnen und Vertretern. Der Gipfel stand im Zeichen hybrider Bedrohungen und extremistischer Propaganda und hatte sowohl die Entwicklungen im Laufe der COVID-19-Pandemie, den Angriffskrieg Russlands gegen die Ukraine als auch die Präventionsarbeit in der Struktur der DSN zum Thema. Die unverändert große Bedeutung der Präventionsarbeit wurde in den Eingangsreden des Bundesministers für Inneres Gerhard Karner, des Generaldirektors für die öffentliche Sicherheit Franz Ruf und des Direktors der DSN Omar Haijawi-Pirchner unterstrichen.

Neben den laufenden Stakeholder-übergreifenden Vernetzungsaktivitäten im Bereich der Extremismusprävention ist es eine zentrale Aufgabe der strategischen Prävention, einen Überblick über Radikalisierungstendenzen in der Gesellschaft zu gewinnen und durch aktuelle und bedarfsorientierte Informationen mögliche Auswirkungen auf die Bevölkerung aufzuzeigen. Aus diesem Grund wurde Anfang 2022 das SORA-Institut mit einer Studie zur Frage nach „Psychosozialen Mustern extremistischer Einstellungen“

beauftragt. Das SORA-Institut führte hierzu von Mai bis Juli 2022 eine Telefon- und Onlineumfrage unter rund 2.000 Personen in Österreich durch. Diese Stichprobengröße ist repräsentativ für Österreich und erlaubte evidenzbasierte Rückschlüsse auf den Grad der Polarisierung und die Zustimmung zu rechtsextremistischen und verschwörungsideologisch aufgeladenen Narrativen.

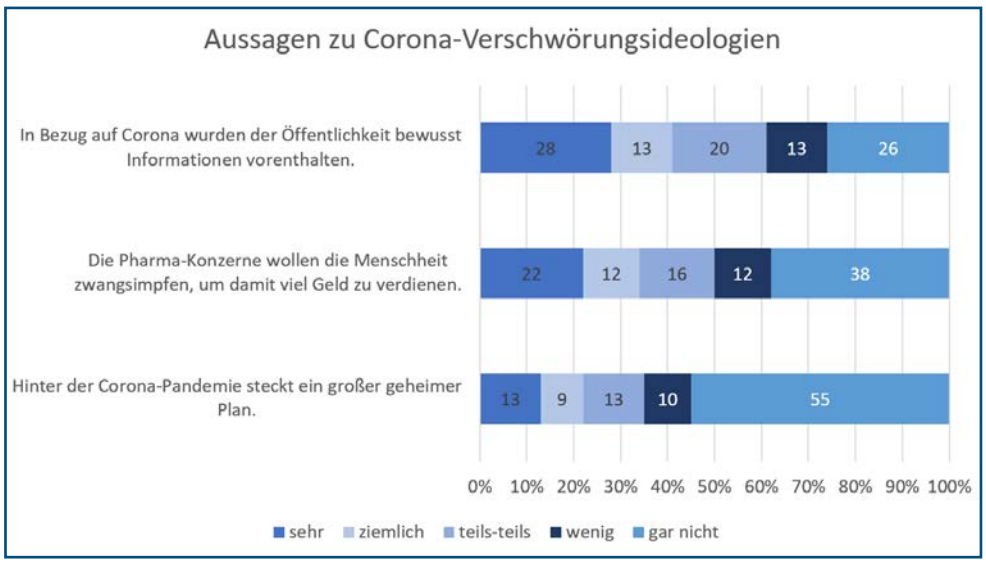

Abbildung 1:
Studie psychosoziale Muster hinter extremistischen Einstellungen in Zusammenhang mit der COVID-19 Pandemie in Österreich, Empirische Studie des SORA-Instituts im Auftrag des BMI, Wien 2022

Die Studienergebnisse zeigen, dass durch Krisen und Extremsituationen radikalere Ideen entstehen und sich in der Gesellschaft manifestieren können. Die Bewegung der Corona-Maßnahmen-Gegner hat gezeigt, dass sich diese Ideen in gesellschaftlichen Dynamiken zu Extremismen weiterzuentwickeln drohen. In Zusammenarbeit mit dem SORA-Institut wurden die Daten der Studie ausgewertet und die daraus gewonnenen Erkenntnisse werden in präventive Maßnahmen umgewandelt. Die Aufklärung von und über Verschwörungsideologien ist hierbei ein zentraler Anknüpfungspunkt für Behörden.

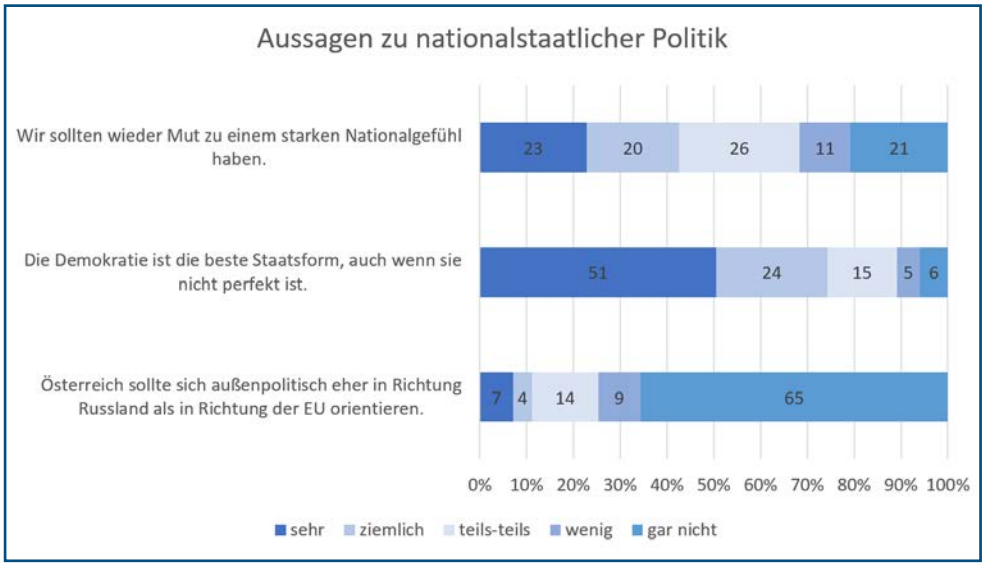

Abbildung 2:
Studie psychosoziale Muster hinter extremistischen Einstellungen in Zusammenhang mit der COVID-19 Pandemie in Österreich, Empirische Studie des SORA-Instituts im Auftrag des BMI, Wien 2022

3.5 „Synergieeffekte im Kampf gegen Terrorismus und Extremismus" – verstärkte Kooperation

Im Jahr 2022 lag ein wichtiger Fokus auf der weiteren Intensivierung der Zusammenarbeit mit dem Bundesministerium für Justiz (BMJ) – insbesondere den Staatsanwaltschaften, den Vollzugsgerichten, der Koordinationsstelle für Extremismusprävention und Deradikalisierung des Bundesministeriums für Justiz sowie den Justizanstalten in ganz Österreich. Dazu fanden regelmäßige Vernetzungstreffen zu Themen wie Aus- und Fortbildung sowie Öffentlichkeitsarbeit statt, und der Informationsaustausch zu Insassinnen und Insassen, die wegen einer strafbaren Handlung nach dem Verbotsgesetz oder wegen der §§ 246, 247a, 247b, 278b bis 278g und 282a StGB oder nach dem 25. Abschnitt des StGB verurteilt beziehungsweise verdächtigt sind, wurde vertieft. Ein besonderer Schwerpunkt lag auf der Neugestaltung des Austausches relevanter Informationen, welche die Justizanstalten für die Aufrechterhaltung der Sicherheit und Ordnung benötigen, sowie jenen Informationen aus dem Strafvollzug, welche die Sicherheitsbehörden für die Evaluierung von eventuell zu setzenden sicherheitspolizeilichen Maßnahmen anlässlich einer Haftentlassung verwenden.

3.5.1 Kooperation mit den Vollzugsgerichten im Rahmen von Fallkonferenzen

Seit 1. Dezember 2022 regelt § 152 Abs. 2a StVG (Entscheidung über eine bedingte Entlassung), dass die Vollzugsgerichte vor jeder Entscheidung über die bedingte Entlassung eines oder einer wegen einer strafbaren Handlung nach dem Verbotsgesetz oder wegen der §§ 246, 247a, 247b, 278b bis 278g und 282a StGB oder nach dem 25. Abschnitt des StGB Verurteilten eine Fallkonferenz einzuberufen haben. Das Gesetz sieht hierbei die Mitwirkungspflicht der Koordinationsstelle für Extremismusprävention und Deradikalisierung (BMJ) sowie der Verfassungsschutzbehörden (DSN und/oder die

für Staatsschutz zuständigen Organisationseinheiten der Landespolizeidirektionen) vor. Der Clearingstelle Deradikalisierung der DSN kommt im Vorfeld dieser Fallkonferenzen eine koordinative Schnittstellenfunktion innerhalb der Sicherheitsbehörden zu. Dabei nehmen Vertreterinnen und Vertreter der Clearingstelle nach Möglichkeit persönlich an den Fallkonferenzen teil, um die Einschätzungen der Sicherheitsbehörden mit den Vollzugsrichterinnen und Vollzugsrichtern auszutauschen.

Sofern eine Fallkonferenz gemäß § 152 Abs. 2a StVG (Entscheidung über eine bedingte Entlassung) unterbleibt oder Insassinnen und Insassen mit Ende ihrer Freiheitsstrafe entlassen werden, obliegt es den Staatsschutzbehörden nach den Maßgaben der gesetzlichen Bestimmungen zu prüfen, ob eine Fallkonferenz gemäß § 6a SNG (Fallkonferenz Staatsschutz) einberufen werden muss. Im Rahmen einer solchen Fallkonferenz kommt es, so dies notwendig und sachlich gerechtfertigt erscheint, zu einem intensiven Austausch mit den Strafvollzugsbehörden.

3.5.2 Vernetzung

Im Jahr 2022 wurde auch die Vernetzung zwischen Bediensteten der Justizanstalten sowie der DSN und den für Staatsschutz zuständigen Organisationseinheiten der Landespolizeidirektionen intensiviert. So wurde durch das Bundesministerium für Justiz eine gemeinsame Tagung ausgerichtet, im Rahmen derer wichtige Aspekte der Arbeit der Behörden wechselseitig vorgestellt, die bisherige Zusammenarbeit evaluiert und offene Fragen der Bediensteten erörtert wurden. Es wurde zudem die Institutionalisierung derartiger gemeinsamer Tagungen und deren jährliche Abhaltung beschlossen.

3.5.3 Kooperationen im Schulungs- und Ausbildungsbereich

Im Rahmen der Vernetzungstreffen zwischen der DSN und der Koordinationsstelle für Extremismusprävention und Deradikalisierung wurde vereinbart, dass für Mitarbeiterinnen und Mitarbeiter der Justizanstalten – das heißt Justizwachebeamtinnen und Justizwachebeamte – ein Kontingent an Ausbildungsplätzen bei künftig stattfindenden Lehrgängen der Staatsschutzprävention zur Verfügung gestellt wird. Darüber hinaus besteht die Möglichkeit, Vortragende der DSN in die Grundausbildungen Straf- und Maßnahmenvollzug zu entsenden, um Bedienstete des BMJ insbesondere im Bereich des Erkennens von Radikalisierung zu schulen.

Zudem konnte in Kooperation mit Vertreterinnen und Vertretern der Staatsanwaltschaften ein Ausbildungsmodell ins Leben gerufen werden, bei dem vertiefende kriminalpolizeiliche Inhalte vermittelt und bestehende Problemstellungen praktischer und rechtlicher Natur behandelt werden können. Ziel der Ausbildung ist folglich nicht nur die Schaffung eines gegenseitigen Verständnisses, sondern insbesondere auch die Steigerung der Effektivität strafprozessualer Ermittlungen durch Einsatz zielgerichteten Wissens. In Zeiten der Digitalisierung und in Anbetracht der rasant fortschreitenden Entwicklung im Cyberbereich ist ein gut funktionierendes Zusammenspiel von Kriminalpolizei und

Staatsanwaltschaft für die Bekämpfung krimineller Strukturen und verfassungsschutzrelevanter Bedrohungslagen unerlässlich.

3.5.4 Joint Action Day

Auch im Berichtsjahr 2022 fanden in Österreich Schwerpunktaktionen statt. Eine Schwerpunktaktion in Justizanstalten liegt vor, wenn ein zur Aufrechterhaltung der Sicherheit und Ordnung über den routinemäßigen Dienstbetrieb hinausgehender, planmäßiger und nach einsatztaktischen Grundsätzen vorbereiteter Einsatz stattfindet. Dieser wird lagebedingt mit einem definierten Einsatzziel angeordnet und erfolgt unter Zuziehung von Exekutivkräften der Justizwache aus der betreffenden Justizanstalt oder mehreren Justizanstalten – im Bedarfsfall auch unter Beiziehung von externen Kräften, wie jenen des Bundesministeriums für Inneres. Erfolgt eine Schwerpunktaktion ressortübergreifend, wird diese als „Joint Action Day" bezeichnet.

Im Oktober 2022 wurden durch die DSN und die für Staatsschutz zuständigen Organisationseinheiten der Landespolizeidirektionen Unterstützungsleistungen in Form von Amtshilfe erbracht. Insgesamt wurden 184 Haftträume – 146 davon mit Bezug zum TeBG (Terror-Bekämpfungs-Gesetz) – sowie 253 Insassinnen und Insassen, 142 davon mit TeBG-Bezug, durchsucht. Verdächtige Gegenstände wurden gesichtet und im Anschluss sichergestellt. Schwerpunktaktionen werden anlassbezogen bei konkreten Hinweisen als Folge der regelmäßig durchzuführenden Gefahren- und Risikoanalysen oder als Stichprobe im Sinne des § 102 Abs. 2 StVG (Sicherung der Ordnung in der Anstalt) durchgeführt. Vor jeder geplanten Schwerpunktaktion ist die Volksanwaltschaft in Kenntnis zu setzen.

4 Akzente im Verfassungsschutz 2022

4.1 EU-Sanktionen gegen Russland – Umsetzung in Österreich

4.1.1 Entstehung der EU-weiten Sanktionen gegen Russland

Angesichts der völkerrechtswidrigen russischen Aggression war und ist eine geschlossene und geeinte Reaktion und Antwort der Europäischen Union unabdingbar. Die Europäische Union und somit auch Österreich haben unmittelbar politisch und wirtschaftlich reagiert und das bereits seit der Annexion der Krim im Jahr 2014 bestehende Sanktionsregime erheblich ausgeweitet und verschärft. Damit setzt die Europäische Union ein deutliches Zeichen gegen den Krieg und die damit einhergehenden völkerrechtswidrigen Handlungen.

Das Ziel von Sanktionen ist es, den Bewegungs- sowie wirtschaftlichen Handlungsspielraum von Personen und Unternehmen erheblich einzuschränken, um den Staat, gegen den sich die Sanktionen richten, zum politischen Einlenken und in weiterer Folge an den Verhandlungstisch zu bewegen. Um dieses Ziel zu erreichen, wird der Druck auf das russische Regime kontinuierlich erhöht, wodurch wiederum eine Schwächung seiner Wirtschaft bewirkt werden soll. Gleichzeitig dürfen die Folgen für die europäische Wirtschaft sowie mögliche Auswirkungen auf Bürgerinnen und Bürger in Europa nicht außer Acht gelassen werden.

Die EU-weiten Sanktionen gegen Russland umfassen verschiedene Arten von Einschränkungen und richten sich gegen juristische und natürliche Personen. Es gibt allgemeine und sektorspezifische Sanktionen wie etwa Finanz-, Energie-, Verkehrs- und Wirtschaftssanktionen. Diese untersagen beispielsweise bestimmte Importe, Exporte oder generell das Eingehen von Geschäftsbeziehungen. Die Sanktionen umfassen außerdem das Einfrieren von Vermögenswerten sowie Reisebeschränkungen für sanktionierte Personen. Die aktuellen EU-Sanktionen gegen Russland wurden von der Europäischen Kommission in Form von „Sanktionspaketen“ beschlossen. Das neunte Paket wurde Ende 2022 verabschiedet.

4.1.2 Österreichische Rechtsgrundlagen

Die gesetzlichen Grundlagen für die Umsetzung des Sanktionenregimes stützen sich in Österreich neben den unmittelbar wirkenden Verordnungen der EU auf das „Bundesgesetz über die Durchführung internationaler Sanktionsmaßnahmen“ (Sanktionengesetz 2010 – SanktG) sowie auf das Außenwirtschaftsgesetz 2011 (AußWG 2011). Das Sanktionengesetz verteilt die Zuständigkeiten auf mehrere Behörden, weshalb ein reibungsloses Zusammenwirken aller Involvierten essentiell ist. Obwohl alle EU-Mitgliedstaaten verpflichtet sind, die unmittelbar anwendbare EU-Verordnung einheitlich auszulegen, gibt es aktuell – den verschiedenen nationalen Sanktionengesetzen geschuldet – noch keine einheitliche Implementierung der Sanktionen auf Ebene der Mitgliedstaaten. Parallel dazu steht die Mehrheit der Mitgliedstaaten (darunter auch Österreich) vor der

großen Herausforderung, grenzüberschreitende und in der Regel bewusst verschleierte, internationale Gesellschaftskonstrukte aufzuschlüsseln und die dahinterstehenden Personen und Einrichtungen zu identifizieren. Einschlägige Gesellschaften nutzen oftmals vorgeschobene Kontaktpersonen und verschleiern dadurch bewusst die tatsächlichen Beteiligungsverhältnisse. Komplexe behördenübergreifende Zuständigkeitsregelungen erschweren zudem die effiziente und zielgerichtete Implementierung des Sanktionenregimes in Europa.

4.1.3 Umsetzung der Sanktionen in Österreich

Dem Gesetzeswortlaut des Sanktionengesetzes (§§ 6 und 8 SanktG) folgend obliegen dem BMI bzw. der DSN in erster Linie Überwachungspflichten, etwa im Hinblick auf die Einhaltung von unmittelbar anwendbaren Sanktionsmaßnahmen der EU sowie gewisse Mitteilungspflichten gegenüber Gerichten. Zur Wahrnehmung dieser Aufgaben hat die Behörde das Recht, die hierfür erforderlichen Auskünfte und Meldungen einzuholen sowie Daten zu verarbeiten. Darüber hinaus gibt es auch andere Ministerien und Behörden, denen in ihren Wirkungsbereichen Zuständigkeiten im Zuge der Durchsetzung und Überwachung der Sanktionen zukommen. Hier ist vor allem die Oesterreichische Nationalbank (OeNB) zu nennen, die für das Einfrieren von Geldern von sanktionierten Personen zuständig ist.

Um die Umsetzung der Sanktionen so effizient und zielgerichtet wie möglich zu gestalten, wurde im März 2022 die interministerielle Task Force „Sanktionen“ eingerichtet, die durch einen Vertreter der DSN geleitet wird. Die Task Force setzt sich aus jenen Ministerien und Behörden zusammen, die im Zusammenhang mit der Überwachung und

Durchsetzung der Sanktionen Zuständigkeiten innehaben. Dazu zählen neben dem BMI auch Vertreterinnen und Vertreter des Bundeskanzleramtes, des Bundesministeriums für europäische und internationale Angelegenheiten (BMEIA), des Bundesministeriums für Finanzen (BMF), des Bundesministeriums für Justiz (BMJ), des Bundesministeriums für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie (BMK), des Bundesministeriums für Arbeit und Wirtschaft (BMAW), der Oesterreichischen Nationalbank (OeNB), der Finanzmarktaufsicht (FMA) sowie der Kommunikationsbehörde Austria. Aufgabe der regelmäßig tagenden Task Force ist es, den jeweiligen Umsetzungsstand der Sanktionen abzustimmen, Informationen auszutauschen, Synergien zu finden und die Maßnahmen bei rechtlich komplexen Sachverhalten zu koordinieren, um so einen professionellen behördlichen Austausch auf kurzem Wege zu gewährleisten.

Ein ähnliches Modell gibt es auch auf EU-Ebene – die Task Force „Freeze and Seize". Dieses Gremium tritt in regelmäßigen Abständen virtuell zusammen, um die effektive Durchsetzung der Sanktionen zu forcieren und komplexe Sachverhalte und Rechtsfragen zu erörtern. Zudem werden zwischen den Mitgliedsländern Informationen betreffend die unterschiedlichen Herangehensweisen und die dabei auftretenden Herausforderungen ausgetauscht – mit dem Ziel, praktikable und vor allem einheitliche Lösungen zu finden.

4.1.4 „Einfrieren" von Vermögenswerten

Die Europäische Union erlässt infolge eines GASP-Beschlusses[8] und der einstimmigen Annahme dieses Beschlusses durch den Rat eine unmittelbar anwendbare Verordnung, in der alle sanktionierten natürlichen und juristischen Personen angeführt sind. Die zuständigen Behörden in Österreich führen anschließend, abhängig von der Art der sanktionierten Vermögenswerte, Ermittlungen durch. Wenn beispielsweise der Verdacht besteht, dass eine sanktionierte Person Eigentümerin oder Eigentümer einer Immobilie ist, werden primär das Grundbuch und das Register der wirtschaftlichen Eigentümerinnen oder Eigentümer geprüft. Sollte sich der Verdacht bestätigen, wird in weiterer Folge das zuständige Grundbuchgericht informiert, welches eine amtswegige Eintragung vornimmt, wodurch die Immobilie „eingefroren" wird – im Sinne einer deklaratorischen Wirkung (die Rechtswirkung ist bereits vor dem Rechtsakt eingetreten). Dadurch kann die Immobilie weder belastet noch veräußert und auch in keiner Art und Weise kommerziell verwendet werden. Die OeNB hingegen friert die Konten von sanktionierten Personen ein. Diese haben dadurch keinerlei Zugriff mehr auf die auf den Konten befindlichen Gelder. Bei Wirtschaftsgütern, die nicht in entsprechenden behördlichen Registern aufscheinen, ist die Identifizierung und das Einfrieren deutlich schwieriger. Die konkrete Vorgehensweise ist somit vom jeweiligen Einzelfall abhängig.

---

8 Die Europäische Union erlässt infolge eines Gemeinsamen Außen- und Sicherheitspolitik (GASP)-Beschlusses und der einstimmigen Annahme dieses Beschlusses durch den Rat eine unmittelbar anwendbare Verordnung, in der alle sanktionierten natürlichen und juristischen Personen aufgeführt sind.

Zahlen, Daten und Fakten zu den Sanktionen gegen Russland (Stand 14.04.2023)

Auf europäischer Ebene sind 1.473 natürliche Personen und mehr als 207 Unternehmen und Einrichtungen sanktioniert. Österreich befindet sich im EU-Vergleich bei der Umsetzung im Spitzenfeld: von EU-weit knapp 21,5 Milliarden Euro wurde ein erheblicher Teil in Österreich ermittelt.

Aktuell beläuft sich das gesamte in Österreich eingefrorene Vermögen auf rund 2 Milliarden Euro. Diese Zahl setzt sich aus dem Einfrieren von Konten und anderen Vermögenswerten zusammen. So wurden über 200 Konten und Depots von sanktionierten Personen eingefroren. Darüber hinaus tätigt die DSN laufend Erhebungen und Abklärungen, die bereits zu zahlreichen Meldungen an die Firmenbuch- bzw. Grundbuchgerichte geführt haben.

4.1.5 Wirksamkeit der Sanktionen

Es ist festzuhalten, dass die EU-Sanktionen deutlich langsamer wirken als dies von vielen Expertinnen und Experten erwartet wurde. Dies kann anhand der Tatsache erklärt werden, dass die Russische Föderation seit Verhängung der ersten EU-Sanktionen im Jahr 2014 akribisch daran arbeitet, die eigene Wirtschaft unabhängiger und resilienter gegenüber westlichen beziehungsweise internationalen Sanktionen zu machen, wie beispielsweise durch die Einführung einer Alternative zum westlichen Finanztransaktionssystem SWIFT. Dennoch führte der Einbruch der Importe in den ersten Monaten des Krieges zu massiven Störungen im russischen Industriesektor und zu teils erheblichen sozioökonomischen Schäden. Zudem haben seit Kriegsbeginn bereits über 1.000 multinationale Unternehmen Russland verlassen.

Seitens der österreichischen Bundesregierung wurde der Unterstützung der Ukraine im Jahr 2022 oberste Priorität eingeräumt. Ein bedeutender Beitrag dazu war und ist die bestmögliche und stringente Umsetzung der Sanktionen gegen einzelne Personen, Institutionen und Unternehmen.

4.2 Spionage im Kontext Russland-Ukraine mit Fokus auf den Cyberbereich

Neben der klassischen militärischen Dimension des physischen Kampfes besitzt der Krieg auf beiden Seiten auch eine Dimension im Cyberbereich. Hierbei sind die Angriffe vielschichtig: Sie reichen von der Mobilisierung einer weltweit verstreut lebenden russischen und ukrainischen Diaspora über organisierte Gruppierungen von Cyberkriminellen bis hin zu staatlich gesteuerten Angriffen durch Nachrichtendienste. Ebenso vielseitig wie

die Profile der handelnden Akteurinnen und Akteure sind auch die Ziele der einzelnen Cyberangriffe: Während DDoS-Angriffe gezielt die Internetanbindung einzelner Unternehmen und Organisationen temporär stören, spezielle Schadsoftware zum Zerstören von Daten eingesetzt wird oder Sabotageangriffe darauf abzielen, industrielle Steueranlagen außer Betrieb zu setzen und Datenleaks staatlicher Einrichtungen eine unüberschaubare Fülle an Informationen liefern, finden Spionagekampagnen in den meisten Fällen im Verborgenen statt.

4.2.1 Cyberangriffe vor 2022

Hervorzuheben ist, dass Cyberangriffe, insbesondere von russischer Seite, nicht erst seit Beginn des aktuellen Krieges eine wichtige Rolle im Rahmen der hybriden Kriegsführung spielen, sondern auch schon während der russischen Annexion der Krim 2014 verstärkt in Erscheinung getreten sind. So wurde zum Beispiel im Mai 2014 ein Cyberangriff auf die ukrainischen Präsidentschaftswahlen kurz vor Veröffentlichung der Wahlergebnisse aufgedeckt, welcher den Spitzenkandidaten einer ultranationalistischen rechts-außen Partei mit einem Stimmenanteil von 37 % (anstatt des tatsächlichen Ergebnisses von 1 %) zum Wahlsieger erklärt hätte. Der staatliche russische Nachrichtensender Russia Channel One berichtete trotz Aufdeckung des Angriffs genau diese manipulierten Werte, die in der eingesetzten Schadsoftware codiert waren.

Ein anderer prominenter Cyberangriff im selben Kontext verursachte Ende 2015 einen großflächigen Stromausfall, der mehrere hunderttausend Personen in der Westukraine betraf. Angegriffen wurden dabei mehrere Stromversorger, allerdings konnten nur bei einem davon Netzausfälle verursacht werden. Auffällig waren allerdings Intensität und Aufwand der Attacke: Während industrielle SCADA-Systeme gezielt angegriffen und physische Netzkomponenten zerstört beziehungsweise außer Betrieb gesetzt wurden, konnten die Festplatten von Workstations und Servern des Verwaltungspersonals komplett gelöscht und so die Wiederherstellung per Fernwartung verhindert werden. Parallel dazu attackierte man mit einem DDoS-Angriff das Callcenter des Betreibers, um die Kommunikation mit Kundinnen und Kunden zu erschweren. Die initiale Kompromittierung hatte nach einer tiefergehenden Analyse des Vorfalls schon Monate zuvor stattgefunden, indem maßgeschneiderte E-Mails mit Malware an ausgewählte Zielpersonen geschickt worden waren. Wie ukrainische Strafverfolgungsbehörden im Nachhinein berichteten, war dies kein einzelner isolierter Angriff, sondern nur einer von mehreren parallelen Angriffen, der jedoch nicht abgewehrt werden konnte. Auch wenn sich der tatsächliche Schaden in Grenzen hielt – die Stromversorgung konnte innerhalb weniger Stunden wiederhergestellt werden –, diente er der Angreiferin oder dem Angreifer wohl primär zum Aufbau beziehungsweise als Test destruktiver Maßnahmen gegen die Zivilbevölkerung eines anderen Staates.

„SCADA (Supervisory Control and Data Acquisition)-Systeme“ bezeichnen industrielle Steuerungsanlagen. Diese dienen allgemein zum Überwachen, Analysieren und Steuern von technischen Prozessen sowohl lokal vor Ort als auch remote aus der Ferne.

Ein weiterer Angriff, der auch Schaden in anderen Staaten anrichtete, war die „NotPetya“-Kampagne 2017 (vergleiche Kapitel Cybersicherheit), bei der im Zuge einer sogenannten Supply Chain-Attacke eine kompromittierte Version der in der Ukraine weit verbreiteten Buchhaltungssoftware M.E.doc als vermeintliches Software-Update durch den Hersteller an eine Vielzahl von Opfern verschickt wurde.

„Supply Chain-Attacke“ ist ein Angriff, bei dem das intendierte Opfer nicht direkt angegriffen wird, sondern ein Zulieferer von Hard- oder Software, der möglicherweise schlechter geschützt ist als das eigentliche Ziel. Dabei wird durch manipulierte Produkte, die zum Beispiel Schadsoftware beinhalten, das Vertrauensverhältnis zwischen dem Opfer und seinen Geschäftspartnern ausgenutzt.

Einmal gestartet, verbreitete sich die Software durch Ausnutzung verschiedener Schwachstellen und Angriffsvektoren innerhalb von Windows-Netzwerken und kompromittierte weitere Systeme. Diese wurden vorgeblich verschlüsselt und deren Daten wie bei anderer „klassischer“ Ransomware nur gegen Bezahlung wieder zugänglich gemacht. Allerdings handelte es sich hierbei nicht wie angenommen um eine Version der bekannten Ransomware „Petya“, sondern um einen sogenannten Wiper, der im Hintergrund Daten unwiederbringlich löschte, anstatt diese zu verschlüsseln. Durch die selbstständige Verbreitung im Unternehmensnetzwerk waren auch zahlreiche internationale Unternehmen von diesem Angriff betroffen, die Niederlassungen in der Ukraine besaßen, darunter auch österreichische. Der bei dieser Supply Chain-Attacke weltweit angerichtete Schaden wurde auf mehrere Milliarden Euro geschätzt. Westliche Staaten und auch die EU ordneten den Angriff dem russischen Militärnachrichtendienst „Glawnoje Raswedywatelnoje Uprawlenije“ (GRU) zu.

„Wiper“ ist eine Schadsoftware, die darauf abzielt, Daten zu vernichten und Systeme unverwendbar zu machen. Wiper tarnen sich manchmal als Ransomware und täuschen sogar Ähnlichkeiten zu bekannter Ransomware vor, löschen die Daten im Hintergrund aber unwiederbringlich.

4.2.2 Cyberangriffe auf Russland und die Ukraine

Die Vielschichtigkeit von Cyberangriffen zeigt sich besonders im Kontext des aktuellen Krieges. Während die oben angeführten Vorfälle eindeutig staatlichen APT-Gruppierungen zugerechnet werden, lässt sich aktuell ein Zusammenspiel von eben diesen Hacktivistinnen und Hacktivisten und Cyberkriminellen beobachten.

„Advanced Persistent Threat (APT)" bezeichnet einen fortgeschrittenen, zielgerichteten Cyberangriff, der über einen längeren Zeitraum unter großem Ressourcenaufwand durchgeführt wird und meist darauf abzielt, im System des Opfers lange unentdeckt zu bleiben.

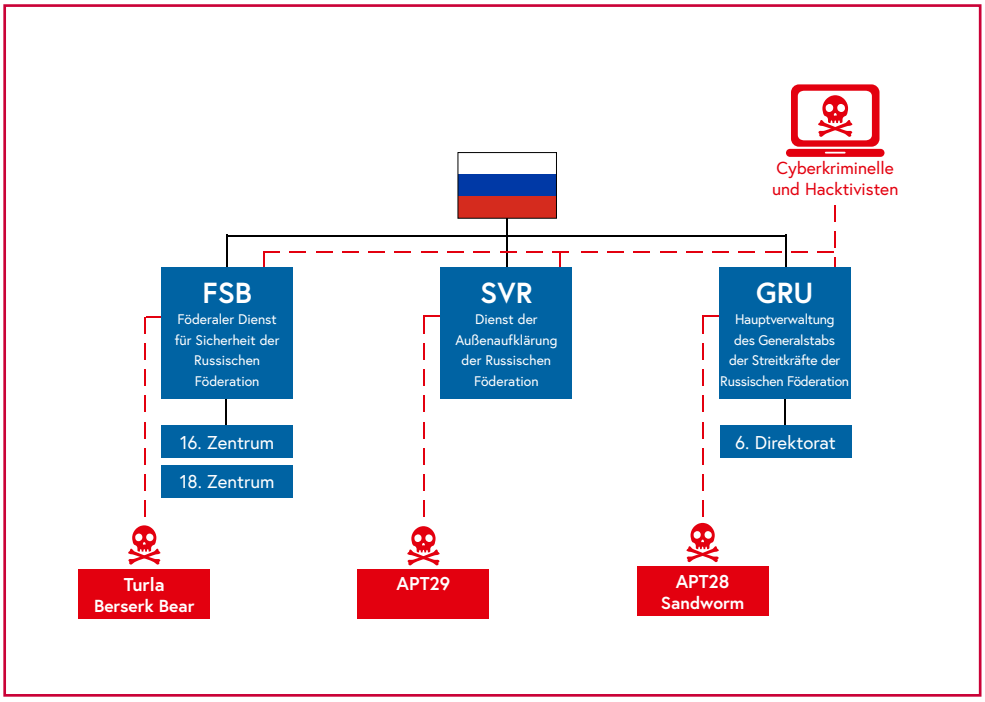

Abbildung 3: Zugehörigkeiten der Russland zugeschriebenen APT-Gruppen (Abbildung angelehnt an https://www.valisluureamet.ee/doc/raport/2018-en.pdf)

Während die Ukraine öffentlich unter dem Slogan „Hacking for Ukraine" um Sympathisantinnen und Sympathisanten im In- und Ausland wirbt, die koordiniert russische Ziele mit DDoS-Attacken angreifen beziehungsweise andere Formen von Cyberangriffen durchführen sollen, kooperiert Berichten zufolge auch der GRU mit nationalistischen Hacker-Gruppen.

Seitens der Ukraine führten diese Angriffe zu einer Vielzahl von russischen Datenleaks: So wurde zum Beispiel bereits im April 2022 eine Liste mit über 600 mutmaßlichen russischen Agentinnen und Agenten veröffentlicht, die in verschiedenen europäischen Ländern stationiert sein sollen. Auch verschiedene russische Institutionen standen im Visier der Hackerinnen und Hacker: Unter anderem wurden große Mengen an internen

Daten der russischen Zensurbehörde „Roskomnadzor“ sowie der russischen Zentralbank im Internet veröffentlicht. Abseits von Datenleaks gab es aber auch andere Ziele: So wurde nach ukrainischen Angaben eine russische Papierfabrik, die maßgeblich für die russische Nachschub-Logistik sein soll, durch Angriffe auf interne Datenbanken und SCADA-Systeme außer Betrieb gesetzt und vorübergehend blockiert. Andere Aktivistinnen und Aktivisten halfen mit, anhand verschiedener Informationsquellen (unter anderem Social Media) russische Soldatinnen und Soldaten, die an mutmaßlichen Kriegsverbrechen beteiligt waren, zu identifizieren. Welche Angriffe von ukrainischen Nachrichtendiensten selbst oder durch Gleichgesinnte beziehungsweise Hacktivistinnen und Hacktivisten im In- und Ausland durchgeführt wurden, lässt sich schwer beurteilen. Grundsätzlich ist aber über die Kriegsdauer hinweg ein deutlicher Anstieg der Professionalität und der offensiven Fähigkeiten der ukrainischen Akteurinnen und Akteure zu beobachten.

Seitens Russlands lässt sich ebenfalls eine Kooperation beziehungsweise Instrumentalisierung von Hacktivistinnen und Hacktivisten beobachten. Neben nationalistischen Gruppierungen, die Gleichgesinnte offen zum Angriff auf die Ukraine, aber auch auf westliche Länder, die die Ukraine unterstützen, aufrufen – sei es aus Überzeugung oder aus einer erhofften „wohlwollenden“ Behandlung durch die russischen Behörden –, existieren auch noch engere Formen der Kooperation. Beispielsweise wurden mehrere Fälle bekannt, bei denen dem GRU zugerechnete APT-Gruppierungen Wiper-Schadsoftware gegen ukrainische Systeme einsetzten. Innerhalb eines Tages nach dem Einsatz dieses Sabotageakts wurden gestohlene Daten der betroffenen Organisationen durch Hacktivistengruppierungen im Internet veröffentlicht.

Auch Cyberkriminelle, allen voran Ransomware-Gruppierungen, sind in die Kriegshandlungen in vielerlei Art und Weise involviert. Diese arbeiten oftmals stark arbeitsteilig: Initiale Kompromittierung, Ausbreitung der Schadsoftware sowie Verschlüsselungen von Daten werden häufig von verschiedenen Akteurinnen und Akteuren durchgeführt. Nachdem sich die Ransomware-Gruppe Conti öffentlich als pro-russisch outete, wurden interne Dokumente und Nachrichten von pro-ukrainischen Komplizinnen und Komplizen gesammelt und veröffentlicht. Diese „Conti-Leaks“ gaben Sicherheitsforscherinnen und Sicherheitsforschern Einblicke in die Organisation und in die technischen Werkzeuge und Vorgehensweisen moderner Ransomware-Gruppierungen. Darüber hinaus lieferten sie Nachweise, dass die Gruppierung mit einem russischen Nachrichtendienst zusammenarbeitete und Informationen über Journalistinnen und Journalisten sowie Oppositionelle beschaffte.

4.2.3 Cyberangriffe auf EU-Staaten

Die Befürchtung eines Überschwappens von Cyberangriffen auf EU-Staaten, wie im Fall von NotPetya im Jahr 2017, hat sich bis dato nicht bewahrheitet. Die Lage ist jedoch als anhaltend angespannt zu bewerten.

An Russland angrenzende Staaten meldeten im Berichtsjahr wiederholt Russland zuzurechnende Cyberangriffe. Die Vergangenheit zeigte, dass sich Cyberangriffe nur schwer in ihrer Auswirkung abschätzen und begrenzen lassen. So könnte ein Cyberangriff auf Infrastrukturen in der Ukraine durch sogenannte „Kaskadeneffekte" auch weitreichende Folgen für Mitgliedstaaten der EU nach sich ziehen. Beispielhaft sei hier der Angriff auf das Satellitennetzwerk VIASAT erwähnt, der dem russischen Staat zugeordnet wurde. Neben dem vermutlich eigentlichen Ziel, nämlich die ukrainische Internetinfrastruktur, welche auch von Polizei und Militär verwendet wird, zu schädigen, kam es im Zuge der Angriffe über ein manipuliertes Firmwareupdate auch zu Ausfällen bei circa 3.000 Windrädern in Deutschland, die via KA-SAT bedient wurden. Nachdem das US-Raumfahrtunternehmen SpaceX sein Satelliteninternetprodukt „Starlink" in die Ukraine geliefert hatte, wurde auch dieses Unternehmen Ziel russischer Cyberangriffe.

Aufgrund vergangener Erfahrungen sowie dank massiver Unterstützung durch westliche Staaten und Unternehmen konnten die IT-Infrastruktur der Ukraine rasch adaptiert, die Abwehrmaßnahmen verbessert und die Verteidigungsfähigkeit erhöht werden. Im Gegenzug hat sich das Niveau der Sicherheit der IT-Infrastruktur in den EU-Staaten bei weitem nicht in derselben Geschwindigkeit weiterentwickelt. Vor dem Hintergrund, dass vor allem aus dem Spektrum pro-russischer Hacktivistinnen und Hacktivisten auch Angriffe auf Unterstützerstaaten der Ukraine zu erwarten beziehungsweise bereits mehrmals erfolgt sind, ist hier eine erhöhte Bedrohungslage evident. Zu Beginn des Krieges riefen Unterstützerinnen und Unterstützer der Ukraine zum Angriff auf jene Unternehmen auf, die sich nicht freiwillig aus Russland zurückgezogen hatten, sondern weiterhin Geschäfte in beziehungsweise mit Russland machten – darunter befanden sich auch österreichische Unternehmen. Mit der Verhängung von EU-weiten Sanktionen und der zunehmenden wirtschaftlichen Isolation Russlands verstummten diese Aufrufe aber zunehmend. Mit Ende 2022 ging dann Russland dazu über, die Energie- und andere Infrastrukturen in der Ukraine großflächig mit Raketenbeschuss und Kamikazedrohnen zu zerstören. Die Folgen waren und sind unter anderem kurzfristige und längerfristige Blackouts. Dadurch verkleinerte sich die Angriffsfläche der Ukraine für pro-russische Hacktivistinnen und Hacktivisten, und die so freigewordenen Ressourcen konzentrieren sich in der Folge verstärkt auf Ziele außerhalb der Ukraine. So kam es auch in Österreich bereits zu aktivistisch geprägten DDoS-Angriffen auf Unternehmen und Organisationen.

In Bezug auf Cybercrime besteht zunehmend die Gefahr, dass Russland gemäß seiner politischen Agenda entsprechende Angriffe vermehrt steuern und bestimmte Angriffe unterstützen könnte. Während die Mehrheit der Ransomware-Angriffe nach wie vor finanziell motiviert sind, existieren Hinweise darauf, dass einzelne Ransomware-Gruppierungen bei ihren Angriffen Unterstützung von russischen Nachrichtendiensten erhalten hatten. Derartige Angriffe können als Druckmittel gegen jene Staaten benutzt werden, die die Ukraine offen unterstützen, oder sich gezielt gegen Energieversorger richten, wie

bereits wiederholt beobachtet werden konnte. Indizien dafür, welchen Anteil russische Akteurinnen und Akteure weltweit im Bereich Cybercrime besitzen, zeigt die Statistik von Sicherheitsdienstleistern: Während sich in den Tagen direkt nach dem Einmarsch Russlands in die Ukraine das Auftreten von Schadsoftware in der Ukraine schlagartig vervielfachte, nahmen die registrierten Angriffe in allen anderen westlichen Staaten signifikant ab.

Viele Beobachterinnen und Beobachter sowie Expertinnen und Experten waren verwundert, dass es der russischen Seite nicht gelungen ist, durch Cyberangriffe kriegsbeeinflussende massive Störungen in der Ukraine zu verursachen. Dies mag einerseits an den entsprechenden und oben erwähnten Vorbereitungen der Ukraine liegen, aber auch daran, dass der Stellenwert und die Effizienz der Cyberkomponente bei aktivem Kriegsgeschehen überschätzt wurde. So äußerten sich Expertinnen und Experten, dass es Russland mitunter schwerfiel, die kinetischen Angriffe mit Cyberangriffen zu koordinieren beziehungsweise letztere mit der Geschwindigkeit des Kriegsgeschehens nicht Schritt halten konnten. Dies birgt die Gefahr, dass die für Cyberangriffe zuständigen Kräfte zunehmend frei werden und sich auf Ziele außerhalb der Ukraine konzentrieren könnten, wo sie auf relativ niederschwelliger Ebene im Rahmen hybrider Attacken durchaus empfindliche oder auch nachhaltige Störungen verursachen könnten, ohne offiziell einer Kriegshandlung bezichtigt zu werden.

Dies könnte unter anderem für die Energieversorgung in Europa, vor allem in den Wintermonaten, ein zusätzliches Gefahrenmoment bedeuten. Darüber hinaus wäre eine Störung der Energieversorgung auch ein strategisches Instrument, um die Unterstützung der Ukraine durch die westliche Staatengemeinschaft ins Wanken zu bringen.

Neben den evidenten Gefahren und Gefahrenpotentialen bieten die Erfahrungen im Zusammenhang mit dem Krieg in der Ukraine die Chance, daraus zu lernen und gesamteuropäisch – vor allem aber in Österreich – die Resilienz weiter zu steigern und gleichzeitig die Angriffsfläche zu minimieren. Dies sollte in einen iterativen Prozess mit der Erkenntnis überführt werden, dass nicht das Erreichen und Halten eines Status-Quo, sondern nur die ständige Verbesserung der Schlüssel in einer von Schnelllebigkeit und geopolitischen Konflikten geprägten Zeit ist, um die Sicherheit in Europa und in Österreich zu garantieren.

Der **„iterative Prozess“** ist ein Ansatz, bei dem ein Projekt, Produkt oder Vorhaben erstellt, weiterentwickelt und verbessert wird. Teams, bei denen ein iterativer Prozess zum Einsatz kommt, erstellen, testen und überarbeiten einen Ablauf so lange, bis sie mit dem Endergebnis zufrieden sind.

4.3 Präsidentschafts- und Parlamentswahlen in der Türkei 2023 – Mögliche Auswirkungen/Folgen auf die Sicherheitslage in Österreich

4.3.1 Einleitung

Im Jahr 2023 finden in der Türkei sowohl Parlaments- als auch Präsidentschaftswahlen statt. Dabei sind auch in Österreich lebende Personen mit türkischer Staatsbürgerschaft wahlberechtigt.

In Österreich durchgeführte türkische Urnengänge haben schon in der Vergangenheit immer wieder und speziell in den „heißen" Phasen eines Wahlkampfes in unterschiedlicher Intensität Aufmerksamkeit auf sich gezogen. Dies ist auch im Zusammenhang mit dem teils hohen gesellschaftlichen Polarisierungsgrad in der Türkei zu sehen. Dieser kann sich – aufgrund der engen kommunikativen Vernetzung mit dem Herkunftsland – anlassbezogen auf die Lebensrealitäten der in Österreich lebenden aus der Türkei

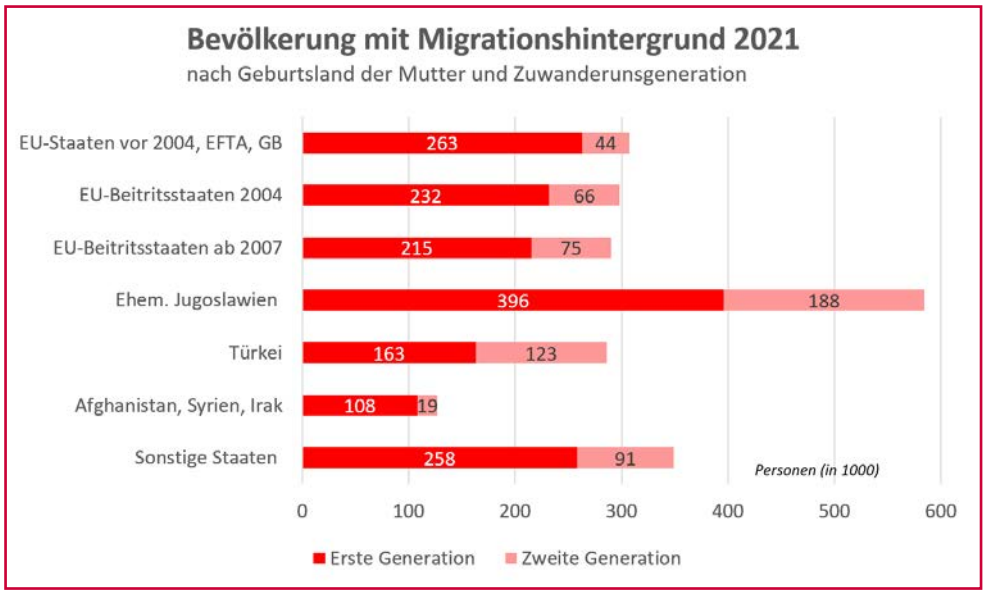

Abbildung 4:
Der Österreichische Integrationsfonds gliedert in einer Statistik Personen mit türkischem Migrationshintergrund nach erster und zweiter Generation (eigene Darstellung)

abstammenden beziehungsweise türkischen Staatsbürgerinnen und Staatsbürger übertragen. Als „Höhepunkte" sind die Jahre 2015 (zwei Wahlgänge), 2016 (Reaktionen auf den Putschversuch) und 2017 (Referendum über die Verfassungsänderung in Richtung Präsidialsystem) zu sehen. Schon zuvor, im Jahr 2014, war es anlässlich des Besuchs des damaligen türkischen Ministerpräsidenten in Wien zu Kundgebungen und Gegenkundgebungen gekommen. Diese ähnelten in Art und Umfang bereits den Reaktionen auf den Putschversuch vom Juli 2016.

4.3.2 Demographischer Kontext

Laut Statistik Austria lebten mit Stand 1. Dezember 2022 insgesamt 117.625 Personen mit türkischer Staatsbürgerschaft in Österreich. Für den Zeitraum des Jahres 2021 rechnet

dieselbe Quelle mit einem positiven Wanderungssaldo nach Österreich von 794 Personen (3.075 Personen mit türkischer Staatsangehörigkeit sind nach Österreich eingereist, 2.281 Personen haben Österreich verlassen).

4.3.3 Frühere Wahlen

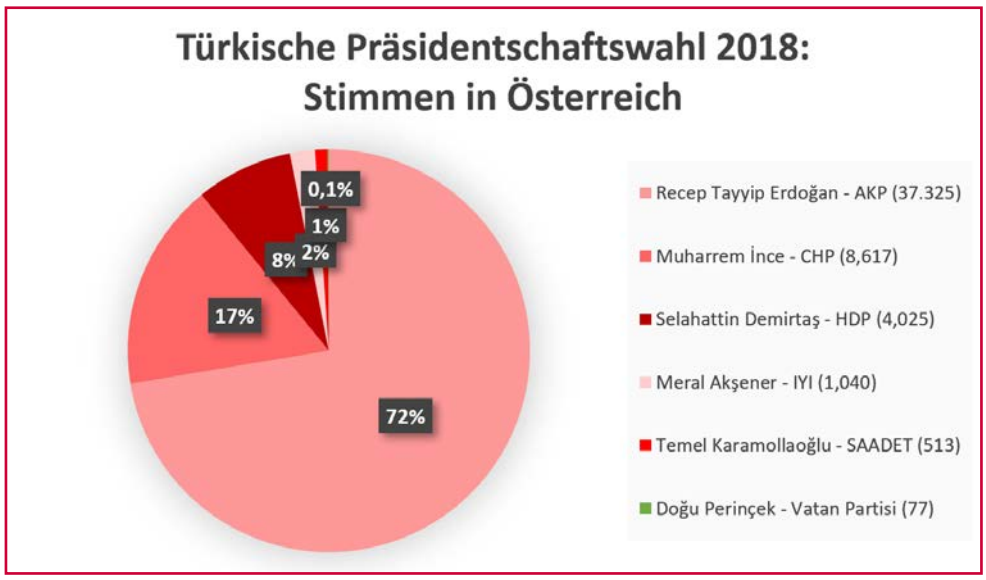

Abbildung 5:
Besonders deutlich fiel das Votum in Österreich lebender türkischer Staatsangehöriger für den Staatspräsidenten aus. Auszugehen ist von einer Wahlbeteiligung von knapp unter 50 %.

Im Jahr 2018 (Präsidentschafts- und Parlamentswahlen) waren laut türkischer Wahlbehörde 106.290 Personen türkischer Staatsangehörigkeit in Österreich wahlberechtigt. Die Stimmabgabe war an den Generalkonsulaten der Türkei in Österreich möglich. Mit rund 32.000 Stimmen brachte die Parlamentswahl laut Wahlbehörde überdurchschnittlich viele Stimmen aus Österreich für die AKP (Partei für Gerechtigkeit und Aufschwung). Zweitstärkste Kraft wurde die pro-kurdische Demokratische Partei der Völker (HDP) mit 6.092 Stimmen, noch vor der oppositionellen Republikanischen Volkspartei (CHP) mit knapp 5.900 Stimmen. Danach folgte mit rund 4.600 Stimmen die stark nationalistisch orientierte Partei der Nationalistischen Bewegung (MHP), politische Heimat der Ülkücü/Idealisten-Bewegung. Die MHP-Abspaltung IYI Parti erreichte in Österreich 1.414 Stimmen. Insgesamt wird von einer Wahlbeteiligung in Österreich von knapp unter 50 % ausgegangen (in der Türkei selbst lag die Wahlbeteiligung deutlich höher). Auffällig war, dass die Ergebnisse, die MHP (aktuell Juniorpartner der AKP) in Österreich erreichen konnte, deutlich unter dem Türkei-weiten Ergebnis von 11,1 % liegen. Prozentuell besonders ausgeprägt war der Gewinn der AKP in Österreich.

Bereits beim Referendum 2017 über die verfassungsrechtliche Umgestaltung des türkischen Staates von einem parlamentarischen zu einem Präsidialsystem – für welches von AKP und MHP geworben wurde – gab es unter den Wählerinnen und Wählern aus Österreich signifikant mehr Ja-Stimmen als im Durchschnitt in der Türkei, wo die Ja-Stimmen nur knapp die Nein-Stimmen übertrafen. Aller Wahrscheinlichkeit nach ist auch bei den Wahlen 2023 hinsichtlich der Stimmen in Österreich von einer Mehrheit für das

konservativ-islamische Lager auszugehen, was sich zudem in einer Mehrheit der Stimmen aus Österreich für die Partei des amtierenden Präsidenten niederschlagen dürfte. Das Jahr 2023 bildet dabei einen besonderen symbolischen Rahmen: Zum hundertsten Mal jährt sich die Gründung der Republik Türkei.

4.3.4 Entwicklungen

Auch im Berichtszeitraum 2022 besuchten türkische Politikerinnen und Politiker Österreich. Manche Besuche erfolgten offiziell im Rahmen demokratisch-institutioneller beziehungsweise internationaler Kooperationsformate. Im Vordergrund stand dabei die Pflege bi- und multilateraler Beziehungen. Andere Besuche bedienten hingegen primär politische Vorfeld- und Lobbying-Organisationen in Österreich und galten teils auch Verbänden, die mit Kultusangelegenheiten befasst sind. Dabei stand der parteipolitische, auf den Wahlkampf ausgerichtete Charakter im Vordergrund. Ansprechpartnerinnen und Ansprechpartner beziehungsweise Organisatorinnen und Organisatoren sind auch politische Vorfeldorganisationen, wie sie etwa die Dokumentationsstelle Politischer Islam beschreibt. Perspektivisch sind diese Besuche bereits im Kontext des Wahlkampfes zu sehen.

Zudem sind nachrichtendienstliche und nachrichtendienst-ähnliche Aktivitäten zu verzeichnen, die teils über bereits länger bekannte Möglichkeiten individueller Berichterstattung (zum Beispiel via Smartphone-App) hinausgehen. Quantitative als auch demographische Faktoren begünstigen Aufklärungstätigkeiten und Informationsbeschaffungen in Österreich. Im Fokus stehen dabei jene Gruppierungen, die in der Türkei als Terrororganisationen geführt werden. Die Auswirkungen dieser Aktivitäten wurden (bereits vor dem Berichtszeitraum) etwa im Zuge von Verhaftungen aus der Türkei abstammender oder türkischer Staatsbürgerinnen oder Staatsbürger in der Türkei erkennbar. Diese Verhaftungen während eines Türkei-Aufenthaltes bauen eine Art „Drohkulisse“ auf und wirken als Signal nach Österreich.

Weiters kam es im Berichtsjahr 2022 auch zu Protesten sowie Solidaritäts- beziehungsweise Sympathie-Bekundungen der hiesigen Gleichgesinnten mit der Arbeiterpartei Kurdistans (PKK) und den mit ihr verbundenen Milizen. Das Emblem der PKK ist, ebenso wie Symbole der Ülkücü-Bewegung („Graue Wölfe“) und der DHKP/C (Revolutionäre Volksbefreiungspartei/Front), vom Symbole-Gesetz erfasst. Die Solidaritäts-Kundgebungen verlaufen in der Regel friedlich, können aber infolge wechselseitiger Provokationen starke polizeiliche Absicherungsmaßnahmen erforderlich machen, um Gewalteskalationen vorzubeugen. Punktuell und anlassbezogen fanden, kausal mit den Entwicklungen in den Kurdengebieten verknüpft, auch unangemeldete Demonstrationen statt. Der in diesem Zusammenhang entstehende Aktionismus setzt teils auch auf Blockaden und Besetzungen, oftmals in Kooperation mit ideologisch nahestehenden Gruppierungen des linken beziehungsweise linksextremen Spektrums. Nicht zu unterschätzen ist das

an das politische Gegenüber gerichtete Provokationskalkül. Vereinzelt mündeten daher Aktionen in Sachbeschädigungen.

4.3.5 Risikopotenziale im Hinblick auf den Wahlkampf

Grundsätzlich können Aktivitäten, die der Wahlwerbung dienen, in Österreich Spannungen zwischen ideologischen Lagern innerhalb der Gruppe der Türkeistämmigen verschärfen. Aktionistische Kampagnen können dabei auf schwelende Konflikte des türkischen Staates mit extremistischen beziehungsweise terroristischen Gruppierungen abzielen und zur Eskalation wechselseitiger Provokationen beitragen. Grundsätzlich umfasst das extremistische Spektrum sowohl den Türkei-bezogenen und pro-kurdischen Linksextremismus als auch Bestrebungen mit rechtsextremen Ideologiebestandteilen, die teils islamistisch unterlegt sind.

Konflikte und potenziell daraus resultierende Eskalationen sind auch vor dem Hintergrund der Ereignisse beziehungsweise Entwicklungen der letzten Jahre zu sehen:

Die Vorkommnisse im Juni 2020 in Wien-Favoriten zeigten exemplarisch, wie rasch Sicherheitsvorfälle in der Türkei beziehungsweise den Kurdengebieten auch in Österreich auf die Sicherheitslage einwirken können. Die Ausschreitungen in Favoriten verdeutlichten auch unterschiedliche Voraussetzungen und Merkmale der politischen Lager. Während in der Sympathisantenszene des türkisch-kurdischen Linksextremismus

ein teils hoher Organisationsgrad vorliegt und Botschaften beziehungsweise politische Vorgaben zeitnah und koordiniert auf die Straße gebracht werden können, wurde beim stark türkisch-nationalistisch geprägten Personenreservoir deutlich, dass sich Diskurse, Symbole und Parolen aus den Herkunftsregionen teils verselbständigt haben. Reaktionen auf Veranstaltungen des politischen Gegenübers können dann auch spontan und ohne im Hintergrund steuernde Akteurinnen und Akteure eine Eigendynamik entfalten und zu (lokal begrenzten) Eskalationen führen. Territorialansprüche und „Erlebnisorientierung" auf der einen und geplant umgesetztes Provokationskalkül auf der anderen Seite sind ebenfalls Variablen, die im Falle einer Eskalation zusätzliche Dynamik erzeugen können. Unterstützt werden solche volatilen Mobilisierungsphänomene auch durch ad-hoc-Arrangements via Messenger-Dienste und soziale Medien. Als Erklärungsmodell für die Ausschreitungen in Favoriten greifen reduktionistische, monokausal auf ethnische Merkmale beziehungsweise Zuschreibungen abstellende Ansätze jedenfalls zu kurz.

Die fallweise und anlassbezogene Kooperation von Gruppierungen, die dem Türkei-bezogenen Linksextremismus zugeordnet werden können, mit anderen Akteurinnen und Akteuren des linksextremen Spektrums (ohne primären Auslandsbezug) könnte auch während des türkischen Wahlkampfes 2023 in Österreich für erhöhte Mobilisierungszahlen sorgen.

Die unmittelbaren Auswirkungen einer sich verschlechternden Sicherheitslage in der Türkei und den benachbarten Ländern auf die Sicherheitslage in Österreich zeigten sich auch in einer Reihe von angemeldeten und unangemeldeten Demonstrationen in Österreich. Diese waren die Reaktion auf militärische Angriffe der Türkei auf PKK-nahe Ziele in Syrien, welche wiederum in Reaktion auf den unter Einsatz einer Bombe durchgeführten Terroranschlag in Istanbul im November 2022 erfolgten.

Türkeistämmige und türkische Staatsbürgerinnen und Staatsbürger in Österreich unterliegen grundsätzlich einem erhöhten Risiko der Instrumentalisierung oder Aufklärung – je nach politischer Verortung – durch einen ausländischen Nachrichtendienst. Dieses Phänomen könnte sich bis zum Wahltermin hin verschärfen. Möglich wäre etwa die Profilierung politischer Gegnerinnen und Gegner sowie das gezielte Stören politischer Veranstaltungen von Mitbewerberinnen und Mitbewerber. Derartige Modi Operandi könnten sich auch auf die Aktivitäten der jeweiligen politischen Vorfeldorganisationen auswirken. Regierungsnahe politische Vorfeldorganisationen könnten zur Umsetzung von (Des-)Informationskampagnen herangezogen werden. Es könnte zu Einschüchterungsversuchen oppositionell eingestellter Personen durch türkisch-nationalistische oder rechtsextreme Personen und Gruppierungen kommen. Rechtsextreme Akteurinnen und Akteure könnten zudem versuchen, sich im Zuge des türkischen Wahlkampfes in Österreich zu profilieren und über diskriminierende Diskurse nach Aufmerksamkeit streben.

Phänomene, die in den letzten Jahren registriert wurden, könnten auch im Rahmen des Wahlkampfes 2023 eine Rolle spielen. Zu Problemen könnte dies vor allem dann führen, wenn dabei Botschaften verbreitet werden, die sich gegen die Grundsätze der liberal-demokratischen österreichischen Verfassungsordnung richten, zu Gewalt aufrufen oder dazu beitragen, Integration zu hemmen. Beispielhaft lassen sich anführen:

- Verdeckte Partei- bzw. Wahlveranstaltungen und damit verbundene Reisen politischer Funktionärinnen und Funktionäre aus der Türkei nach Österreich. Aufgrund des konspirativen Charakters solcher Veranstaltungen wäre auch die Sicherheitsdimension schwerer kalkulierbar. Allfällig zu ergreifenden Maßnahmen bliebe damit nur mehr eine sehr geringe Vorlaufzeit
- Verdeckte Wahlwerbung und Verteilung von Wahlwerbemitteln, damit verbundene Schaffung materieller oder institutioneller Anreize, derartige Aktivitäten durchzuführen
- Instrumentalisierung von Vereinen/Verbänden in Österreich für Zwecke des Wahlkampfes
- Wechselseitige Provokationen im Umfeld der in Österreich eingerichteten Wahllokale
- Wechselseitige Störungen von Wahlkampfveranstaltungen
- Polarisierung in Österreich als Folge von Wahlkampf-Polemik

Grundsätzlich bergen Türkei-bezogene Propaganda- und Wahlkampftätigkeiten in Österreich das Risiko, integrationshemmend zu wirken – bis hin zur Entstehung nationalistischer Echokammern und extremistischer Nährböden.

4.4 Zunahme antisemitischer Gesinnung bei hochradikalisierten islamistischen Gefährderinnen und Gefährdern

Antisemitismus ist grundsätzlich ein inhärenter Bestandteil der Ideologie des Islamismus, insbesondere im Verständnis der Muslimbruderschaft. Seit jeher wird der Staat Israel als der große Feind betrachtet, den es zu bekämpfen gilt. Das Narrativ in Teilen der muslimischen Bevölkerung als Opfer von Verfolgung hat mit dem Israel-Palästina-Konflikt einen stetigen Nährboden. Dies liegt zum einen an der Siedlungspolitik des Staates Israel in Palästina, speziell dem Westjordanland, zum anderen an der angespannten Situation in der Stadt Jerusalem, wo sich mit der al-Aqsa-Moschee, dem Felsendom und der Klagemauer auf dem Tempelberg einige der höchsten Heiligtümer des Islams und des Judentums auf engstem geografischen Raum befinden.

Eine israelfeindliche Haltung ist oftmals das verbindende Element zwischen den sonst eher zerstrittenen arabischen Ländern und eint auch strenggläubige Musliminnen und Muslime über ihre ethnische Zugehörigkeit hinweg.

Im Berichtsjahr 2022 zeigte sich islamistischer Antisemitismus unter anderem an folgendem Beispiel: Am 30. April 2022 fuhr eine fünfköpfige, amtsbekannte Personengruppe mit einem Kraftfahrzeug, auf dessen Motorhaube eine grün-weiße Shahada-Flagge montiert war, durch den zweiten Wiener Gemeindebezirk. Von zumindest einem Insassen wurden dabei wüste Beschimpfungen beziehungsweise hetzerische Äußerungen gegenüber einem – der Kleidung nach – Angehörigen des jüdischen Glaubens getätigt. Das Verhalten wurde durch eine Streifenbesatzung der Landespolizeidirektion Wien wahrgenommen. In weiterer Folge wurden alle im Fahrzeug befindlichen Personen gemäß § 283 StGB (Verhetzung) angezeigt sowie über Anordnung der Staatsanwaltschaft Wien sofort einvernommen. Gegen eine Person wurde durch das Gericht die sofortige Festnahme angeordnet; diese Person befindet sich nach wie vor in Strafhaft.

4.5 Wirtschaftsschutz, Wirtschaftsspionage und Proliferation

Auch für die österreichische Wirtschaft sind in den letzten Jahren die Herausforderungen komplexer geworden. Der bestehende und im Zunehmen begriffene Wirtschaftskonflikt zwischen den USA und China bedeutet für Europa und damit auch die heimischen Unternehmen ein Spannungsfeld, in dem die Gefahr von Wirtschaftsspionage zunehmend stärker wird. Zudem wurde mit dem Angriffskrieg Russlands gegen die Ukraine deutlich, wie stark kritische Infrastrukturen und ihre Zulieferer zum Ziel ausländischer Spionagetätigkeit werden können. Und mit steigender Inflation und in wirtschaftlich unsicheren Zeiten gewinnt Wirtschaftsspionage noch weiter an Bedeutung. Dabei können nicht nur kritische Infrastrukturen zum Ziel von Spionageangriffen werden: Aufgrund der globalen Krisen- und Kriegsszenarien schätzt die DSN die Bedrohungslage für die heimische Wirtschaft derzeit auch ganz allgemein als erhöht ein. Um dieser Gefahr adäquat begegnen zu können, wurden mit dem Wirtschaftsschutz der DSN im Berichtsjahr entsprechende Gegenmaßnahmen zum Schutz österreichischer Unternehmen eingeleitet.

Heimische Unternehmen standen in der Vergangenheit sowohl mit Russland als auch der Ukraine in wirtschaftlicher Verbindung. In Kriegszeiten kann jede Information über Produktions- und Lieferketten der gegnerischen Kriegspartei wertvoll und somit Anlass für verstärkte Spionageaktivitäten sein. Mit der Einführung des Staatsschutz- und Nachrichtendienstgesetzes (SNG) wurde der DSN mit § 7 SNG (Verfassungsschutzrelevante Beratung) die Möglichkeit eingeräumt, verstärkt präventiv im Bereich der Wirtschaftsspionage und Proliferation zu wirken. Diesem gesetzlichen Auftrag kommt der Verfassungsschutz auch mit Effektivität nach.

4.5.1 Wirtschaftsschutz

Im September 2022 schlossen die Wirtschaftskammer Österreich (WKO) und die DSN eine Kooperationsvereinbarung zum Wirtschaftsschutz ab. Wirtschaftsschutz beschreibt die Strategie der DSN zur präventiven Bekämpfung von Wirtschafts- und Industriespionage. Die dazu eingerichteten mobilen Präventionsteams der DSN sind in ganz Österreich aktiv und sensibilisieren österreichische Unternehmen proaktiv hinsichtlich der Gefahren von Wirtschafts- und Industriespionage.

Für Unternehmen besteht zudem die Möglichkeit, unter der E-Mail-Adresse wirtschaftsschutz@dsn.gv.at einen Beratungstermin zu vereinbaren. Bei den Erstberatungen werden mit der Geschäftsführung oder jenen Mitarbeiterinnen und Mitarbeitern, die für die Sicherheit im Unternehmen zuständig sind, erste Parameter möglicher Bedrohungslagen für das Unternehmen abgeklärt. In einem nächsten Schritt besteht die Möglichkeit, ausgewählte Mitarbeiterinnen und Mitarbeiter hinsichtlich der Gefahren von Wirtschafts- und Industriespionage sensibilisieren zu lassen. Diese Präventionsmaßnahme zielt vor allem auf Bedienstete in den Bereichen Vertrieb sowie Forschung und Entwicklung ab. Dabei werden den Mitarbeiterinnen und Mitarbeitern des Unternehmens von den Expertinnen und Experten der DSN die Grundzüge nachrichtendienstlicher Angriffe auf Unternehmen vorgestellt. Ein wichtiger Punkt ist das sichere Verhalten bei Dienstreisen ins Ausland und beim Erstkontakt mit potenziellen Neukunden. Der DSN-Wirtschaftsschutz etablierte sich im ersten Jahr seines Bestehens auch als Ansprechpartner für konkrete Anfragen von Unternehmen. Dabei konnten Verdachtsfälle der Wirtschaftsspionage und der Proliferation aufgegriffen und behördlich ab- und aufgeklärt werden.

4.5.2 Wirtschaftsspionage – Trend zu kombinierten Angriffen

Ein wichtiger Faktor beim Schutz eines Unternehmens vor Wirtschaftsspionage ist eine robuste Cybersicherheitsstrategie. Bei Spionageangriffen auf heimische Unternehmen bestätigt sich der internationale Trend, dass von Angreiferinnen und Angreifern zunächst automatisiert die Cybersicherheitsinfrastruktur eines Unternehmens gescannt wird. Die Ergebnisse dieser automatisierten Scans werden in weiterer Folge von der Täterschaft auf Schwachstellen ausgewertet. Kommen die Angreiferinnen oder Angreifer zu dem Entschluss, dass sich ein Angriff auf das Unternehmen lohnt, werden komplexere Angriffsstrategien entwickelt. Im Falle derartiger kombinierter Angriffe kann der Wirtschaftsschutz der DSN die Unternehmen ebenso unterstützen wie bei Angriffen ausländischer Nachrichtendienste mittels Tarnidentitäten. Diese werden oft über Jahre hinweg mittels Firmengründungen in Drittstaaten aufgebaut, um als vermeintlicher Geschäftspartner oder Kunde das heimische Unternehmen zu täuschen. Der Wirtschaftsschutz der DSN trägt damit präventiv dazu bei, die personelle, organisatorische und technische Sicherheit der Unternehmen effizient zu stärken.

4.5.3 Proliferation – Der Krieg in der Ukraine verstärkt die Gefahr der Proliferation

Mit dem russischen Angriff auf die Ukraine ist der Krieg nach Europa zurückgekehrt. In Zeiten bewaffneter Auseinandersetzungen nehmen erfahrungsgemäß nicht nur Spionageaktivitäten zu, sondern auch die Proliferation von Waffen. Verhinderung beziehungsweise Abwehr dieser Gefahren sind wichtige Aufgaben des Verfassungsschutzes. Ein verbreitetes Narrativ nach Ausbruch des Krieges in der Ukraine war, dass die Waffen, die in die Ukraine geliefert werden, über kriminelle Netzwerke zurück nach Europa gelangen könnten. Diese Gefahr ist evident, aber gleichzeitig auch Teil russischer Desinformationskampagnen, um Europa und andere Länder von Waffenlieferungen an die Ukraine abzuhalten. Um die Gefahr eines möglichen Rückflusses von Waffen für Österreich einschätzen und abwehren zu können, hat die DSN ihre Bemühungen zur Vernetzung mit europäischen und internationalen Sicherheitsbehörden verstärkt. Aus diesem Grund wurde das österreichische Projekt „National Firearms Focal Point“ (NFFP) unter Beteiligung von Europol und Bundeskriminalamt initiiert.

Österreich ist im Kontext der Proliferation nicht nur Transitstaat proliferationsrelevanter Güter, sondern aufgrund seiner hochentwickelten industriellen Produktion sowie der Vielzahl an klein- und mittelständischen Unternehmen, die in Teilbereichen weltweit führend sind, auch Zielland für illegale Beschaffungsaktivitäten. Eine besondere Problematik stellen dabei vor allem sogenannte Dual-Use-Güter (das heißt Waren oder Produkte, die sowohl für zivile Anwendungen als auch für militärische Zwecke geeignet sind) dar, wobei in jüngerer Zeit vorrangig neue Technologien wie 3D-Drucker im Fokus von proliferationsverdächtigen Netzwerken standen. Einerseits ist die Beschaffung von 3D-Druckern zur Herstellung von Waffen ein lohnendes Ziel für diese Netzwerke, andererseits sind die Materialien, die für die Produktion im 3D-Drucker verwendet werden, ein klassischer Fall von Dual-Use-Vergehen, bei denen heimische Industriebetriebe oftmals getäuscht werden. Gerade in diesem Bereich setzt der DSN-Wirtschaftsschutz einen Schwerpunkt in der Sensibilisierung und Beratung heimischer Unternehmen.

VERFASSUNG SCHÜTZEN

SICHERHEIT GEWÄHRLEISTEN