Bundesministerium
Inneres

Direktion Staatsschutz
und Nachrichtendienst

Verfassungsschutzbericht 2021

Verfassungsschutzbericht 2021

Wien, 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 DSN und BMI

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

Direktor der DSN
Omar Haijawi-Pirchner

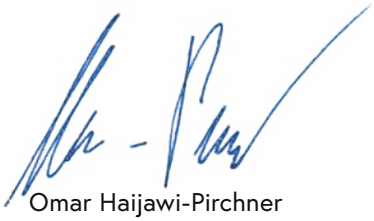
das Jahr 2021 markierte einen Meilenstein in der Geschichte des österreichischen Verfassungsschutzes. Nach einem umfangreichen Reformprozess begann die „Direktion Staatsschutz und Nachrichtendienst“ (DSN) am 1. Dezember 2021 ihre Arbeit und gewährleistet seither als unverzichtbare Frühwarnorganisation die Sicherheit Österreichs. Die DSN ist die starke Antwort des Bundesministeriums für Inneres auf verfassungsgefährdende Angriffe. Österreich muss seine demokratischen Interessen aktiv schützen und verteidigen. Werden Risiken früher wahrgenommen, so können rechtzeitig entsprechende Gegenmaßnahmen ergriffen werden. Diese verantwortungsvolle Aufgabe haben die Verfassungsschutzbehörden inne. Die neue Organisation DSN verwirklicht die Erfordernisse einer modernen Sicherheitsbehörde und ist somit adäquat ausgestattet, um dieser Aufgabe nachzugehen.

Die DSN übernimmt den inhaltlichen Aufgabenbereich ihrer Vorgängerorganisation, des „Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung“ (BVT), weist jedoch in ihrer Aufbau- und Ablauforganisation fortschrittliche Veränderungen auf. Im Reformprozess wurde die DSN mit entsprechenden Eigenschaften ausgestattet, um aktuelle Bedrohungen effizienter bekämpfen zu können. Die innerorganisatorische Trennung der Bereiche Staatsschutz und Nachrichtendienst führte zu einer Spezialisierung in der Aufgabenwahrnehmung: Im Bereich Staatsschutz erfolgen die polizeilichen Ermittlungen mit dem vorrangigen Ziel, verfassungsschutzrelevante Gefahren abzuwehren. Der Bereich Nachrichtendienst ist auf die Gewinnung und Analyse verfassungsschutzrelevanter Informationen und die Gefahrenerforschung im Zuständigkeitsbereich ausgerichtet. Gemeinsam geben die beiden Bereiche ein umfassendes Bild über die verfassungsschutzrelevanten Bedrohungslagen in Österreich, wodurch die DSN präventiv gegen potenzielle Gefahren handeln kann.

Die höchste Priorität der DSN liegt darin, die Bevölkerung Österreichs sowie die verfassungsmäßigen Einrichtungen der Republik vor terroristisch, ideologisch oder religiös motivierter Kriminalität zu schützen. Damit das gelingen kann, ist das Vertrauen in den Verfassungsschutz essenziell. Das Vertrauen der Bevölkerung ist dabei genauso wichtig wie das Vertrauen nationaler und internationaler Partnerinnen und Partner. Vertrauen wird durch Transparenz gestärkt. Daher gibt der Verfassungsschutzbericht einen Einblick in die Aufgabenbereiche der Verfassungsschutzbehörden sowie aktuelle und mögliche verfassungsschutzrelevante Entwicklungen. Neben konkreten Ereignissen, die den Verfassungsschutz im Jahr 2021 beschäftigt haben, werden Trends und Entwicklungstendenzen auf nahende Herausforderungen und Entwicklungen für den Aufgabenbereich des Verfassungsschutzes dargestellt.

Die 2021 umgesetzte Reform des Verfassungsschutzes bedeutet einen äußerst wichtigen Schritt in der Sicherheit der Republik und garantiert, dass Österreichs demokratische Rechte und Freiheit geschützt werden und die Österreicherinnen und Österreicher weiterhin in Sicherheit leben können.

Gerhard Karner
Bundesminister für Inneres



Omar Haijawi-Pirchner
Direktor der DSN

1 Verfassungsschutz – der wirkungsvolle Schutzschild der Republik Österreich

Der Verfassungsschutzbericht bildet seit Jahren die Tätigkeiten und Leistungen der Verfassungsschutzbehörden ab. Mit der Reform des Verfassungsschutzes durch die Direktion Staatsschutz und Nachrichtendienst (DSN) ist es auch notwendig, den Verfassungsschutzbericht neu zu gestalten. Der Verfassungsschutzbericht für das Jahr 2021 wurde von der DSN verfasst, auch wenn er die Tätigkeiten der Vorgängerorganisation wiedergibt. Erst der Verfassungsschutzbericht 2022 wird einen Überblick über die Arbeit und Erfolge der DSN geben können. Um zielgerichtet verfassungsgefährdenden Angriffen entgegenwirken zu können, verfolgt die DSN ein konkretes Leitbild. Aus diesem ergibt sich eine Vorausschau auf die künftige Verfassungsschutzarbeit der DSN.

LEITBILD

Direktion Staatsschutz und Nachrichtendienst (DSN)
Verfassung schützen – Sicherheit gewährleisten

Wer sind wir?

Wir, die Direktion Staatsschutz und Nachrichtendienst (DSN), sind sowohl polizeiliche Staatsschutzbehörde als auch ziviler Inlandsnachrichtendienst der Republik Österreich.

Wir schützen die Republik sowie ihre Bürgerinnen und Bürger vor allen Ausprägungen des Extremismus und des Terrorismus, vor Spionage- und Cyberangriffen und bekämpfen illegalen Waffenhandel und entsprechende terroristisch, ideologisch oder religiös motivierte Kriminalitätsfelder.

Uns obliegt die Identifizierung, die Vorbeugung, die Ermittlung und das Abwehren von verfassungsgefährdenden Bedrohungen gegen die demokratische Freiheit und Sicherheit Österreichs.

Als ziviler Nachrichtendienst agieren wir als ein Frühwarnsystem mit der präventiven Aufgabe der **Gefahrenerforschung** mit nachrichtendienstlichen Mitteln.
Wir versorgen die Bedarfsträgerinnen und Bedarfsträger mit allen erforderlichen Informationen nach wissenschaftlichen Standards.

Die effizienten **Gefahrenkontrolle** erfordert eine gute Zusammenarbeit zwischen zivilem Nachrichtendienst und polizeilichem Staatsschutz.
Wir setzen alles daran verfassungsgefährdende Straftaten zu verhindern und klären diese Straftaten gemeinsam mit der Staatsanwaltschaft auf.

Als polizeilicher Staatsschutz setzen wir uns die sicherheitspolizeiliche **Gefahrenabwehr** und die kriminalpolizeiliche Ermittlung mit präventiven sowie repressiven Mitteln der Strafverfolgung zum Ziel.

Wir sind die Hüter der schützenswertesten Güter der Republik Österreich: der demokratischen Freiheit und Sicherheit.

Wir sind die unverzichtbare Frühwarnorganisation im Dienste von und zum Schutz der Republik Österreich sowie ihrer Bürgerinnen und Bürger.

Unsere Vision

Wir weisen eine hohe Wachsamkeit in Bezug auf verfassungsgefährdende Bedrohungen auf und bereiten uns präventiv auf das Abwehren dieser Bedrohungen nach rechtsstaatlichen Mitteln vor.

Wir setzen auf das gegenseitige Vertrauen unserer Partnerinnen und Partner im In- und Ausland. Wir stellen uns rasch auf sich verändernde Bedrohungsumgebungen ein. Wir sorgen für Ihren Schutz.

Unsere Mission

Für uns gilt

- Gefahren erforschen – Gefahren kontrollieren – Gefahren abwehren
- Wir erfüllen unsere Aufgaben auf Grundlage der rechtlichen Rahmenbedingungen und auf Basis des gesetzlichen Auftrages:
- Rasches und flexibles Reagieren auf krisenhafte Entwicklungen
- Effizientes Sammeln und Auswerten von Informationen und Wissen
- Erstellen von wissenschaftlich fundierten Analysen und Gefährdungs- beziehungsweise Risikoeinschätzungen
- Kontrollieren von Bedrohungen und Gefahren
- Zielgerichtetes Beobachten und Ermitteln
- Umsetzen von präventiven und verhältnismäßigen Maßnahmen
- Kooperieren mit Partnerinnen und Partnern aus dem In- und Ausland
- Zusammenarbeiten mit Behörden und der Zivilgesellschaft

Warum benötigt die Republik Österreich die DSN als zuständige Behörde für Verfassungsschutz?

Die stärkste Antwort auf Extremismus und Terrorismus ist das entschlossene Zusammenhalten der Gesellschaft und das gemeinsame Verteidigen der demokratischen und verfassungsmäßigen Grund- und Freiheitsrechte. Die österreichische Gesellschaft ist durch Grundwerte vereint, insbesondere Demokratie und Rechtsstaatlichkeit, sowie die Besinnung auf zu gewährleistende Menschenrechte.

Österreichische, demokratische Interessen müssen aktiv geschützt und verteidigt werden. Je früher man Risiken wahrnimmt, desto früher können Gegenmaßnahmen ergriffen werden. Dies sind die ureigenen Aufgaben für uns als Verfassungsschutzbehörde.

Das Etablieren eines Nachrichtendienstes in Österreich hat die Schaffung eines Informationsvorsprungs in Bezug auf verfassungsgefährdende Bedrohungen sowie die zielgerichtete Gefahrenabwehr durch staatsschutzrelevante Ermittlungen zum Ziel.

Werte und Haltungen der Direktion Staatsschutz und Nachrichtendienst

Folgende Werte und Haltungen sind für uns die Grundlage für authentisches Handeln und eine konsistente Innen-Außen-Perspektive:

Unparteilichkeit & Unvoreingenommenheit

Bei unserer Tätigkeit gehen wir unparteilich und unvoreingenommen vor und sind uns unserer besonderen Verantwortung im Umgang mit Vertraulichkeit und Loyalität gegenüber den gesetzlichen Aufgaben der DSN bewusst.

Allen Strömungen jenseits des demokratischen Spektrums gilt die gleiche Aufmerksamkeit.

Vertraulichkeit & Integrität

Wir schützen vertrauliche Informationen unserer Partnerinnen und Partner sowie unserer Quellen für den Erfolg unserer Arbeit.

Das Vertrauen der Öffentlichkeit erarbeiten wir uns durch Integrität und Professionalität.

Transparenz & Kontrolle

Wir sind uns unserer verantwortungsvollen Tätigkeit im Namen der Republik Österreich bewusst, respektieren und unterstützen die parlamentarischen Kontrollmechanismen und den Rechtsschutz, gehen sorgfältig und behutsam mit uns anvertrauten Informationen um und unterstützen Transparenz und die Dialoge mit Partnerinnen und Partnern.

Für die DSN gilt: soviel Transparenz wie möglich, soviel Geheimhaltung wie nötig.

Professionalität & Kompetenz

Wir zeigen höchste Professionalität und Einsatzbereitschaft für die Tätigkeit im Sinne der Republik Österreich.

Chancengleichheit, Vielfalt und die Vereinbarkeit von Beruf und Privatleben sind für uns genauso wichtig, wie eine wertschätzende Führungskultur und die Möglichkeit zur Fort- und Weiterbildung.

Für unsere Aufgabenerfüllung erhalten wir die Anerkennung und die Wertschätzung der Bevölkerung, der in- und ausländischen Partnerinnen und Partner sowie der obersten politischen Organe.

Durch die neue Organisation des Verfassungsschutzes in Österreich ergibt sich eine strukturelle Gliederung in Staatschutz und Nachrichtendienst. Um beide Bereiche ausreichend beleuchten zu können, wird im Verfassungsschutzbericht, neben der Darstellung der sicherheits- und kriminalpolizeilichen Aufgabenfelder und den Ereignissen des Jahres 2021, ein Fokus auf die Vorfeldbeobachtung, also auf Prognosen, Trends und Entwicklungstendenzen, gerichtet. Dadurch werden die auf den Verfassungsschutz zukommenden Herausforderungen und Entwicklungen umfassender als bisher aufgezeigt.

Aus Gründen der Einheitlichkeit werden die bisher im Verfassungsschutzbericht enthaltenen statistischen Zahlen oder Kenngrößen künftig nur mehr im Sicherheitsbericht dargestellt, der auf Grundlage des Sicherheitspolizeigesetzes jährlich dem National- und dem Bundesrat vorgelegt wird.

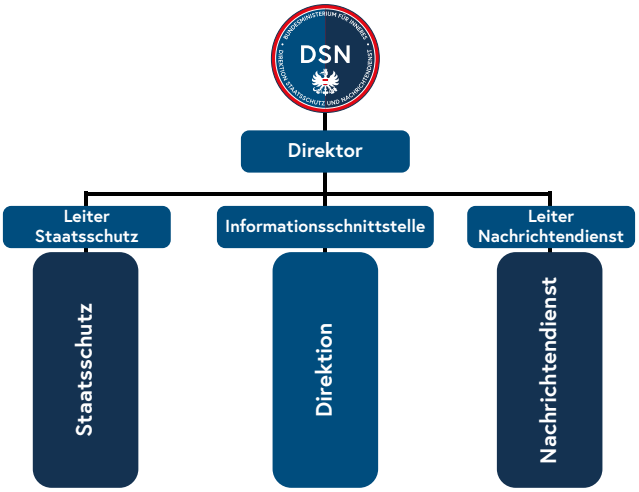
Der neue Verfassungsschutzbericht ist durch die Themensetzung ein Gefahrenradar sowie durch bildliche Inhalte moderner als seine Vorgänger. Mit Start der DSN erhält nicht nur der Verfassungsschutz, sondern ebenso der Verfassungsschutzbericht eine Aufwertung. Transparenz steht im Zentrum der DSN und die Öffentlichkeit soll – wie es das Staatsschutz- und Nachrichtendienstgesetz (SNG) vorsieht – über aktuelle und mögliche verfassungsschutzrelevante Entwicklungen informiert werden.

2 Reform des österreichischen Verfassungs-schutzes

Im Februar 2020 fiel der Startschuss für den größten Reformprozess des Verfassungsschutzes in der Geschichte Österreichs. Ziel der Reform war es, den Verfassungsschutz umfassend neu aufzustellen und das Vertrauen der österreichischen Bevölkerung und der nationalen und internationalen Partner wiederzugewinnen. Durch gesetzliche Änderungen wurde die neue Verfassungsschutzbehörde strukturell in die Bereiche Staatsschutz und Nachrichtendienst getrennt. Diese strikte Trennung dient der Stärkung der Gefahrenaufklärung. Darüber hinaus wurden in allen Bereichen internationale Standards etabliert, aufgezeigte Sicherheitsmängel behoben und die Anforderungsprofile für Mitarbeiterinnen und Mitarbeiter des Verfassungsschutzes gesetzlich normiert. Die Reform erlaubt es dem Verfassungsschutz auf neue sowie bereits bestehende Bedrohungslagen, die durch transnationalen Terrorismus, gewaltbereiten Extremismus, Spionage, Proliferation und Cyber-Angriffe entstehen können, zeitnah und angemessen zu reagieren.

Mit Inkrafttreten des Staatsschutz- und Nachrichtendienstgesetzes (SNG) am 1. Dezember 2021 wurde die Direktion Staatschutz und Nachrichtendienst eingerichtet. Die Aufgabe des Verfassungsschutzes nimmt die Direktion Staatsschutz und Nachrichtendienst als Zentralstelle gemeinsam mit den für Staatsschutz zuständigen Organisationseinheiten der Landespolizeidirektionen in jedem Bundesland wahr. Die für Staatsschutz zuständigen Organisationseinheiten der Landespolizeidirektionen unterliegen aktuell noch einem Reformprozess.

Die klare Trennung von Aufgaben ist zentrales Element der Direktion Staatsschutz und Nachrichtendienst (DSN). Um zwischen den Bereichen Staatsschutz und Nachrichtendienst einen umfassenden Informationsaustausch und eine enge Zusammenarbeit zu gewährleisten, wurde in der DSN eine Informationsschnittstelle eingerichtet. Die Koordinierung dieser beiden Aufgabenbereiche erfolgt im Gemeinsamen Informations- und Lagezentrum. Diese Organisationseinheit ist dem Direktor der DSN direkt unterstellt. Für die beiden Bereiche Staatsschutz und Nachrichtendienst wurde jeweils ein Leiter bestellt.



Zur Gewährleistung eines raschen und umfangreichen Informationsaustausches wurden im Gemeinsamen Informations- und Lagezentrum Arbeitsgruppen zu verschiedenen Phänomenbereichen eingerichtet, an denen Expertinnen und Experten aus den Bereichen Staatsschutz und Nachrichtendienst teilnehmen, die im jeweiligen Aufgabenbereich gewonnenen Informationen austauschen und Lagebilder sowie Gefährdungseinschätzungen erstellen.

Einhergehend mit der Einrichtung der Direktion wurden jene Maßnahmen umgesetzt, die einer sofortigen Neuregelung bedurften. Dazu zählte neben der bereits begonnenen Beseitigung von technischen und baulichen Sicherheitsmängeln die Professionalisierung des Personalmanagements gemäß internationaler Standards. Dies betraf Themen wie die allgemeinen Kriterien der Personalauswahl, eine generelle und sich in regelmäßigen Abständen wiederholende Sicherheitsüberprüfung der Bediensteten sowie das Thema Aus- und Fortbildung der Mitarbeiterinnen und Mitarbeiter. Bei der Überprüfung der Bediensteten wurde die bereits vorhandene Sicherheitsüberprüfung um eine Vertrauenswürdigkeitsprüfung für alle Mitarbeiterinnen und Mitarbeiter, die mit der Vollziehung von Aufgaben im Bereich des Verfassungsschutzes betraut sind, erweitert. Die Vertrauenswürdigkeitsprüfung ist die Abklärung der Vertrauenswürdigkeit eines Menschen anhand personenbezogener Daten und enthält eine umfassende Überprüfung des Vorlebens sowie der aktuellen Lebensumstände. Diese Erweiterung ist aufgrund des sensiblen Aufgabenbereiches notwendig und dient zur Einschätzung, ob sich aufgrund persönlicher Interessen, Kontakte oder Tätigkeiten ein Risikopotenzial für die Tätigkeit im Bereich des Verfassungsschutzes ergibt. In der Direktion Staatsschutz und Nachrichtendienst kommen zudem neue Qualitätsmanagement- sowie Qualitätssicherungssysteme zum Einsatz, um Sicherheits- und Qualitätsmängel zu beheben und die interne Kontrolle der Tätigkeit zu verbessern. Die Wirkung dieser Systeme wird im Rahmen regelmäßiger Audits überprüft.

Das neue Staatsschutz- und Nachrichtendienstgesetz (SNG) regelt die Zuständigkeiten und Befugnisse der beiden Bereiche Staatsschutz und Nachrichtendienst.

Gemäß § 1 Abs. 4 SNG umfasst der Staatsschutz den vorbeugenden Schutz vor verfassungsgefährdenden Angriffen. Durch den Gesetzgeber wurde mit der Verankerung des § 6a SNG die Möglichkeit geschaffen, zusätzlich zu polizeiinternen Fallbesprechungen der Organisationseinheiten im Sinne des § 1 Abs. 3 SNG auch Fallkonferenzen mit externen Institutionen (Behörden, Bildungseinrichtungen, Einrichtungen im Bereich der Extremismusprävention oder der sozialen Integration) abzuhalten. Ebenso dienen die verfassungsschutzrelevante Beratung gemäß § 7 SNG sowie die in § 8a SNG verankerte Gefährderansprache zur Deradikalisierung diesem Zwecke. Durch letztere werden Personen, von denen aufgrund vorangegangener Verwaltungsübertretungen nach Art. III Abs. 1 Z 4 EGVG, § 3 Abzeichengesetz oder § 3 Symbole-Gesetz, anzunehmen ist, sie werden einen verfassungsgefährdenden Angriff begehen, im Rahmen einer

Gefährderansprache nachweislich über rechtskonformes Verhalten belehrt. Bei dieser Belehrung wird insbesondere auf das Gefährdungspotential durch Radikalisierung und die damit verbundenen Rechtsfolgen eingegangen und auf Deradikalisierungsprogramme hingewiesen.

Für die Zwecke des Schutzes der verfassungsmäßigen Einrichtungen und deren Handlungsfähigkeit, von Vertretern ausländischer Staaten und anderen Völkerrechtssubjekten, der kritischen Infrastruktur, der Bevölkerung vor extremistischer Kriminalität, vor Gefährdungen durch Spionage und nachrichtendienstlicher Tätigkeit als auch durch Proliferation obliegt dem Bereich Nachrichtendienst die Gewinnung und Analyse von Informationen gemäß § 8 Abs. 1 SNG, als auch die erweiterte Gefahrenerforschung gemäß § 6 Abs. 1 SNG. Während die Gewinnung und Analyse von Informationen der Beurteilung von verfassungsschutzrelevanten Bedrohungslagen dient, ist die erweiterte Gefahrenerforschung die Beobachtung einer Gruppierung, wenn im Hinblick auf diese damit zu rechnen ist, dass es zu mit schwerer Gefahr für die öffentliche Sicherheit verbundener Kriminalität kommt. Zur bestmöglichen Aufgabenerfüllung stehen spezifische Befugnisse zur Informationsgewinnung zum Zwecke des Verfassungsschutzes zur Verfügung. So wird ein umfassendes Wissen über die aktuelle Lage, Entwicklungen und künftige Szenarien generiert, das als Frühwarnsystem adäquate Handlungsstrategien entwickeln lässt.

Die obersten Organe der Vollziehung (Art. 19 Bundesverfassungsgesetz, B-VG) sowie die mit der Leitung der gesetzgebenden Körperschaften des Bundes und der Länder betrauten Organe sind von der Direktion Staatsschutz und Nachrichtendienst gemäß § 8 Abs. 2 SNG über verfassungsschutzrelevante Bedrohungen zu unterrichten. Zur Stärkung der parlamentarischen Kontrolle wurden umfassende Berichtspflichten im SNG verankert. Damit wird sichergestellt, dass die Öffentlichkeit, der Bundesminister für Inneres sowie der Ständige Unterausschuss des Ausschusses für Innere Angelegenheiten des Parlaments über die Tätigkeit des Verfassungsschutzes informiert werden.

Die Direktion Staatsschutz und Nachrichtendienst erfüllt mit ihrer neuen Struktur die Anforderungen einer modernen Sicherheitsbehörde, um zielgerichtet ihrer Aufgabe, nämlich die Bevölkerung sowie die verfassungsmäßigen Einrichtungen der Republik Österreich vor terroristisch, ideologisch oder religiös motivierter Kriminalität zu schützen, gerecht zu werden. Der Verfassungsschutz wird stärker im Vorfeld von strafbaren Handlungen tätig und investiert in die Erforschung von Gefahren ebenso wie in deren Abwehr. Die Direktion Staatsschutz und Nachrichtendienst ist somit die qualifizierte Einrichtung, um sowohl das Vertrauen der Partner, als auch das Vertrauen der österreichischen Bevölkerung zurückzugewinnen und einen wirkungsvollen Schutzschild für die Republik Österreich darzustellen.

3 Verfassungs-schutzrelevante Phänomen-bereiche

3.1 Extremismus und staatsfeindliche Verbindungen

3.1.1 Rechtsextremismus

3.1.1.1 Überblick

Der Begriff Rechtsextremismus wird als Sammelbezeichnung für politische Überzeugungen und Bestrebungen angesehen, welche von Fremdenfeindlichkeit, Rassismus, Antiislamismus und Antisemitismus geprägt sind und daher mit Inkaufnahme beziehungsweise Duldung von Gewalt erreicht werden sollen. Die demokratische Rechtsordnung und die pluralistischen Gesellschaftsauffassungen werden abgelehnt. In seiner äußersten Steigerungsform kann sich Rechtsextremismus bis hin zum Rechts-Terrorismus steigern, um systematisch gegen politische Gegner, Opfergruppen rechtsextremistischer Weltanschauungen und staatliche Institutionen beziehungsweise ihre Repräsentantinnen und Repräsentanten vorzugehen.

3.1.1.2 Aktuelle Lage

Wie schon in den Vorjahren stellen rechtsextremistische Aktivitäten eine Gefährdung sowie ein nicht zu unterschätzendes Risiko für die demokratischen Institutionen in Österreich dar. Auch die selbst definierten Feindbilder blieben im Wesentlichen unverändert und umfassen weiterhin insbesondere Jüdinnen und Juden, Musliminnen und Muslime, Islamistinnen und Islamisten, Asylwerberinnen und Asylwerber sowie Migrantinnen und Migranten, Aktivistinnen und Aktivisten des linken Spektrums, die Polizei, Institutionen der Massenmedien, die Europäische Union und das demokratische System.

Das Risiko zunehmender rechtsextrem motivierter Tathandlungen und nachhaltiger Radikalisierung von Personen, Szenen, Bewegungen und Gruppierungen steigt. Allgemein findet momentan eine Vermischung unterschiedlicher rechtstendenziöser bis rechtsfanatisierter Gruppierungen, die sich in Wechselwirkung bei gemeinsamer Propaganda stärken, statt.

Ummantelt mit harmlos erscheinenden, besonders für jugendliche Erlebniswelten ansprechenden Sprachumdeutungen (z. B. „großer Austausch“ statt „Überfremdung“, „Remigration“ statt „Massenabschiebung“, „Kultur“ statt „Rasse“) wurden dabei von neurechten Gruppierungen rechtsextremistische, antisemitische und rassistische Weltanschauungen auf subtilem Wege an die Zivilgesellschaft herangeführt, die Grenzen des Sagbaren allmählich verschoben und rechtsgerichtete Grundhaltungen in der Öffentlichkeit zunehmend normalisiert. Das Risiko, das von neurechten Akteurinnen und Akteuren ausgeht, liegt somit vor allem in der gewaltbesetzten Rhetorik: Durch neue, vorwiegend unbelastete und attraktiver wirkende Begrifflichkeiten werden altbekannte Rassismen und gruppenbezogene Menschenfeindlichkeit verschleiert und lassen damit die Hemmschwelle zur Gewaltverherrlichung und -bereitschaft sinken. Indem es ihnen im Zuge der Corona-Protestveranstaltungen gelang, ihre verschwörungsideologischen Deutungsmuster einer breiteren Bevölkerungsschicht zugänglich zu machen, förderten sie letztendlich das Radikalisierungs-, Polarisierungs- und Spaltungspotenzial in der Gesellschaft.

Aufgrund gewaltbereiter Anhängerinnen und Anhänger ist gegenwärtig eine hochgradige Verfassungsschutz-Relevanz ausgehend von Gruppierungen und einzelnen Aktivistinnen und Aktivisten der Corona-Maßnahmen-Gegner-Bewegung (CMG-Bewegung) evident. Die allgemeine Bedrohungslage ist derzeit weniger durch öffentliche Auftritte der Maßnahmengegnerschaft als durch konspirative Treffen der CMG-Führungskader mit Vertretern von nationalsozialistisch-inspirierten Gruppierungen und Vertretern der „Neuen Rechten“ gegeben. Erstere versucht auf den nach wie vor bestehenden, jedoch deutlich im Rückgang befindlichen Nachhall des antidemokratischen und staatsfeindlichen CMG-Kerns Einfluss zu nehmen, um ihre eigene Reichweite zu erhöhen und ihre Ideologie innerhalb dieser bewegungsübergreifenden Vernetzungsstrukturen zu legitimieren.

Unter dem Deckmantel einer suggerierten Solidarität mit der besorgten österreichischen Bevölkerung wurden vor allem von der IBÖ beziehungsweise der DO5 die virtuellen und realen Demonstrationen als Radikalisierungs- und Rekrutierungsräume genutzt.

Die Ungewissheit innerhalb der österreichischen Bevölkerung wurde opportunistisch eingesetzt und für ihre Zwecke instrumentalisiert. Die beschlossenen Maßnahmen zur Eindämmung der Corona-Pandemie haben gezeigt, wie rechtsextreme Gruppierungen die Sorgen und Ängste aufgreifen, um in weiterer Folge ihre eigene Erzählung zu verankern. Dadurch entstand ein Ringen um die Deutungshoheit, durch welches ein

breiteres Publikum erreicht wurde und ein erhöhtes Radikalisierungspotenzial entstanden ist. Ihr vorrangiges Ziel war, die Überwindung der herrschenden demokratischen, rechtsstaatlichen gesellschaftlichen Ordnung voranzutreiben. Weltanschauungen, die eine von Globalisierung und Pluralismus geprägte demokratische Gesellschaftsstruktur systematisch ablehnen, sollten durch die Unterwanderung eines Aktionismus, der große Teile der österreichischen Bevölkerung erreichte, einen breiteren politischen Resonanzraum erhalten. Dadurch konnte das bestehende Netzwerk rechtsextremistischer Gruppierungen und Exponenten graduell ausgebaut werden, um mehr Einfluss zu gewinnen und gesellschaftspolitische Diskurse zu verschieben. Hierfür bedienten sie sich ihrer bekannten Strategie, Themen und Geschehnisse mit hoher emotionaler Wirkung aufzugreifen und zu besetzen. In der milieuübergreifenden Vermengung mit Corona-Maßnahmen-Gegnern (CMG), Verschwörungsideologen und -ideologinnen, Esoterikern und Esoterikerinnen und anderen Szeneproponenten und -proponentinnen wurden die pandemiebedingten Entwicklungen mit Weltverschwörungen gedeutet, um einfache, sinn- und identitätsstiftende Erklärungen für komplexe Fragestellungen zu liefern.

Aufgrund der Corona-Maßnahmen in europäischen Ländern konnten keine Kampfsportveranstaltungen, die seit geraumer Zeit zu Vernetzungszwecken dienen, und auch Veranstaltungen innerhalb der rechtsextremen Musikszene stattfinden. Somit fielen die Möglichkeiten zur Rekrutierung potenzieller Sympathisantinnen und Sympathisanten, die propagandistischen und finanziellen Komponenten sowie der netzwerk- und szenebildende Charakter beinahe zur Gänze weg. Vereinzelt traten Aktivistinnen und Aktivisten dieser Szene im Rahmen von Demonstrationen gegen die Corona-Maßnahmen auf.

„Neue Rechte“

Die Identitäre Bewegung Österreich (IBÖ) sieht sich als Vertreterin der „Neuen Rechten“ in Österreich. In ihrer Kommunikation nach außen wird Bedacht darauf genommen, dass bisherige von rechtsextremen Gruppierungen verwendete Elemente der NS-Ideologie sowie eine offen rassistische Weltanschauung durch eine neue Terminologie (z. B. werden weniger belastete Ausdrücke wie Ethnopluralismus anstatt „Überfremdung“ verwendet) versteckt werden. Somit versucht die „Neue Rechte“ sich deutlich von nationalsozialistisch inspirierten Gruppierungen abzugrenzen. Trotz dieser „offiziellen“ Ablehnung zum Nationalsozialismus und Gruppierungen die sich vom NS-Regime inspiriert fühlen, wird von den Identitären in ihrer Argumentation wiederholt auf die literarischen und politischen Wegbereiter für das Dritte Reich zurückgegriffen, um so eine verdeckte Brücke in diesen politischen Bereich zu schlagen. Mit der Flüchtlingskrise ab dem Jahr 2015 kam zu der Islamfeindlichkeit das Element offener Asylfeindlichkeit hinzu. Von der IBÖ wurde erkannt, dass das Schüren der Unzufriedenheit mit der etablierten Politik – im Zusammenhang mit ungelösten Problemen im Asylwesen, von verunsicherten Bürgerinnen und Bürgern

aufgenommen wurde und damit auch Zugang in jene Gesellschaftsschichten gefunden werden konnte – die sich bisher nicht von rechtsextremer Rhetorik angesprochen fühlten.

Die in der politischen Arbeit verwendeten Narrative umfassen dabei oftmals Botschaften zur versteckten Akzeptanz von Gewaltbereitschaft. Die Aufarbeitung einschlägiger IBÖ-Veröffentlichungen bestätigen, dass die Gruppierung Gewalt in der politischen Auseinandersetzung nicht nur nicht ausschließt, sondern diese auch positiv beantwortet. Mit der Attacke von Christchurch im März 2019 fanden sich erstmals über Kontinente hinweg jene Elemente der geistigen Brandstiftung, die unter anderem auch von der IBÖ in die Welt gesetzt wurden, als Grundlage und Rechtfertigung für einen folgenschweren Anschlag mit 50 Toten.

Die IBÖ weist einen sehr hohen Organisationsgrad auf, der bisher auf unterschiedliche Rechtskonstruktionen gestützt war: So bildeten mehrere Vereine, zwei Ausbildungszentren und andere assoziierte Organisationen sowie der Onlinehandel „Phalanx Europa“ (Onlinehandel des rechtsextremen Identitären Martin S., bei dem Kleidung, Bücher, und Accessoires gekauft werden konnten) lange Zeit ein umfassendes Netzwerk zur Sicherung der politischen Arbeit beziehungsweise zur erfolgreichen Rekrutierung von Aktivistinnen und Aktivisten. Im Zuge von gerichtlichen Ermittlungsverfahren konnte jedoch nachgewiesen werden, dass Vereine teilweise als Umgehungskonstruktionen für die Steuerung von Geldflüssen genutzt wurden beziehungsweise nie ihren eigentlichen Vereinszweck erfüllten. In der Folge wurden daher Untersagungsverfahren bei den zuständigen Vereinsbehörden eingeleitet und in einem oberösterreichischen Fall bereits in erster und zweiter Instanz abgeschlossen.

Die rechtsextreme Gruppierung „Die Österreicher – DO5“ wurde Ende 2019/Anfang 2020 von zwei IBÖ-Aktivisten gegründet. Ein Gründungsmitglied war bereits die Führungspersönlichkeit der IBÖ beziehungsweise nahm er eine führende Rolle bei den paneuropäischen Aktionen der Identitären ein, wie zum Beispiel bei der „Defending Europe Mission“ im Mittelmeer im Sommer 2017, wo Identitäre aus mehreren europäischen Ländern versuchten, eine Zusammenarbeit zwischen NGOs und Schleppern bei dem Transport von Flüchtlingen nach Europa zu beweisen. Die zweite Führungspersönlichkeit der DO5 war bis zur Gründung der „Österreicher“ ein IBÖ-Aktivist, dieser trat allerdings nicht als prominentes Mitglied der Identitären in Erscheinung. Seine Beziehungen zu dem deutsch-amerikanischen Reichsbürgersympathisanten, selbsternannten Wunderheiler und Verschwörungsideologen Bernd K. alias Leonard C. und seiner Gruppierung „Instinct Based Medicine System“ (IBMS) lassen einen Bezug dieses Aktivisten zu staatsfeindlichen Gruppierungen vermuten.

Die offizielle Motivation für die Gründung der DO5 war, eine Bewegung zu formieren, die allen Bürgerinnen und Bürgern offensteht und in der sich Angehörige jeder Altersklasse engagieren können. Die IBÖ war im Gegensatz dazu laut Eigendefinition

eine elitäre Jugendbewegung, deren Mitglieder vorrangig aus dem studentischen Milieu stammten. Vermutlich spielte allerdings die Überlegung, dass die Identitäre Bewegung aufgrund ihrer Strafverfahren und der größtenteils negativen Berichterstattung in den österreichischen Medien keine neuen Aktivistinnen und Aktivisten rekrutieren beziehungsweise Spendengelder lukrieren konnte – insbesondere in Zusammenhang mit den Verbindungen ihres Anführers Martin S. zum Christchurch-Attentäter Brenton T. – eine wichtige Rolle.

Die Ziele der DO5 decken sich zum Großteil mit jenen, welche die Identitären seit fast einem Jahrzehnt propagieren. Sie treten gegen die „Überfremdung" in Österreich, insbesondere in Wien, auf. Eine zentrale Rolle nimmt der ebenfalls seit langem von den „Neuen Rechten" angesprochene „Bevölkerungsaustausch" beziehungsweise „Great Reset" ein.

„The Great Reset" ist eine transnational geläufige Verschwörungserzählung, die besonders im Zuge der Corona-Pandemie auf großen Anklang gestoßen ist. Die Anhängerinnen und Anhänger dieser Verschwörungserzählung – die „Globalisten" – stehen in diesem Zusammenhang für eine geheime globale Elite, die im Hintergrund agiert. Diese nutzt die zunehmende Globalisierung in diversen Lebensbereichen sowie die Corona-Pandemie und ihre prekären Auswirkungen auf die Gesellschaft für ihre Ziele. Dabei wollen sie die bestehenden Nationalstaaten und „europäischen beziehungsweise weißen Völker" nach eigenen Vorstellungen umgestalten und untergraben. An diese Ansichten knüpfen eine Vielzahl altbekannter rechtsextremistischer, nationalistischer und antisemitischer Narrative an.

In diesem wird den „politischen Eliten" in Europa unterstellt, bewusst die „weiße" europäische Bevölkerung gegen eine muslimische/arabische/afrikanische einzutauschen beziehungsweise eine Mischung aus diesen absichtlich herbeiführen zu wollen. Während der COVID-19-Pandemie unterstützten die DO5 viele Argumente der Corona-Maßnahmen-Kritiker beziehungsweise -leugner und kritisierten die Maßnahmen als überzogen und Beschneidung der verfassungsmäßig gewährten Grundrechte. Zuletzt traten die Aktivistinnen und Aktivisten auch gegen die von der österreichischen Regierung verabschiedete Impfpflicht auf. Das taktische Motiv war in diesem Fall ebenfalls, den Frust vieler Bürgerinnen und Bürger aufzufangen und für die eigenen Zwecke zu nutzen.

Der Fokus der linksextremen Gruppierungen in Österreich legte sich mit dem Entstehen der DO5 sofort auf diese. Aus diesem Grund kam es seit dem Jahr 2020 zu mehreren Zwischenfällen, an denen DO5-Aktivistinnen und Aktivisten sowie Mitglieder von linksextremen Gruppierungen beteiligt waren. Aufgrund der ökonomischen und gesellschaftlichen Probleme lässt die derzeitige Situation in Österreich den Rückschluss

zu, dass die Spannungen zwischen den beiden verfeindeten Gruppierungen auch in der nächsten Zeit nicht abnehmen werden.

Deutschnationale Burschenschaften

Nach den napoleonischen Kriegen Anfang des 19. Jahrhunderts formierten sich im deutschsprachigen Raum zahlreiche männliche Studentenverbindungen, die Burschenschaften genannt werden. Mit dem aufkommenden nationalistischen Gedankengut in Europa und der deutschen Reichsgründung im Jahr 1871, die auch von den deutschen Burschenschaften unterstützt wurde, begründen auch heute noch die (pflicht-)schlagenden österreichischen Burschenschaften ihre politischen Aktivitäten, Handlungen und Ziele (die meisten deutschnationalen Burschenschaften führen schlagende Mensuren aus. Dies bedeutet, dass Mitglieder das Fechten erlernen und dies bei einer Mensur bestreiten können). Ebenso führte der zu dieser Zeit steigende Antisemitismus innerhalb der Gesellschaft dazu, dass Menschen jüdischen Glaubens von den Studentenverbindungen ausgeschlossen wurden und ein generelles Aufnahmeverbot für Menschen jüdischen Glaubens vollzogen wurde. Im 20. Jahrhundert unterstützten deutschnationale Burschenschaften zum Teil den Nationalsozialismus, da es zwischen den Zielen der NSDAP und der Burschenschaften einige Überschneidungen gab. Zahlreiche dieser Traditionen wurden nach dem Zweiten Weltkrieg, insbesondere von österreichischen deutschnationalen Burschenschaften, weiter gepflegt und werden auch heute noch ausgeübt. Aus diesem Grund wird unter anderem die Republik Österreich von diesen Studentenverbindungen abgelehnt, da sie diesen Staat als Teil Deutschlands ansehen beziehungsweise sich die Mitglieder der Studentenverbindungen als „Deutsche“ definieren und sehen.

Allgemein sind deutschnationale Burschenschaften als homogene Gruppe anzusehen und politisch im rechten Spektrum angesiedelt. Zwischen den einzelnen Burschenschaften ist ein dichtes Netzwerk vorhanden. Aufgrund dieses Netzwerks zwischen den Burschenschaften und den Verbindungen zur Politik gibt es zahlreiche Mitglieder, die hochrangige Funktionen in Politik, Verwaltung und Wirtschaft einnehmen.

Aufgrund des Verbotsgesetzes, das jegliche Befürwortung, Gutheißung und Verbreitung von nationalsozialistischem Gedankengut in Österreich verbietet, der beschriebenen Ideologie und der problematischen Auseinandersetzung von deutschnationalen Burschenschaften mit dem Nationalsozialismus, kam und kommt es regelmäßig zu strafrechtlichen Verfahren gegen Mitglieder dieser Burschenschaften. Neben dem Verbotsgesetz finden auch immer wieder Ermittlungen wegen Verhetzung statt, da oftmals andere Ethnien, Religionsgemeinschaften, Bevölkerungsgruppen etc. als minderwertig gegenüber dem „Deutsch- und Christentum“ gesehen werden. Die meisten Tathandlungen werden in den sozialen Medien und der digitalen Welt begangen.

Weiters konnte von den Verfassungsschutzbehörden beobachtet werden, dass Kontakte zu rechtsextremen Gruppierungen, wie der Identitären Bewegung, vorhanden sind und gemeinsam an Demonstrationen teilgenommen wird beziehungsweise solche miteinander veranstaltet werden. Oftmals sind auch personelle Überschneidungen zu finden – beispielsweise ist ein Mitglied einer deutschnationalen Burschenschaft auch ein Aktivist der Identitären Bewegung.

3.1.1.3 Fälle 2021

Unter dem Pseudonym „Mr. Bond" verbreitete der österreichische Staatsbürger Philip H. im Internet seit mindestens 2016 unerkannt nationalsozialistisch geprägte Liedtexte. Seine Lieder inspirierten den rechtsterroristischen Attentäter von Halle, Stephan B., der versuchte, am 9. Oktober 2019, dem höchsten jüdischen Feiertag, die Hallesche Synagoge zu stürmen und in weiterer Folge zwei Personen tötete. Der von ihm live im Internet gestreamte Anschlag wurde akustisch durch ein Lied von „Mr. Bond" unterlegt.

Bis zum Zeitpunkt dieser Tat war „Mr. Bond" der Öffentlichkeit weitgehend unbekannt und eher ein szenerelevantes Internet-Phänomen, nun geriet er jedoch in den Fokus der Polizeibehörden.

Nach monatelangen Ermittlungen des Verfassungsschutzes in Zusammenarbeit mit dem LVT und dem LKA Kärnten konnte so die Identität des rechtsextremen Rappers ausgeforscht werden. Bei der Hausdurchsuchung wurden zahlreiche Datenträger, Waffen, eine Reichkriegsflagge, Liedtexte sowie sonstige Beweismittel, darunter auch NS-Devotionalien, sichergestellt. Seitens der Staatsanwaltschaft Wien wurde die Festnahme von Philip H. angeordnet.

Philip H. alias NS-Rapper „Mr. Bond" hatte sich die HipHop-Kultur angeeignet und diese mit seiner rechtsextremen Weltsicht vermischt. In seinen meist englischsprachigen Liedern dichtete er bekannte alte und neue Musikstücke zu rassistischen Hasstiraden um. Mit seiner Musik wurde er zu einer Art Ikone für Rechtsextreme.

Philip H. übersetzte auch das englischsprachige Manifest des Christchurch-Attentäters Brenton T., der am 15. März 2019 bei einem Anschlag auf zwei Moscheen 51 Menschen tötete und widmete ihm den Song „Holding Out For A Tarrant".

Im Jahr 2016 veröffentlichte Philip H. seine erste CD und bis 2019 – dem Jahr der tödlichen Anschläge von Christchurch und Halle – folgten dieser vier weitere Veröffentlichungen.

Philip H. bekannte offen seine Sympathie für rechtsextreme Anschläge. Am 21. Juni 2019 schrieb er nach dem Mord durch den deutschen Rechtsextremisten Stephan E. an dem Kasseler CDU-Politiker Walter Lübcke in einem US-amerikanischen Forum: „Wir haben einen neuen deutschen Helden!".

Aufgrund der Huldigungen der Attentäter, der schon seit Jahren immer wieder veröffentlichten Lieder und Videos, die zu Hass und Gewalt aufrufen sowie der eigenen Waffenaffinität war von einer besonderen Gefährlichkeit des Philip H. auszugehen. Es bestand der Verdacht, dass dieser selbst ein Attentat planen oder andere weiter dazu animieren könnte, Anschläge beziehungsweise Attentate zu begehen. Auch die Tatsache, dass für ihn nach seiner Festnahme Huldigungen durch Gleichgesinnte im Internet veröffentlicht und in die Haftanstalt Postkarten mit nationalsozialistischem Inhalt versendet wurden, unterstreicht seine Ambitionen, andere mit seinen Liedern zur Begehung von Straftaten anzustiften.

Bei der weiteren Auswertung konnte der Bruder des Philip H., Benjamin H., als Beitragstäter ermittelt werden. Des Weiteren wurde Benjamin H. als jene Person identifiziert, die sich hinter der antisemitischen und verhetzenden Website „Judas Watch" verbirgt. Die Website hatte Jüdinnen und Juden sowie nicht-jüdische Personen und Parteien aufgelistet und wegen Multikulturalismus, Kulturmarxismus, Feminismus, Kommunismus etc. „angeprangert". Jüdische Namen wurden, ähnlich dem vom NS-Regime zur Stigmatisierung eingesetzten Judenstern, mit einem gelben Davidstern markiert. Zudem wurde zu jeder Person auf der Liste eine erklärende Kurzinformation bereitgestellt, warum diese als „Feind" gelistet wurde.

Zwischenzeitlich wurde Philip H. im Zuge der Verhandlung am Landesgericht Wien im Sinne der Anklage – nicht rechtskräftig – schuldig erkannt und wegen nationalsozialistischer Wiederbetätigung zu zehn Jahren Haft verurteilt. Das Gericht ging dabei von einer „besonderen Gefährlichkeit" aus.

Wie der vorsitzende Richter in der Urteilsbegründung darlegte, ist die von der Staatsanwaltschaft angenommene „besondere Gefährlichkeit" des in rechtsextremen Kreisen populären „Mr. Bond" nicht von der Hand zu weisen.

Auch sein Bruder Benjamin H. wurde im Zuge der Verhandlung im Sinne der Anklage – nicht rechtskräftig – schuldig erkannt. Er wurde zu einer unbedingten Haftstrafe von vier Jahren verurteilt.

3.1.1.4 Trends und Entwicklungstendenzen

Im Hinblick auf mögliche künftige Entwicklungen kann davon ausgegangen werden, dass sich im Falle eines allmählichen Abflauens des Protestaktivismus und des damit einhergehenden Mobilisierungspotenzials in der Bevölkerung – bedingt etwa durch die Eindämmung der Corona-Pandemie beziehungsweise Normalisierung der Lage oder einer grundsätzlichen „Protestmüdigkeit" – die Argumentationslinien und Aktivitäten rechtsextremistischer Propagandistinnen und Propagandisten wieder verschieben. Der aktionistische Schwerpunkt dürfte sich in der virtuellen und realen Welt von der Corona-/Impf-Thematik weg und wieder hin zu altbekannten asyl- und

fremdenfeindlichen Agitationen sowie zu potenziell neuen Protestanlässen ausrichten. Zugleich liegt die Vermutung nahe, dass durch das Schwinden der Corona-Problematik als ideologisch relevantes Betätigungsfeld eine gemeinsame Sondierung neuer Mobilisierungsmöglichkeiten erfolgen wird. Es könnte wieder verstärkt auf regionale Vernetzungsaktivitäten, Bildungsinitiativen und eine professionalisierte Protestkultur fokussiert werden. Damit könnte von neurechten Akteurinnen und Akteuren weiterhin der Versuch unternommen werden, meinungsbildend im öffentlichen Diskurs zu wirken und ihn zu verändern, sich als patriotische Widerstandsaktivistinnen und -aktivisten zu inszenieren und neue, vorwiegend junge Mitglieder zu rekrutieren.

Vor diesem Hintergrund und den gegenwärtigen gesellschaftspolitischen Entwicklungen sowie ihren Auswirkungen auf den öffentlichen Diskurs wird auch künftig vom Rechtsextremismus ein erhöhtes verfassungsschutzrelevantes Risiko ausgehen. Dies begründet sich nicht nur in den milieutypischen Agitationen rechtsextremistischer Gruppierungen, sondern insbesondere auch in den permanenten Unterwanderungs- und Einflussversuchen ihrer Akteurinnen und Akteure auf das virtuelle und öffentliche Protestgeschehen im Kontext der Corona-Pandemie. Es ist davon auszugehen, dass Proponentinnen und Proponenten des heimischen organisierten Rechtsextremismus sowie der neurechten Bewegungen allfällige Kundgebungen gegen die Corona-Maßnahmen wieder vermehrt als Plattform nutzen und vereinnahmen könnten, um ihre Aktionen öffentlichkeitswirksam umzusetzen und ihre eigene Reichweite zu erhöhen. Vor allem die Beteiligung von gewaltaffinen beziehungsweise -bereiten Szene-Exponentinnen und -Exponenten an Kundgebungen und Demonstrationen birgt eine schwer kalkulierbare Gefahr in sich, die sich durch mögliche Zusammenstöße mit der politischen „Gegnerschaft“ aus dem linksradikalen bis -extremistischen Spektrum verschärfen könnte.

Bestrebungen, die sich weltanschaulich gegen die Grundprinzipien einer Demokratie richten – seien es rassistische, antisemitische, islam- oder andere fremdenfeindliche Meinungsäußerungen und Tathandlungen – gefährden nicht nur die öffentliche Ruhe, Ordnung und Sicherheit, sondern auch den sozialen Frieden und den gesamtgesellschaftlichen Zusammenhalt in Österreich wie auch in anderen Staaten.

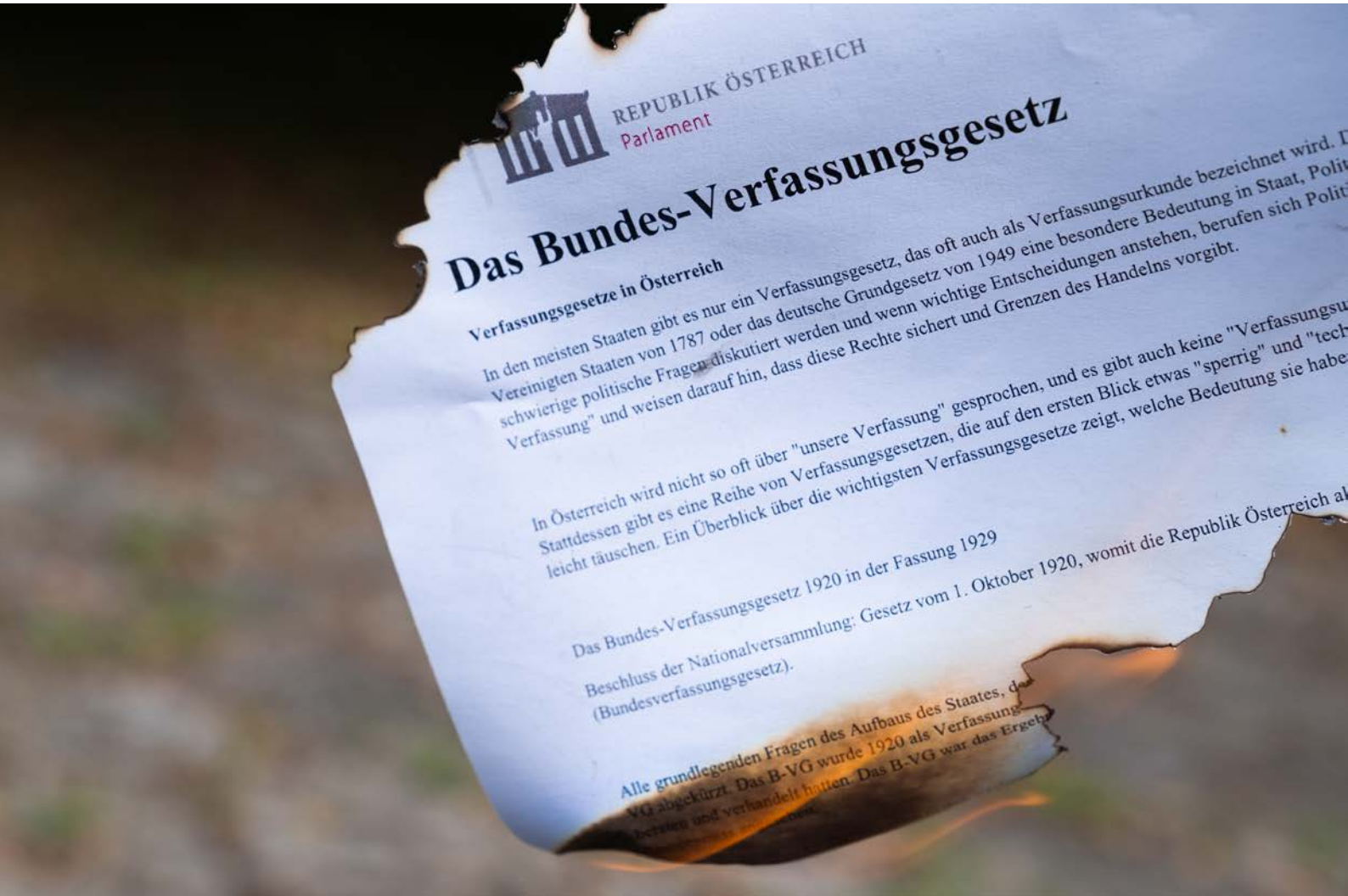
Internationale Bezüge des Rechtsextremismus in Österreich zeigen sich etwa in der Einbettung wirkstarker Verschwörungserzählungen in globale, nationale Grenzen transzendierende Diskurse. Gleichzeitig bietet der Besuch von Veranstaltungen (z. B. Kampfsport oder Musik) die Möglichkeit, sich international auszutauschen beziehungsweise zu vernetzen, wenn auch mit einer durch Corona stark veränderten Dynamik. Internationale Bezüge und inhaltsbezogene Vernetzungen zwischen rechtsextremistischen Milieus und Akteurinnen und Akteuren zeigen sich auch in der wechselseitigen Rezeption rassistisch-neonazistisch geprägter Musik (siehe beispielhaft „Mr. Bond“).

Sobald das gesellschaftliche Interesse an der Pandemie rückläufig ist, könnte es zu einem Rückgang von großdimensionierten Protestveranstaltungen und zu einer Zunahme konspirativen Verhaltens im virtuellen Raum – unter anderem aufgrund des Verbots der öffentlichen Verwendung der IBÖ/DO5-Symbole nach dem Symbole-Gesetz aus Juli 2021 – sowie zu gruppentypischen Vernetzungen und Protestagitationen als Provokation linksgerichteter Gruppierungen kommen. Gerade konspirative Vernetzungen erhöhen dabei das Risiko von Rekrutierungen aus kriminellen, gewaltaffinen Bereichen. Die Möglichkeit eines Gewaltaktes durch einen politisch fanatisierten Einzelaktivisten, eine Einzelaktivistin, einen geistig abnormen Rechtsbrecher oder eine geistig abnorme Rechtsbrecherin kann grundsätzlich nicht völlig ausgeschlossen werden und stellt eine nicht zu quantifizierende Risikoebene dar. Entwicklungen wie diese hätten kurz-, mittel- und langfristige Auswirkungen auf die Sicherheitslage in Österreich.

3.1.2 Staatsfeindliche Verbindungen

3.1.2.1 Überblick

Staatsfeindliche Verbindungen sind Gruppierungen, die die Existenz der Republik Österreich und deren Institutionen nicht anerkennen und folglich das hoheitsrechtliche Handeln des Staates ablehnen. Zwei unterschiedliche Weltanschauungen bilden die Grundlage ihres Tuns: Eine Strömung vertritt die Reichsbürgerideologie, die den Bestand des Deutschen Reiches auf Grundlage der Weimarer Verfassung weiterhin als gegeben ansieht und den völkerrechtlich legitimierten Bestand der Republik Österreich und der Bundesrepublik Deutschland abstreitet. Die andere Strömung lehnt ein Justizsystem



des positiven Rechts ab, das unmittelbar durch Naturrecht beziehungsweise Common Law abgelöst werden sollte.

> **Common Law** ist ein vor allem im angelsächsischen Raum vorherrschendes Rechtssystem, das sich nicht nur auf Gesetze, sondern vorrangig auf vergangene Urteile, das heißt auf Präzedenzfälle, stützt.

Gemein ist ihnen die Ansicht, dass der Staat Österreich über keine Hoheitsrechte verfügt und ein Privatunternehmen ist, ebenso die Mitarbeiterinnen und Mitarbeiter des öffentlich-rechtlichen Sektors. Anerkannt werden ausschließlich die von ihnen propagierten Rechtssysteme beziehungsweise die von ihnen errichteten virtuellen und tatsächlichen Parallelstrukturen im Justiz- und Sicherheitsbereich. Ausfluss daraus ist ein breiter, radikaler und oftmals militanter Widerstand gegen das Handeln österreichischer Staatsorgane. Ihre unterstützenden Personen sind davon überzeugt, dass „das System" zeitnah zusammenbricht und dann ihr Konzept von der gesamten Bevölkerung angenommen wird.

3.1.2.2 Aktuelle Lage

Ab dem Jahr 2017 wurde durch zahlreiche polizeiliche sowie justizielle Maßnahmen gegen die Führungspersönlichkeiten und Mitglieder der größten staatsfeindlichen Verbindungen wie dem „Staatenbund Österreich", dem „International Common Law Court of Justice (ICCJV)" und dem „Global Common Law Court of Justice (GCCL/GCLC)" auf rechtlichem Weg vorgegangen. So konnten in den Folgejahren (nach 2019) mehrere Aktivistinnen und Aktivisten von österreichischen Gerichten zu mehrjährigen Haftstrafen verurteilt werden.

Mittlerweile wurden mehrere hundert Personen wegen staatsfeindlicher Agitationen von österreichischen Gerichten verurteilt beziehungsweise befinden sich in einem Strafverfahren. Die Großzahl der Anzeigen gegen Staatsverweigerinnen und Staatsverweigerer betrafen die Delikte §§ 105, 107, 246 StGB (Nötigung, Gefährliche Drohung, Staatsfeindliche Verbindungen) und Anstiftungen zu Amtsdelikten.

Bei den vorher genannten größeren staatsfeindlichen Verbindungen wie dem „Staatenbund Österreich" und dem ICCJV kamen noch Betrugsdelikte hinzu, da die betroffenen Personen eigene Dokumente wie Personal- und Diplomatenausweise, KFZ-Kennzeichen und behördliche Dokumente wie Grundbucheinträge, Gewerbescheine etc. kreierten, diese zum Verkauf anboten und die Geschädigten im Glauben ließen, diese im Rechtsverkehr verwenden zu können.

Nach den ersten Verurteilungen, die auch medial begleitet wurden, konnte von den Verfassungsschutzbehörden ab dem Jahr 2019 ein stetiger Rückgang der Agitationen der Staatsverweigererszene beobachtet werden. Allerdings ist seit der zweiten

Hälfte des Jahres 2021 wieder ein leichter Anstieg in der Szene bemerkbar. Der sogenannte „Papierterrorismus“ – das Verfassen von zig-seitigen Einsprüchen und Protestnoten inklusive pseudojuristischer Abhandlungen an österreichische Behörden, um Verwaltungsverfahren zu erschweren und in die Länge zu ziehen – von Anhängerinnen und Anhängern diverser Gruppierungen und Einzelaktivistinnen und Einzelaktivisten nahm wieder zu.

Der Anstieg der Agitationen ab Beginn des Jahres 2021 ist mit Sicherheit auch auf die COVID-19-Pandemie zurückzuführen. Im Zuge der mehrmonatigen großen Proteste im ganzen Bundesgebiet gegen die Maßnahmen der Bundesregierung zur Bekämpfung der COVID-19-Pandemie und der Impfplicht konnten von den Verfassungsschutzbehörden zahlreiche Argumentationslinien der staatsfeindlichen Verbindungen beobachtet werden. Hierzu zählen Verschwörungserzählungen im Bezug zur COVID-19-Pandemie und zur Impfung sowie jene Verschwörungserzählungen, die von der in den letzten Jahren an Popularität gewinnenden QAnon-Bewegung – die ebenfalls in Österreich von der Staatsverweigererszene propagiert wird – verbreitet werden. Weiters konnte festgestellt werden, dass zahlreiche prominente Corona-Maßnahmen-Gegner zuvor in der Staatsverweigererszene aktiv waren.

3.1.2.3 Fälle 2021

Im Berichtsjahr 2021 wurden zahlreiche Anhänger der Staatsfeindlichen Verbindungen angeklagt beziehungsweise verurteilt. Vor allem Mitglieder der beschriebenen Gruppierungen wie dem Staatenbund Österreich, dem ICCJV und dem GCLC wurden zu teilweise unbedingten Haftstrafen verurteilt. Unter den Verurteilten befanden sich auch Führungspersönlichkeiten (insbesondere jener des ICCJV und des GCLC) der genannten Gruppierungen.

Weiters wurde der Gründer des GCLC, der deutsche Staatsbürger Carl Peter H. am 23. September 2021 aufgrund eines internationalen Haftbefehles bei einer Anti-Corona-Kundgebung in Liechtenstein von den dortigen Behörden festgenommen. Zwischenzeitlich erfolgte die Auslieferung nach Österreich und H. kam in Untersuchungshaft. Dieses sowie zahlreiche weitere Gerichtsverfahren gegen Mitglieder und Aktivisten der Staatsverweigererszene werden auch im Jahr 2022 noch stattfinden.

3.1.2.4 Trends und Entwicklungstendenzen

Die mehrjährigen Haftstrafen und das damit verbundene Fehlen von Führungspersonen schwächte die Szene. Nach dem erneuten Aufkommen der Staatsfeindlichen Verbindungen zu Beginn des Jahres 2021 und dem damit verbundenen neuen „Papierterrorismus“ wird die Szene auch künftig nach neuen Wegen suchen, um dem ihrer Ansicht nach „Privatunternehmen“ Österreich zu schaden. Jedoch ist nicht von einer zunehmenden Gewalttätigkeit auszugehen, sondern vielmehr von neuen Formen der versuchten Behinderung des Verwaltungsapparats. Mit dem erwarteten Abflauen der Corona-

Pandemie ist ein Bedeutungsverlust der bisherigen Verschwörungserzählungen zu erwarten. Dennoch hat sich ein Kern gebildet, der die bereits gesetzten Narrative umdeuten oder in einem neuen Mantel präsentieren kann.

3.1.3 Linksextremismus

3.1.3.1 Überblick

Linksextremismus ist ein Sammelbegriff für kommunistische und anarchistische Einflüsse sowie Ideologien, die grundsätzlich Demokratie als Herrschaftsform – die politische Ordnung oder das politisches System, in dem die Macht und Regierung vom Volk ausgeht – ablehnen. Ziel ist die Schaffung einer egalitären Gesellschaft, welche die demokratische Grundordnung ablehnt und zur Durchsetzung ihrer Ideologie Gesetzesbrüche und teilweise Gewalt in Kauf nimmt.

Aufgrund unterschiedlicher Ansichten innerhalb der linksextremen Szene erfolgte eine Spaltung in eine autonom-anarchistische und marxistisch/leninistisch/trotzkistische Bewegung. Marxismus-Leninismus ist eine im linken Spektrum angesiedelte Staatsdoktrin der 1920er Jahre in der Sowjetunion und bezeichnet eine theoretische Vorgabe für den Kampf zwischen gesellschaftlichen Klassen. Trotzkismus ist eine Richtung des „reinen“ Marxismus mit einer starken Nähe zum Leninismus. Gemeinsam ist ihnen der Wunsch nach dem Ersatz des bürgerlich-kapitalistischen Systems durch eine herrschaftsfreie Gesellschaft beziehungsweise einen sozialistischen Staat.

Insbesondere Aktivistinnen und Aktivisten, die dem autonom-anarchistischen Spektrum zuzuordnen sind, verfolgen das Ziel, die bestehende Staats- und Gesellschaftsordnung zu beseitigen. Sie sehen in den staatlichen Institutionen der freiheitlichen Demokratie und im westlichen bestehenden Parlamentarismus einen Gegner, den es mit allen möglichen Mitteln zu bekämpfen und letztendlich durch ein anarchistisches beziehungsweise herrschaftsfreies System zu ersetzen gilt. Die marktwirtschaftliche Eigentumsordnung und der demokratische Rechtsstaat werden von ihren Anhängenden als „verschmolzene Einheit" (kapitalistisches System) angesehen. Diese Staatsform dient ihrer Ansicht nach nur der Ausbeutung und Unterdrückung der Arbeiterklasse und des Niedriglohnsektors durch wenige Privilegierte („monetäre Elite der Gesellschaft"). Aus diesem Grund ist die Gleichheit und Freiheit der Menschen im kapitalistischen System nur Schein und Trug. Obwohl sie die kommunistischen Regime des ehemaligen Ostblocks kritisieren – da aufgrund der Größe der Gesellschaften und des hierarchischen Staatsapparats wieder Herrschaftsverhältnisse entstanden sind – sehen sie in revolutionärer Gewalt ein legitimes Mittel zur Veränderung der Gesellschaftsstrukturen.

Schlussendlich wird dem Kapitalismus auch die Schuld an den „globalen Hauptproblemen" wie Krieg, Umweltzerstörung, Rassismus, Fremdenfeindlichkeit und materieller Ungleichheit gegeben. Politische Reformen könnten oftmals die Symptome der gesellschaftlichen und wirtschaftlichen Probleme lösen, aber niemals langfristig wirken. Aus diesem Grund ist letztendlich ausschließlich die Vernichtung des kapitalistischen Systems und seiner Einrichtungen, wie politischer Institutionen, das Ziel.

3.1.3.2 Aktuelle Lage

Linksextremistinnen und Linksextremisten geben meist durch Proteste (Abhaltung von Kundgebungen) ihre Meinung gegen gesellschaftliche Missstände oder politische Geschehnisse kund. Oftmals wird bewusst auf die Formulierung konstruktiver Kritik verzichtet. Diese „Fehlentwicklungen und Missstände" seien der Beweis für das Nichtfunktionieren des kapitalistischen Systems, das es so schnell wie möglich zu überwinden beziehungsweise abzuschaffen gilt. Insbesondere das Verständnis der Autonomen, Gewalt als legitimes Mittel anzusehen, wird von den Verfassungsschutzbehörden als Risiko für die öffentliche Ruhe, Ordnung und Sicherheit eingestuft.

Das Gefährderumfeld in der linksextremistischen Szene bildet sich überwiegend aus mehreren autonomen und anarchistischen Gruppierungen. Militanz und Gewaltakzeptanz der Aktivistinnen und Aktivisten ist ein identitätsstiftendes und zentrales Element dieser Gruppierungen. Es handelt sich dabei überwiegend um auf kurz- und mittelfristige Dauer ausgerichtete Verbindungen, die sich häufig mit dem Ziel der Umsetzung gewalttätiger Proteste – und damit strafrechtlicher Tatbestände – vereinigen. Hier können vor allem Sachbeschädigungen und Körperverletzungen durch linksextreme Aktivistinnen und Aktivisten beobachtet werden. Geschädigte beziehungsweise Opfer dieser Taten sind

meist politische Gegner wie Mitglieder von schlagenden studentischen Verbindungen (Burschenschaften), Aktivistinnen und Aktivisten der IBÖ, die als stärkste und populärste rechtsextreme Gruppierung gilt, aber auch staatliche Institutionen und deren Vertreterinnen und Vertreter, die ideologisch ebenfalls als Hauptfeind angesehen werden.

Bei den einzelnen Gruppierungen ist eine starke Fluktuation der Aktivistinnen und Aktivisten beobachtbar. Oftmals sind neue Mitglieder nur über einen kurzen Zeitraum bei den Verbindungen aktiv und schließen sich dann einer anderen Gruppe an oder steigen überhaupt aus dem Milieu aus. Die meisten der beschriebenen Gruppierungen nehmen bei großen Demonstrationen teil. Hier versuchen die einzelnen linksextremen Verbindungen im Rahmen der Demonstrationen ihre Vorstellungen in die Tat umzusetzen. In anderen Worten, militantere Gruppen wollen mit dem politischen Gegner und der Exekutive in Konflikt geraten und strafbare Handlungen wie Sachbeschädigungen und Widerstände gegen die Staatsgewalt setzen. Allerdings muss hier angemerkt werden, dass innerhalb der einzelnen Gruppierungen Bezugsgruppen bestehen, die relativ autonom bei diesen Demonstrationen handeln. Je nach Situation, Möglichkeit und Stimmung werden strafbare Handlungen von diesen Kleingruppen gesetzt beziehungsweise versucht zu setzen. Aufgrund der Grundideologie gibt es keine hierarchischen Strukturen und somit kann jede Aktivistin und jeder Aktivist autonom nach eigenem Ermessen handeln. Obwohl es vor allem bei Großdemonstrationen des Öfteren Vorbesprechungen einzelner Gruppierungen gibt, um den Ablauf der Demonstration zu akkordieren, bleibt es letztendlich jedem einzelnen Aktivisten und jeder einzelnen Aktivistin selbst überlassen, wie sich dieser oder diese bei solchen Veranstaltungen verhält und welche Handlungen umgesetzt werden.

Innerhalb des Linksextremismus ging im Jahr 2021 die größte Gefahr für die Funktions- und Handlungsfähigkeit des Staates beziehungsweise der Verfassung von autonom-anarchistischen Gruppierungen in Österreich aus. Diese splitten sich in viele (regionale) Verbindungen auf. Unter diesen Gruppierungen bestehen oftmals Kontakte, um an verschiedenen Aktivitäten, insbesondere Demonstrationen, gemeinsam teilzunehmen. Ebenfalls kann festgestellt werden, dass einzelne Personen in mehreren Gruppierungen aktiv sind. Oftmals sind diese Aktivistinnen und Aktivisten die Bindeglieder zwischen zwei oder mehreren Formationen. Aufgrund der Ideologie der autonom-anarchistischen Gruppierungen, welche die „Herrschaftsfreiheit“ propagieren, ist es sehr schwer, tatsächliche Führungspersönlichkeiten innerhalb der Gruppierungen beziehungsweise der ganzen Szene zu eruieren, da sie diese auch nach offizieller Lesart ihrer Überzeugungen (Nichtakzeptanz von Herrschaftsverhältnissen) nicht akzeptieren. Aufgrund der teilweise hohen Präsenz im Internet, und hier vor allem in den sozialen Medien, können Sprachrohre innerhalb der Gruppierungen immer wieder festgestellt werden.

Bedingt durch die in quantitativer Hinsicht eher kleine linksextreme Szene in Österreich sowie aufgrund des Umstandes, dass internationale Veranstaltungen und sonstige Anlässe im Jahr 2021 aufgrund der Corona-Pandemie kaum stattfanden,

war das Mobilisierungspotenzial in personeller Hinsicht im Berichtszeitraum deutlich eingeschränkt.

Die linksextreme Szene verfügt über diverse Auslandskontakte, wenngleich diese aufgrund der coronabedingten Reiseeinschränkungen im Jahr 2021 stark reduziert wurden. Die internationalen Verbindungen weisen allerdings kein stabiles und strukturiertes Netzwerk auf, sondern basieren primär auf Einzelkontakten beziehungsweise auf Solidarisierungskampagnen mit Gruppierungen im Ausland, wenn diese in den Fokus von Strafverfolgungsbehörden geraten. In der linksextremen Szene in den Universitätsstädten sind allerdings vermehrt in Österreich wohnhafte ausländische Studentinnen und Studenten aktiv, die sich sowohl bei universitäts- und bildungspolitisch motivierten Protesten engagieren als auch an antifaschistischen Aktionen beteiligen.

3.1.3.3 Fälle 2021

Seit dem Jahr 2020 konnten durch linksextreme Täter Attacken auf Vertreter der IBÖ beziehungsweise Örtlichkeiten, welche diese benützen, festgestellt werden.

Im März 2020 wurde von fünf männlichen Mitgliedern bzw. weiteren unbekannten Tätern der ANTIFA Wien versucht, eine angemeldete Versammlung am Karlsplatz in Wien von IBÖ/DO5-Aktivisten mit Gewalt zu verhindern. Dabei wurden die IBÖ/DO5-Mitglieder attackiert bzw. einer davon verletzt. Ebenso brachten die Täter Equipment und Werbematerial für die Veranstaltung der rechten Gruppierung an sich und versuchten, diese zu zerstören.

Einige Monate später wurden durch einen linksextremen Aktivisten, welcher bereits bei dem Angriff im März beteiligt war, drei Anhänger bei einer IBÖ/D05-Veranstaltung in der Wiener Innenstadt angegriffen und durch Faustschläge verletzt.

Im August 2020 attackierten abermals drei bekannte Aktivisten mit weiteren unbekannten Tätern der ANTIFA Mitglieder der IBÖ/DO5, als diese einen Stammtisch in Wien abhalten wollten. Dabei wurden mehrere Anhänger der IBÖ/DO5 verletzt.

Durch gemeinsame Ermittlungen des LVT Wien mit dem BVT im Berichtsjahr konnten insgesamt sieben linksextreme Aktivisten ausgeforscht werden, die für zumindest eine Attacke verantwortlich waren. Die Beschuldigten wurden aufgrund der Tatbestände §§ 883 StGB (Körperverkletzung), 91 StGB (Raufhandel), 125 StGB (Sachbeschädigung) angeklagt. Der Prozess startete im Frühjahr 2022 am LG Wien.

Eine weitere Tathandlung, welche der linksextremen Szene in Österreich zugeschrieben wird, war das Anzünden und schwere Beschädigen eines Funkwagens der Polizei in Innsbruck im Februar 2021 mit Hilfe eines Brandbeschleunigers. Auslöser für diese Aktion dürfte die Kundgebung zum Thema „Grenzen töten“ in Innsbruck am 30. Jänner

2021 gewesen sein, wo Polizeikräfte mehrere Aktivistinnen und Aktivisten festnahmen, als diese sich nicht an die COVID-Bestimmungen hielten bzw. den Tatbestand des Widerstandes gegen die Staatsgewalt setzten.

3.1.3.4 Trends und Entwicklungstendenzen

Die Aktivitäten und Mobilisierungspotenziale der linksextremen Szene in Österreich bleiben voraussichtlich stark von aktuellen politischen, sozioökonomischen und gesellschaftlichen Entwicklungen und Ereignissen beeinflusst. Als Entwicklungstrend ist demnach zu erwarten, dass auch weiterhin primär das Aktionsfeld „Antifaschismus" ein das gesamte linksextreme Spektrum umfassendes Mobilisierungspotenzial besitzen wird. Neben den in den letzten Jahren evidenten Mobilisierungsschwerpunkten könnten in Zukunft verstärkt auch Aktivitäten der „Neuen Rechten" sowie Auswirkungen von internationalen Krisenherden zu (gewalttätigen) Aktionen und Protestkundgebungen führen.

Des Weiteren ist mittel- bis langfristig damit zu rechnen, dass die österreichische linksextreme Szene durch die Themenfelder „Entmilitarisierung" und „Verteilungsgerechtigkeit" einen erheblichen Mobilisierungs- und Aktivitätsschub erlebt. Diese Annahme impliziert auch die Möglichkeit einer Zunahme von gewalttätigen Aktionen.

Indikatoren für die Planung von terroristischen Anschlägen oder den Aufbau von terroristischen Strukturen sind in der linksextremen Szene nicht evident und zumindest kurzfristig auch nicht zu erwarten.

3.2 Islamismus und islamistischer Terrorismus

3.2.1 Überblick

Islamistischer Extremismus bezeichnet eine sich religiös legitimierende Form des politischen Extremismus, der versucht, einen islamischen Staat und eine Gesellschaft mit der Scharia als einzig gültige Rechtsordnung durch (gewaltsame) Methoden herbeizuführen, die den demokratischen Rechtsstaat missachten, bedrohen oder beseitigen. Dies bedeutet im Umkehrschluss eine Ablehnung der westlichen Lebensweise und der Prinzipien einer demokratischen, aufgeklärten Gesellschaft.

Diese Arten von Ideologien spielen mit Ängsten ungefestigter junger Menschen. Sie bieten einfache Lösungen für komplexe Probleme und schüren Feindbilder und Gewaltbereitschaft. Der **Salafismus**, der seine Bezeichnung vom Begriff der „rechtschaffenen Altvorderen" (Arabisch: as salaf as salih) herleitet, wird als eine islamistische Ideologie verstanden, die eine Rückkehr zu einem Islam aus der Zeit des Propheten Muhammad und der ersten Muslime der Frühzeit, im 7. bis 9. Jahrhundert, propagiert. Der Islam wird somit als soziale und normative Ordnung nach dem Willen Gottes konzipiert, an der sich jede Muslimin

und jeder Muslim in allen Lebenssituationen zu orientieren hat. Gleichzeitig wird jegliche Anpassung der Islamauslegung an sich verändernde gesellschaftliche und politische Gegebenheiten als „unislamische Neuerung“ abgelehnt. Die salafistische Ideologie bietet also eine praxisorientierte Lebensanleitung, die in einer globalisierten und durch Unsicherheiten geprägten Gesellschaft einfache Antworten auf vielschichtige soziale oder ökonomische Herausforderungen bereithält. Diese Ausschließlichkeit einer „gottgewollten“ islamischen Ordnung trägt aber auch dazu bei, Andersdenkende abzulehnen beziehungsweise als Feindbild zu betrachten. Die kompromisslose Verfolgung der eigenen ideologischen Ziele kann schließlich zur Akzeptanz und Anwendung von Gewalt führen.

Die salafistische Ideologie und die aus ihr hervorgegangenen heterogenen Bewegungen zählen seit Jahren zu den dynamischsten islamistischen Bestrebungen. Während sich Vertreter des politischen Salafismus auf intensive Propagandatätigkeiten (Missionierung) stützen, um politischen und gesellschaftlichen Einfluss zu gewinnen, sieht der jihadistische Salafismus die Anwendung von extremistischer Gewalt (Terrorismus) als Mittel zur Zielerreichung vor.

Seit rund 40 Jahren wird das Konzept des Jihad von einer Szene vereinnahmt, die sich im Zuge des Afghanistan-Krieges zwischen 1979 und 1989 gebildet hat.

> **Jihad** wird im Sinne eines islamistischen Extremismus als „Heiliger Krieg“ gegen die Feinde des Islam verstanden. Mit dem bewaffneten Kampf soll dem Islam zum Sieg über den „Unglauben“ verholfen und die Wiedererrichtung eines Kalifates beziehungsweise islamischen Staates erreicht werden.

Der **Jihadismus** kann dementsprechend als die radikalste Form des Salafismus bezeichnet werden und hat mit terroristischen Organisationen wie Al-Qaida (AQ), dem Islamischen Staat (IS) oder mit diesen affiliierten Gruppen und Netzwerken bekannte Proponenten.

Die Errichtung eines islamischen Staates und damit einhergehend die Wiedererrichtung des Kalifats ist das zentrale Ziel vieler islamistisch-extremistischer Gruppen, allerdings gibt es unterschiedliche Vorstellungen über den Zeitpunkt der Zielerreichung. Während Al-Qaida das Kalifat als Ergebnis am Ende eines Prozesses der Bekämpfung und Überwindung westlicher Interessen und Einflussnahmen sieht, nutzte der Islamische Staat seine territoriale Ausbreitung in Syrien und im Irak dazu, das Kalifat auszurufen und es damit an den Anfangspunkt für die Wiederherstellung eines längst vergangenen Herrschaftsgebietes zu stellen. Die Proklamation eines islamischen Staates war auch ein zentraler Pull-Faktor für die Ausreisebereitschaft tausender Musliminnen und Muslime aus Europa in Richtung Syrien und Irak.

3.2.2 Aktuelle Lage

Terroristische Organisationen, wie der sogenannte Islamische Staat oder Al-Qaida und die mit diesen affiliierten Gruppierungen, stellten auch im Jahr 2021 eine latente Gefahr für Europa und Österreich dar. Das Phänomen des transnationalen islamistischen Terrorismus hat sich in den letzten Jahren allerdings gewandelt. Der IS konnte das in den Jahren 2016 und 2017 verlorene Gebiet in Syrien und im Irak auch im Jahr 2021 nicht zurückerobern und agiert daher weiterhin im Untergrund. Erfolge konnten allerdings die als „Provinzen" bezeichneten Ableger des IS in der afrikanischen Sahel-Zone sowie in Afghanistan verzeichnen. Diese setzten jedoch hauptsächlich auf regionale Ziele. Auch Al-Qaida legte den Fokus im Jahr 2021 auf regionale Konflikte und war vor allem darauf bedacht, den eigenen Status in Afghanistan zu festigen. Dieser Prozess der Regionalisierung wird mit hoher Wahrscheinlichkeit weiter andauern.

Wie auch in den Jahren zuvor stellt der islamistische Extremismus und Terrorismus ein erhöhtes Bedrohungspotenzial für Österreich dar. Österreich engagiert sich als Teil der Europäischen Union und somit der westlichen Gesellschaften im Kampf gegen den transnationalen islamistischen Terrorismus. In diesem Zusammenhang zeigte man in den vergangenen zwei Jahren zudem eine konsequentere Vorgehensweise gegen den islamistischen Extremismus, indem auch nicht gewalttätige Islamisten in den Fokus der Strafverfolgungsbehörden rückten. Mit diesem Vorgehen bietet Österreich eine Projektionsfläche und ein Feindbild für den ideologischen Diskurs islamistischer Extremistinnen und Extremisten. Die Existenz und Verfestigung einer autochthonen Szene von in erster Linie jungen Musliminnen und Muslimen mit Migrationshintergrund (in der zweiten und dritten Generation) sowie von Personen, die zum Islam konvertiert sind, sind ein zentrales Merkmal dieser Entwicklungen.

Das Bedrohungsbild des islamistischen Extremismus und Terrorismus weist seit mehreren Jahren feststehende Komponenten auf, welche die Gefährdung der Sicherheit Österreichs direkt oder indirekt beeinflussen: Foreign Terrorist Fighters und die Rückkehr aus Kriegs- und Krisengebieten, Online- und Offline-Radikalisierung und die Nutzung des Internet als Radikalisierungs- und Rekrutierungsinstrument.

Foreign Terrorist Fighters

Unter **„Foreign Terrorist Fighters (FTF)“** werden Personen subsumiert, durch die in ein anderes Land reisen, um dort terroristische Aktivitäten in unterschiedlicher Form, wie z. B. durch Teilnahme an Kampfhandlungen, Ausbildungen/Trainings oder Planungen, zu unterstützen.

Das Phänomen der FTF und das damit verbundene Gefährdungspotenzial haben mit der territorialen Zerschlagung des IS in Syrien und Irak grundsätzlich nicht an Aktualität verloren, jedoch ist es zu einer Verschiebung der Gefahrenmomente gekommen. Gegenwärtig ist die Gefahr von Ausreisen in das syrisch-irakische Kriegs- beziehungsweise Krisengebiet eher gering, dafür richtet sich der Fokus auf die Situation in den Internierungslagern im Nordosten Syriens, die mögliche Rückkehr primär von Frauen und Kindern und das Mobilisierungspotenzial von zurückgekehrten oder an der Ausreise gehinderten FTF. Dass dieses Mobilisierungspotenzial tatsächlich real ist, hat der Terroranschlag in Wien vom 2. November 2020 bewiesen. Der Attentäter wurde im Jahr 2018 an der Ausreise nach Syrien gehindert und führte ein Jahr nach seiner bedingten Haftentlassung den Anschlag in der Wiener Innenstadt aus. Der Umstand, dass nach einer Entlassung aus der Haft die betroffene Person einen terroristischen Anschlag verübt, ist kein Einzelfall, sondern in Europa bereits mehrfach passiert, wie Fälle im Vereinigten Königreich oder in Deutschland zeigen.

Die Flüchtlings- beziehungsweise Internierungslager in den Kurdengebieten, in denen in erster Linie Familienangehörige – hauptsächlich Frauen und Kinder – ehemaliger IS-Kämpfer untergebracht sind, zählen gegenwärtig zum größten Radikalisierungs- und Rekrutierungsraum für einen wiedererstarkenden IS. Die Situation in diesen Lagern ist dabei in mehrfacher Hinsicht problematisch. Die anhaltende Wasserknappheit und die damit verbundenen hygienischen Probleme sowie stockende Hilfslieferungen aufgrund pandemiebedingter Grenzschließungen erschweren die Lebensverhältnisse vor Ort. Diese Situation bildet eine wichtige Grundlage für ein islamistisch gesteuertes Opfernarrativ, um einerseits Vergeltungsschläge zu argumentieren und um andererseits zahlreiche Spendenaufrufe und -aktionen, vor allem im Internet, zu organisieren. Unklar bleibt hierbei, wer die gesammelten Gelder schlussendlich erhält, wodurch die Gefahr der Terrorismusfinanzierung nicht auszuschließen ist. Darüber hinaus stellen diese Lager einen Radikalisierungs- und Rekrutierungshotspot dar, wo möglicherweise eine neue Generation von Kämpferinnen und Kämpfern sowie Unterstützerinnen und Unterstützern eines IS-Kalifats heranwächst. Nach der Rückkehr können erlangte Kampferfahrungen, traumatische Erlebnisse und damit einhergehende gesellschaftsgefährdende Verhaltensänderungen sowie eine mögliche ausgereifte Radikalisierung ein Sicherheitsrisiko für Österreich darstellen. Bezüglich dieser Gefährdungsmomente können in einem ersten Schritt von den Sicherheits- und Strafverfolgungsbehörden Maßnahmen gesetzt werden,

längerfristig stellt die Reintegration dieser Personen jedoch eine gesamtgesellschaftliche Herausforderung dar.

Die Gesellschaften in Europa werden in den kommenden Jahren in Bezug auf das Phänomen der Radikalisierung gefordert sein. Um das komplexe Phänomen der Radikalisierung und Rekrutierung verstehen und ihm begegnen zu können, haben sowohl die Institutionen der Europäischen Union als auch die Mitgliedstaaten selbst umfangreiche Maßnahmen ergriffen.

Radikalisierungsräume

Radikalisierung im islamistischen Bereich ist und bleibt ein fester Bestandteil des Bedrohungsbildes und auch die Räume, wo Radikalisierung stattfindet, haben sich über die vergangenen Jahre nicht geändert: das Internet in Verbindung mit einem unmittelbaren sozialen Umfeld von zumeist Gleichaltrigen sowie Justizanstalten.

Generell ist festzustellen, dass neue technische Standards wie 5G oder bessere Hard- und Softwareverschlüsselungsverfahren, in wesentlich kürzerer Zeit im Umlauf sind als sich die diesbezüglich rechtlichen Rahmenbedingungen für das Ermittlungsverfahren ändern könnten.

Das Internet und hier vor allem soziale Netzwerke tragen nicht nur zur Radikalisierung bei, indem islamistische und jihadistische Inhalte abgerufen werden können, sondern bilden gleichzeitig auch ein Rekrutierungsfeld im Rahmen der ersten Knüpfung von Kontakten, die dann später in der realen Welt vertieft werden können. Das bedeutet, dass Radikalisierung online und offline stattfindet, denn neben dem Austausch über Social Media und virtuellen Freundschaften bleiben gemeinschaftsbildende Aktivitäten im Rahmen von Ausflügen, Lokalbesuchen oder sportlichen Aktivitäten ein wichtiger Faktor.

Propaganda in der digitalen Welt

Im Zusammenhang mit der Verbreitung islamistisch-extremistischer Propaganda war zu beobachten, dass online abrufbare Predigten von zum Teil seit Jahren inhaftierten Predigern immer noch eine große Strahlkraft besitzen und einzelne Inhalte immer wieder in Postings auf sozialen Plattformen rezipiert und in einen aktuellen Kontext gesetzt werden. Gleichzeitig ist eine Schnelllebigkeit extremistischer und jihadistischer Inhalte erkennbar, die zum Teil dem Charakter der jeweils verwendeten sozialen Plattformen, beispielsweise TikTok, geschuldet ist. Die Altersstruktur der Rezipientinnen und Rezipienten dieser Propaganda liegt teilweise im Jugendalter, wobei sowohl Musliminnen und Muslime als auch Konvertitinnen und Konvertiten betroffen sind.

Das Internet spielt bei weiblichen Radikalisierungsverläufen grundsätzlich eine wichtige Rolle, nicht zuletzt deshalb, weil viele der Mädchen beziehungsweise Frauen zum Teil aufgrund der traditionellen Lebensweise nicht so einfach Zugang zu einem Islam- beziehungsweise Koranunterricht in einer Moschee oder dem Freitagsgebet haben. In der Kommunikation im virtuellen Raum werden teilweise die gleichen streng-religiösen und ideologisch forcierten Verhaltensregeln durch Userinnen übernommen wie in der realen Welt, was unter anderem dazu führt, dass ein Chat mit einer männlichen Person nur unter Aufsicht einer weiteren Teilnehmerin beziehungsweise eines weiteren Teilnehmers geführt werden darf.

Grundsätzlich werden die Radikalisierungsphasen durch das Internet immer kürzer, gleichzeitig nimmt aber auch die Tiefe des ideologischen Wissens ab. Das könnte auch daran liegen, dass es sich mitunter um ein jugendkulturelles Konfrontationsverhalten gegenüber der Mehrheitsgesellschaft handelt, dem in Form islamistisch-extremistischer Propaganda Ausdruck verliehen wird. Aber auch aus dieser jugendlichen Protesthaltung heraus können sich extremistische Einstellungen verfestigen und zu einer Akzeptanz oder Anwendung von Gewalt als Mittel zur Zielerreichung führen.

Allgemein kann festgestellt werden, dass der islamistische Extremismus und Terrorismus in der Nutzung moderner Techniken und Medien vorangeschritten und gleichzeitig eine Zunahme des aktionistischen Potenzials und der Gewaltbereitschaft erkennbar ist. Die Verbreitung der Ideologie und die in diesem Zusammenhang aktiv im Internet stattfindende Radikalisierung spiegelt sich auch in einem Großteil jener Ermittlungsverfahren wider, die im Jahr 2021 zu Verurteilungen geführt haben. Hierbei reicht die Bandbreite der Handlungen vom Versenden von IS-Propagandamaterial, über ideologisch motivierte Gewaltdelikte oder Terrorismusfinanzierung, bis hin zu Ausreisen in das syrisch-irakische Krisen- beziehungsweise Kriegsgebiet (die Ausreise lag zum Zeitpunkt der Verhandlung bereits mehrere Jahre zurück) sowie weitreichenden Radikalisierungs- und Rekrutierungsaktivitäten im Internet durch das Erstellen von Kanälen oder Chatforen, die Bereitstellung von radikal-islamistischen Predigten, Übersetzungstätigkeiten etc.

Radikalisierung in Justizanstalten

Justizanstalten spielten bei der Radikalisierung einiger der bedeutendsten Gewalt befürwortenden extremistischen Ideologinnen und Ideologen inner- und außerhalb Europas eine wichtige Rolle. Sie können auf Grund ihrer besonderen Struktur als förderliches Umfeld für Radikalisierung und Rekrutierung gesehen werden. Hierbei spielen eine Reihe von Faktoren zusammen, die zu einer Zunahme der Radikalisierung führen können, wie beispielsweise das harte Umfeld infolge des Freiheitsentzugs, die soziale Marginalisierung, die psychische oder physische Gewalt und der Gruppenzwang.

Justizanstalten sind Krisenumgebungen, die ein Bedürfnis nach Zugehörigkeit, Gruppenidentität, Schutz und – für manche Insassinnen und Insassen – religiöser Führung entstehen lassen.

Mögliche weitere Faktoren, die zum Radikalisierungsprozess in Justizanstalten beitragen, sind die unvermeidbare Nähe zu Extremistinnen und Extremisten, die Unzufriedenheit mit dem Rechtssystem, unerlaubte Korrespondenz mit Extremistinnen und Extremisten, der Zugang der Inhaftierten zu Medien mit radikalen Inhalten etc. All diese Umstände können dazu führen, dass im Rahmen der Verbüßung einer Haftstrafe die extremistische Einstellung beibehalten oder sogar verstärkt wird, was im schlimmsten Fall zu einem Terroranschlag führen kann.

Basierend auf den Erfahrungen aus dem Terroranschlag in Wien und den damit einhergehenden Empfehlungen seitens der Untersuchungskommission wurde nicht nur die Zusammenarbeit mit dem Bundesministerium für Justiz, insbesondere mit der Generaldirektion für den Strafvollzug und freiheitsentziehende Maßnahmen, verstärkt. Darüber hinaus wurden auch im Rahmen des Terror-Bekämpfungs-Gesetzes (TeBG) Rahmenbedingungen geschaffen, die im Falle von bedingten Entlassungen bei einschlägig verurteilten islamistischen Extremistinnen und Extremisten eine bessere Kooperation und einen verstärkten Informationsaustausch zwischen den Sicherheitsbehörden, der Justiz und den in die Aufsicht einer bedingten Entlassung involvierten Einrichtungen ermöglichen.

3.2.3 Fälle 2021

Der Fall eines jungen Mädchens zeigt, wie das Internet und die sozialen Plattformen die Radikalisierung fördern können, um dann in einem zweiten Schritt als Informationsquelle und Mittel zum Zweck für extremistische Aktivitäten zu dienen. Das betroffene Mädchen wächst in stabilen Familienverhältnissen auf. Die Familie ist zwar muslimischen Glaubens, praktiziert diesen aber kaum bis gar nicht. In der Phase des Erwachsenwerdens ist das Mädchen mit krisenhaften Erlebnissen im schulischen und familiären Kontext konfrontiert, die zu einer gewissen Unsicherheit im Umgang mit diesen Erfahrungen führen. Diese Phase der Unsicherheit macht das junge Mädchen für einfache Erklärungsmuster und Lösungsansätze empfänglich und genau das bietet eine islamistische Ideologie wie der Salafismus. Das Mädchen versucht zunächst in einer verstärkten Hinwendung zum Glauben mit ihren Problemen fertig zu werden und nutzt das Internet als Informationsquelle zum Thema Islam. Sie gerät jedoch sehr schnell auf einschlägige Webseiten und Foren, in denen sie Aufmerksamkeit, Unterstützung und Zuwendung erfährt. Die streng religiösen Handlungsanleitungen geben ihr eine Richtlinie vor, an der sie sich in Bezug auf ihr Verhalten und äußeres Erscheinungsbild orientieren kann. Diese Verhaltensveränderung stößt in ihrer Familie auf Unverständnis und zum Teil auch auf Ablehnung bis hin zu

Verboten, was aber wiederum zur Folge hat, dass das Mädchen noch mehr Zeit im Internet und bei ihren virtuellen Freunden verbringt. Ihre Aktivitäten im Internet stoßen aufgrund des traditionellen Rollenverständnisses bald an ihre Grenzen, weshalb sie die virtuelle Identität eines Mannes annimmt, um sich in Chatforen auch zu den Themen des bewaffneten Kampfs und Anschlägen austauschen zu können. Durch ihr Verhalten online und die Inhalte ihrer Postings gerät sie in den Fokus des Verfassungsschutzes. In weiterer Folge wird ein Ermittlungsverfahren wegen Mitgliedschaft in einer terroristischen Vereinigung und kriminellen Organisation eingeleitet. Nachdem sich ihre Beiträge zu Anschlagsplänen zu konkretisieren beginnen und auch eine mögliche Ausreise in das syrisch-irakische Kriegs- und Krisengebiet im Raum steht, erfolgt die Festnahme durch die Verfassungsschutzbehörden. Das Mädchen wird in Untersuchungshaft genommen. Die Auswertung der Inhalte auf den sichergestellten Datenträgern gestaltet sich als sehr arbeits- und ressourcenintensiv, da neben unzähligem Propagandamaterial in Form von Bild-, Audio-, Videodateien und Dokumenten mehr als 100.000 gespeicherte Chats zu finden sind. Zwischenzeitlich erklärt ein durch die Staatsanwaltschaft in Auftrag gegebenes Gutachten die Schuldunfähigkeit des Mädchens aufgrund der Voraussetzungen des § 4 Abs. 2 Z 1 Jugendgerichtsgesetz (JGG), was zur sofortigen Haftentlassung und Verfahrenseinstellung führt.

Die Verfahrenseinstellung wird aus Sicht des jungen Mädchens dahingehend interpretiert, nichts falsch gemacht zu haben, weshalb sie nach kurzer Zeit wieder in einschlägigen Chatforen unterwegs ist. Der Versuch, sie im Rahmen eines Programms zur Ideologiedekonstruktion und Deradikalisierung von ihren islamistisch-extremistischen Überzeugungen zu entfernen, scheitert. Schließlich bringt sie ihr virtuelles und zum Teil auch reales Verhältnis zu einigen Personen, die im Zusammenhang mit dem Terroranschlag vom 2. November 2020 in Wien verhaftet werden, erneut in den Fokus staatspolizeilicher Ermittlungen, im Verlauf derer unter anderem ihr Mobiltelefon sichergestellt und Untersuchungshaft verhängt wird. Die Auswertung der Inhalte ihrer Datenträger zeigen eine ungebrochene Konsumation, aber auch Versendung islamistischer Terrorpropaganda, auch mit direkter Verbindung zum Terroranschlag in Wien, was zu einer Anklage unter anderem nach §§ 278b Abs. 2 (Mitglied einer terroristischen Vereinigung) und 278a (Kriminelle Organisation) StGB führt. Im Herbst 2021 kommt es zu einer Verurteilung von 24 Monaten, davon acht Monate unbedingt, mit einer Probezeit von drei Jahren. Die gerichtlichen Auflagen zur bedingten Entlassung sehen unter anderem die Teilnahme an einem Ausstiegs- und Deradikalisierungsprogramm sowie Bewährungshilfe vor.

Der Straftatbestand der staatsfeindlichen Verbindung (§ 246 StGB) im Zusammenhang mit islamistischen Extremismus und Terrorismus

Der Straftatbestand der staatsfeindlichen Verbindung, der ursprünglich mit dem Aufkommen des Phänomens der Reichsbürgerinnen und Reichsbürger geschaffen wurde, wurde im Jahr 2021 erstmals auch im Rahmen eines Strafverfahrens im Bereich des islamistischen Extremismus und Terrorismus angeklagt und erstinstanzlich verurteilt. Die terroristische Vereinigung Islamischer Staat wird hier auch als staatsfeindliche Verbindung qualifiziert, deren Zweck es ist, durch den Jihad als bewaffneten Kampf und somit auf gesetzwidrige Weise einen nach dem islamischen Recht ausgerichteten islamischen Staat vorerst in Syrien und im Irak, später auch in Europa und somit in Österreich und schließlich weltweit zu errichten. Dieses Vorhaben würde die Republik und ihre Unabhängigkeit sowie die verfassungsmäßigen Einrichtungen ernstlich gefährden (siehe § 246 Abs. 1 StGB). Der Angeklagte soll sich in dieser staatsfeindlichen Verbindung führend betätigt und für sie Mitglieder geworben haben (siehe § 246 Abs. 2 StGB), indem er durch Vorträge und Predigten in einem Verein und einer Moschee sowie durch Bücher, Skripten und Audiodateien das Konzept des Jihad und die Teilnahme an diesem als religiöse Pflicht jedes Muslims dargestellte. Der bewaffnete Kampf gegen die Ungläubigen wiederum dient der Wiedererrichtung eines Kalifats und somit der Beseitigung des demokratischen Rechtsstaates.

3.2.4 Trends und Entwicklungstendenzen

Das größte Gefahrenpotenzial geht in Europa weiterhin von radikalisierten Einzeltäterinnen und Einzeltätern sowie autonom agierenden Kleinstgruppen aus, die Anschläge ohne direkten Auftrag oder Anleitung einer terroristischen Organisation ausführen. Auch der Trend zu niederschwelligen Taten mit einfachen Tatmitteln wie Messern und Fahrzeugen, die wenig bis kaum logistische Vorbereitungen bedürfen, wird mit hoher Wahrscheinlichkeit anhalten. Bevorzugte Ziele islamistischer Terroristen dürften auch weiterhin leicht zugängliche Menschenansammlungen bleiben, wobei erfahrungsgemäß davon auszugehen ist, dass die Zielauswahl eher willkürlich erfolgt und vorrangig auf die Zivilbevölkerung fokussiert. Der islamistisch-motivierte Anschlag auf den Politiker David Amess am 15. Oktober 2021 in Essex, Großbritannien, hat jedoch gezeigt, dass auch Personen des öffentlichen Interesses gezielt Opfer terroristischer Anschläge werden können. Es ist evident, dass insbesondere der IS vermehrt zu Anschlägen in europäischen Ländern aufruft.

Afghanistan

In Afghanistan erfolgte in den Sommermonaten des Jahres 2021 eine Machtübernahme durch die Taliban. Islamistinnen und Islamisten deuteten den militärischen Sieg weltweit zur „Niederlage des Westens und seiner Werte“ um. Dies führte auch in den sozialen Netzwerken österreichischer Sympathisantinnen und Sympathisanten zu einer spürbaren Euphorie. Die Wahrscheinlichkeit, dass Afghanistan zukünftig zum bevorzugten Zielland für europäische Jihadistinnen und Jihadisten wird, ist kurz- und mittelfristig jedoch als gering anzunehmen. Dies liegt zum einen daran, dass die Taliban derzeit keine transnationale islamistisch-terroristische Agenda verfolgen, zum anderen aber auch an den kaum vorhandenen ethnischen und sprachlichen Anknüpfungspunkten. Eine Beteiligung von europäischen Jihadistinnen und Jihadisten am Kampf des IS gegen die Taliban erscheint ideologisch denkbar, bleibt aber aufgrund infrastruktureller Gründe ebenso wenig wahrscheinlich. Überdies scheint der Kampf zwischen zwei islamistischen Akteuren in Europa wenig Anklang zu finden.

Foreign Terrorist Fighters

Österreich gehört im Vergleich zu anderen europäischen Staaten zu jenen Ländern mit einer, an der Einwohnerzahl gemessen, überproportional hohen Anzahl an „Jihad-Reisenden“ (Foreign Terrorist Fighters, FTF) sowie an unterbundenen Ausreisen. Die Gruppe der aus Kriegs- und Krisengebieten – zu nennen sind vor allem Syrien und Irak – nach Österreich zurückgekehrten FTF ist bislang vergleichsweise klein geblieben. Ungeachtet dessen bleibt die generelle Einschätzung aufrecht, dass von kampferprobten, nach Europa zurückkehrenden Jihadistinnen und Jihadisten eine potenzielle Bedrohung ausgeht. Es muss mit einer anhaltenden Bereitschaft zu Anschlägen und Anwendung von Gewalt gerechnet werden. Dies ist insbesondere dann der Fall, wenn FTF bereits an Kampfhandlungen teilgenommen haben und eine gesenkte Hemmschwelle in Bezug auf die Anwendung von Gewalt vorliegt. Überdies genießen Rückkehrende hohes Ansehen in der islamistischen Szene, was wiederum ihre Möglichkeiten vergrößert, Personen zu rekrutieren und zu radikalisieren. Außerdem stellen vormals an der Ausreise gehinderte Personen aufgrund mangelnder „Bedeutsamkeit“ eine nicht zu vernachlässigende Gefahr dar.

Wanderprediger aus dem Westbalkan

Im Westbalkan-Raum hat sich ein salafistisches Milieu etabliert, das einerseits versucht gesellschaftliche Bruchlinien in der Region zu verstärken, andererseits aber auch eine Ausstrahlungswirkung auf die Westbalkan-Diaspora in Österreich im Sinne eines identitätsstiftenden Bezugspunktes hat. Die salafistische Westbalkan-Szene in Österreich ist weiterhin aktiv. Dabei bewegen sich sogenannte „Wanderprediger“, die oft aus Ländern des Westbalkan kommen, überregional innerhalb des Bundesgebiets und bekommen

vertiefte Einblicke in die Besucherschaft unterschiedlicher salafistischer Moscheen. Es ist damit zu rechnen, dass diese „Wanderprediger“ neben Aufgaben der inneren Mission auch verstärkte Vernetzungen der salafistischen Szene anstreben werden. In Österreich spielen darüber hinaus lokale Moscheevorstände und Predigerpersönlichkeiten mit Westbalkan-Hintergrund eine zentrale Rolle bei der Radikalisierung. Sie verfügen meist über ausreichende Sprachkenntnisse, um diejenigen zu erreichen, deren Muttersprache Deutsch ist, oder die in Österreich aufgewachsen sind und hauptsächlich in deutscher Sprache kommunizieren.

Salafismus

Im Bereich der salafistischen Propaganda sind Anwerbungspraktiken der sogenannten „Street-Dawa“, wie etwa öffentliche Auftritte und Koranverteilungsaktionen („Lies!“), in Österreich in den Hintergrund getreten. Gründe dürften unter anderem in der Corona-Pandemie und deren Begleitmaßnahmen und Folgeerscheinungen zu finden sein. Diese haben auch die islamistische Szene in Österreich beeinflusst und zu einer Verlagerung der Aktivitäten von der „Straße“ in den Online-Bereich geführt. Dennoch muss mit anhaltenden Radikalisierungsprozessen gerechnet werden, denn mit einer Zunahme von „Online-Zeit“ haben sich Menschen in einem größeren Umfang als in der Zeit vor der Corona-Pandemie den radikalisierenden Inhalten einschlägiger sozialer Medien widmen können, was zu einer zusätzlichen Verfestigung islamistischer Narrative geführt haben könnte.

Islamismus im Zusammenhang mit der Corona-Pandemie

Grundsätzlich hat die Corona-Pandemie noch zu keiner Verschärfung der terroristischen Bedrohungslage in Österreich geführt. Einschlägige Medien interpretierten das Coronavirus als „Gottesstrafe“ und wirksame biologische Waffe gegen westliche Gesellschaften in dem Sinne, dass keine zusätzlichen Tathandlungen von menschlicher Seite nötig wären. Außerdem haben die in Österreich ergriffenen Maßnahmen zur Eindämmung der Pandemie über einen längeren Zeitraum hinweg zu einer Einschränkung von Großveranstaltungen geführt, wodurch potenzielle Angriffsziele ausfielen. Festzuhalten ist jedoch, dass es bei Einzelpersonen durch länger andauernde Isolationserfahrungen zu einer damit einhergehenden erhöhten Anfälligkeit für eine extremistische Radikalisierung gekommen sein könnte. Zudem könnten eine durch die Pandemiebekämpfung bedingte strenge staatliche Haushaltspolitik in Österreich und die damit verbundenen wirtschaftlichen Härten für sozioökonomisch schwächere Teile der Gesellschaft einen längerfristigen Radikalisierungsschub im islamistischen Milieu auslösen. Hinzu kommen Herausforderungen im Zusammenhang mit Migration, die Überforderung und fremdenfeindliche Ressentiments auslösen könnten und einen allgemeinen Vertrauensverlust in staatliche Institutionen zur Folge hätten. Damit bleibt der gesellschaftliche Zusammenhalt in Österreich auf die Probe gestellt.

3.3 Spionageabwehr und Cybersicherheit

3.3.1 Spionageabwehr

3.3.1.1 Überblick

Unter Spionage wird das geheime Beschaffen sowie Erlangen noch unbekannter Informationen oder geschützten Wissens verstanden. Der Begriff der Spionage wird ergänzend für Handlungen durch Staaten oder Dritte verwendet, die nachteilige Handlungen setzen. Die erlangten Informationen werden folglich im eigenen wirtschaftlichen, politischen oder militärischen Machtbereich verwendet, um einen Vorteil beziehungsweise Vorsprung zum Gegenüber zu generieren.

Nach dem Strafgesetzbuch bestehen für den Verfassungsschutz im Bereich der Spionageabwehr folgende primäre Deliktszuständigkeiten:

- § 124 StGB (Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses zugunsten des Auslands)
- § 242 StGB (Hochverrat)
- §§ 252 bis 257 StGB (Delikte betreffend Landesverrat)
- § 316 StGB (Hochverräterische Angriffe gegen einen fremden Staat)
- § 319 StGB (Militärischer Nachrichtendienst für einen fremden Staat)
- § 320 StGB (Verbotene Unterstützung von Parteien bewaffneter Konflikte)

Staatliche Nachrichtendienste zeichnen sich dadurch aus, dass ihre Erkenntnisse nur einem eingeschränkten Personenkreis zugänglich sind. Im Laufe der Jahrhunderte haben sich die Aufgaben, die Strukturen und die Rahmenbedingungen, beispielsweise die gesetzlichen Bestimmungen oder politischen Systeme, nachrichtendienstlicher Aktivitäten und Ziele geändert.

Generell sind die Erkenntnisse der staatlichen Nachrichtendienste ein Beitrag zur Entscheidungsfindung der obersten politischen und militärischen Führung. Nachrichtendienste entstanden primär aus militärischen Notwendigkeiten, ihr Erfassungsspektrum bezog aber auch andere, vor allem sicherheitspolitische Faktoren, wie die wirtschaftliche Lage und die Innen- und Außenpolitik, mit ein.

Organisationsstruktur, Aufgaben und Befugnisse von Nachrichtendiensten sind weltweit sehr unterschiedlich. So können beispielsweise inlands- und auslandsnachrichtendienstliche Tätigkeiten, aber auch zivile und militärische Informationsgewinnung, getrennt organisiert sein oder aber einheitlich durch eine Nachrichtendienstorganisation wahrgenommen werden.

Zur Erfüllung ihrer nachrichtendienstlichen Aufgaben kommen bei den unterschiedlichen Nachrichtendiensten häufig ähnliche Methoden zum Einsatz, beispielsweise HUMINT, SIGINT, IMINT oder OSINT.

HUMINT: Als Human Intelligence wird die klassische Spionage bezeichnet, welche sich der Gewinnung von Erkenntnissen durch menschliche Quellen bedient.

SIGINT: Signal Intelligence sind Informationen, die durch die Erfassung und Analyse der elektronischen Signale und Kommunikation eines bestimmten Ziels gewonnen werden.

IMINT: Unter Imagery Intelligence versteht man das Sammeln von Informationen über Satelliten- und Luftaufnahmen.

OSINT: Open Source Intelligence beschreibt die Informationsgewinnung aus frei verfügbaren offenen Quellen (zum Beispiel Sozial- und Berufsnetzwerke, Nachrichten, Webseiten).

3.3.1.2 Aktuelle Lage

Die Neuorganisation des österreichischen Verfassungsschutzes wurde mit in Kraft treten des Staatschutz- und Nachrichtendienstgesetzes (SNG) am 1. Dezember 2021 umgesetzt. Darüber hinaus wurden mit diesem Datum das Sicherheitspolizeigesetz, das Strafgesetzbuch, die Strafprozessordnung 1975 und das Tilgungsgesetz 1972 geändert. Diese Gesetzesänderungen führten auch in der Spionageabwehr zu weitreichenden Änderungen und Neuerungen. Von besonderer Bedeutung für die Arbeit des Verfassungsschutzes im Bereich der Spionageabwehr ist die Novellierung des § 256 StGB (Geheimer Nachrichtendienst zum Nachteil Österreichs). Die Strafdrohung wurde von bis zu drei auf bis zu fünf Jahren Freiheitsstrafe angehoben. Strafbare Handlungen gemäß § 256 StGB sind somit seit 1. Dezember 2021 Verbrechen im Sinne des § 17 StGB. Ein Nachrichtendienst ist eine zumeist staatliche Organisation, die zur Gewinnung von Erkenntnissen über politische, sicherheitsbezogene oder ökonomische Lagen offen und verdeckt Informationen sammelt, die gewonnenen Erkenntnisse auswertet und an politische Verantwortungsträger als Informations- beziehungsweise Entscheidungsgrundlage weiterleitet. Dem nachrichtendienstlichen Bereich der DSN obliegt bei Vorliegen bestimmter Voraussetzungen die Aufgabe der Beobachtung von Gruppierungen. Wesentlichste Voraussetzung dafür ist, dass damit zu rechnen ist, dass es zu mit „schwerer Gefahr“ für die öffentliche Sicherheit verbundener Kriminalität kommt. Diese in § 6 Abs. 1 SNG genannte „schwere Gefahr“ kann nach herrschender Meinung erst angenommen werden, wenn mit der Begehung von Verbrechen (also Handlungen, die mit mehr als dreijähriger Freiheitsstrafe bedroht sind) zu rechnen ist. Somit kann seit der Gesetzesnovelle für die Begründung der Voraussetzungen des § 6 Abs. 1 SNG auch der Tatbestand des geheimen Nachrichtendienstes zum Nachteil Österreichs herangezogen werden.

Aktuell stark wahrnehmbar ist die ansteigende Nutzung hybrider Methoden zum Zweck der strategischen Einflussnahme. Darunter kann ein methodischer, mitunter nichtlinearer Einsatz von unterschiedlichen Fähigkeiten, über das gesamte „DIMEFIL-Spektrum“ (DIMEFIL steht für Diplomatic/Political, Information, Military, Economic, Financial, Intelligence, Legal) erstreckend, verstanden werden. Dies geschieht stets mit der Zielsetzung, das Gegenüber in seiner Handlungs- und Reaktionsfähigkeit zu beeinträchtigen und so eine Schwächung oder Destabilisierung herbeizuführen. Darunter können mitunter Desinformationskampagnen, Cyberangriffe oder die Nutzung organisierter Kriminalität mit dem Ziel der Förderung von Unsicherheiten subsumiert werden. Das hybride Kontinuum weist dabei stets innen- und außenpolitische Bezüge auf und kann von der Einflussnahme bis hin zum bewaffneten Angriff reichen.

Nach wie vor nutzen ausländische Staaten den neutralen Boden Österreichs als ein präferiertes Tätigkeitsgebiet für nachrichtendienstliche Aktivitäten. Bei der Auswahl des Operationsgebietes spielen eine Vielzahl an begünstigenden Faktoren, die Österreich als Standort mitbringt, eine wesentliche Rolle: Zu nennen sind dabei die gute geopolitische

Lage, die Niederlassung einer Reihe von internationalen Organisationen bis hin zur wirtschaftlichen Stärke des Landes. Von Relevanz ist auch die im Überblick angeführte Gesetzeslage, die mitunter für ausländische Dienste ein Operieren auf österreichischem Staatsgebiet aufgrund der vergleichsweise sehr niedrigen Strafdrohung attraktiv macht. Überdies können die österreichischen Nachrichtendienste im Vergleich zu anderen europäischen Diensten in der Aufklärung nur auf minimal-invasive Befugnisse zurückgreifen, mit denen die Operationen fremder Nachrichtendienste im Bundesgebiet nur schwer bis kaum nachzuweisen sind.

Österreich ist nicht nur logistischer Knotenpunkt und Einsatzraum für fremde Dienste, sondern auch selbst Ziel nachrichtendienstlicher Beeinflussung und Ausspähung. Vorrangig bieten hierzulande sogenannte Legalresidenturen, die im gesamten Bundesgebiet verteilt sind, den Deckmantel für die Spionagetätigkeit ausländischer Nachrichtendienste. Unter dem Begriff der Legalresidentur wird der Stützpunkt eines fremden Nachrichtendienstes verstanden, der im Gastland in einer offiziellen Vertretung, z. B. in Botschaften, Konsulaten, internationalen Organisationen oder in einer halboffiziellen Niederlassung, beispielsweise in Vereine, Kulturzentren, Presseagenturen, Fluggesellschaften oder sonstigen Unternehmensstandorten seines Landes getarnt ist. Gezielt wird von den an den Auslandsvertretungen tätigen Nachrichtendienstoffizieren unter dem Schutz der diplomatischen Tarnung der Status als Diplomat ausgenutzt und so auch eine etwaige strafrechtliche Verfolgung verhindert. Dem Ruf Österreichs als nachrichtendienstliche Drehscheibe gerecht werdend, erstreckt sich der Verantwortungsbereich von in Österreich stationierten Nachrichtendienstoffizieren neben dem Bundesgebiet auch auf andere Länder der Europäischen Union. Die jeweilige Regierung der fremden Macht strebt dabei nach einer Kontrolle von Botschaftsangehörigen sowie im Ausland lebender Staatsbürgerinnen und Staatsbürger. Selbst kleinere autoritäre Staaten mit potenten Nachrichtendiensten nehmen partiell Einfluss auf ihre Staatsbürgerinnen und Staatsbürger im Ausland (Diaspora) und bedienen sich dabei Mitteln, die mit der Rechtsordnung des Gastlandes oft nicht vereinbar sind.

Unter **„Diaspora“** versteht man einen Typ ethnischer und/oder religiöser Minderheiten. Dies sind primär Bevölkerungsgruppen mit über Generationen aufrechterhaltenen Herkunftslandbezügen, deren Selbstverständnis mitunter von traumatischen Erlebnissen geprägt ist. Die grenzüberschreitende Loyalität, Beziehung oder Orientierung sind Wesensmerkmal der Diasporagruppen und unterscheiden diese von anderen Typen ethnischer und/oder religiöser Minderheiten.

In jüngerer Vergangenheit gerieten vor allem auch die aus autoritären Herkunftsländern stammenden Diasporagemeinden Österreichs immer mehr in den Fokus nachrichtendienstlicher Organisationen. Die Kontrolle über die im Ausland lebende

Diaspora stellt ein wesentliches Instrument für die Stärkung der Autorität der jeweiligen Regierungen dar. In Österreich lebende Diasporaangehörige sind ein beliebtes Ziel, da sie den ausländischen Nachrichtendiensten Zugang zu Informationen über Oppositionsbewegungen bieten können, die in weiterer Folge dem Regimeerhalt im jeweiligen Land dienen. Beziehungen ins Herkunftsland bieten daher willkommene Angriffspunkte, die diese Personen in den Fokus von Nachrichtendiensten rücken lassen.

Vom österreichischen Verfassungsschutz wurde in den letzten Jahren vermehrt die Rekrutierung von derartigen „Spitzeln" festgestellt. In Österreich lebende Drittstaatsangehörige werden dabei im Zuge der Wiederausreise nach einem Heimatbesuch von Nachrichtendienstangehörigen, meist unter Androhung von Repressalien, aber auch durch Anbieten von finanziellen Anreizen zur Zusammenarbeit gezwungen beziehungsweise ermutigt. Die Personen werden am Flughafen vor der Ausreise aus fadenscheinigen Gründen festgenommen und einer intensiven Befragung unterzogen. Für die Zusammenarbeit werden den festgenommenen Personen einerseits soziale oder finanzielle Belohnungen in Aussicht gestellt, andererseits werden im Falle der Verweigerung der Zusammenarbeit Repressalien für die Personen selbst oder die im jeweiligen Herkunftsland lebenden Familienangehörigen angedroht.

Auch der Verbreitung von Desinformation im virtuellen Raum und diversen Medien kommt immer größere Bedeutung zu. Solche Unternehmungen verfolgen den Zweck, die westliche Gesellschaft zu schwächen und zu destabilisieren. Durch die bewusste Einflussnahme auf die öffentliche Meinung eines Landes soll die Stimmungslage in eine für sie nützliche Richtung gelenkt werden.

Die Attraktivität Österreichs als Wirtschaftsstandort wird geprägt von seinen fortschrittlichen Unternehmen, herausragenden Hochschulen und Forschungseinrichtungen und Unternehmen, die sich in Nischenmärkten eine entsprechende Reputation aufgebaut haben und in geographischer Zuordnung Marktführer sind. Aufgrund dessen sind die genannten Bereiche einer erhöhten Gefährdung hinsichtlich der (illegalen) Informationsgewinnung durch ausländische Staaten ausgesetzt. Auf der einen Seite wird Spionage durch gezielte Cyberangriffe oder durch das Anwerben von Mitarbeiterinnen und Mitarbeitern der betroffenen Einrichtungen erzielt. Auf der anderen Seite werden Informationen auch durch legale Methoden (Competitive Intelligence) abgegriffen. Um die Rahmenbedingungen für den Wirtschaftsstandort Österreich auch weiterhin attraktiv zu halten und um im Kampf gegen Wirtschafts- und Industriespionage schritthalten zu können, werden für Unternehmen individuelle Sicherheitskonzepte erarbeitet und laufend an die Rahmenbedingungen angepasst. Dies geschieht durch eine enge Kooperation mit Wirtschaft, Wirtschaftsverbänden und Hochschulen.

Competitive Intelligence wird auch als Konkurrenz- beziehungsweise Wettbewerbsbeobachtung bezeichnet. Darunter versteht man die kontinuierliche Beobachtung des wirtschaftlichen Umfeldes sowie die Erkundung des Marktes und das systematische Sammeln und Auswerten der gewonnenen Erkenntnisse über Konkurrenten, Kunden und andere Marktfaktoren.

Nachfolgend finden sich die Hauptakteure der gegen Österreich gerichteten Spionage und Einflussnahme. Die Schwerpunkte in der Zielsetzung aller Nachrichtendienste werden sowohl von innen- und außen-, als auch wirtschaftspolitischen Zielen der jeweiligen Länder bestimmt.

Russische Föderation

Seit geraumer Zeit agieren russische Nachrichtendienste in Österreich mit unverändert hoher Intensität. Zu den Nachrichtendiensten der Russischen Föderation gehören der zivile Auslandsnachrichtendienst SVR, der militärische Auslandsnachrichtendienst GRU sowie der Inlandsnachrichtendienst FSB. Je nach Kompetenz erstrecken sich die Aktivitäten auf unterschiedliche Zielbereiche. So gehören zu den Aufgaben des SVR mitunter das Ausspähen der Arbeitsmethoden und der Zielsetzungen heimsicher Nachrichtendienste und Sicherheitsbehörden. Dabei bedienen sich der SVR sowie auch die anderen Nachrichtendienste sowohl der offenen Informationsgewinnung (Internetquellen, Presse etc.) als auch der konspirativen Informationsbeschaffung, insbesondere durch nachrichtendienstliche Anwerbung von Mitarbeiterinnen und Mitarbeitern in Einrichtungen, die für die Russische Föderation von besonderem Interesse sind.

Volksrepublik China

Speziell der Großraum Wien ist für Nachrichtendienste der Volksrepublik China bevorzugtes Operationsgebiet. Zu den für Österreich relevanten chinesischen Nachrichtendiensten zählen das Ministeriums für Staatssicherheit (MSS) als ziviler Inlands- und Auslandsnachrichtendienst sowie das Ministerium für öffentliche Sicherheit (MPS), da es über nachrichtendienstliche Einheiten verfügt. Ebenso agiert in Österreich der militärische In- und Auslandsnachrichtendienst (MID). Dieser hat die Aufgabe, Informationen über militärische Kapazitäten von ausländischen Militärkräften sowie wissenschaftliche und technologische Informationen mit militärischem Bezug zu sammeln.

Islamische Republik Iran

Im Laufe der Jahre hat sich auch das Netzwerk der iranischen Nachrichtendienste in Österreich verbreitet. Für die zivile Inlands- wie auch Auslandsaufklärung ist das Ministerium für Nachrichtenwesen (MOIS) zuständig. Der militärische In- und Auslandsnachrichtendienst geht aus der Iranischen Revolutionsgarde hervor und wird als IRGC-IO (Islamic Revolutionary Guard Corps Intelligence Organization) bezeichnet. Eine nicht unwesentliche Rolle spielt auch die militärische Spezialeinheit Quds-Force, die neben extraterritorialen Militäroperationen auch auf nachrichtendienstliche Informationsgewinnung spezialisiert ist.

Republik Türkei

Österreich ist für türkische Nachrichtendienste aufgrund der Vielzahl an türkischen Institutionen und der großen türkischstämmigen Gemeinde von besonderem Interesse. Als zentraler Akteur fungiert dabei der türkische Nachrichtendienst MIT, der unmittelbar dem türkischen Staatspräsidenten untersteht. Das Hauptaugenmerk der türkischen Nachrichtendienste liegt insbesondere auf Regimekritikerinnen und Regimekritikern und Gegnerinnen und Gegnern sowie auf der Aufklärung der Gülen Bewegung und der PKK, da diese von der türkischen Regierung als extremistische beziehungsweise terroristische Vereinigung eingestuft werden.

3.3.1.3 Fälle 2021

In einem durch den Verfassungsschutz im Jahr 2021 abgeschlossenen Fall hatte eine aus dem Ausland stammende Österreicherin annähernd zwei Jahre lang zum Nachteil der Republik Österreich für einen ausländischen Nachrichtendienst aus Angst sowie gegen finanzielle Entlohnung spioniert. Die Person wurde im Jahr 2018 bei der Wiederausreise aus ihrem Herkunftsland am dortigen Flughafen festgenommen und inhaftiert. Vorgeworfen wurde ihr im Zuge dessen die Mitgliedschaft in einer terroristischen Organisation. Diese Anschuldigung war ein Argument, welches jeder Grundlage entbehrte. Der Vorwurf resultierte aus einer führenden Tätigkeit in einem in Österreich etablierten Verein einer Oppositionsbewegung. Während der Inhaftierung wurde von Angehörigen des ausländischen Nachrichtendienstes erheblicher Druck auf die Festgenommene ausgeübt. Im Falle einer Kooperation mit dem ausländischen Geheimdienst stellte man ihr im Gegenzug eine Haftentlassung und eine damit verbundene Rückkehr nach Österreich in Aussicht, während im Falle einer Nicht-Kooperation eine entsprechende Haftstrafe in ihrem Heimatland angedroht wurde. Die monetäre Abgeltung der Dienstleistung für die zur damaligen Zeit in finanziellen Schwierigkeiten befindliche Person wurde

im gegebenen Fall ebenfalls zugesichert. Letztendlich entschloss sich die Person zu einer Zusammenarbeit mit dem ausländischen Nachrichtendienst und gab dessen Mitarbeiterinnen und Mitarbeitern Personendaten von vermeintlich oppositionellen Personen in Österreich preis. Nach ihrer Haftentlassung und der Rückkehr nach Österreich kooperierte sie gegen Bezahlung und aus Angst vor Repressalien mit dem ausländischen Geheimdienst. Die Spionagetätigkeit erstreckte sich auf das Sammeln und Übermitteln von sensiblen Informationen über in Österreich lebende „Oppositionelle". Im Zuge des Verfahrens wurde nachgewiesen, dass sensible Informationen über zumindest 100 in Österreich lebende Personen an diesen Nachrichtendienst im Ausland weitergeleitet wurden.

Der ausländische Nachrichtendienst erteilte dabei konkrete Informationsbeschaffungsaufträge. So ordnete er beispielsweise die Strukturerhebung von Kulturvereinen und die Ermittlung und Übermittlung von Daten neuer Funktionäre und Funktionärinnen beziehungsweise Vorstandsmitgliedern an. Auf Grundlage derartiger „Denunzierungen" erfolgten bei Reisen in dieses Land in der jüngeren Vergangenheit weitere Inhaftierungen durch den dortigen Nachrichtendienst. Aus Angst, aber auch zur Erhaltung der finanziellen Zuwendungen, meldete die Person diese Tätigkeit des ausländischen Nachrichtendienstes der österreichischen Polizei nicht.

Die Verbindung zum ausländischen Nachrichtendienst erfolgt häufig über in Österreich lebende, vermittelnde Personen. Wie in der obigen Beschreibung erwähnt, werden für diese Tätigkeiten Nachrichtendienstmitarbeiterinnen und -mitarbeiter an sogenannten Legalresidenturen beschäftigt, an denen diese oftmals unter dem Deckmantel der diplomatischen Immunität die Spionagetätigkeit verüben. Zudem werden strafbare Handlungen meist im Herkunftsland gesetzt. Die Strafverfolgung gestaltet sich in derartigen Fällen aus mangelndem Mitwirkungsinteresse der betroffenen Länder schwierig.

Umso wichtiger erscheint in diesem Kontext die koordinierte Zusammenarbeit der Straf- und Sicherheitsbehörden, um dem Phänomen wirkungsvoll entgegenzutreten. Diese Zusammenarbeit erstreckt sich hierbei auch auf den Erfahrungsaustausch mit internationalen Justiz- und Polizeibehörden. Durch intensive nationale Aufklärungsarbeit im Rahmen von Sicherheitsdialogen mit örtlichen Vereinen wird zudem vom Verfassungsschutz ein wichtiger Beitrag zur Aufklärungsarbeit beziehungsweise Prävention geleistet. Der Schutz der Bürgerinnen und Bürger Österreichs vor der Einflussnahme ausländischer Nachrichtendienste und deren Repressalien ist ein wesentlicher Beitrag zur Erhaltung der demokratisch gesicherten persönlichen Grund- und Freiheitsrechte.

3.3.1.4 Trends und Entwicklungstendenzen

Die Republik Österreich wird aufgrund ihrer geografischen Lage und ihrer Bedeutung als Wirtschafts- und Forschungsstandort auch weiterhin ein bevorzugtes Operationsgebiet

für ausländische Nachrichtendienste bleiben. Als größte Bedrohungen im Rahmen nachrichtendienstlicher Aktivitäten stellen sich einerseits Anwerbungsversuche geeigneter und qualifizierter Informationsbeschaffungsquellen und andererseits Versuche der Einflussnahme zur Manipulation der westlichen Gesellschaften sowie der Schwächung und Destabilisierung der politischen Situation des Ziellandes dar.

Anwerbungsversuche zielen primär auf Akteurinnen und Akteure im Hightech-Bereich, auf diplomatische und akademische Kreise, Think Tanks, wirtschaftliche Akteurinnen und Akteure, Personen mit Beratungsfunktionen für Regierungsbehörden, politische Funktionärinnen und Funktionäre, hochrangige Beamtinnen und Beamte, Staatsangestellte, Führungskräfte staatlicher Strategieunternehmen oder junge europäische Diplomatinnen und Diplomaten im Ausland ab. Angepasst an das technologische Zeitalter erfolgt im Vorfeld der direkten Anwerbungsversuche oftmals eine Vorselektion geeigneter Quellen mit Hilfe sozialer Medien wie etwa LinkedIn.

Versuche der Einflussnahme durch ausländische Nachrichtendienste dienen dem Zweck der Destabilisierung eines Staates, der Schaffung von Unruhe und Ungewissheit sowie der gesellschaftlichen Polarisierung durch Einflussnahme auf die öffentliche Meinung, um die Stimmungslage eines Landes in eine für sie nützliche Richtung zu lenken. Dieses Vorgehen kann eine Beeinträchtigung des Vertrauens in demokratische Prozesse sowie eine allgemeine Gefährdung der liberalen demokratischen Ordnung sowie der öffentlichen Ruhe, Ordnung und Sicherheit nach sich ziehen. Methoden der versuchten Einflussnahme können dabei von Desinformationskampagnen in Form von „Fake News“ oder „Online Trolling“, der Veröffentlichung gehackter geheimer Dokumente und Emails („doxing“) durch WikiLeaks und DCLeaks.com über Cyber-Angriffe bis hin zu Cyber-Spionagemethoden reichen.

> **Fake News** sind Falsch- und Fehlinformationen, die häufig über soziale Medien verbreitet werden. **Online Trolling** ist das absichtliche Beleidigen, Diffamieren oder Belästigen von Personen auf sozialen Medien beziehungsweise im digitalen Raum. **Doxing** ist das Suchen und Veröffentlichen von (privater) Information über eine Person, zumeist mit böswilliger Absicht.

Das von Desinformationskampagnen ausgehende Gefahrenpotenzial für die Öffentlichkeit und demokratische Systeme ist vielfältig. Das Resultat ist die Generierung von Konfliktinszenierungen, Irritationen, Ängsten, populistischen Zuspitzungen, Chaos und Desinformiertheit, die sich wiederum negativ auf die Gesellschaft beziehungsweise auf subjektive Wahrnehmungen auswirken. „Fake News“ in Form einer politischen Agenda können Akteurinnen und Akteuren dazu dienen, Wahrnehmungen und

Handlungen nationaler sowie internationaler Empfängerkreise in die gewünschte Richtung zu lenken und entsprechend zu formen. Ein weiteres Problem ist die weltweite Verbreitungsmöglichkeit von „Fake News“. Alleine in sozialen Medien wie Twitter oder TikTok verbreitete Falschinformationen können zu Protesten führen, die gravierende politische Auseinandersetzungen und Unruhen nach sich ziehen können. Es kann davon ausgegangen werden, dass staatliche Akteurinnen und Akteure auch in Zukunft in Destabilisierungskampagnen, versuchten Einflussnahmen auf die inneren Angelegenheiten anderer Länder sowie Spionagehandlungen involviert sein werden. In diesem Zusammenhang ist das Thema „Hybride Bedrohungen“ relevant.

Um Beziehungen aufzubauen, die in weiterer Folge der Sammlung vertraulicher Informationen dienen, wird auf altbewährte Methoden im HUMINT-Bereich wie Rekrutierung, Cyber-Operationen, Desinformationskampagnen oder wirtschaftliche Einflussnahme zurückgegriffen. Zudem wird auch die sogenannte „Oppositionellen-Beobachtung“ innerhalb diverser Diasporas im Land eine anhaltend wichtige Rolle im Kontext der Informationsbeschaffung und versuchter Einflussnahme spielen. Hierbei wird versucht Personen auszuspähen, die beispielsweise als regierungskritisch gegenüber ihrem Heimatland wahrgenommen werden, oder es werden umfassende Strukturanalysen der im Ausland ansässigen Diaspora durchgeführt. Auch kann es zum Versuch kommen, direkten Druck auf die Zielpersonen auszuüben, indem sie mit kompromittierenden Informationen über ihr Privatleben oder Drohungen gegen im Heimatland lebende Verwandte oder Freundinnen und Freunde zur Kooperation genötigt werden.

Insbesondere erfolgreiche Unternehmen und Forschungseinrichtungen zählen zu den bevorzugten Zielen von Akteurinnen und Akteuren im Bereich der Wirtschaftsspionage. Es ist aber davon auszugehen, dass ausländische Nachrichtendienste mit hoher Intensität und unter Einsatz aller zur Verfügung stehenden Mittel bestrebt sind, in den Besitz von Know-how, Daten, Plänen, Technologien, Patenten, Kalkulationen etc. derartiger Betriebe und Einrichtungen zu gelangen.

3.3.2 Cybersicherheit

3.3.2.1 Überblick

Der EU-Cybersicherheitsrechtsakt definiert Cybersicherheit als alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzerinnen und Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen.

Im Zeitalter zunehmender Digitalisierung steigt die Anzahl der Cyberangriffe rasant an. Zugleich bedienen sich immer mehr Nachrichtendienste dieser Methoden und entdecken so neue Wege und Möglichkeiten. Dabei erstreckt sich das Spektrum vom klassischen Ausspähen von Daten über gezielte Desinformation bis hin zur Sabotage.

Im Hinblick auf den Verfassungsschutz werden unter dem Begriff „Cyberangriff“ sowohl von außen als auch von innen - durch sogenannte Innentäterinnen oder Innentäter - geführte Angriffe auf ein Computernetzwerk zum Zwecke der Informationsgewinnung, der Sabotage oder sonstiger Einflussnahme subsumiert.

Nach dem Strafgesetzbuch bestehen im Bereich der Cybersicherheit folgende primäre Deliktszuständigkeiten:

- § 118a StGB (Widerrechtlicher Zugriff auf ein Computersystem)
- § 119 StGB (Verletzung des Telekommunikationsgeheimnisses)
- § 119a StGB (Missbräuchliches Abfangen von Daten)
- §§ 126a bis 126c StGB (Datenbeschädigung, Störung der Funktionsfähigkeit eines Computersystems, Missbrauch von Computerprogrammen oder Zugangsdaten)

Eine Zuständigkeit des Verfassungsschutzes im Cyberbereich besteht grundsätzlich dann, wenn sich die strafbaren Handlungen gegen verfassungsmäßige Einrichtungen und ihre Handlungsfähigkeit oder gegen kritische Infrastruktur richten.

3.3.2.2 Aktuelle Lage

Cyberangriffe stellen ein besonderes Gefahrenpotenzial dar, da diese durch die betroffene Stelle oftmals zeitverzögert oder gar nicht bemerkt werden, während die Angreiferin oder der Angreifer Zugriff auf eine Vielzahl von Daten hat. Ein weiterer Grund für die Zunahme von Cyberangriffen ist auch die Anonymität im Internet, welche die Ausforschung der Angreiferinnen und Angreifer erschwert. Einzelne Akteurinnen und Akteure können so durch kostengünstige Mittel, gepaart mit ihren Fähigkeiten, Handlungen mit relativ hohen Erfolgsaussichten setzen. Im Rahmen eines derartigen Angriffs können relevante Folgen für die Sicherheit Österreichs herbeigeführt werden, deren Tragweite im Vorfeld oft nur schwer abschätzbar ist. Die Steigerung der digitalen Widerstandsfähigkeit ist daher eine der obersten Prioritäten und stellt zugleich eine zentrale Herausforderung für Staat, Wirtschaft, Wissenschaft und Gesellschaft dar. Neben der Abwehr von Cyberbedrohungen erfordert aber auch die Aufklärung und Strafverfolgung eine intensive Zusammenarbeit der zuständigen Behörden, sowohl im Inland als auch im internationalen Rahmen, da die Täterinnen und Täter oftmals aus dem Ausland agieren.

Die Telearbeit hat, unter anderem durch die Corona-Krise, in den vergangenen Jahren zunehmend an Bedeutung gewonnen und wird aller Wahrscheinlichkeit nach zukünftig im modernen Arbeitsleben vermehrt zum Einsatz kommen. Damit einhergehend werden zunehmend Remote-Tools genutzt, um Zugriff von außen auf die jeweiligen IT-Systeme zu erhalten. Im Umkehrschluss wird Angreiferinnen und Angreifern dadurch aber auch ein erweiterter Aktionsradius geboten, wodurch es im globalen Kontext zu einem markanten Anstieg der Angriffsflächen für Cyberattacken diverser Ziele gekommen ist.

Kritische Infrastrukturen im Sinne des § 74 Abs. 1 Z 11 StGB sind jene Einrichtungen (Systeme, Anlagen, Prozesse, Netzwerke oder Teile davon),

- die eine wesentliche Bedeutung für das staatliche Gemeinwesen haben und
- durch deren Beeinträchtigung oder Ausfall gravierende Auswirkungen für die öffentliche Sicherheit, die medizinische Versorgung oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung oder das effektive Funktionieren von staatlichen Einrichtungen herbeigeführt würden.

Die im Auftrag von staatlichen Nachrichtendiensten durchgeführten Angriffe dienen vorrangig der Informationsbeschaffung oder der bewussten Störung von Abläufen. In jüngster Vergangenheit wurden aber auch vermehrt Aktivitäten registriert, die der gezielten Verbreitung von Desinformation zur politischen Einflussnahme dienen. Die Auswahl der Angriffsziele orientiert sich dabei insbesondere an den Vorgaben der jeweiligen Staatsspitze. Daher sind neben Politik, Wirtschaft und Forschung sowohl kritische

Infrastrukturen als auch NGOs zunehmend der Gefahr von Cyberangriffen ausgesetzt und rücken folglich vermehrt in den Fokus von sogenannten APT-Gruppierungen. In diesen Fällen trifft die Zuständigkeit den österreichischen Verfassungsschutz.

APT steht für **„Advanced Persistent Threat"** und bezeichnet einen komplexen, zielgerichteten und effektiven Angriff auf IT-Strukturen durch einen gut ausgebildeten und ressourcenstarken Angreifer.

Auch im Jahr 2021 hatten kritische Infrastrukturen und verfassungsmäßige Einrichtungen in Österreich mit einer Vielzahl an Bedrohungen aus dem Cyberraum zu kämpfen. Die dahintersteckenden Akteure verfolgten unterschiedliche Motive und wählten verschiedene Maßnahmen, um in die IT-Systeme ihrer Ziele einzubrechen. Die Angriffe reichten von einfach konzipierten Phishingangriffen zum Diebstahl von Zugangsdaten, über Ransomware, wodurch Daten verschlüsselt werden, um diese nur gegen ein hohes Lösegeld freizugeben, bis zu APT-Gruppierungen, hinter denen in den meisten Fällen staatliche Akteure stecken, die am Informationsdiebstahl mit dem Ziel der klassischen oder Wirtschaftsspionage interessiert sind.

Während Angriffe von APT-Gruppierungen einen eher kleinen Teil der Bedrohungsakteure im Cyberraum abbilden, kommt es in regelmäßigen Abständen zu Angriffen staatlicher Natur, welche die nationale Sicherheit und die österreichische Souveränität beeinflussen bzw. gefährden können.

APT29 ist eine Hackergruppierung, die einem ausländischen Nachrichtendienst zugeschrieben wird. Seit dem Jahr 2008 wurden Ministerien, Forschungseinrichtungen und Think Tanks in Europa und in NATO-Mitgliedsstaaten mehrfach Opfer von APT29.

In Österreich besonders aktiv agierende Cyberakteurinnen und Cyberakteure sind überwiegend der Russischen Föderation und China zuzuordnen, aber auch der Iran bedient sich immer öfter der Cyberspionage. Namentlich hervorzuheben sind in diesem Kontext insbesondere die APT-Akteure APT29 und TURLA. Zu deren Angriffszielen gehören neben internationalen Organisationen Staaten wie Großbritannien, die USA und sonstige NATO-Mitglieder, die Nachbarstaaten Russlands sowie Länder der Europäischen Union.

3.3.2.3 Fälle 2021

Im Frühjahr 2021 begann eine der Gruppierung APT29 zugerechnete Phishingkampagne, die über mehrere Monate hinweg weltweit Ziele im behördlichen Sektor angriff. Die

Angriffe zeichneten sich durch einen wiederholenden Modus Operandi aus, welcher trotz des „lauten“[1]. Vorgehens für die Angreifer lohnenswert schien.

Unter **Phishingangriffen** wird der Versand von manipulierten E-Mails verstanden, die den Empfänger zu einer Handlung verleiten sollen, damit der Versender letztendlich an Informationen bzw. Daten des Nutzers gelangt. Dabei enthält die E-Mail vor allem schädliche Anhänge, schädliche Weblinks oder betrügerische Dateneingabeformulare.

Hierbei bediente sich die Tätergruppe meist kompromittierter E-Mail-Accounts unterschiedlicher nationaler Behörden, um bei der Übermittlung des gefälschten Vorwandes mit größerer Glaubwürdigkeit aufzutreten. In den E-Mails wurden entweder für den Zeitpunkt relevante und täuschend echt aussehende Dokumente, Einladungen für Veranstaltungen oder lediglich für den Parteienverkehr der absendenden Organisation relevante Informationen zur Kenntnisnahme übermittelt. Das gemeinsame Ziel der unterschiedlichen Köder war es, den Benutzer oder die Benutzerin zum Antworten und zum Interagieren mit der vom Angreifer kontrollierten E-Mail-Adresse oder zum Öffnen des Anhangs oder Links zu verleiten.

Diese Phishing E-Mails wurden weltweit innerhalb eines kurzen Zeitfensters an eine Vielzahl an Regierungseinrichtungen und internationale Organisationen übermittelt. Die Zieladressen waren oftmals im Internet auffindbar, wodurch die Vorbereitung des Angriffs für den Täter erleichtert wurde. Trotz des breit gestreuten Vorgehens der Gruppierung und der dadurch bedingten geringen Wahrscheinlichkeit, über längere Zeit unerkannt zu bleiben, wurde versucht, zumindest bei einigen Adressaten durch Unachtsamkeit Zugriff auf die Zielsysteme zu erhalten.

Cobalt Strike ist eine umfangreiche Software zum Aufklären, Angreifen und Fernsteuern von Computersystemen sowie dem verdeckten Exfiltrieren von Daten. Vertrieben als Software zum Testen der Sicherheit des eigenen Netzwerkes sowie der Detektion von Cyberangriffen in sogenannten „Red Team“ Engagements wird Cobalt Strike aber auch vielfach in Zuge von „echtem“ Cybercrime und von APT-Gruppierungen wie APT29 verwendet. Durch mehrere Leaks des Cobalt Strike Quellcodes ist die Software mittlerweile online auch ohne Bezahlung verfügbar.

1 Im Gegensatz zum „leisen“ Vorgehen anderer staatlicher Akteure, die sich durch vorsichtige und gezielte Angriffsmethoden auszeichnen, wählte APT29 ein gegenteiliges Vorgehen und versuchte gleichzeitig, eine große Menge an potentiellen Zielen anzugreifen. Durch dieses „laute“ Vorgehen können solche Angriffe relativ rasch entdeckt und abgewehrt werden.

Bei jeder Kampagne werden unterschiedliche technische Mechanismen verwendet, um ein kleines Programm auszuführen, das dazu dient, als Vorreiter des Einbruchs im IT-System des Ziels die Tür für die eigentliche Schadsoftware „offen zu halten". Diese Applikation lädt von einem Server einen Cobalt Strike Beacon (deutsch: „Signalfeuer") nach, um dem Angreifer direkten Zugriff zum Zielsystem zu geben. Dieser ermöglicht beispielsweise Benutzerpasswörter oder Informationen zum IT-Netzwerk auszulesen und die nächsten Schritte für die Informationsbeschaffung zu tätigen.

Innerhalb der ersten Stunden wird vom Angreifer versucht, die eigenen Rechte zu erhöhen („Priviledge Escalation"), um weitreichendere Befugnisse und Daten auf dem System zu erlangen. Zur weiteren Verfolgung des Informationsdiebstahls werden unterschiedliche Methoden mit Hilfe des Cobalt Strike Frameworks angewendet, um innerhalb des Netzwerks auf weitere IT-Systeme zugreifen zu können („Lateral Movement"), ebenso um an die im Rahmen der Informationsbeschaffung benötigten Daten zu kommen. Diese Daten werden extrahiert („Exfiltration") und stehen sodann für klassische nachrichtendienstliche Analysen bereit.

3.3.2.4 Trends und Entwicklungstendenzen

Eine in den letzten Jahren stark zunehmende Bedrohung stellen Ransomware-Angriffe dar. Das florierende Geschäftsmodell, gekoppelt mit gravierenden Hürden bei der Strafverfolgung von ausgeforschten Straftätern in Ländern, die mit westlichen Strafverfolgungsbehörden nicht kooperieren, deutet auf eine Kontinuität dieser Problematik, wenn nicht sogar eine mögliche Steigerung hin. Aufgrund der Lukrativität wird von einer weiter steigenden Professionalisierung und Aufgabenteilung der Täter ausgegangen, um eine Skalierung der Operationen und der Einnahmen zu ermöglichen. Dies bedeutet konkret, dass Ransomware-Angriffe für Vereine, KMUs, NGOs, Behörden und auch große Konzerne eine Gefahr darstellen. Versprechungen unterschiedlicher Gruppierungen, bestimmte Bereiche wie den Bildungs- und Gesundheitssektor nicht anzugreifen, konnten nicht bestätigt werden.

Sicherheitsmaßnahmen am Perimeter eines Unternehmensnetzwerkes sind nach wie vor relevant, jedoch treten durch den technologischen Fortschritt Felder wie das Management mobiler Endgeräte außerhalb des Perimeters oder auch die Absicherung von Accounts von Cloud Services verstärkt in den Vordergrund. Insbesondere die Kompromittierung solcher Accounts, wie bereits bei diversen Vorfällen beobachtet, stellt eine Herausforderung an die forensische Analyse dar, da Aktionen des Angreifers durch klassische Methoden wie Datenträger- oder Netzwerkforensik beim Endbenutzer typischerweise nur sehr schwer einsehbar und entsprechende Logging-Daten des Cloud Anbieters nur eingeschränkt verfügbar sind. Ein weiterer Angriffspunkt sind Kompromittierungen des Cloud Anbieters selbst sowie dessen eigener Infrastruktur. Trotz vergleichsweise hoher Sicherheitsstandards stellen diese durch die Menge an Daten ein lohnendes Ziel dar.

Nicht außer Acht zu lassen ist ebenso die Gefahr für Systemkomponenten für tägliche Versorgungsprozesse der Zivilgesellschaft. Bei der Automatisierung von Prozessen und Industrieanlagen wird immer mehr auf „Industrial Control Systems“ (ICS)-Geräte zurückgegriffen. Angriffe auf solche Systeme können durch dadurch hervorgerufene Ausfälle oder Manipulationen zu realen Auswirkungen auf Versorgungsleistungen führen. Diese Art von Angriffen wurde in den letzten Jahren weltweit zwar nur vereinzelt festgestellt, die steigende Anzahl dieser Geräte bringt aber eine grundsätzliche Erhöhung des Risikos mit sich.

3.4 Internationaler Waffenhandel und Proliferation

3.4.1 Internationaler Waffenhandel

3.4.1.1 Überblick

Unter dem Begriff des illegalen Waffenhandels wird die Weitergabe von sowie der Handel mit Waffen in ihrer Gesamtheit und ihren Einzelteilen durch Verstoß gegen nationale oder internationale Rechtsvorschriften verstanden.

Kriminelle Aktivitäten im Bereich des illegalen Handels mit Waffen, Kriegsmaterial und Explosivstoffen sind nicht nur kriminalpolizeiliches Bearbeitungsgebiet, sondern auch von Relevanz für den Staatsschutz, da diese bei regionalen und überregionalen Konflikten zum Einsatz kommen und deren illegale Lieferung und Verwendung verhindert werden soll.

3.4.1.2 Aktuelle Lage

Sowohl für den österreichischen Verfassungsschutz als auch auf Ebene der Europäischen Union spielt die Bekämpfung des internationalen illegalen Waffenhandels eine immer wichtigere Rolle, da dieses Kriminalitätsfeld auch im Zusammenhang mit terroristischen Straftaten oder der Organisierten Kriminalität zu sehen ist.

Die Republik Österreich verfügt im internationalen Vergleich über eine liberale Waffengesetzgebung. Kriminelle nützen die unterschiedlichen nationalen Rechtslagen und Rechtslücken aus, wodurch Sicherheitsbehörden bei der Feststellung des Weges von der legalen Produktion zum illegalen Umlauf regelmäßig auf Schwierigkeiten stoßen.

Österreich wird auch im Kontext mit der Erzeugung von Waffen und Kriegsmaterial aufgrund der hier ansässigen Produktionsunternehmen eine besondere Rolle zugeschrieben. Exporte von Waffen und Kriegsmaterial aus österreichischem Bundesgebiet unterliegen zwar strengen Kriterien, jedoch sind wesentliche Waffenteile, das sind komplexe, schwer herzustellende Teile, die unabdingbar für die Funktion einer Schusswaffe sind – wie das Griffstück – frei erhältlich und werden nicht in einschlägigen Registern, also dem Zentralen Waffenregister oder dem Waffenbuch, erfasst. Diese frei erhältlichen Waffenteile weisen zwar aufgrund der EU-Richtlinie EU 2017/853 eine Waffennummer auf, werden jedoch gemäß der österreichischen Gesetzeslage und der dort verankerten Legaldefinition nicht als wesentlicher Waffenteil geführt. In anderen EU-Ländern sind diese Waffenteile strafrechtlich geschützt beziehungsweise werden sogar zum Teil als Kriegsmaterial subsumiert (zum Beispiel das Griffstück und Gehäuse einer Maschinenpistole).

Kriminelle Aktivitäten in Österreich und Europa beziehen sich verstärkt auch auf den Umbau von Schreckschusspistolen zu schussfähigen Waffen.

> **Schreckschusspistolen** sind Waffen, die zum ausschließlichen Abfeuern von Knallpatronen, Gasen oder Flüssigkeiten erzeugt wurden.
>
> **Schussfähigen Waffen** sind Waffen, mit denen feste Körper, also Geschosse, durch einen Lauf in eine bestimmbare Richtung verschossen werden können.

Aufgrund der stabileren Bauart werden derzeit vorwiegend Schreckschusspistolen aus Drittländern, die nicht den strengeren EU-Richtlinien unterliegen, in scharfe beziehungsweise vollfunktionsfähige Schusswaffen umgebaut. Legal importierte Schreckschusswaffen werden durch Täterinnen und Täter oder Tätergruppen umfunktioniert und als illegale Waffen am Schwarzmarkt angeboten beziehungsweise kommen bei kriminellen Aktivitäten zum Einsatz. Insbesondere in Großbritannien ist diese Vorgehensweise aufgrund der höheren Preise für illegale Schusswaffen bereits sehr spezialisiert, zumal sogar scharfe illegal selbstlaborierte Munition für

Schreckschusswaffen Verwendung findet. Keinesfalls darf die Wirkung und Langlebigkeit solcher Live-Firing-Waffen unterschätzt werden.

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.

Im EU-Aktionsplan fordert die Europäische Kommission die Mitgliedstaaten dringend auf, die Einrichtung von personell voll ausgestatteten und geschulten Anlaufstellen für Schusswaffen sicherzustellen, um die Zusammenarbeit auf operativer und strategischer Ebene zu optimieren. Aus diesem Grund wurde das österreichische Projekt National Firearms Focal Point (NFFP) mit Beratung der Europäischen Kommission sowie unter Beteiligung des österreichischen Verbindungsbüros bei Europol, dem Bundeskriminalamt und der DSN und ihren nachgeordneten Behörden initiiert.

3.4.1.3 Fälle 2021

Im Berichtsjahr konnten im Zuge einer Amtshandlung in einer Wiener Wohnung – unter einer Badewannenabdeckung versteckt – 24 Stück manipulierte und dadurch schießfähige Schreckschusswaffen sowie 24 Stück Schalldämpfer sichergestellt werden.

Bei besagten Pistolen handelt es sich grundsätzlich um Schreckschusswaffen der Marke „Zoraki“, die in höchst professioneller Weise zu scharfen Waffen umgebaut und mit dementsprechenden Schalldämpfern ausgestattet wurden. Dieses Vorgehen ist insofern als professionell zu bezeichnen, da für eine derartige Modifizierung jedenfalls waffentechnische Vorkenntnisse sowie der Zugang zu entsprechenden Maschinen erforderlich sind. Der vom Verfassungsschutz ausgeforschte Verdächtige konnte Wochen später an der Grenzübergangstelle Nickelsdorf festgenommen werden. Das sichergestellte Fahrzeug wurde geröntgt, sondiert und von jeweils einem Sprengstoff- beziehungsweise Waffenspürhund sowie einem Suchtgifthund durchsucht. Durch das professionelle Vorgehen der Sicherheitsbehörden wurden schließlich mehrere strafrechtsrelevante Sicherstellungen durchgeführt. Durch das Landesgericht Eisenstadt wurde der Beschuldigte rechtskräftig zu einer sechsjährigen Freiheitsstrafe verurteilt.

3.4.1.4 Trends/Entwicklungstendenzen

Das Internet (sowohl Clearnet als auch Darknet) wird als Vertriebsmöglichkeit von Schusswaffen und Munition immer weiter etabliert. Eine nicht unwesentliche Rolle stellten in den letzten Jahren, aber auch künftig soziale Netzwerke und Messengerdienste dar.

Auf diversen virtuellen Plattformen werden sowohl Exponate angeboten als auch mit verschiedenen Waffen oder Waffenteilen und Kriegsmaterialien gehandelt.

Im Hinblick auf den illegalen internationalen Waffenhandel stand in den vergangenen Jahren vor allem der Umbau bzw. die Reaktivierung von mangelhaft deaktivierten oder zu Schusswaffen umgebauten Schreckschusswaffen im Mittelpunkt. Es besteht die begründete Annahme, dass aufgrund von bereits umgesetzten bzw. geplanten Gesetzesänderungen diese Beschaffungswege künftig geschlossen werden und sich die illegale Beschaffung auf den Modus Operandi des Zusammensetzens von Waffenbestandteilen (in Bezug auf Österreich z.B. Griffstücke) verlagern wird.

Dabei werden zielgerichtet unterschiedliche nationale Gesetzgebungen genutzt, die den Erwerb bestimmter Waffenbestandteile national regeln. Dadurch können diese Bestandteile in jenen Ländern erworben werden, in denen niedrigere oder keine rechtlichen Hürden bestehen. In weiterer Folge werden diese dann, in der Regel unter Missachtung etwaiger Ein- und Ausfuhrbestimmungen, in jene Länder ausgeführt, in denen diesbezüglich restriktive rechtliche vorliegen. Das Ziel besteht darin, die erworbenen Waffeneinzelteile zu einer voll funktionsfähigen Schusswaffe zusammenzusetzen und so in den Besitz einer nicht weiter nachvollziehbaren (da nicht registrierten) Schusswaffe zu gelangen.

Dies kann auch durch Kombination legal erworbener Bestandteile mit selbst angefertigten Bestandteilen (in der Regel Lauf oder Verschluss) erfolgen. Zudem stellt die zunehmende Nutzung von 3D-Druckern zur Herstellung von Waffen bzw. Waffenteilen eine weitere enorme Herausforderung dar.

3.4.2 Proliferation

3.4.2.1 Überblick

Als **Proliferation** wird die Weiterverbreitung von atomaren, biologischen oder chemischen Massenvernichtungswaffen und entsprechenden Waffenträgersystemen beziehungsweise der zu deren Herstellung verwendeten Produkte, einschließlich des dazu erforderlichen Know-hows, bezeichnet.

3.4.2.2 Aktuelle Lage

In Anbetracht der Vielzahl an internationalen und innerstaatlichen Konflikten und des Missbrauchs von Waffen jeglicher Art durch substaatliche Gruppierungen, die in den Besitz chemischer, biologischer, radioaktiver oder nuklearer Stoffe gelangen könnten, erhöht sich der Risikofaktor für den Bereich der Proliferation erheblich.

Die Bekämpfung der Proliferation zählt weiterhin zu den zentralen Sicherheitsaufgaben Österreichs. Die Gefahr, dass Massenvernichtungswaffen, Trägersysteme, „Dual-Use Güter“ (bezeichnet Waren oder Produkte, die sowohl für zivile Anwendungen als auch für

militärische Zwecke (=doppelte Verwendbarkeit) geeignet sind. Voraussetzung für eine Exportgenehmigung ist die eindeutige Feststellung einer ausschließlich zivilen Nutzung durch den Endempfänger) 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 der wesentlichen proliferationsbezogenen Gefährdungen dar.

Österreich ist in diesem Zusammenhang 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 „Dual-Use"-Güter dar.

Ein Problem mit welchem die Ermittler in diesem Zusammenhang immer wieder konfrontiert werden, ist die Nachverfolgung des Weges von der legalen Produktion bis zum illegalen Inverkehrbringen. Es gibt unzählige Möglichkeiten die Weitergabe beziehungsweise den Transport von „Dual-Use" Güter zu verbergen, wie zum Beispiel die falsche Deklarierung beim Verkauf oder der Ausfuhr, den Einsatz von Zwischenhändlern, die Verbergung des End-Verbrauchers und die Trennung der jeweiligen Güter in verschiedene unauffällige Einzelpakete.

3.4.2.3 Fälle 2021

Durch einen entsprechenden Hinweis wurde dem Verfassungsschutz im Berichtsjahr bekannt, dass ein slowakischer Staatsbürger einem moldauischen Staatsbürger ca. 900 Gramm von angereichertem Uran 235 zum Preis von 3.000 Euro je Gramm zum Kauf angeboten hatte (Gesamtwert von 2.700.000 Euro). Der slowakische Staatsbürger bestand jedoch darauf, das Geschäft in Wien durchzuführen. Aus diesem Grund erhielten die österreichischen Sicherheitsbehörden ein Rechtshilfeersuchen sowie eine gerichtliche Anordnung zur Durchführung von verdeckten Ermittlungen, eines Scheinkaufes sowie zur optischen und akustischen Überwachung von Personen.

Aufgrund des nicht auszuschließenden Risikos, dass im Zuge des Einsatzes tatsächlich Uran 235 zum Vorschein kommen und dadurch die einschreitenden Bediensteten gefährden würde, wurde wegen der befürchteten Strahlenbelastung größtes Augenmerk auf die Vorbereitung der Amtshandlung gelegt. Im Vorfeld wurden alle notwendigen Sicherheitsmaßnahmen in Absprache mit den involvierten Einheiten – insbesondere in Hinblick auf die Einsatztaktik – getroffen. Die Örtlichkeit sowie der Zeitpunkt wurden unter Rücksichtnahme auf ein möglichst geringes Erregen von Aufsehen und unter Wahrung der bestmöglichen Risikominimierung gewählt.

Nach entsprechenden Messungen mit einem geeichten Strahlenmessgerät im Zuge des Einsatzes sowie einer strahlentechnischen Fernmessung (bei der keine Strahlung festgestellt werden konnte) erfolgte die Zugriffsfreigabe und vorläufige Festnahme von drei Personen. Nach dem Zugriff intervenierte ein „CBRN-Team" (CBRN ist die Abkürzung für chemisch, biologisch, radiologisch und nuklear) und führte eine Freimessung sämtlicher am Einsatzort befindlicher Personen, Fahrzeuge und sonstiger Objekte durch. Dabei konnte ebenfalls keine Strahlung festgestellt werden.

Der als Uran 235 übergebene Gegenstand wurde in weiterer Folge an ein Labor für eine eingehende Untersuchung und Abklärung überstellt. Im Ergebnis handelte es sich dabei um einen Gegenstand, der professionell zur Täuschung allfälliger Käufer mit Wuchtgewichten, Watte, Sand und Dünger gefüllt war.

Zwei Personen wurden schlussendlich wegen schweren Betruges angezeigt und zu einer Freiheitsstrafe in der Dauer von fünf beziehungsweise zweieinhalb Jahren verurteilt.

3.4.2.4 Trends und Entwicklungstendenzen

Die Verbreitung atomarer, biologischer oder chemischer Massenvernichtungswaffen, sogenannter Weapons of Mass Destruction (WMD), stellt weltweit eines der größten Sicherheitsrisiken dar. Unterschiedliche Akteurinnen und Akteure werden sich auch künftig bemühen, in den Besitz solcher Waffen und der für deren Einsatz erforderlichen Trägertechnologie zu gelangen, um diese im Rahmen bewaffneter Konflikte oder zur Durchsetzung politischer Ziele einzusetzen. Um solche Bestrebungen zu unterbinden, wurden seitens der Vereinten Nationen (UN) sowie seitens der EU Sanktionen verhängt. Es kann davon ausgegangen werden, dass es weiterhin zum Versuch der Umgehung derartiger Sanktionen kommen wird.

Ziele der Beschaffung von WMD können die Vervollständigung bestehender Arsenale, die Verbesserung der Lagerfähigkeit, Einsetzbarkeit und Wirkung bestehender Waffen oder die Entwicklung neuer Waffensysteme darstellen. Im Allgemeinen soll erreicht werden, bestehende Zulieferungsabhängigkeiten aus dem Ausland abzubauen, um eine Autarkie im Bereich der Entwicklung und Herstellung relevanter Technologien zu erlangen. Zur Zielerreichung versuchen die betreffenden Akteurinnen und Akteure, erforderliche Produkte und einschlägiges Know-how im Ausland zu gewinnen. Dabei wenden sie auch Methoden der Informationsbeschaffung an, die im jeweiligen Zielland außerhalb des gesetzlichen Rahmens liegen.

Zielländer für Beschaffungsaktivitäten sind in erster Linie all jene Industrienationen, die relevante Produktionsstandorte vorweisen oder führende Rollen in der Technologieentwicklung einnehmen. Von besonderem Interesse sind jene Unternehmen, die unter Sanktionen stehende Produkte herstellen oder liefern können. Auch Universitäten

und wissenschaftliche Einrichtungen sind Ziele von Informationsbeschaffungsaktivitäten, um den notwendigen Wissenstransfer vorzubereiten.

Zur Informations- und Güterbeschaffung werden Verschleierungstaktiken aus Firmennetzwerken und Tarnidentitäten, die Möglichkeiten neuer Bezahldienste (Krypto-Währungen) sowie das Internet (DarkNet) genutzt. Die Finanzierung der Beschaffung und der damit verbundenen Nebenkosten werden vom sanktionierten Staat getragen. Um Transaktionen zu verschleiern, wird auch auf Formen der Geldwäsche zurückgegriffen. Dual-Use-Güter nehmen im Themenbereich Proliferation einen besonderen Stellenwert ein. Güter dieser Art können beispielsweise im Kontext technologischer Entwicklungen wie in Fertigungsmaschinerien relevant sein. Der kostengünstige und barrierefreie Erwerb solch elektronischer Artikel (zum Beispiel Drohnen) stellt eine anhaltend große Herausforderung bei der Bekämpfung von Proliferation und Waffenhandel dar.

4
Schutz und Prävention

4.1 Schutz der obersten Organe und verfassungsmäßigen Einrichtungen

4.1.1 Überblick

Als Sicherheitsbehörde übernimmt die DSN verschiedenste Aufgaben zum Schutz vor verfassungsgefährdenden Angriffen. Zum zentralen Betätigungsfeld zählt der vorbeugende Schutz von gesetzlich normierten, besonders schutzwürdigen Rechtsgütern wie verfassungsmäßigen Einrichtungen und deren Handlungsfähigkeit. Das grundsätzliche Modell des vorbeugenden Schutzes basiert auf der Erstellung einer Gefährdungseinschätzung inkl. Festlegung einer Gefährdungsstufe. Unter Berücksichtigung dieser festgelegten Gefährdungsexposition werden individuell gefährdungsbezogene sicherheitspolizeiliche Personen- und Objektschutzmaßnahmen konzipiert, veranlasst und mit den operativ ausführenden Organisationseinheiten koordiniert.

In Abhängigkeit der Ergebnisse der Gefährdungseinschätzungen in Bezug auf innen- und außenpolitische Vorgänge, die jeweils generell vorherrschende, persönliche Gefährdungsexposition sowie oftmals kurzfristig entstehende beziehungsweise sich dynamisch entwickelnde Gefährdungsmomente ist es Aufgabe der Verfassungsschutzbehörden, geeignete objekt- und personsbezogene Bewachungsformen und/oder Überwachungsformen zu veranlassen, um das angestrebte Schutzniveau zu erreichen.

Einen weiteren Schwerpunkt bildet das Erstellen von objektschutztechnischen Sicherheitskonzepten und Sicherheitsberatungen für verfassungsmäßige Einrichtungen und oberste Organe. Wird beispielsweise eine neue Regierung angelobt, bietet die DSN den Obersten Organen – wie dem Bundeskanzler bzw. der Bundeskanzlerin oder den Ministerinnen und Ministern – Sicherheitsberatungen an. In einer solchen Sicherheitsberatung wird auf die speziellen Gefahren im Zusammenhang mit den jeweiligen Aufgaben eingegangen und entsprechende Sicherheitsmaßnahmen werden empfohlen. Anschließend wird ein Sicherheitskonzept erstellt und eine Prüfung der notwendigen Sicherheitsmaßnahmen durchgeführt. Darüber hinaus ist die DSN Verbindungsstelle für die Sicherheitsbeauftragten der verfassungsmäßigen Einrichtungen und führt mit diesen einen regelmäßigen Sicherheitsdialog.

4.1.2 Aktuelle Lage

Nach wie vor bietet öffentlichkeitswirksames Handeln von politischen Entscheidungsträgerinnen und Entscheidungsträgern neben legitimen demokratiepolitischen Kontroversen auch eine große Projektionsfläche als lohnendes Angriffsziel für Polemik, Agitation sowie tätlichen Aktionismus. Ferner stellen strafrechtlich relevante Drohungen gegen politische Repräsentantinnen und Repräsentanten sowie Einrichtungen oder gegen Personen des öffentlichen Lebens national wie international

seit jeher bekannte Gefährdungsbilder dar. Grundsätzlich richten sich einschlägige Bedrohungshandlungen vorwiegend nicht gegen die jeweilige Funktion an sich, sondern gegen die Person als Funktionsträgerin oder Funktionsträger selbst oder vielmehr gegen von der Person kommunizierte Aktivitäten beziehungsweise politische Absichten.

Das Drohgeschehen des Jahres 2021 wurde maßgeblich von den Themen der COVID-19-Maßnahmengesetzgebung sowie den Geschehnissen rund um öffentlich bekannte Vorwürfe und strafrechtliche Ermittlungen gegen eine Regierungspartei und ihre Funktionäre bestimmt. Phasenweise hatte sich die regierungskritische Agitation sowohl quantitativ als auch qualitativ derart intensiviert, dass sowohl Eskalationen in Form von Aktionismus, Protesten und Ausschreitungen im Nahebereich von Regierungsgebäuden als auch tätliche Angriffe gegenüber politischen Repräsentantinnen und Repräsentanten plausible Konsequenzen waren.

In diesem Zusammenhang ist es nachvollziehbar, dass im Berichtsjahr vorwiegend all jene mit diesen Themenbereichen befassten Politikerinnen und Politiker und Behörden als favorisiertes Adressatenziel von bedenklichen Eingaben beziehungsweise bedrohlichen Zuschriften auszumachen waren. Weiters war zu beobachten, dass ein Großteil aller Eingaben affektgetriebene Unmutsäußerungen wie Protestbekundungen, Rücktrittsaufforderungen, Beschimpfungen sowie Verwünschungen beinhalteten, die als inkriminierend zu qualifizieren sind. Von allen im Beobachtungszeitraum 2021 bekannt gewordenen Eingaben wiesen 13,5 Prozent den strafrechtlich relevanten Tatbestand einer gefährlichen Drohung oder Nötigung beziehungsweise schweren Nötigung auf, was mit Blick auf das Vorjahr einen Anstieg um mehr als die Hälfte bedeutet.

Eine Analyse hinsichtlich der den Drohschreiben zugrundeliegenden Motivlagen gibt eindeutigen Aufschluss über die prädominanten Themenschwerpunkte im Jahr 2021. Wenig überraschend entfallen die größten Anteile auf die Motivlagen „Corona-Maßnahmenkritik“ sowie „Persönliche/Andere Gründe“, die gemeinsam um mehr als ein Drittel im Vergleich zum vorhergehenden Beobachtungszeitraum zunahmen. Die übrigen Phänomenbereiche und Motivlagen stellen mit Deliktsfällen im niedrigen einstelligen Bereich vergleichsweise sehr geringe Anteile dar. Der Motivlage „persönliche/andere Gründe“ können mannigfaltige Beweggründe für eine Aversion gegenüber einem bestimmten Funktionsträger oder einer bestimmten Funktionsträgerin zugrunde liegen, weshalb sich hier keine aussagekräftige und zielsichere Prognose anstellen lässt. Generisch betrachtet sind aber Themen wie Intransparenz, persönliche Skandale, Machtmissbrauch oder der Verdacht korrupten Verhaltens ohnedies gebräuchliche Nährböden, um den Unmut der Bevölkerung auf sich zu ziehen und damit das Protestverhalten maßgeblich zu beeinflussen.

Etwas mehr als die Hälfte der strafrechtlich relevanten Eingaben wurden über Social-Media-Plattformen in Form von öffentlich einsehbaren Kommentaren oder persönlichen

Nachrichten, etwas unter ein Drittel per E-Mail und weniger als ein Fünftel analog in Briefform oder mittels Telefonanruf übermittelt.

4.1.3 Fälle 2021

Obwohl die Intensität an schriftlichen Eingaben im Jahr 2021 im Vergleich zu den vorhergehenden Jahren auf eine erhöhte Plausibilität der realen Tatverwirklichung in Form von tätlichen Übergriffen auf staatliche Institutionen vermuten lassen hätte können, wurden keine Ereignisse verzeichnet, die einen Eingriff in die körperliche Unversehrtheit von Obersten Organen bedeutet hätten. Jedoch erfolgten mehrere Sachbeschädigungen an beziehungsweise im unmittelbaren Nahbereich von Regierungsgebäuden, die allerdings keine ernsthafte Bedrohung für die physische Integrität verfassungsmäßiger Einrichtungen darstellten. Ferner ereignete sich bei einem öffentlichen Auftritt von mehreren Regierungsmitgliedern eine Störaktion von Corona-Maßnahmen-Gegnern sowie eine weitere Störaktion von Tierrechtsaktivisten und -aktivistinnen während eines Medientermins eines Regierungsmitglieds.

Eine männliche Person, die auf der rechten Körperseite ein Messer in einer Messescheide trug, versuchte im Berichtsjahr beim Haupteingang des Bundeskanzleramtes zum Bundeskanzler vorzudringen, indem auf eine persönliche Vorsprache bzw. Terminvereinbarung mit dem Bundeskanzleramt gedrängt wurde. Die Torsicherung vor Ort konnte die Person unter Einhaltung der Eigensicherung von ihrem Vorhaben abbringen, diese entfernte sich in weiterer Folge. Es wurde eine Sofortfahndung eingeleitet, hierbei konnte die bewaffnete Person durch die WEGA angehalten und eine Identitätsfeststellung durchgeführt werden.

Die regelmäßige sowie anlassbezogene Auswertung jener sicherheitsrelevanten Vorfälle bildet eine wichtige Grundlage zur Überprüfung der Wirksamkeit bestehender Sicherheitsmaßnahmen bei verfassungsmäßigen Einrichtungen und geben Anlass zur kontinuierlichen Identifizierung von Verbesserungspotential.

4.1.4 Trends und Entwicklungstendenzen

Allgemein ist langfristig davon auszugehen, dass ein annähernd gleich hohes, quantitatives Niveau an Drohschreiben gehalten wird oder sich dieses sogar erhöht, zumal die Hemmschwelle für radikale Agitation im Cyberraum unter dem vermeintlichen Deckmantel der Anonymität weiterhin sinken dürfte und verbale Tabus zusehends nicht mehr existieren. Es gilt nun zu beobachten, ob die in letzter Zeit eingerichteten Meldestellen zum Thema „Hass im Netz“ zu einer wünschenswerten gegenteiligen Entwicklung beitragen werden.

Im Lichte der im Jahr 2021 im Bereich „Drohschreiben“ evidenten Größenordnung und der dabei zutage getretenen verbalen Aggressivität kann nicht ausgeschlossen werden, dass in einer nächsten Eskalationsstufe auch physische Angriffe oder gewalttätige Handlungen

gegen politische Funktionsträgerinnen oder Funktionsträger zur Umsetzung gelangen. Die in jüngerer Zeit wiederholt bei Exponenten des rechtsextremen Spektrums erfolgten Aushebungen von teils umfangreichen Waffenbeständen illustrieren die potenziell von extremistischen Kreisen – aber auch von radikalisierten Einzelaktivsten – ausgehenden Gefahren und Herausforderungen im Bereich des Personen- und Objektschutzes.

4.2 Präventionsarbeit im Verfassungsschutz

Mit Gründung des Bundesweiten Netzwerks Extremismusprävention und Deradikalisierung (BNED) im Jahr 2017 wurde in der Extremismusprävention und Deradikalisierungsarbeit im Verfassungsschutz eine Struktur geschaffen, die durch koordinierte Zusammenarbeit – Mitglieder sind unter anderem mehrere Ministerien, zivilgesellschaftliche Organisationen und die Bundesländer – allen Formen des Extremismus mit einer gesamtgesellschaftlichen Antwort begegnet. Auch während der COVID-19-Pandemie wurde die initiierten Arbeiten im BNED fortgesetzt. Alle bereits eingesetzten Arbeitsgruppen – Antisemitismus, Verschwörungserzählungen, Regionale Netzwerke in den Bundesländern, Nationaler Aktionsplan Extremismusprävention und Deradikalisierung – haben ihre Expertise im Sinne der Umsetzung der Aufwertung der Agenden des BNED gebündelt. Die konsequente Weiterentwicklung des BNED zu einer bundesweiten Koordinationsstelle konnte damit nahtlos in der neuen Behördenstruktur der DSN fortgesetzt und ausgebaut werden.

Unter der Koordinierung des Bundesministeriums für Inneres erfolgte die Erarbeitung des österreichischen Aktionsplans Extremismusprävention und Deradikalisierung (NAP) durch das BNED als strategisches und gesamtgesellschaftliches Gremium. Der Maßnahmenkatalog wird österreichweit eine erste Zusammenstellung von zielgerichteten Maßnahmen und Empfehlungen zur Bekämpfung aller Formen des Extremismus aus Sicht von Expertinnen und Experten darstellen.

Einen fixen Bestandteil des fachlichen Diskurses im Bereich Extremismusprävention stellt der Präventionsgipfel dar. Auf Grund der COVID-19-Pandemie musste der Präventionsgipfel 2021 kurzfristig abgesagt und auf das Jahr 2022 verschoben werden. Der Präventionsgipfel fungiert als jährlich stattfindende Fachtagung von Akteurinnen und Akteuren der Extremismusprävention und Deradikalisierung. Die thematischen Schwerpunkte des Präventionsgipfels im Jahr 2022 werden hybride Bedrohungen, Prävention, Radikalisierung und zukünftige Herausforderungen im Kontext der zunehmenden gesellschaftlichen Polarisierung sein.

Das im September 2020 initiierte Ausstiegs- und Deradikalisierungsprogramm KOMPASS wurde 2021 in Kooperation mit dem Verein NEUSTART fortgeführt. Da es jedoch aufgrund der Einschränkungen im Zuge der COVID-19-Pandemie nicht möglich war, die vorgegebenen Fallzahlen im ursprünglich vorgesehenen Projektzeitraum zu

erreichen, wurde das Projekt bis Ende Dezember 2022 verlängert. Das Ausstiegs- und Deradikalisierungsprogramm wurde für ausstiegswillige Personen geschaffen und bezieht alle Formen des Extremismus mit ein. Grundsätzlich ist eine freiwillige Teilnahme am Projekt KOMPASS Voraussetzung für die Aufnahme.

Bis Ende des Jahres 2021 wurden insgesamt 20 Fälle zum Clearing an KOMPASS übergeben. Fünf Klientinnen und Klienten, die einer Teilnahme an dem Projekt zugestimmt hatten, befanden sich aktiv in Betreuung. Bei den bisherigen Kandidatinnen und Kandidaten für das Projekt KOMPASS handelt es sich um Personen aus dem rechts- sowie aus dem islamistisch-extremistischen Spektrum.

Präventionsarbeit erfolgt aber auch durch den Verfassungsschutz selbst. Um Bedrohungen entgegenzuwirken, ist es ein fester Grundsatz in der Präventionsarbeit, sich mit relevanten Akteurinnen und Akteuren sowie Betroffenen auszutauschen und geeignete Maßnahmen zu setzen, sodass jegliche Schäden von Personen beziehungsweise Einrichtungen abgewendet werden können. Vor allem bei Protesten gegen Maßnahmen zur Eindämmung der Corona-Pandemie war eine zunehmende Radikalisierung der Proteste zu beobachten. Immer mehr Berufsgruppen waren von Drohungen und Übergriffen betroffen – vor allem der Gesundheitsbereich. Die Aufgabe der Sicherheitsbehörden ist es, aktiv über Bedrohungen und zu erwartende Szenarien zu informieren und damit präventiv tätig zu werden. So wurden im Dezember 2021 unter dem Titel „Pandemie und Protest“ zwei Online-Sensibilisierungsveranstaltungen mit Medienvertreterinnen und Medienvertretern sowie Akteurinnen und Akteuren aus dem Gesundheitsbereich durchgeführt. Schließlich richtet sich der präventive Fokus des Verfassungsschutzes auf die Stärkung und den Schutz von Betroffenen.

4.3 Kooperation und Kommunikation als essentieller Teil des Schutzes der kritischen Infrastruktur

Der Schutz der kritischen Infrastruktur gewann schon bisher vor dem Hintergrund einer latenten Bedrohung durch terroristische Anschläge, einer tendenziell steigenden Kriminalität im Cyberbereich, aber auch einer stetig steigenden Komplexität der Vernetzung der sektoralen Versorgungsaufgaben an Bedeutung. Auch die steigende Abhängigkeit, im Speziellen des Individuums, aber auch der Gesellschaft und des Staates allgemein von einer funktionierenden Infrastruktur, sind maßgebliche Parameter für die vorbeugenden Schutzmaßnahmen durch staatliche Behörden.

Als kritische Infrastruktur gelten in Österreich unter anderem Betreiber und Anbieter von Produkten und Dienstleistungen aus den Sektoren Energie, Gesundheit, Hilfs- und Einsatzkräfte, Transport und Verkehr, Finanzen, Wasser- und Abfallwirtschaft, Informations- und Kommunikationstechnologien, Lebensmittel, chemische Industrie, Sozial- und

Verteilsysteme, verfassungsmäßige Einrichtungen und Forschungseinrichtungen. Diese Sektoren stehen nicht nur in einer komplexen Vernetzung zueinander, sie sind zudem wichtige Parameter im Bereich der Resilienz des Staates und der wirtschaftlichen Stabilität.

Den Verfassungsschutzbehörden obliegt die operative Umsetzung der Maßnahmen zur Erhöhung der Resilienz sowie der Sicherheit der Unternehmen der sogenannten kritischen Infrastruktur. Die strategische Ausrichtung wird durch das Bundeskanzleramt sowie das Bundesministerium für Inneres mit dem Beirat des „Austrian Program for Critical Infrastructure Protection“ (APCIP) bestimmt. Im Falle der Notwendigkeit von Assistenzleistungen werden diese durch das österreichische Bundesheer geleistet. Im Falle der COVID-19-Pandemie war dies auch im Jahr 2021 in verschiedenen Bereichen erforderlich.

Nicht nur die Sicherheit und Resilienz der Unternehmen soll mithilfe des Programmes APCIP erhöht werden, sondern auch die Resilienz der österreichischen Bevölkerung wie auch des österreichischen Staates.

Die Verfassungsschutzbehörden setzen zur Aufrechterhaltung der Funktionsfähigkeit der Unternehmen und der Versorgungssicherheit der Bevölkerung auf eine rasche, effiziente und kompetente Kommunikation und Kooperation. Entscheidend dafür ist die Übermittlung und Interpretation von Informationen, die Vernetzung von präventiven Maßnahmen und Maßnahmenempfehlungen genauso wie die Abklärung von Bedürfnissen der Unternehmen in einem Krisenfall, um einen Ausfall oder eine Unterbrechung der Dienste, Produktionen oder sonstiger Dienstleistungen zu verhindern. Im Laufe der COVID-19-Pandemie wurden die Unternehmen regelmäßig zu grundsätzlichen Problemstellungen befragt, um diese Informationen bei der Weiterentwicklung von Verordnungen beziehungsweise in der Maßnahmenerstellung im Hinblick auf das weitere Funktionieren der Infrastruktur berücksichtigen zu können.

Gemäß der Leitlinie des Programms zum Schutz der kritischen Infrastruktur kann der Schutz jener Unternehmen und Organisationen, die kritische Infrastruktur betreiben, nur durch eine vertrauensvolle Kooperation erfolgen und dadurch zum Ziel – der Steigerung der gesamtstaatlichen Resilienz – führen.

Vor diesem Hintergrund wurde seitens der Verfassungsschutzbehörden mit den Unternehmen der kritischen Infrastruktur, die sich auf der sogenannten „Austrian Critical Infrastructure“-Liste befinden, seit mehreren Jahren eine Kommunikation und Kooperation aufgebaut. Genau diese Kooperation und Kommunikation erwies sich in der Pandemie einerseits als hilfreich für die staatlichen Stellen selbst, aber ebenso essentiell für die Unterstützung der Unternehmen und Organisationen.

Um eine Informationsweitergabe für die Unternehmen in der Pandemie zu gewährleisten, wurde seitens der zuständigen Organisationseinheit im Verfassungsschutz bereits im Jahr 2020 im SKKM (Staatliches Krisen- und Katastrophenmanagement)-Koordinierungsstab COVID-19 des BMI eine direkte Kontaktstelle eingerichtet. Dies ermöglichte den raschen Austausch von Informationen und Problemstellungen zwischen den einzelnen Stakeholdern. Über diese zentrale Kontaktstelle „WIDA" (Wirtschaft und Daseinsvorsorge), aber auch durch persönliche Kontakte zwischen den Mitarbeiterinnen und Mitarbeitern des Verfassungsschutzes und den jeweiligen Sicherheitsverantwortlichen in den Unternehmen und Organisationen, wurde die direkte Kommunikation wesentlich verstärkt. Diese direkte Informationsschiene bewährte sich sowohl am Beginn der COVID-19-Pandemie als auch in der Phase der COVID-19-Impfungen in Unternehmen sowie Ende 2021 beim Auftreten der Omikron-Variante.

Neben kriminellen und intentionalen Risiken, die eine Pandemie mit sich bringt, waren die Unternehmen mit einer Reihe von organisatorischen Problemstellungen konfrontiert. Diese unterschiedlichen Herausforderungen änderten sich im Verlauf der Pandemie. Waren es zu Beginn 2020 noch Schwierigkeiten im Bereich eines eingeschränkten Waren- und Dienstleistungsverkehrs – sowohl in Europa als auch international – herrschten 2021 hauptsächlich Probleme im Bereich des Impfmanagements, der Corona-Maßnahmen-Gegner oder auch starke Personaleinschränkungen durch die Omikron-Variante. Da speziell durch diese Variante eine starke Belastung der Bevölkerung aufgrund der erhöhten Ansteckungsrate befürchtet wurde – die sich in weiterer Folge auf die Ausfallszahlen der Mitarbeiterinnen und Mitarbeiter der Unternehmen auswirken sollte – waren entsprechende Vorbereitungsmaßnahmen für die Unternehmen von großer Bedeutung.

Speziell die Omikron-Variante versetzte sowohl die staatlichen Einrichtungen als auch die Unternehmen durch die befürchteten hohen Ausfälle von Personal in Alarmbereitschaft. So wurden schon kurz nach Auftreten der Variante in mehreren Runden Maßnahmen von Expertinnen und Experten evaluiert, um die Versorgungsleistungen der kritischen Infrastruktur aufrechtzuerhalten. Durch das zuständige Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz wurden entsprechende Maßnahmenempfehlungen erlassen. Die Unternehmen bereiteten sich in unterschiedlicher Weise auf einen größeren Ausfall von Personal vor beziehungsweise versuchten diesem durch Vorsorgemaßnahmen vorzubeugen. So wurde beispielsweise in einigen Unternehmen im Energiesektor, wie zu Beginn der Pandemie, eine Kasernierung von Kernpersonal beziehungsweise Spezialkräften vorbereitet und teils umgesetzt. Viele Unternehmen trennten ihr Personal in unterschiedliche Teams, die untereinander keinerlei Kontakt hatten. So traten beispielsweise Fahrzeugführerinnen und Fahrzeugführer den Dienst direkt im Fahrzeug an und nicht wie üblich in einem Betriebsgebäude. Außerdem setzten viele Unternehmen weiterhin auf Homeoffice. Im IKT-Sektor war dies die weitverbreitetste Maßnahme zur Abwendung eines möglichen größeren Ausfalls

von Personal. Andere Unternehmen, beispielsweise im Lebensmittelsektor, bereiteten die Zusammenlegung von Filialen vor, um im Bedarfsfall mit verringertem Personal den Betrieb aufrechtzuerhalten.

Durch die sehr differenzierten Maßnahmen, die sich in den einzelnen Unternehmen im Laufe der Pandemie bewährten, konnte ein Versorgungsausfall abgewendet werden. Selbst zum Höhepunkt der Omikron-Variante im Winter 2021/2022 mussten lediglich auf Grund von Personalausfällen vereinzelt in Unternehmen Unterstützungsleistungen durch unternehmensexternes Personal (zum Beispiel durch das Österreichische Bundesheer) geleistet werden.

Die COVID-19-Pandemie und ihre Auswirkungen zeigten sehr deutlich, dass die Zusammenarbeit zwischen staatlichen Stellen und Unternehmen der kritischen Infrastruktur in Kooperation mit weiteren Protagonisten, zum Beispiel der Wirtschaftskammer Österreich (WKÖ), sehr gut funktionierte. Die bereits aufgebauten Strukturen im Sinne des APCIP waren dafür bestens geeignet. Durch die ständige Kommunikation mit den Unternehmen konnte die Stabstelle SKKM-WIDA als Informations-Plattform einen essentiellen Beitrag zur Krisenbewältigung leisten. Das positive Feedback der Unternehmen zeigt, dass dieser „Single Point of Contact" eine nicht zu unterschätzende Hilfestellung in der Krisenbewältigung war. Insgesamt wurde im Jahr 2021 die Möglichkeit der Kontaktaufnahme in über 1.200 Fällen genutzt.

Neben dieser Serviceleistung für die Unternehmen durch die Durchführung der Kooperationsplattform wurden seitens der Verfassungsschutzbehörden weitere Maßnahmen angeboten und durchgeführt.

Ein wichtiger Bestandteil war die rasche Übermittlung von Gesetzes- und Verordnungstexten inklusive einer jeweiligen Analyse beziehungsweise Kurzfassung der wichtigsten Aspekte. Auch die Übermittlung wichtiger Länderinformationen war für viele Unternehmen im Hinblick auf den Verkehr von Pendlerinnen und Pendlern sowie Dienstreisen von großer Bedeutung.

Darüber hinaus wurden Unternehmen auch proaktiv seitens des Verfassungsschutzes über allfällige Risiken und Bedrohungen mit Bezug zu COVID-19 informiert. Dabei wurde unter anderem auf ein bereits bewährtes Instrument zurückgegriffen. In Form von Workshops wurden neben anderen sicherheitsrelevanten Themen auch die besonderen Herausforderungen der Unternehmen, „best practices" und „lessons learned" ausgetauscht. Die Vernetzung untereinander, die sich bei derartigen Veranstaltungen ergab, wurde von den teilnehmenden Unternehmen nicht nur positiv aufgenommen, sondern in weiterer Folge auch genutzt und war weiterhin ein wichtiger Baustein in der Krisenbewältigung der Unternehmen.

Im Hinblick auf sich entwickelnde Risiken waren in einigen Sektoren verstärkte Maßnahmen notwendig. So wurden, ob der zunehmenden Aggressivität, der verbalen Anfeindungen, aber auch aufgrund einer stärkeren Bedrohung für das Gesundheitspersonal, Krankenhausbetreiber, Sicherheitsverantwortliche von Krankenhäusern, Impfstraßenbetreiber und Verantwortliche von Rettungsorganisationen und Sozialdiensten über Verhaltensempfehlungen und Empfehlungen für Vorsichtsmaßnahmen durch die Verfassungsschutzbehörden informiert. Ergänzend wurde durch die jeweiligen Landespolizeidirektionen mittels Überwachung beziehungsweise Bestreifung besonders im Fokus stehender Objekte die Sicherheit von Personen und Einrichtungen gewährleistet.

Auch im Fall von Medienunternehmen, gegen die ebenfalls ein Anstieg an aggressiven Handlungen verzeichnet werden musste, wurden individualisierte Vorsichtsmaßnahmen erarbeitet und weitergegeben. Diese wurden zusätzlich durch persönliche Sensibilisierung und Begehungen vor Ort unterstützt.

Eine wichtige Erkenntnis aus der COVID-19-Pandemie besteht darin, dass das bestehende Kooperations- und Kommunikationsverhältnis zwischen den Unternehmen, den Bundesministerien und sonstigen Stakeholdern und den Verfassungsschutzbehörden ein essenzieller Baustein in der Krisenbewältigung war und auch weiterhin sein wird. Durch die bereits jahrelange Kooperation und das entstandene Vertrauen sowie den persönlichen Kontakt der Protagonisten untereinander war zumeist eine kurze Reaktionszeit gegeben. Dies erleichterte die Bewältigung der COVID-19-Pandemie für die Unternehmen der kritischen Infrastruktur sowie der systemkritischen Unternehmen entscheidend.

4.4 Die Fokussierung auf die Pandemie in der Pandemie – Repressive und parallel-präventive Krisenbewältigung

Während einer Ausnahmesituation – beispielsweise einer Pandemie – wird ein Großteil der Ressourcen dieser Krise gewidmet werden.

Der Nebeneffekt dabei ist jedoch, dass dabei die sonst übliche Präventivarbeit für allfällige weitere Risiken, Schwachstellen und Bedrohungen vernachlässigt werden könnte. Man fokussiert derart auf die aktuelle Herausforderung, dass auf weitere Risiken kein oder zu wenig Augenmerk gelegt wird. Die Eintrittswahrscheinlichkeit anderer Risiken hat dabei jedoch nicht abgenommen.

Ein solches Risiko ist beispielsweise eine Versorgungsstörung für die Bevölkerung. Eine solche extreme Versorgungsstörung könnte beispielhaft der Verlust der Stromversorgung darstellen. Der plötzliche überregionale Verlust über einen längeren Zeitraum – ein

Blackout – hätte massive Auswirkungen auf die Unternehmen der kritischen Infrastruktur und in weiterer Folge auf die Versorgungssicherheit der Bevölkerung.

So wurden im Jahr 2021 zumindest drei Vorfälle im europäischen Stromnetz – in Kroatien, Spanien und Polen – beobachtet, die durchaus die Qualität für einen großflächigen Ausfall der Stromversorgung haben hätten können. Diese konnten durch die Kompetenz der Übertragungsnetzbetreiber abgewendet werden. Ob dies jedoch immer möglich sein wird, kann beziehungsweise sollte nicht mit Gewissheit angenommen werden.

Von Seiten einiger Unternehmen der kritischen Infrastruktur wurde das Risiko einer plötzlichen und länger andauernden Unterbrechung der Stromversorgung erkannt und trotz der andauernden Pandemie als weiteres Risiko eingestuft. Im Laufe des Jahres konnte eine starke Steigerung der Anfragen diesbezüglich an den Verfassungsschutz wahrgenommen werden. Durch persönliche Beratung der Organisationen und durch Workshops wurde versucht, die Unternehmen für die jeweiligen individuellen Herausforderungen und Bedrohungen zu sensibilisieren.

Zudem soll durch die Übergabe von Digital-Funkgeräten an zentrale Unternehmen der kritischen Infrastruktur die Kommunikation im Ernstfall, beispielsweise im Falle eines Blackouts, für eine gewisse Zeit aufrechterhalten werden können.

Das Beispiel der Risikobewertung einer möglichen Unterbrechung der Stromversorgung und deren Auswirkung auf ein Unternehmen und dadurch auf die Bevölkerung zeigt, dass es wichtig ist, in Krisenzeiten einen ganzheitlichen Ansatz der Risikobewältigung anzustreben. Einige Unternehmen der kritischen Infrastruktur in Österreich setzen dies bereits um. Die Erfahrungen aus der COVID-19-Pandemie kommen auch der Bewältigung anderer Risiken zugute. So ist beispielsweise in vielen Betrieben die Stabsarbeit wesentlich besser aufgestellt als dies noch vor zwei Jahren der Fall war. Auch durch die Erfahrung und Beschäftigung mit den Kernprozessen und dem dafür notwendigen Schlüsselpersonal in der Pandemie konnten Maßnahmen für weitere Risiken besser ausgearbeitet worden.

4.5 Kritische Infrastruktur im Zusammenhang mit Corona-Maßnahmen-Gegnern

Im Jahr 2021 konnten die Verfassungsschutzbehörden einen generellen Anstieg des von der Corona-Maßnahmengegnerschaft (CMG) ausgehenden Gefährdungspotenziales feststellen. Der Ton hat sich verschärft, auch und gerade im Hinblick auf die erwartete Impfpflicht. Damit einhergehend stiegen auch die potenziellen Gefährdungen von Unternehmen der kritischen Infrastruktur. Insbesondere galt dies für die Sektoren

Gesundheit, Hilfs- und Einsatzkräfte, IKT beziehungsweise Medien, Energie, Lebensmittel, Transport und Verkehr sowie Sozial- und Verteilungssysteme.

Ein nicht zu unterschätzender Faktor war auch die „Bestätigung", die die CMG-Szene durch die Demonstrationen und Ausschreitungen in anderen europäischen Ländern erfuhren. Unter den Personen, die ihre Freiheitsrechte bedroht sahen und auf die Straße gingen, mischten sich vermehrt radikale Elemente aus dem rechten und linken politischen Lager. Die Querdenker-Szene, Anhänger von Verschwörungserzählungen und staatsfeindliche Verbindungen hatten sich ebenfalls in die CMG-Szene eingegliedert, um diese Proteste für ihre Sache zu nutzen.

Die wirtschaftlichen und sozialen Folgen der Pandemie trugen dazu bei, dass sich Teile der Impfgegnerinnen und Impfgegner, die sich aus allen Schichten der Bevölkerung zusammensetzten, zunehmend radikalisierten. Das dabei zu Tage tretende Aggressionspotenzial zeigte, dass die Agitationen aus dem Kreis weltanschaulich motivierter CMG-Aktivistinnen und -Aktivisten eine Reihe realistischer Gefährdungsszenarien auch für kritische Infrastrukturen darstellten, die weit über ein vertretbares Protestverhalten hinausgingen.

4.5.1 Vorfälle im Zusammenhang mit Corona-Maßnahmen-Gegnern

Der Unmut drückte sich im Berichtsjahr auch abseits von angemeldeten oder unangemeldeten Protestveranstaltungen wie Demonstrationszügen, Standkundgebungen oder Autokorsos aus. So musste festgestellt werden, dass mit Zunahme der Verfügbarkeit des Impfstoffes auch die Zunahme der Corona-Maßnahmen-Gegner einherging. Die Deliktsformen reichten von gefälschten Impfzertifikaten bis zum Handel mit infiziertem Speichel. Das im Herbst 2021 geplante Impfgesetz verhärtete die Ablehnungsfront noch zusätzlich.

So kam es zum Beispiel im Bereich des Gesundheitssektors zu einem starken Anstieg von verbalen Anfeindungen des medizinischen Personals in Krankenhäusern, Impfstraßen oder auch im Bereich der niedergelassenen Medizin. Im April versendete ein unbekannter Täter Ansichtskarten an verschiedene, an der Impfkampagne teilnehmende Ärztinnen und Ärzte. Auf diesen Karten propagierte er den Vergleich von Senfgas mit mRNA-Impfstoffen. Durch die Aufmachung sowie der hergestellten Verbindung mit einem chemischen Kampfstoff, nämlich einem Hautgift, fühlten sich die Empfängerinnen und Empfänger zum Teil bedroht.

Der CMG-Aktionismus bei Test- und Impfzentren reichte von Belästigungen der Belegschaft und Impfwilligen, Sachbeschädigungen, z. B. Verkleben von Schlössern, bis hin zur Brandstiftung, wobei es zu einem Sachschaden bei einer Teststation kam. Zudem kam es zu Sachbeschädigungen bei Arztpraxen, wie Hakenkreuzeinritzungen an einer Praxistür und Drohungen gegen Ärztinnen und Ärzte, die Impfungen durchführten.

Auch im Bereich der Sozialdienste, der Rettungsdienste oder auch bei Apotheken war diese Anfeindung spürbar. Das wachsende Aggressionspotential der CMG-Szene reichte von Belästigungen der medizinischen Belegschaft wie auch Impfbefürworterinnen und -befürwortern bis zu Sachbeschädigungen, Brandstiftung und Drohungen. Speziell in den sozialen Medien wurden Aufrufe und verbale Drohungen bis hin zu Morddrohungen gegen Politikerinnen und Politiker, Ärztinnen und Ärzte, Bediensteten im Bereich der öffentlichen Sicherheit oder auch Personen, die öffentlich für eine Impfung eintraten oder diese wissenschaftlich unterlegten, feststellbar. Die sozialen Medien wiederum waren die geeignete Plattform für die Kontaktaufnahme der CMG-Szene mit Gleichgesinnten. Eine Steigerung der Eintragungen wie auch der verbalen Drohkulisse spiegelte dies wider.

In einem Fall kam es auch bei Mitarbeiterinnen und Mitarbeitern einer Impfstraße zu kriminellen Handlungen. Diese stempelten mehrere „Blanko-Impfpässe" ab, versahen diese mit einem Chargen-Aufkleber des Impfstoffes und verkauften diese, ohne dass die Impfung durchgeführt wurde. Auch das Computersystem wurde manipuliert, um nicht verabreichte Impfungen eintragen zu können.

In Bezug auf die Medien war ebenfalls eine starke Ablehnung gegen die Informationsdistribution seitens der Presse durch CMG-Agitationen feststellbar, insbesondere in sozialen Netzwerken. Die Anfeindungen reichten von physischen und verbalen Aggressionshandlungen gegen Journalistinnen und Journalisten während der Berichterstattung bei Demonstrationen und Kundgebungen bis hin zu Aufrufen zu Gewalt gegen Redakteurinnen und Redakteuren sowie Redaktionsräumlichkeiten von Medienunternehmen. Diese Drohungen richteten sich teils auch gezielt gegen Personen, deren Namen veröffentlicht wurden. In den sozialen Medien wurde zu Demonstrationen und Abo-Kündigungen aufgerufen. Die Aggressionshandlungen gegenüber der Presse unterstrich auch eine Bombendrohung gegenüber dem ORF in Oberösterreich sowie unterschiedlicher Aktionismus gegenüber diversen ORF-Standorten zu Jahresbeginn. Die Unzufriedenheit innerhalb der CMG-Szene mit der Berichterstattung wurde durch diverse Kundgebungen vor unterschiedlichen ORF-Landesstudios, über das Einschlagen von Fensterscheiben im ORF-Zentrum, Aufrufen zu Cyberangriffen und Aktionismen bei diversen ORF-Standorten bis hin zu einem Drohbrief sowie Terrordrohungen gegen den ORF zu Jahresende weitergeführt.

Im Transportsektor ergaben sich im Jahr 2021 ebenso wie im Vorjahr Herausforderungen mit der Maskenpflicht im öffentlichen Verkehr. Mit der Dauer der Maskentragepflicht wuchs auch die Ablehnung, die sich gegen das Personal der öffentlichen Verkehrseinrichtungen richtete. Die Palette der Vorfälle reichte von verbalen Attacken bis zu körperlichen Angriffen. Auch Passagiere, die auf die Trageverpflichtung aufmerksam machten, gehörten zu den Opfern.

In Bezug auf den Lebensmittelsektor wurde seitens der CMG-Szene in einem offenen Social-Media-Kanal gegen ein Unternehmen zum Boykott aufgerufen. Ursache dafür dürfte die mediale Verlautbarung der Möglichkeit von COVID-19-Schutzimpfungen in bestimmten Filialen dieses Unternehmens gewesen sein.

Aber nicht nur einige Unternehmen der Zivilgesellschaft mussten die steigenden Agitationen feststellen, auch der Staat, vertreten durch die Sicherheitsbehörden und die Hilfs- und Einsatzkräfte, konnte den Anstieg der Ablehnung mit dem steigenden Widerstand bei gleichzeitiger Zunahme der Gewaltbereitschaft wahrnehmen. Das Spektrum reichte von Unmutsäußerungen über zivilen Ungehorsam bis hin zum Widerstand gegen die Staatsgewalt. Darüber hinaus kam es bei einigen teils unangemeldeten beziehungsweise untersagten Demonstrationen und Kundgebungen wiederholt auch zu verletzten Exekutivbeamtinnen und Exekutivbeamten.

4.5.2 Schutzmaßnahmen für kritische Infrastruktureinrichtungen

Im Zusammenhang mit dem Schutz kritischer Infrastrukturen wurden durch die Verfassungsschutzbehörden vorbeugende sowie lage- und situationsangepasste Schutzmaßnahmen gesetzt, um das Funktionieren selbiger zu gewährleisten.

Im Bereich des **Schutzes kritischer Infrastruktur** (SKI) setzten die Verfassungsschutzbehörden folgende Schutzmaßnahmen:

- Sensibilisierungsschreiben an alle Krankenhausbetreiber und Krankenhäuser in Bezug auf die Gefahr durch spontane CMG-Aktionismen in oder im Umfeld von Krankenanstalten.
- Telefonische Beratungsgespräche mit Sicherheitsverantwortlichen der Sektoren Gesundheit, Sozial- und Verteilungssysteme, IKT beziehungsweise Medien, Hilfs- und Einsatzkräfte, Transport und Verkehr in Bezug auf Sensibilisierung der Mitarbeitenden und auf die aktuelle CMG-Gefährdungs- und Demonstrationslage.
- Sensibilisierungsschreiben an den Sektor Sozial- und Verteilungssysteme aufgrund hinweisbezogener abstrakter Möglichkeit von spontanen Aktionismen durch CMG-Aktivisten.
- Maßnahmenempfehlungen für den Gesundheitsbereich (Arztpraxen, Impfstraßen, Ambulanzen, Krankenhäuser etc.)
- Anordnung der verstärkten Bestreifung gefährdeter Unternehmen der Sektoren Gesundheit und IKT.
- Sensibilisierungsgespräche mit Vertretern österreichischer Medien

4.5.3 Ausblick

Im Kontext der öffentlichen Maßnahmen-Diskussion sind weiterhin Proteste der CMG-Szene zu erwarten. Deshalb stellen strafbare Handlungen oder physische Übergriffe weiterhin denkbare Gefährdungsszenarien dar. Dies gilt insbesondere für den Fall, dass künftig wieder Verschärfungen von Corona-Maßnahmen notwendig werden sollten. Eine von Teilen der

CMG-Aktivistinnen und -Aktivisten ausgehende potentielle Gefährdung von obersten Organen und Einrichtungen der kritischen Infrastrukturen sowie von systemrelevanten Unternehmen, die in die „Impfprozesse“ eingebunden sind, ist als realistisch zu bewerten.

5 Akzente im Verfassungsschutz 2021

5.1 Die Gegner der Corona-Maßnahmen und ihre Protestbewegung

Im Zuge der Corona-Pandemie wurden seitens der Bundesregierung zum Schutz der Bevölkerung umfangreiche Maßnahmen beschlossen, um der Ausbreitung und den gesundheitsschädlichen Auswirkungen des Coronavirus entgegenzuwirken. Wie bereits im Jahr 2020 führten diese staatlichen Eingriffe auch 2021 zu einem Protestaufkommen, das sich im Laufe des Jahres auf unterschiedliche Art und Weise manifestierte. Unter dem Deckmantel der Kritik an den Corona-Maßnahmen vermischten sich unterschiedliche Agenden und Motive, die von heterogenen Gruppen getragen und artikuliert wurden.

Dies führte dazu, dass gemäßigte Vertreter der Corona-Proteste in den einschlägigen Social-Media-Kanälen wiederholt mit jenen des radikalen Flügels aneinandergerieten. Dessen ungeachtet fanden aber weiterhin gemeinsame Protestzüge statt, mit dem Ziel, möglichst geschlossen aufzutreten, um eine größere Wahrnehmung in der Mehrheitsbevölkerung zu generieren.

5.1.1 Rückhalt der Corona-Demonstrationen in der österreichischen Bevölkerung

Die im Frühjahr und Herbst 2021 häufig stattgefundenen Corona-Demonstrationen stießen in der österreichischen Bevölkerung mehrheitlich auf keine Zustimmung. So

unterstützten 17 Prozent der österreichischen Bevölkerung die Proteste, 15 Prozent der Befragten gaben an, selbst an solchen teilnehmen zu wollen. 12 Prozent äußerten ihre Bereitschaft, auch an einer nicht angemeldeten Kundgebung teilzunehmen.

In der Gruppe der Corona-Maßnahmen-Gegner ist eine starke wissenschaftskritische bis wissenschaftsfeindliche Einstellung feststellbar. Beinahe 80 Prozent halten das Coronavirus für nicht gefährlicher als eine schwere Grippe und für über 90 Prozent sind in den wissenschaftlichen Beiräten der Regierung die „falschen Expertinnen und Experten" vertreten. Im Zentrum der Kritik der befragten Corona-Maßnahmen-Gegner steht das „unnötige politische Schüren von Ängsten mit Hilfe von nicht notwendigen und verfassungswidrigen Maßnahmen". 70 Prozent fordern eine Gleichstellung von „Schulmedizin" und „Alternativmedizin". Beinahe genauso viele Befragte sind der Meinung, dass die natürlichen Selbstheilungskräfte ausreichen, um das Virus zu bekämpfen. Aus Enttäuschung über die Herangehensweise der Regierung und dem Unverständnis über den wissenschaftlichen Konsens ist eine zunehmende Abwendung vom etablierten System evident, die eine Einfallspforte und einen Anknüpfungspunkt für systemfeindliche extremistische Bewegungen eröffnet.

5.1.2 Die Corona-Protestbewegung im internationalen Vergleich

Auch außerhalb Österreichs war 2021 ein Jahr, das vom Kampf gegen das Coronavirus und seinen Folgen bestimmt war. In zahlreichen europäischen Ländern gingen Menschen auf die Straße, um gegen Maßnahmen zu protestieren, die zur Eindämmung der Pandemie verordnet wurden. Die Motivlage der Corona-Maßnahmen-Gegner war mit jener in Österreich vergleichbar. Auch in anderen Staaten konnte eine Beeinflussung der Protestbewegungen durch rechtsradikale und systemkritische Kräfte beobachtet werden. Ein Katalysator für den Unmut bei den Gegnerinnen und Gegnern jeglicher Maßnahmen war 2021 der „Grüne Pass", der in der zweiten Jahreshälfte in den meisten europäischen Ländern eingeführt wurde. Die Intensität und die Methoden der Proteste selbst unterschieden sich im internationalen Vergleich, wie die folgenden Beispiele veranschaulichen.

Im Juli 2021 kam es zu mehrwöchigen Großdemonstrationen in Frankreich, bei denen mehrere 100.000 Menschen gegen die Maßnahmen und Zugangsbeschränkungen auf die Straße gingen. Die Proteste wurden teilweise auch von Vertreterinnen und Vertretern der Gelbwesten-Bewegung organisiert, was zu einer erhöhten Mobilisierung führte. Im Zuge der Demonstrationen kam es wiederholt zu gewalttätigen Zusammenstößen mit der Polizei. Im französischen Überseegebiet Guadeloupe kam es zu tagelangen Krawallen. Frankreich war sogar gezwungen, Eliteeinheiten der Polizei und Anti-Terroreinheiten nach Guadeloupe zu entsenden.

In Deutschland fanden über das Jahr hinweg in zahlreichen Städten Corona-Proteste statt. Kundgebungen im klassischen Sinn waren im Zuge der Hygienebestimmungen

der Regierung untersagt worden. In Folge wurden neue Protestformen entwickelt, die sich „Spaziergänge“ nannten und als nicht angemeldete Protestzüge durch deutsche Städte führten. Teilweise machten diese gezielt Halt vor Häusern und Wohnungen von Politikerinnen und Politikern. Damit wurde eine neue Stufe der Bedrohung erreicht, die gezielt gegen Vertreterinnen und Vertreter des Staates gerichtet war. Die Zentren der radikalen deutschen Corona-Protestbewegung waren im Jahr 2021 die Bundesländer Thüringen und Sachsen.

In den Niederlanden kam es in der zweiten Hälfte des Jahres 2021 im Zuge von Corona-Protesten zu gewaltsamen Ausschreitungen. Vor allem junge Männer verübten dabei zahlreiche Sachbeschädigungen, Brandstiftungen und Angriffe auf einschreitende Sicherheitsorgane. Der Grund für diese Ausschreitungen war ein angekündigter Teil-Lockdown im November 2021. Auch in Belgien konnten in diesem Zeitraum ähnliche Gewalteskalationen beobachtet werden.

5.1.3 Ausblick auf die weitere Entwicklung der Corona-Proteste

Eine Prognose hinsichtlich der Entwicklung der Pandemie und des damit verbundenen Protestgeschehens ist auf Grund der Vielzahl an Faktoren schwierig. Proteste waren meist eine Reaktion auf eine Aktion des Staates zur Bekämpfung der Pandemie. Mit dem Abklingen der Infektionszahlen wurden auch die Maßnahmen zurückgenommen und damit fehlte es zunehmend an Mobilisierungsgrundlagen für die Veranstalterinnen und Veranstalter von Corona-Protesten. Der „Erfolg“ der systemfeindlichen Gruppierungen, die Corona-Demonstrationen für ihre Zwecke instrumentalisierten, ist, dass Misstrauen gegen etablierte Pfeiler der Gesellschaft und des Staates gesät wurde, das in Teilen der Bevölkerung möglicherweise zu einer länger andauernden Entfremdung von demokratischen Institutionen führen könnte. Das Ziel muss es sein, diese Menschen wieder zurückzuholen und ihnen die Möglichkeit zu bieten, den Staat als vertrauensvollen Akteur wahrzunehmen und nicht als „Feind“, den es zu bekämpfen gilt.

5.2 Antisemitismus in Zeiten der Pandemie

Sätze und Wörter wie „Der Holocaust hat nie stattgefunden“, „9/11 wurde von der US-amerikanischen Regierung inszeniert“, „globale Eliten“ sowie die „Hochfinanz“ kontrollieren die Welt. Verschwörungserzählungen wie diese sind stets präsent und kommen vorwiegend dann zum Einsatz, wenn komplexe gesellschaftspolitische und wirtschaftliche Umbrüche sowie gravierende Veränderungen für die Gesellschaft eintreten, beispielsweise kriegerische Konflikte, Naturkatastrophen, ökonomische Krisen oder Pandemien. Sogenannte Verschwörungsanhänger versuchen das Geschehene alternativ einzuordnen und liefern in der Regel leicht „verständliche“ Erklärungsansätze. Dabei werden multikausale Sachverhalte ausgeblendet und Zufälle ausgeschlossen. Zufälle werden als Teil eines „weltumspannenden Plans“ interpretiert, unter dem Motto:

„Nichts passiere ohne Grund". Dass die Bildung von Verschwörungsmythen und gezielter Desinformation oftmals nahezu in Echtzeit mit Eintritt bedeutender Ereignisse erfolgen, ist darauf zurückzuführen, dass Fakten oder wissenschaftliche Erkenntnisse bewusst ausgeblendet oder antizipativ infrage gestellt werden.

In rechtsextremen Szenen, Bewegungen und Gruppierungen sind Verschwörungserzählungen Teil der ideologischen Kommunikationsstrategie. Festzuhalten ist, dass diese „Theorien" nicht ausschließlich nur von Vertreterinnen und Vertretern oder Aktivistinnen und Aktivisten des rechtsextremen Spektrums verwendet werden. Durch die Nutzung sozialer Medien finden diese zunehmend auch in nicht extremistischen Internet-Diskussionsforen und Online-Plattformen Einzug. Verschwörungserzählungen werden zu einem einfach verständlichen „Erklärungsmodell" nach dem „Freund-Feind-Schema", das „Ungereimtheiten" in ein geschlossenes Weltbild einordnet, Feindbilder bedient und scheinbar attraktiver als die Realität erscheint.

5.2.1 Die Pandemie als Aktivierung antisemitistischer Erklärungsmodelle

Seit dem Ende des Zweiten Weltkriegs erlebten Österreich und große Teile der Welt keine derartig gravierenden Entwicklungen und Ereignisse wie in Zusammenhang mit der gegenwärtigen Corona-Pandemie. Millionen von Erkrankten und Toten weltweit, Gesundheitssysteme unter größten Belastungen, enorme wirtschaftliche Herausforderungen und massive Eingriffe in das Leben der Menschen stellen Politik, staatliche Institutionen und medizinische Einrichtungen vor beispiellose Herausforderungen. Die scheinbar „unsichtbare" Bedrohung stellt mit den einhergehenden hochkomplexen Problemstellungen die perfekte Ausgangslage für die Entstehung und Verbreitung von Verschwörungsmythen dar.

Wie auch schon bei Epidemien beziehungsweise Pandemien in der Vergangenheit, zirkulierten bereits unmittelbar nach Bekanntwerden des Coronavirus antisemitische Verschwörungserzählungen. Von Beginn an wurde die Corona-Krise auch im Ideologiebereich des Rechtsextremismus national und international verstärkt instrumentalisiert.

In vielen konspirativen Modellen werden Szenarien entworfen, wonach mächtige „Strippenzieher" oder die „zionistische Lobby" die internationale Politik lenke und dabei auch biologische Waffen zur vermeintlichen Zielerreichung einsetze. Darüber hinaus werden Behauptungen aufgestellt, dass es das Ziel einer vermeintlich jüdischen Weltverschwörung sei, die Weltbevölkerung zu „versklaven", bis hin zur gezielten „Dezimierung". Ein bekanntes antisemitisches Narrativ, das in der Moderne stets einen zentralen Platz innehatte und nun reaktiviert wird, ist die Vorstellung einer „jüdischen Elite", die sich auch diese Krise zunutze mache. Die Frage nach den „Gewinnern" und

den „Verantwortlichen“ wird von Extremistinnen oder Extremisten rasch beantwortet und propagiert.

Paradoxerweise sehen sich Teile der Corona-Maßnahmen-Gegner und/oder Corona-Leugner als „die neuen Juden“. Der Vergleich mit Holocaust-Opfern stellt eine grobe Verharmlosung des NS-Terrors dar. Die öffentliche Agitation wird für den eigenen „Opferstatus“ („Täter-Opfer-Umkehr“) genutzt und gleichzeitig die nationalsozialistische Vernichtungspolitik trivialisiert. Bei (Protest-)Kundgebungen werden z. B. gelbe „Judensterne“ mit der Aufschrift „Ungeimpft“ getragen oder Slogans wie „Impfen macht frei“, angelehnt an den Schriftzug, „Arbeit macht frei“ am Tor des NS-Konzentrations- und Vernichtungslagers Auschwitz-Birkenau, werden auf Pappschildern skandiert.

Insbesondere im Kontext des Corona-Diskurses sind die Inhalte in den sozialen Medien im Internet sowie in einschlägigen Publikationen vorwiegend durch Generalisierungen, das heißt die triviale Einteilung in „Gut und Böse“, geprägt. Grauzonen werden sukzessive ausgespart. Offizielle Stellungnahmen seitens etablierter Medien, der Wissenschaft und/oder staatlicher Institutionen werden als „unwahr“ deklariert und der vermeintlich „Schuldige“ ist bereits ausgemacht. „Endlich die Wahrheit zu sagen“, gehört zu bewusst provozierten Kampagnen, wie sie häufig von Rechtsextremistinnen und Rechtsextremisten geführt werden. „Alte Feindbilder“ werden bewusst an die aktuelle Situation angepasst und antisemitistische Stereotype tradiert. Beispielhaft kann hier die Dämonisierung exponierter Persönlichkeiten wie George Soros (in rechtsextremen Kreisen wie auch in Verschwörungserzählungen steht der Holocaustüberlebende, Investor und Philanthrop sinnbildlich für den „allmächtigen Juden“, sein Name als „Code“ für „Macht“, „Geld“ und „Einfluss“ von außen) sowie die anhaltende Kritik an der österreichischen Bundesregierung und an „globalen Eliten“ angeführt werden. Letztgenannte seien nämlich die „wahren und eigentlichen Feinde“, welche die „Nationalstaaten und Völker zerstören wollen“. Darüber hinaus wird mit Stichwörtern wie „Corona-Diktatur“ oder „Impfzwang“ gezielt auf gesellschaftlichen Vorurteilen aufgebaut. Vor diesem Hintergrund werden rechtsextreme Positionen kommunikativ anschlussfähig gemacht und für Protestmobilisierungen instrumentalisiert.

5.2.2 Die vielen Krisen und die einfachen Antworten

Von Teilen des rechtsextremen Spektrums wird die Corona-Pandemie als „Beweis“ für die „Theorie“, einer vermeintlich „jüdischen Weltverschwörung“, die nach der „Weltherrschaft“ strebe, angesehen. Aber nicht nur das Coronavirus wird als Narrativ für konspirative Verschwörungsmythen missbraucht. Neben der Flüchtlingsthematik in Österreich und in Europa, werden unter anderem auch kriegerische Konflikte in konspirative Welterklärungsmodelle mit dem Ziel eingebettet, dass all diese Entwicklungen nur einem Zweck dienen: Der Einführung einer „Neuen Weltordnung“. Eine „kleine“ aber „einflussreiche“ Gruppe – häufig in George Soros als „Sündenbock“ personifiziert – wird für ein globales Problem verantwortlich gezeichnet und abermals

zum vermeintlichen „Krisenprofiteur“. Die Formulierungen der einzelnen „Theorien“ sind grundsätzlich ähnlich. Situationsbedingt werden sie allerdings mit „passenden“ Stichwörtern versehen. Beispielsweise wurde im Zuge der Flüchtlingsbewegungen aus dem arabischen Raum nach Europa in den Jahren 2015 und 2016 von Teilen des rechtsextremen Spektrums der Verschwörungsmythos propagiert, dass es sich hierbei um eine vermeintliche „Unterwanderung“ durch den Islam in Europa handle – „gesteuert“ werde diese von „Juden“. Solch bizarre Behauptungen finden nicht nur im extremistischen Spektrum Zuspruch und Verbreitung, sondern aktivieren rechtsextremes Gedankengut, Antisemitismus sowie Fremden- und Islamfeindlichkeit auch bei noch kaum bis schwach ideologisierten und weltanschaulich unbedarften Personenkreisen. Stereotype werden somit tradiert und über Jahrzehnte hinweg als passende Argumentationslinien für alternative „Erklärungsmodelle“ herangezogen.

5.2.3 Antisemitismus als permanente Herausforderung

Das Phänomen Antisemitismus hat sich im Laufe der Geschichte stets entwickelt und es kamen neue Akteurinnen und Akteure sowie Ausdrucksformen zum Vorschein. Allesamt belegen sie, dass es den einen Antisemitismus nicht gibt, sondern, dass Antisemitismus als ideologisches Konstrukt in einer Komplexität vorhanden ist, die sich über ideologische Grenzen hinwegsetzt und die es zu erkennen und zu bekämpfen gilt.

Die in „alternativen Medien“ sowie im Internet und den sozialen Medien offen propagierte antisemitische Hetze, tätliche Angriffe, einschlägige Schmieraktionen beziehungsweise Sachbeschädigungen, (Protest-)Kundgebungen, die durch antisemitisch eingestellte Personen initiiert und organisiert werden, das fremdenfeindliche Meinungsklima oder auch die Zunahme antisemitischer Vorfälle, stellen für jüdische Personen und ihre Einrichtungen einen gesteigerten Risikofaktor dar. Ferner erfahren antisemitische Verschwörungserzählungen nicht nur Zuspruch und Verbreitung, sondern gewinnen an Popularität und Unterstützung bei einem breiten ideologischen Spektrum. Speziell in Zeiten von Krisen und allgemeiner Verunsicherung hat die Frage der Sicherheit an Relevanz und Aktualität gewonnen. Das Mobilisierungspotential antisemitischer Agitationen in Österreich ist gegeben. Im Zentrum der Agitation stehen jede Art von Holocaust-Leugnung und -Relativierung (sekundärer Antisemitismus) sowie der antiisraelische/antizionistische Antisemitismus. Der antiisraelische/antizionistische Antisemitismus negiert das Existenzrecht Israels und diffamiert den jüdischen Staat, indem er Israel einen „Vernichtungskrieg“ (gegen die Palästinenser) und eine Politik der „Ausrottung“ vorwirft. Zudem kann nicht ausgeschlossen werden, dass internationale Trends und Tathandlungen, wie Anschläge auf Synagogen in den USA und Deutschland, Aus- und Rückwirkungen auf die österreichische Extremistenszene haben. Diese Entwicklungen stellen die Sicherheitsbehörden vor neue Herausforderungen, denen mit aller Aufmerksamkeit, Beobachtung und Schärfe entgegen zu treten ist.

5.3 Hybride Bedrohungen – Eine Herausforderung für den Verfassungsschutz

5.3.1 Lagedarstellung und Prognose

Hybride Bedrohungen durch staatliche und nicht staatliche Akteurinnen und Akteure stellen eine ernstzunehmende Bedrohung für Österreich und die EU dar. Verschiedene Akteurinnen und Akteure versuchen durch illegitime Methoden ihren Einfluss in fremden Staaten zu verstärken. Das Vertrauen der Öffentlichkeit in staatliche Institutionen soll untergraben und Staaten sollen destabilisiert werden. Das passiert sowohl durch konventionelle als auch durch unkonventionelle Mittel. Österreich war bislang vor allem von Desinformationskampagnen, wirtschaftlicher Einflussnahme und dem Versuch der Einflussnahme auf bestimmte Diasporagemeinschaften betroffen.

Der Begriff **„Hybrid Threats“** beziehungsweise Hybride Bedrohungen wurde durch den amerikanischen Politikwissenschaftler Frank G. Hoffman geprägt[2]. Dieser beschreibt den Terminus der hybriden Bedrohung als vielgestaltige Vorgehensweise staatlicher und nicht staatlicher Akteurinnen und Akteure im Rahmen einer „ganzheitlichen Kriegsführung“. Diese neue Art der Bedrohung kann am besten mit dem aus dem internationalen Diskurs bekannten Ausdruck „to win the war before the war“ beschrieben werden.

Dazu zählen:

- Cyberangriffe
- Desinformationskampagnen
- Verbreitung von Propaganda in Medien
- Ausübung wirtschaftlichen Drucks
- Terrorismusfinanzierung
- Instrumentalisierung von Migrantinnen und Migranten
- Maßgeschneiderter Gewalteinsatz als äußerstes Mittel (z. B. verdeckte militärische Operationen)

Hybride Akteurinnen und Akteure sind oftmals im Cyberraum zu verorten, da sie durch die weltweit fortschreitende Digitalisierung neue potenzielle Schwachpunkte von Staat, Gesellschaft und Wirtschaft optimal anvisieren können. Im Cyberraum können sie mittels Desinformationskampagnen die öffentliche Meinung beeinflussen, indem sie gezielt Diskussionen in sozialen Netzwerken, bis hin zur Manipulation von Informationen auf diversen Nachrichtenportalen, steuern. Die handelnden Akteurinnen und Akteure agieren

2 Hoffman, Frank G. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, VA: Potomac Institute for Policy Studies, 2007.

in der Regel verdeckt oder bestreiten jegliche Beteiligung. Sowohl Angreifer als auch deren Ziele bleiben unbekannt. Internationale Regelungen werden übergangen, allerdings ohne die Schwelle zum offenen Krieg zu überschreiten. Dieser Graubereich ermöglicht es hybriden Akteurinnen und Akteuren, systemische Schwachpunkte gezielt anzugreifen. Einige Staaten benutzen Desinformationskampagnen gezielt als außenpolitisches Druckmittel. Sie zielen darauf ab, bereits existierende gesellschaftliche Spaltungslinien zu verstärken und zu beeinflussen. Letztlich können auf diese Weise politische Apathie und Verdrossenheit erzeugt und Wahlergebnisse derart beeinflusst werden, dass politische Entscheidungsträgerinnen und Entscheidungsträger destabilisiert und delegitimiert werden. Der gesellschaftliche Zusammenhalt soll zerstört und falsche Entschlüsse und Reaktionen forciert werden. In der Regel werden Informationen aus dem Kontext gerissen, verkürzt dargestellt oder mit Fakten vermischt, wodurch sich das Erkennen von solchen Falschinformationen als äußerst schwierig gestalten kann.

Offene und pluralistische Staaten wie Österreich sind im Gegensatz zu autokratischen Staaten anfälliger für hybride Bedrohungen, da sie die Gesellschaft nicht in derselben Art und Weise kontrollieren. Politische Entscheidungen können dazu führen, dass sich Teile der Bevölkerung als Verlierer sehen. In Demokratien wie Österreich kann dies von staatlichen und nicht staatlichen Akteurinnen und Akteuren als Ankerpunkt für hybride Strategien genutzt werden, um solche Stimmungen aufzugreifen und weiter zu befeuern. Deshalb ist es entscheidend, das dynamische und facettenreiche Wesen von hybriden Strategien bestmöglich zu verstehen, um die verschleierten Erscheinungsformen bereits frühzeitig erkennen zu können.

5.3.2 Erkennen von Desinformationskampagnen

Immer mehr Menschen informieren sich primär oder ausschließlich im Internet – vorrangig in sozialen Medien. Im Cyberraum gestaltet es sich jedoch oftmals äußerst schwierig desinformierende Inhalte zu identifizieren, zumal hybride Akteurinnen und Akteure mitunter ein hohes Maß an Professionalität an den Tag legen und ihre Instrumente fortwährend analysieren und anpassen. Die COVID-19-Pandemie dient hierbei als Paradebeispiel, wie Menschen verunsichert und Staaten durch Desinformationskampagnen unter Druck gesetzt werden können.

Das frühzeitige Erkennen von Desinformation stellt daher eine zentrale Herausforderung für Österreich dar. Durch einen präventiven Ansatz und das kritische Hinterfragen von Informationen kann das Bewusstsein der Bevölkerung für das Vorhandensein von Desinformationskampagnen erhöht und geschärft werden. Im Bundeskriminalamt wurde zudem eine Ansprechstelle eingerichtet, um rasch auf Desinformationskampagnen reagieren zu können.

Zentrale Fragen im Umgang mit Informationen:

- Woher kommt die Information?
- Wo ist sie veröffentlicht?
- Welche Form hat die Information?
- Wer ist der Verfasser der Information?
- Wie wird der Inhalt präsentiert?

Das Erkennen dieser komplexen, oft indirekten und im Verborgenen ablaufenden Aktionen stellt für die betroffenen Staaten eine große Herausforderung dar. Eine mögliche Antwort auf hybride Bedrohungen ist die Stärkung der gesamtstaatlichen und internationalen Resilienz. Dabei werden die eigenen Schwächen holistisch analysiert beziehungsweise beurteilt und durch verschiedene Strategien die Widerstandsfähigkeit der Bevölkerung erhöht. Österreich arbeitet eng mit internationalen Partnern wie dem „Zentrum gegen hybride Bedrohungen“ in Helsinki zusammen, um hybriden Bedrohungen möglichst umfassend und wirksam begegnen zu können.

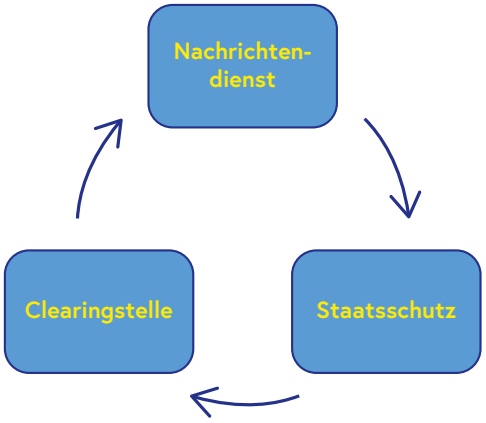
5.4 Prävention durch Information und Kooperation

Extremistische Ideologien jeglicher Form gelten nach wie vor als eine große Bedrohung für die Sicherheit in Österreich. Präventionsarbeit kann hier ein effektives Instrument zur Verhinderung und Vorbeugung von Extremismus sein, sofern eine gezielte und frühzeitige Maßnahmensetzung erfolgt.

Eine zentrale Aufgabe der Verfassungsschutzbehörden liegt demnach im Bereich der Prävention.

In der Präventionsarbeit der Sicherheitsbehörde ist im Umgang mit Extremismus und Radikalisierung die Anwendung eines kooperativen gesamtstaatlichen und gesamtgesellschaftlichen Sicherheitsansatzes wesentlich.

Prävention in der DSN hat die Aufgaben, Wissen zu generieren, Wissen zu teilen und Wissen zu vermitteln, weshalb die Präventionsarbeit in allen Bereichen der Behördenstruktur verankert wurde.



Der Fokus liegt dabei auf Sensibilisierungsmaßnahmen, dem konsequenten Auf- und Ausbau von präventiven Strukturen zur Vernetzung, der Steuerung und Förderung einer koordinierten Zusammenarbeit, Präventionsmaßnahmen zur Förderung der Deradikalisierung sowie einer standardisierten österreichweit koordinierten staatspolizeilichen Präventionsarbeit.

5.4.1 Prävention im Bereich Nachrichtendienst

Die Prävention im Bereich Nachrichtendienst erarbeitet im Kontext der präventiven Aufgabe der Gefahrenerforschung unter Anwendung multiprofessioneller Unterstützungssysteme, insbesondere durch Wissenschaft und Forschung, strategische Konzepte und Handlungsempfehlungen zur Prävention, Deradikalisierung und zum Wirtschaftsschutz.

Ziel ist es, die von extremistischen Ideologien ausgehenden Risiken zu verringern und damit einhergehend eine Steigerung des subjektiven Sicherheitsgefühls innerhalb der österreichischen Gesellschaft zu erreichen.

Die grundsätzlichen Aufgaben der Prävention im Bereich Nachrichtendienst sind einerseits

- der systematische Aus- und Aufbau von gesamtgesellschaftlichen Vernetzungsstrukturen und
- die vernetzte Zusammenarbeit mit Wissenschaft, Forschung und Entwicklung

sowie andererseits

- die Identifikation von notwendigen Präventionshandlungsfeldern,
- strategische Überlegungen zum Setzen von geeigneten und verhältnismäßigen Maßnahmen,
- das frühzeitige Erkennen von Radikalisierungsentwicklungen im Bundesgebiet und
- Transparenz und Bürgernähe durch das mobile Präventionsteam.

In der strategischen Präventionsarbeit bedient sich die DSN entsprechender Koordinierungsstrukturen und Gremien, um bestmöglich zu gewährleisten, dass der erforderliche gesamtstaatliche, gesamtgesellschaftliche und kooperative Sicherheitsansatz erfüllt wird. Nur so kann es gelingen, ganzheitliche Maßnahmen mit möglichst hoher Wirkung zu setzen.

Mit dem BNED wurde bereits im Jahr 2017 erfolgreich eine gesamtstaatliche und gesamtgesellschaftliche Koordinierungsstruktur etabliert, die in Zukunft noch weiter ausgebaut werden soll. Dabei werden strategische Handlungsempfehlungen sowie Präventionsmaterialien durch Expertinnen und Experten erarbeitet. Darüber hinaus ist eine wissenschaftliche Begleitung möglich, die anlassbezogen genutzt wird.

Für den weiteren Ausbau der strategischen Präventionsarbeit der DSN ist es unerlässlich, einen erweiterten Wissenstransfer mit Wissenschaft und Forschung, mit der Zivilgesellschaft sowie mit Expertinnen und Experten zu etablieren. Ziel ist es, in der sicherheitsbehördlichen Maßnahmensetzung im Präventionsbereich eine laufend begleitende Analyse aus möglichst umfassender Perspektive zu implementieren und damit eine Erweiterung um wissenschaftliche und praxistaugliche Ansätze mit größtmöglicher Wirkung zu erreichen.

5.4.2 Clearingstelle Deradikalisierung

Die im Dezember 2021 mit Einrichtung der DSN etablierte Clearingstelle Deradikalisierung, angesiedelt im Gemeinsamen Informations- und Lagezentrum (GILZ) der DSN, fungiert zur Gewährleistung eines effektiven Gefährdermanagements als zentrale Koordinations- und Steuerungsstelle innerhalb der Organisation und arbeitet in enger Kooperation mit der strategischen Prävention im Nachrichtendienst sowie der Staatsschutzprävention.

Im Rahmen des Gefährdermanagements agiert die Clearingstelle als Kommunikationsschnittstelle zwischen anderen Behörden (z. B. der Koordinationsstelle für Extremismusprävention und Deradikalisierung im Straf- und Maßnahmenvollzug des Bundesministeriums für Justiz) und dem Staatsschutz sowie dem Nachrichtendienst. Darüber hinaus koordiniert die Clearingstelle Fallkonferenzen gem. § 6a SNG, unterstützt interne Fallkonferenzen mittels Informationsbeschaffung und teilt das Wissen, das im Rahmen dieser Konferenzen generiert wird, mit den Leitungsgremien der DSN.

Die Clearingstelle Deradikalisierung administriert zudem das im Jahr 2020 initiierte Aussteiger- und Deradikalisierungsprogramm KOMPASS und arbeitet laufend an der Entwicklung neuer Präventionsprojekte, vor allem im Bereich der Primärprävention.

5.4.3 Prävention im Bereich Staatsschutz

Mit der Trennung der Bereiche Staatsschutz und Nachrichtendienst in der DSN wurde die Prävention auch direkt im Staatsschutz implementiert. Ein wesentliches Ziel der Prävention

im Staatsschutz ist die Förderung der Bereitschaft und Fähigkeit des Einzelnen, sich über eine Bedrohung seiner Rechtsgüter Kenntnis zu verschaffen und Angriffen entsprechend vorzubeugen. Die operative Staatsschutzprävention soll dabei als zentrale Anlaufstelle für Aus- und Fortbildungen innerhalb der Behörde und in weiterer Folge auch innerhalb des Bundesministeriums für Inneres im Themenschwerpunkt Extremismusprävention fungieren. Eine standardisierte, österreichweit koordinierte Ausbildung von Präventionsbeamtinnen und Präventionsbeamten im Bereich Extremismusprävention stellt eine der wichtigsten Maßnahmen bei der Umsetzung einer effizienten und effektiven staatspolizeilichen Präventionsarbeit dar. Ausgebildete Präventionsbeamtinnen und Präventionsbeamte sollen österreichweit in unterschiedlichen Formaten die Zielgruppe der Jugendlichen direkt im schulischen und indirekt im außerschulischen Kontext erreichen und als Ansprechpartnerinnen und Ansprechpartner für Gemeinden, Bürgermeister, Organisationen und Unternehmen zur Verfügung stehen.

Für die hochwertige Umsetzung der Präventionsarbeit ist eine enge Abstimmung der drei Präventionsstellen in der DSN wesentlich. Dies ermöglicht ein schnelles und vor allem zielgerichtetes Vorgehen zur gemeinsamen Lösungsfindung.

5.5 Wirtschaftsschutz als neuer Schwerpunkt der Prävention im Aufgabenbereich Nachrichtendienst der DSN

Als Wirtschaftsspionage wird im Allgemeinen die staatlich gelenkte oder gestützte Aufklärung und Ausforschung von Unternehmen durch Nachrichten- und Geheimdienste fremder Staaten in Österreich verstanden. Etwas anders verhält es sich bei der Industriespionage. Hier spähen sich in der Regel konkurrierende Unternehmen gegenseitig aus, um Wettbewerbsvorteile und/oder Know-how zu erlangen.

Das Jahr 2021 stand auch im Bereich der Wirtschafts- und Industriespionage unter dem Eindruck der Pandemie. Die Entwicklung, Produktion und Logistik beim Vertrieb von Impfstoffen und Medikamenten weckte beispielsweise das Interesse unterschiedlicher Staaten.

Für die neu eingerichtete DSN ist vor allem der Schutz der heimischen Wirtschaft vor Wirtschaftsspionage ein Schwerpunkt in der Prävention. Dabei unterscheiden sich die nachrichtendienstlichen Aktivitäten fremder Staaten in Österreich nach den jeweiligen strategischen und wirtschaftspolitischen Zielen dieser Länder.

Es kann grundsätzlich zwischen klassischer Wirtschaftsspionage und der Spionage zum Zweck einer Sanktionsumgehung unterschieden werden.

Vor allem die zweite Ausprägung hat aufgrund geopolitischer Entwicklungen und zwischenstaatlicher Konflikte das Potenzial, im Jahr 2022 verstärkt in den Fokus ausländischer Dienste zu geraten.

5.5.1 Wirtschaftsspionage 4.0

Wirtschaftsspionage durch ausländische Dienste sowie die Konkurrenzausspähung im staatlichen Interesse erlebten in den letzten Jahren eine kontinuierliche Veränderung.

Die „klassische" Wirtschaftsspionage vermengt sich immer mehr mit dem Wissensabfluss über IT-Systeme, wobei sich ausländische Nachrichtendienste unterschiedliche Ansätze zunutze machen. Einerseits werden Informationen durch das Abhören von unzureichend verschlüsselten Netzwerkprotokollen, etwa durch überwachte Internet Exchange-Knotenpunkte, mitgelesen. Andererseits kann der Wissensabfluss von heimischen Unternehmen aber auch durch zielgerichtete Einbrüche in deren IT-Systeme erfolgen, die entweder durch ausländische Nachrichtendienste selbst durchgeführt oder von (halb-) staatlichen oder anderen Akteurinnen und Akteuren an kriminelle Hackergruppierungen in Auftrag gegeben werden.

Die althergebrachte Anwerbung von Informanten in Unternehmen ist nach wie vor ein Modus Operandi ausländischer Nachrichtendienste. Doch auch die Anwerbung von menschlichen Quellen in Unternehmen hat sich in den letzten Jahren durch den technologischen Fortschritt verändert. Diverse Beispiele zeigen, dass bei der Anbahnung eines Kontakts zwischen einem ausländischen Nachrichtendienst und einem Unternehmen von den Angreifern oftmals soziale Netzwerke genutzt werden. Vor allem Karriereportale, auf denen sich die Mitarbeiterinnen und Mitarbeiter eines Unternehmens präsentieren, sind ein beliebtes Mittel zur Auskundschaftung von Unternehmen. Es ist evident, dass bei „weichen Zielen", das heißt Mitarbeiterinnen und Mitarbeiter, ansetzende Spionageaktivitäten oftmals zu umfassenden und umfangreichen Informationsgewinnen betreffend Kompetenzen, Strukturen und Zielen von Unternehmen führen.

Oftmals sind es Mitarbeiterinnen und Mitarbeiter von Unternehmen, die aus unterschiedlichen Beweggründen zu Innentäterinnen und Innentätern werden. Für diverse Gegenleistungen werden ausländische Dienste mit Know-how aus dem Unternehmen versorgt. Dabei muss es sich nicht zwangsläufig nur um Patente, Technologien oder Produkte des Unternehmens handeln. Preislisten, Kundendaten und Unternehmensstrategien können bei internationalen Ausschreibungen das Interesse ausländischer Dienste wecken. Durch die Abschöpfung dieser strategischen Informationen sollen Wettbewerbsvorteile für ausländische Konkurrenten geschaffen werden.

5.5.2 Wirtschaftsschutz als ein Schwerpunkt der nachrichtendienstlichen Präventionsarbeit

Vorgänge der Wirtschafts- und Industriespionage stehen zwar nicht im Blickpunkt des medialen Interesses, können aber schwerwiegende Folgen für die betroffenen Unternehmen und die Volkswirtschaft Österreichs nach sich ziehen.

Ausländische Nachrichten- und Geheimdienste sind kreativ bei der Erreichung ihrer Ziele. Oftmals wird es den Angreiferinnen und Angreifern jedoch zu leicht gemacht. Schon einfache Sicherheitsmaßnahmen können eine nachhaltige Wirkung erzielen. Cybersicherheit ist in der gegenwärtigen Lage eine unumgängliche Notwendigkeit bei der Abwehr von Angriffen auf Unternehmen. Ein Präventionskonzept kann bei Regelungen für die private Nutzung dienstlicher Geräte beginnen. Gleichzeitig können Mitarbeiterinnen und Mitarbeiter, die Zugang zu sensiblen Informationen haben, zum Ziel ausländischer Dienste werden. In diesem Bereich der Prävention von Wirtschafts- und Industriespionage setzen die Bemühungen der DSN zum Wirtschaftsschutz an – die Bedrohung für die heimische Wirtschaft in Zeiten des Wandels in Europa wurde erkannt und die Verfassungsschutzbehörden forcieren daher die präventiven Bemühungen zum Schutz des Wirtschafts- und Forschungsstandortes Österreich.

Bundesministerium
Inneres

Direktion Staatsschutz
und Nachrichtendienst

Treten Sie mit der DSN in Kontakt

Wenn Sie Risiken für Ihr Unternehmen erkennen, steht Ihnen die Direktion Staatsschutz und Nachrichtendienst als kompetenter und vertrauenswürdiger Ansprechpartner zur Verfügung.

- Kontaktieren Sie uns unter wirtschaftsschutz@dsn.gv.at
- Die Beratung ist kostenlos, wird vertraulich durchgeführt und erfolgt vor Ort in Ihrem Unternehmen

5.6 Cyber: Mobile Device Security und Pegasus

5.6.1 Überblick

Unter der Bezeichnung „Pegasus“ wurde eine Spionagesoftware eines israelischen Anbieters der breiten Öffentlichkeit bekannt. In den letzten Jahren häuften sich Berichte über die genannte Software, als festgestellt wurde, dass diese oftmals gegen Journalistinnen und Journalisten, Politikerinnen und Politiker sowie Aktivistinnen und Aktivisten, zum Einsatz gebracht wurde. Ursprünglich als ein Mittel für Ermittlungsbehörden zur Aufklärung und

Ermittlung in Fällen der Schwerkriminalität sowie Terrorismus vermarktet, wurde die Software in vielen Fällen für andere Zwecke missbraucht.

Pegasus zeichnet sich nicht nur durch die Wahl der auf einer Vielzahl von Endgeräten verfügbaren Infektionswege aus, sondern auch durch die technische Finesse, die von den Entwicklerinnen und Entwicklern an den Tag gelegt wurde, um die Infektion vor den nichtsahnenden Opfern zu verbergen. Für eine erfolgreiche Infektion reicht teilweise bereits der Empfang einer manipulierten Nachricht ohne das Zutun des Benutzers (Zero-Click). In weiterer Folge setzt sich Pegasus auf den mobilen Endgeräten der Opfer fest, indem bis dahin nicht öffentlich bekannte Schwachstellen in der Software des Betriebssystems beziehungsweise von verbreiteten Anwendungen ausgenutzt werden. Neben dem Ausspionieren von Kommunikationsdaten sowie lokal am System gespeicherten Dateien erlaubt Pegasus nach neuen Analyseerkenntnissen auch den Zugriff auf Cloud-Services im Namen des Opfers.

Selbst ein Neustart des Systems, oft als ein Mittel der Wahl gegen Schadsoftware angeführt, war gegen Pegasus wirkungslos. Die Spionagesoftware täuschte den Nutzerinnen und Nutzern eine Abschaltung des Endgerätes vor, dieses wurde jedoch nie wirklich ausgeschaltet. Da mobile Endgeräte heutzutage technisch überwiegend so gebaut sind, dass die jeweilige Stromquelle, das heißt der Akku, nicht entfernt werden kann, war ein Ausschalten maximal möglich, wenn der Akku aufgrund von Entladung selbst eine Deaktivierung des Endgerätes vornahm. Aber selbst nach diesem Vorgang wurde Pegasus, das sich mittlerweile tief im System festgesetzt hatte, mit dem Systemstart neu gestartet.

Eine Infektion ist für Endbenutzerinnen und Endbenutzer nur über einen komplizierten technischen Aufwand erkennbar. Das Forschungslabor Citizen Lab hat in Verbindung mit Amnesty International hierfür das Mobile Verification Toolkit (MVT) geschaffen, das eine mögliche Infektion anhand der Analyse eines Backups mit Indicators of Compromise (IOC) feststellen kann. Dafür ist es jedoch notwendig, ein verschlüsseltes lokales Backup des jeweiligen Endgerätes zu erstellen und dieses mittels MVT auf eine Infektion überprüfen zu lassen.

> *„This and all previous investigations demonstrate how attacks against mobile devices are a significant threat to civil society globally. The difficulty to not only prevent, but posthumously detect attacks is the result of an unsustainable asymmetry between the capabilities readily available to attackers and the inadequate protections that individuals at risk enjoy.“*
>
> (Amnesty – Forensic Methodology Report: How to catch NSO Group's Pegasus)

Die erwähnten Organisationen waren es auch, die in Verbindung mit Investigativ-journalistinnen und -journalisten ab Juli 2021 mit einer groß angelegten Recherche, im Zuge derer tausende Telefonnummern ausgewertet wurden, die mediale Berichterstattung über die Verwendung und Vorgänge rund um die Spionagesoftware Pegasus anstießen. In der Folge werden bis heute immer wieder Opfer der Spionagesoftware bekannt, die sich teilweise bis in höchste politische Kreise diverser Staaten ziehen. Die NSO Group, die für Pegasus verantwortlich zeichnet, bestritt jedoch immer den Einsatz ihrer Software für unlautere Zwecke und gab an, nicht flächendeckend prüfen zu können, wofür ihre Software eingesetzt würde. Es komme lediglich zu stichprobenartigen Untersuchungen. Sollte dabei etwas aus ihrer Sicht Illegales festgestellt werden, werde die Benutzung der Software für die Urheberin beziehungsweise den Urheber eingeschränkt.

Diese Art der modernen Überwachung stellt Politik, Verwaltung und Zivilgesellschaft vor ein enormes Sicherheitsproblem.

5.6.2 Das mobile Sicherheitsproblem

Mobile Endgeräte sind für jegliche Aufgaben im Alltag ein konstanter Begleiter und fungieren als eines der wichtigsten Kommunikationsmittel. Telefonate, Videokonferenzen, Textnachrichten und E-Mails werden über permanent mitgeführte Mobiltelefone getätigt beziehungsweise abgerufen. Eine Überwachung dieses Geräts gestattet jedes Gespräch und jede Nachricht aufzuzeichnen, als auch mit jedem Schritt eine positionsgenaue Verfolgung der Wege und des jeweiligen Standortes von Benutzerinnen und Benutzern zu ermöglichen. Werden die erwähnten Faktoren mit netzwerktheoretischen Konzepten in Übereinstimmung gebracht, lässt sich auf diese Art nicht nur das infizierte Gerät, sondern ein potentiell größerer Personenkreis überwachen beziehungsweise nachverfolgen. Bestätigt wird diese Theorie durch die Rollen der bekanntgewordenen Opfer sowie die entdeckten Sekundärinfektionen auf Geräten von Kontaktpersonen, wie auch im Fall des in Istanbul ermordeten Washington Post Journalisten Jamal Khashoggi.

Anders als bei klassischen IT-Systemen befinden sich mobile Endgeräte meist nicht hinter mehreren Verteidigungslinien (Firewalls, Netzwerksegmente, VPN-Lösungen) und kommunizieren über teils nicht überwachbare Schnittstellen mit der Außenwelt. Ein Beispiel zur Verdeutlichung dieses Problems ist die von Pegasus ausgenützte Schwachstelle in WhatsApp. Der WhatsApp-Client kommuniziert direkt über die WhatsApp-Server und entzieht sich damit einer Überwachung des Verkehrs, wie es im Gegensatz zu beispielsweise Web-Browsern durch den Einsatz von Proxylösungen möglich wäre. Dieser „Blackbox"-Ansatz macht es Verteidigern schwer, den Datenverkehr auf verdächtige Aktivitäten zu überprüfen.

Grundsätzlich existieren auf mobilen Systemen mittlerweile effektive Sicherheitsmechanismen wie ein ausgeklügeltes Berechtigungsmanagement und eine Isolation verschiedener Apps im Speicher und voneinander. Zudem stehen eigene

Sicherheitscontainer zur Schaffung eines eigenen Bereiches für sensible Daten zur Verfügung. Dem gegenüber stehen allerdings einige wenige „Monokulturen“ an mobilen Plattformen, welche aufgrund ihrer Beschaffenheit die Effektivität der erwähnten Maßnahmen schmälern, was die Attraktivität für Angreifer ungleich erhöht. Beispielweise wurde die proprietäre Chatlösung „iMessage“ schon oftmals als Angriffsvektor verwendet, da diese Applikation standardmäßig auf allen iPhones vorinstalliert ist und die Wahrscheinlichkeit daher groß ist, diese auf dem iOS-Zielgerät als Infektionsvektor vorzufinden.

Hinzu kommt in vielen Fällen eine nachlässige Versorgung von Geräten mit Sicherheitsupdates durch die Hersteller. Einerseits werden durch den Innovationsdruck Geräte oftmals vorzeitig auf den Markt gebracht und erst durch die Nachlieferung von Software- und Sicherheitsupdates dem Prozess der Reifung bei der Kundin und dem Kunden ausgesetzt. Andererseits beginnt mit der Vermarktung des einen bereits die Arbeit an einem neuen Produkt und damit die Umschichtung von Ressourcen innerhalb des Unternehmens. Da der marktwirtschaftliche Erfolg durch den Umsatz getragen wird, werden Geräte oft nach kurzer Zeit nicht mehr mit Updates unterstützt, was Kundinnen und Kunden zum Wechsel auf die neuen Geräte motivieren soll.

Ein weiteres potenzielles Sicherheitsproblem stellen bisher unbekannte Schwachstellen, sogenannte Zero-Days, dar. Informationen über angreifbare Schwachstellen werden teilweise in Millionenhöhe gehandelt. Dementsprechend lukrativ ist der Markt für daran beteiligte Unternehmen, aber auch für Einzelpersonen mit speziellen Fähigkeiten und Kenntnissen. Dem gegenüber sehen sich die Verteidiger mit einer Vielzahl an Soft- und Hardwarelösungen konfrontiert, die es abzusichern gilt, die eben diese Schwachstellen enthalten können. Verdeutlicht wird dies durch den vielzitierten Umstand, dass Angreifer nur einmal, Verteidiger jedoch jedes Mal erfolgreich sein müssen (Defender‘s Dilemma). Das heißt, dass früher oder später ein Angriff erfolgreich sein wird, je nach Ressourcen und Motivation der Angreifer. Folglich ist es essentiell, die Resilienz zu stärken und die Formulierung von klaren und robusten Prozessen zu forcieren, durch die im Ernstfall Schäden begrenzt werden können.

Wie erwähnt sind verglichen mit klassischen IT-Systemen die Verteidigungsmöglichkeiten bei mobilen Endgeräten wesentlich eingeschränkt. Nichtdestotrotz sollten klassische Absicherungsmaßnahmen implementiert werden:

- Netzwerkkommunikation sollte sofern möglich über gesicherte Schnittstellen erfolgen
- Analyse von Gerätelogdateien
- Mobile-Device-Management-Sicherheitslösungen
- Schaffung von Bewusstsein bei Benutzerinnen und Benutzern über aktuelle Bedrohungen

Im Umgang mit gegenwärtigen und künftigen Bedrohungen, wie auch Pegasus, helfen nur der eigenverantwortliche Umgang mit Technik, die entsprechende Awareness sowie die Ressource Mensch als letzte Verteidigungslinie.

5.6.3 Resümee

Anhand der Spionagesoftware Pegasus wurde stellvertretend dargestellt, mit welch komplexen Sicherheitsthemen Regierungen, Verwaltungen, Organisationen aber auch Einzelpersonen im modernen Alltag außerhalb rechtsstaatlicher Prozesse konfrontiert sind. Es sei allerdings darauf hingewiesen, dass neben Pegasus noch diverse andere Anbieter kommerzieller Überwachungssoftware existieren, und somit davon auszugehen ist, dass Pegasus nur die Spitze des Eisbergs darstellt. Die zunehmende technische Komplexität sowie die Anzahl und die Möglichkeiten für Angriffe auf elektronische Systeme steigen exponentiell. Durch die komplexe sicherheitspolitische Lage ist davon auszugehen, dass diese Angriffe weiterhin anhalten beziehungsweise steigen werden. Dies fordert ein entsprechend hohes technisches Niveau der Abwehrmechanismen, aber auch Awareness seitens der Benutzerinnen und Benutzer von elektronischen Endgeräten. Gleichzeitig ist es wichtig, entsprechende Prozesse definiert und umgesetzt zu haben, die eine umfassende Bedrohungsanalyse ermöglichen und Angriffe im Idealfall antizipieren können. Dies wiederrum erfordert entsprechende Ressourcen, die der Bedrohungslage angepasst sind und ständig weiterentwickelt werden. Hier ist besonders der Faktor Mensch zu betonen, da Spezialistinnen und Spezialisten eine knappe Ressource darstellen. Und während Hard- und Softwarelösungen mit entsprechendem Mitteleinsatz auch kurzfristig angeschafft werden können, erfordert die Ressource Mensch einen langfristig ausgerichteten sowie nachhaltigen Ansatz. In der Krise kann nur auf Personal zurückgegriffen werden, das vorhanden und entsprechend ausgebildet ist sowie Erfahrungen und Expertise zu kombinieren vermag.