Bundesministerium
Inneres

Bundesamt für Verfassungsschutz
und Terrorismusbekämpfung

Verfassungsschutzbericht 2020

Verfassungsschutzbericht 2020

Wien 2021

Impressum

Medieninhaber:
Bundesministerium für Inneres
Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT)
1010 Wien, Herrengasse 7
+43 1 531 26-0
einlaufstelle@bmi.gv.at
www.bmi.gv.at

Gestaltung:
Abteilung I/5/b - Kreation und Newsroom

Hersteller:
Digitalprintcenter des BMI
1010 Wien, Herrengasse 7

Inhalt

Sehr geehrte Leserinnen und Leser!

Der vorliegende Verfassungsschutzbericht ist ein Rückblick auf das Kalenderjahr 2020. Ein Jahr, das geprägt war von der Corona-Pandemie und ihren massiven Auswirkungen auf unser wirtschaftliches und gesellschaftliches Zusammenleben. Eine Pandemie, die auch die Arbeit des Verfassungsschutzes maßgeblich beeinflusst hat und leider zu einer Radikalisierung an den extremen Rändern unserer Gesellschaft geführt hat. Diesen neuartigen Herausforderungen und den damit verbundenen Veränderungen wird in einem separaten Kapitel besonderes Augenmerk geschenkt.

Bundesminister
Karl Nehammer, MSc
© BKA / Andy Wenzel

Wie Konflikte aus fremden Staaten nach Österreich hereingetragen werden, haben die gewalttätigen Versammlungen im Juni 2020 in Wien-Favoriten klar aufgezeigt. Das ist eine Entwicklung, vor der wir unsere Augen nicht verschließen dürfen – weder vor offen ausgetragener Gewalt auf unseren Straßen noch vor dem Versuch der bewussten und gezielten Einschüchterung von in Österreich lebenden Menschen. Gerade hier sind der demokratische Rechtsstaat und seine Schutzmechanismen mehr gefordert denn je.

Der Terroranschlag vom 2. November 2020, dem vier Menschenleben zum Opfer fielen, hat uns die Gefahren aufgezeigt, die vom islamistischen Terror ausgehen. Der islamistische Terror ist gegenwärtig wohl die größte extremistische Bedrohung für die europäischen Staaten.

Dieser heimtückische Anschlag hat auch die Arbeit des Verfassungsschutzes in Frage gestellt. Eine umgehend eingesetzte Untersuchungskommission hat die Vorgänge im Vorfeld des Anschlages untersucht und ihre Ergebnisse in zwei umfassenden Berichten vorgelegt.

Gegenwärtig befindet sich die Reform des Verfassungsschutzes bereits in der Phase der Umsetzung. Eine Reform, die seit Februar 2020 im Rekordtempo ausgearbeitet und umgesetzt worden ist. Mit 1. Dezember 2021 wird die „Direktion Staatsschutz und Nachrichtendienst“ (DSN) ihre Arbeit aufnehmen. Erstmals wird Österreich auch über einen Nachrichtendienst verfügen, der Entwicklungen antizipieren und ein wirkungsvolles Schutzschild für unser Land darstellen wird.

Auch der Verfassungsschutzbericht wird durch diese Neustrukturierung einer Evaluierung unterzogen. Er wird daher im kommenden Jahr in anderer, neu strukturierter Form vorliegen und dem berechtigen Interesse an valider Information noch mehr Rechnung tragen.

Karl Nehammer
Bundesminister für Inneres

1 Allgemeines Lagebild

Phänomen Islamistischer Extremismus und Terrorismus

Lagebild

Am Abend des 2. November 2020 kam es zu einem Terroranschlag in Wien, bei dem mit rund 80 Schüssen aus zwei Schusswaffen insgesamt vier Menschen getötet und zahlreiche weitere Personen verletzt wurden. Der 20-jährige Täter, ein österreichischer Staatsbürger mit nordmazedonischen Wurzeln, hatte sich zuvor in Sympathisantenkreisen der terroristischen Organisation „Islamischer Staat" (IS) bewegt und Kontakt zum Milieu der prinzipiell ausreisewilligen Jihadisten der sogenannten „Foreign Terrorist Fighters" (FTF) gehabt. Der Anschlag war kein alleinstehendes Ereignis, sondern folgt der strategischen Logik jihadistischer Terroristen, durch Anschläge einen Zustand der permanenten Einschüchterung zu schaffen.[1]

Bis zum Datum des Anschlages zählte Österreich EU-weit zwar nicht zu den am stärksten durch einen terroristischen Anschlag gefährdeten Ländern, wohl aber zu jenen Ländern mit einer, an der Einwohnerzahl gemessenen, überproportional hohen Anzahl an FTF (wie auch verhinderter Ausreisenden). Damit stellte der islamistische Extremismus auch im Berichtsjahr 2020 eine anhaltende und hohe Bedrohung für Österreich dar. Dazu trugen – wie in den vorangegangenen Berichtszeiträumen – primär salafistische bzw. jihadistische Akteure bei, die maßgeblich die Entwicklungen in diesem Phänomenbereich beeinflussten. In ideologischer Hinsicht besteht unverändert starke Anziehungskraft, was auch weiterhin für Mobilisierung und Zulauf sorgt. Dazu tragen auch politische Konflikte im Nahen und Mittleren Osten sowie in Nordafrika bei. Geschickte propagandistische Überhöhung und Instrumentalisierung von Konflikten islamistischer Akteure gegen die herrschende Ordnung in einigen der Staaten der Region erweisen sich dabei unverändert als ein starker Faktor der Mobilisierung innerhalb dieses Phänomenbereiches.

Maßnahmen gegen islamistische Radikalisierung und nachhaltiger Schutz des demokratischen Prinzips

Am 9. November 2020 kam es an mehreren Orten im Bundesgebiet zu großflächigen Hausdurchsuchungen in solchen Einrichtungen und bei Einzelpersonen, die im Verdacht stehen, im Bereich des legalistischen Islamismus[2] in Österreich aktiv zu sein und der Muslimbruderschaft nahezustehen. Bei dieser handelt es sich um die älteste und

---

1 Aufgrund der zum Berichtszeitpunkt noch laufenden Ermittlungen wird von einer genaueren Darstellung des Tathergangs und Tathintergrunds abgesehen und auf den Abschlussbericht der Untersuchungskommission verwiesen. Siehe www.bmi.gv.at/downloads/Endbericht.pdf (zuletzt abgerufen 09.07.2021).

2 Legalistische Islamisten verfolgen ihre Ziele ohne Anwendung von Gewalt innerhalb der Rahmenbedingungen des demokratischen Rechtsstaates. Sie vertreten und propagieren

stock.adobe.com

einflussreichste sunnitische islamistische Bewegung, deren Ziele auch heute noch in wesentlichen Elementen von der Ideologie ihrer Gründergeneration um Hasan al-Banna geprägt sind: Diese sieht ein politisches und gesellschaftliches System auf islamischer Grundlage vor. Die Muslimbruderschaft verfolgt das Ziel der Errichtung eines politischen und gesellschaftlichen Systems auf der Grundlage von Koran und Sunna. Ihr ideologischer Leitspruch lautet unverändert: „Gott ist unser Ziel. Der Prophet ist unser Führer. Der Koran ist unserer Verfassung. Der Jihad ist unser Weg. Der Tod für Gott ist unser nobelster Wunsch".

Dieses Phänomen, aus dem auch internationale terroristische Organisationen wie die palästinensische Hamas hervorgegangen sind, ist nach eigenen Angaben in mehr als 70 Ländern und in unterschiedlicher Ausprägung vertreten.[3] Die von ihr angestrebte islamistische Staatsform ist mit demokratischen Grundprinzipien wie dem Recht auf freie Wahlen, dem Recht auf Gleichbehandlung sowie der Meinungs- und Religionsfreiheit nicht vereinbar. Das entschiedene Vorgehen gegen jegliche Gruppierungen, die

letztendlich aber eine Interpretation des Islam, welche den Grundsätzen einer liberalen Gesellschaft und den demokratischen Werten diametral entgegensteht.

3 Kamal Helbawy, The Muslim Brotherhood in Egypt: Historical Evolution and Future Prospects, in: Khaled Hroub (Hrsg.), *Political Islam: Context versus Ideology*, London 2010, p. 61.

demokratische Grundprinzipien, wie beispielsweise das Recht auf Gleichbehandlung oder Meinungsfreiheit in Frage stellen, ist Teil der österreichischen Sicherheitsstrategie. Der Schutz des demokratischen Prinzips ist daher oberste Prämisse der österreichischen Staatschutzbehörden. Die Maßnahme richtete sich daher gegen solche Strukturen, die in langfristiger Perspektive zur Polarisierung der Gesellschaft und zur weiteren Radikalisierung der islamistischen Szene in Österreich beitragen können.[4]

Strukturen des gewaltbereiten Islamismus und Jihadismus

Im Kontext von islamistischem Extremismus sind damit einerseits Strukturen eines gewaltfreien islamistischen Extremismus wahrnehmbar. Unter diesen finden sich legalistische Bestrebungen, die eine langfristige Veränderung des gesellschaftlichen und politischen Systems verfolgen und die damit eine Herausforderung für die gesellschaftliche Stabilität in Österreich darstellen. Andererseits gibt es auch salafistisch-jihadistische Strömungen, deren Aktivisten bereit sind, terroristische Anschläge zu verüben. Das gewaltbereite islamistische Spektrum umfasst Akteure und Netzwerke, die regional oder transnational aktiv sein können und die in ideologischer Hinsicht überwiegend den (miteinander konkurrierenden) terroristischen Organisationen „Islamischer Staat" (IS) oder „al-Qaida" (AQ) bzw. deren jeweiligen Ablegern zuzurechnen sind.

Im Berichtsjahr 2020 ging für Österreich die größte Gefahr eher von lose affiliierten oder lediglich inspirierten Einzeltätern als von konkretisierten Gruppierungen aus. Lokale islamistische Gruppen und Netzwerke (in der sogenannten „Home grown"-Szene), vor allem aus der zweiten und dritten Einwanderungsgeneration sowie aus zum Islam konvertierten Personen, bleiben in Österreich und Europa auch weiterhin von Bedeutung.

Das Terrornetzwerk „al-Qaida" (AQ) hat gegenüber dem IS an Breitenwirkung verloren. Dennoch zeichnet sich AQ durch organisatorisch-strukturelle Resilienz aus, da das Netzwerk nach wie vor über Anhänger und Unterstützer verfügt und auf regionale Ableger baut (z.B. „al-Qaida auf der Arabischen Halbinsel", AQAP und „al-Qaida im Islamischen Maghreb", AQIM), die sich der Organisation und ihrer Ideologie verpflichtet fühlen und deren Agenda über Sympathisantenkreise bis nach Europa ausstrahlen könnte.

Propaganda

Parallel zum territorialen Niedergang des IS nach 2014, lässt sich in den vergangenen Jahren im Internet ein signifikanter Rückgang IS-bezogener Propagandaaktivität

4 Da die Auswertung der Maßnahme zum Berichtszeitpunkt noch anhielt, bleibt auch hier eine genauere Darstellung und abschließende Beurteilung den Ergebnissen der laufenden Ermittlungen vorbehalten.

verzeichnen. Dennoch findet islamistische Propaganda nach wie vor Verbreitung und es kommt auf lokaler wie überregionaler Ebene zur Mobilisierung von Anhängern und zur Rekrutierung neuer Unterstützer. Soziale Netzwerke und einschlägige Internet-Kanäle spielen bei der Radikalisierung weiterhin eine zentrale Rolle, da hier jederzeit zielgruppenorientierte islamistische und jihadistische Inhalte abgerufen werden können. Insbesondere als „Echo-Kammern" bekannt gewordene Informationsblasen können eine zusätzliche ideologische Verfestigung und damit einhergehend einen sozialen Rückzug bis hin zur Abschottung bewirken. Das Bedrohungspotenzial liegt in diesem Kontext hauptsächlich bei radikalisierten Einzelaktivisten und potenziellen Nachahmungstätern. Europaweit ist dabei grundsätzlich der Trend bemerkbar, dass islamistische Propaganda besonders auf ein in Europa bzw. im „Westen" lebendes Publikum ausgerichtet ist, um Attentäter zu gewinnen.

Biographische Aspekte

Wie in den vorangegangenen Berichtsjahren bleiben die Motive, sich einer extremistischen Gruppe anzuschließen, sehr vielfältig. Weiterhin können folgende, den Einstieg in religiösen Fanatismus (und in weiterer Folge hin zur extremistischen Gewalt) begünstigende Faktoren angenommen werden:

- Lebens- bzw. Sinnkrisen,
- gefühlte oder tatsächliche Exklusions- und Diskriminierungserlebnisse,
- von der Norm abweichende Lebenswege usw.

Typische Merkmale im sehr heterogenen Feld des Jihadismus bleiben auch weiterhin „gescheiterte Existenzen" (z.B. berufliche Erfolglosigkeit, prekäre Wohnsituation etc.) oder auch mehrjährige Erfahrungen im (klein-)kriminellen Milieu.

Jihad-Reisende

Die Gruppe der aus dem syrisch-irakischen Kriegsgebiet nach Österreich zurückkehrenden Jihad-Reisenden („Foreign Terrorist Fighters", FTF) blieb bislang kleiner als erwartet. Ungeachtet dessen gilt unverändert, dass kampferprobte, nach Europa zurückkehrende Jihadisten auch weiterhin eine potenzielle Bedrohung darstellen, welche durch ihr erlangtes Wissen im Umgang mit Waffen eine zusätzliche Dynamik erhält. Die Bereitschaft, Anschläge durchzuführen bzw. Gewalt anzuwenden, kann dabei nicht ausgeschlossen werden, insbesondere vor dem Hintergrund der Annahme, dass diese Personen an Kampfhandlungen teilgenommen haben oder auch mit Gräueltaten in Zusammenhang gestanden sind. In der Jihadisten- bzw. Islamistenszene genießen Rückkehrende – aufgrund der tatsächlichen oder behaupteten Teilnahme an Kampfhandlungen im Ausland – ein höheres Renommee, was wiederum ihre Möglichkeiten, zu rekrutieren und Einfluss auf Organisationsstrukturen auszuüben, vergrößert. Insgesamt stellen

diese Personen unverändert ein schwer kalkulierbares Gefahrenpotenzial dar, welches sich aus der Verbindung von Kampferfahrung (paramilitärisches Training, Umgang mit verschiedenen Kampfmitteln) mit (auch traumabedingter) Empathielosigkeit und einer damit einhergehenden herabgesenkten Hemmschwelle ergeben kann. Ebenso berücksichtigungswert sind in diesem Zusammenhang zurückkehrende Frauen und Kinder. Diese sind mitunter hoch ideologisiert und aufgrund von Kriegsereignissen und Gräueltaten oftmals erheblich brutalisiert und abgestumpft.

Grundsätzlich zeigen die in Österreich mit Blick auf die FTF ergriffenen präventiven und repressiven Maßnahmen über die Jahre bis hin zum Berichtszeitraum 2020 Wirkung: Bereits seit 2015 ist ein steter Rückgang an Ausreisen aus Österreich festzustellen und die Zahl der Rückkehrer ist in den vergangenen Jahren stark gesunken.

Zahlen zu FTF aus Österreich:
Ende des Jahres 2020 waren dem Bundesamt für Verfassungsschutz und Terrorismusbekämpfung insgesamt 334 aus Österreich stammende Personen bekannt, die sich aktiv am Jihad in Syrien und dem Irak beteiligen oder beteiligen wollten. Davon sind laut unbestätigten Informationen vermutlich 72 Personen in der Region ums Leben gekommen und 95 Personen wieder nach Österreich zurückgekehrt. Weitere 63 konnten an einer Ausreise gehindert werden und halten sich nach wie vor im Bundesgebiet auf. 104 Jihad-Reisende dürften sich noch im Kriegsgebiet befunden haben.

Inhaftierte terroristische Straftäter und Radikalisierung in Gefängnissen

Eine besondere sicherheitspolitische Herausforderung stellen Extremisten dar, die in der Vergangenheit in Österreich zu Haftstrafen verurteilt worden sind und die nach einer Haftentlassung in die Gesellschaft zurückfinden müssen. Darüber hinaus besteht weiterhin die Gefahr, dass verurteilte Rückkehrer in Justizanstalten versuchen, Mithäftlinge zu ideologisieren bzw. zu radikalisieren. Problematisch bleibt, dass während der Haft neue Netzwerke geknüpft werden, die auch nach der Haftentlassung aktiv genutzt werden können.

Jihad-Rückkehrer und haftentlassene Islamisten dürften unverändert die größte Bedrohung darstellen, da sie u.a. als Vorbilder wirken und das Wissen, das sie erworben haben, weiterzugeben versuchen. Obwohl Rückkehrer in vielen Fällen nicht mehr in dem Maß mit dem IS sympathisieren wie noch vor ihrer Abreise, kann nicht ausgeschlossen werden, dass sie sich auch weiterhin an islamistischen Ideologien orientieren.

Flüchtlings- und Gefangenenlager in Syrien

Nach wie vor ist von humanitär prekären Verhältnissen in den Flüchtlingslagern der Konfliktregionen auszugehen. Angenommen werden muss auch weiterhin, dass die desolaten Verhältnisse zur erneuten Radikalisierung beitragen: Die schlechte Behandlung von in Flüchtlings- und Gefangenenlagern befindlichen Personen droht unverändert zum Legitimierungsnarrativ für neue Anschläge zu geraten. Insgesamt leistet dies unverändert weiteren Rekrutierungsbemühungen Vorschub. Besonders problematisch bleibt, dass aus den Lagern Entflohene sich im Untergrund wieder islamistischen Milizen anschließen und versuchen können, nach Europa zu gelangen, um dort terroristisch aktiv zu werden.

Aspekte der Prävention

Die angesichts der terroristischen Bedrohungslage in Österreich geschaffenen gesetzlichen Novellierungen in den vergangenen Jahren führten zu einer umfangreichen Strategie zur Terrorismusbekämpfung[5]. Maßnahmen im Rahmen dieser Strategie waren auch im Berichtsjahr 2020 unverändert aufrecht.

Die österreichischen Staatsschutzbehörden haben in den vergangenen Jahren vermehrt Präventions- und Deradikalisierungsmaßnahmen gesetzt, um extremistischen bzw. terroristischen Herausforderungen möglichst ganzheitlich zu begegnen. Unter der Prämisse eines gesamtstaatlichen Lösungsansatzes in der Bekämpfung von Extremismus und Terrorismus wurde auf Initiative des BVT 2017 das „Bundesweite Netzwerk Extremismusprävention und Deradikalisierung" (BNED) geschaffen. Durch die Anerkennung des BNED am 8. Juli 2020 durch den Ministerratsvortrag wurde das BNED somit als überparteiliches, sachlich objektives und unvoreingenommenes Gremium aus Expertinnen und Experten anerkannt, das sich mit Extremismus-Prävention und Deradikalisierung flächendeckend und ganzheitlich auseinandersetzt.[6]

Mohammed-Karikaturen

Wie rasch und umfassend Ereignisse und Vorfälle in einem Land in internationale Diskurse und Narrative eingebettet sind, zeigte sich beispielhaft an den Veröffentlichungen der

---

5 Das Paket umfasst u.a. die Novellierung des Symbole-Gesetzes (stellt das Zurschaustellen islamistisch-extremistischer Symbolik unter Strafe), die Ausweitung der Entziehung der österreichischen Staatsbürgerschaft (bei Doppelstaatsbürgern, wenn diese außerhalb eines offiziellen Militärdienstes an Kämpfen teilnehmen) sowie die Adaptierung des Grenzkontrollgesetzes (Minderjährige dürfen nur mit Zustimmung eines Obsorgeberechtigten Auslandsreisen außerhalb der EU unternehmen). Zudem wurden internationale Fahndungen nach Jihad-Reisenden intensiviert.

6 Siehe dazu ausführlich der Fachbeitrag „Gesamtgesellschaftlicher Ansatz in der Extremismusprävention und Deradikalisierungsarbeit- das BNED".

Mohammed-Karikaturen[7] in Frankreich. Wie bei früheren Veröffentlichungen kam es auch diesmal zu Kontroversen und scharfer Rhetorik zwischen Frankreich und anderen (islamischen) Staaten.

Unter anderem war es zur Ermordung eines Lehrers in Conflans-Sainte-Honorine gekommen, der im Zuge einer Schulunterrichtsstunde zum Thema Meinungsfreiheit die sogenannten „Mohammed-Karikaturen" des Magazins „Charlie Hebdo" gezeigt hatte. Die Tat selbst wurde durch einen jugendlichen Einzeltäter ausgeführt, war aber zuvor von einer breitenwirksamen Kampagne in sozialen Netzwerken, auch unter Beteiligung von Akteuren aus dem islamistischen Spektrum, begleitet worden. Sie profitierten dabei von weitverbreitetem Unmut über die Veröffentlichung der Karikaturen. Weltweit kam es dadurch zu Gewalttaten gegen französische Einrichtungen. Ferner rief al-Qaida dazu auf, man solle sich al-Qaidas „Kampf gegen den Westen" anschließen und etwa als „lone actor" Anschläge in westlichen Ländern verüben.

Modi operandi

Bei salafistisch-jihadistisch motivierten Terroranschlägen in Europa zeigte sich in den vergangenen Jahren ein Trend weg von zeit- oder ressourcenintensiven Vorbereitungen mit spezifischen Ausbildungen oder sogar Reisen zu einschlägigen Terrorcamps im Ausland. Stattdessen häufen sich niederschwellige und mit vergleichsweise schlichten Tatmitteln ausgeführte Tathandlungen und es scheinen sich „sparsamere" Szenarien zu etablieren, die aber grundsätzlich den Einsatz von zugänglichen Tatmitteln mit größerer Schadenswirkung wie Explosivstoffen oder biologischen und chemischen Kampfmitteln nicht ausschließen müssen.

Unverändert spielen bei der Auswahl der Anschlagsziele strategische und praktische Überlegungen eine Rolle. Das potenzielle Zielspektrum islamistischer Terroristen reicht von Objekten der Kritischen Infrastruktur bis zu sogenannten „weichen Zielen"[8]. Die symbolische Bedeutung von Anschlagszielen hat relativ abgenommen, da sich auch mit niedrig-komplexen Anschlägen wesentliche terroristische Ziele erreichen lassen: hohe mediale Resonanz, potenziell große öffentliche Aufmerksamkeit sowie psychologische Auswirkungen in der Bevölkerung und – im Sinne der Terroristen – politische Reaktionen.

---

7 Bereits 2015 hatte die Veröffentlichung der Karikaturen als Rechtfertigung für einen Angriff auf die Satirezeitschrift „Charlie Hebdo" gedient.

8 Relativ leicht zugängliche Ziele – manchmal auch mit hohem symbolischen Stellenwert – und erhöhtem Personenaufkommen.

Die COVID-19-Pandemie im Phänomenbereich

Grundsätzlich ergaben sich keine substanziellen Auswirkungen des pandemischen Geschehens auf die islamistisch-terroristische Bedrohungslage in Österreich. Islamistische Propaganda-Medien interpretierten COVID-19 häufig als „Strafe Gottes" für den Westen. Das Corona-Virus wurde als eine Art biologische Waffe zum Einsatz gegen westliche Gesellschaften propagiert.

Während einerseits die Maßnahmen in Österreich zur Eindämmung der Pandemie Massenveranstaltungen als potenzielle Anschlagsziele stark reduziert haben, besteht andererseits in der zunehmenden Isolation von Individuen, die für Radikalisierung anfällig sein könnten, ein Risiko (z.B. durch weitere Zunahme von Echo-Kammern). Außerdem wirkten sich Maßnahmen der Pandemiebekämpfung europaweit auf Reisebewegungen rückkehrwilliger Jihadisten aus.

Zusätzlich könnte, als Folge der Pandemie, eine weitere ökonomische-existenzielle Prekarisierung von Personen, die so an den Rand der Gesellschaft gedrängt werden und weiter unter Druck geraten, das Feld potenziell für Radikalisierung Anfälliger gefährlich erweitern.

Das Auftreten und die Verbreitung des Corona-Virus sowie die Maßnahmensetzungen der einzelnen Länder, führten zudem zu Verhaltens- und Strategieadaptionen islamistischer Terroristen. Hatte sich das jihadistische Narrativ zu Beginn der Pandemie auf die Volksrepublik China – respektive den Uiguren-Konnex – fokussiert, wurde dies in weiterer Folge (analog zur Verbreitung des Virus) sukzessive auf westliche Staaten ausgeweitet. Zentral ist hierbei die Interpretation des Corona-Virus als „Soldat Allahs" oder als „Strafe Gottes" für „Kreuzzügler" (Christen), Juden und Apostaten. IS und al-Qaida propagierten, dass die gegenwärtig höhere Vulnerabilität der Länder der „Kreuzzügler" durch eine Intensivierung der Anschläge gegen diese ausgenutzt werden müsse.

Trends und Entwicklungen

In Österreich besteht wie in Europa eine hohe Gefahr von islamistisch motivierten Anschlägen durch radikalisierte Einzeltäter.

Unverändert und weiterhin stellen jihadistisch inspirierte Anschlagsplanungen eine der größten sicherheitspolitischen Herausforderungen für Europa und Österreich dar. Art und Weise terroristischer Anschläge in den letzten Jahren deuten darauf hin, dass sich der Trend der mit relativ schlichten Mitteln durchgeführten Anschläge fortsetzen könnte: Ressourcenärmere, weniger komplexe Methoden der Anschlagsplanung und -durchführung könnten auch in Zukunft aufwendige Ausbildungen und riskante Reisen in terroristische Ausbildungslager nicht mehr unbedingt erfordern.

Trotz der Zerschlagung der Strukturen des „IS-Kalifats“ werden die Attraktivität und Anziehungskraft islamistischer Ideologien, insbesondere mit salafistisch-jihadistischer Prägung, auch in Zukunft weiterbestehen und für Zulauf sorgen. Die dahinterstehenden Ideologeme werden weiterhin Denk- und Handlungsweisen radikalisierter Islamisten prägen.

Nach wie vor tragen lokale islamistische Gruppen und Netzwerke (in der sogenannten „home grown“-Szene) der zweiten und dritten Einwanderergeneration sowie aus zum Islam konvertierten Personen dazu bei, dass Gesellschaften von islamistischer Radikalisierung betroffen sind. Sicherheits- und sozialpolitische Herausforderungen bestehen nach wie vor in der Reintegration vieler Extremisten nach ihrer Haftentlassung.

Erneut ist auf die Bedeutung der Sozialen Medien und einschlägiger Internet-Foren hinzuweisen. Ihre Rolle bei der Radikalisierung ist substanziell, da sie auch weiterhin (wenn auch in rückläufiger Verbreitung) spezielle islamistische beziehungsweise jihadistische Inhalte leicht verfügbar machen. Unverändert tragen sogenannte „Echo-Kammern“ (Informationsblasen) zu Ideologisierung und Abschottung bei, was bei radikalisierten Einzelaktivisten bzw. Nachahmungstätern, die sich von jihadistischer Ideologie inspiriert fühlen, weiterhin ein Bedrohungspotenzial erzeugt.

Die Gefahr von islamistisch motivierten Anschlägen durch radikalisierte Einzeltäter oder autonom agierende Kleinstgruppen und Zellen, die Anschläge ohne direkten Auftrag bzw. Anleitung einer terroristischen Organisation ausführen, bleibt in Europa sehr wahrscheinlich weiterhin erhöht.

Anhänger militant islamistischer Strömungen bzw. von jihadistischer Ideologie Inspirierte könnten verstärkt Cyberoperationen als Waffe für sich entdecken. Großangelegte Angriffe durch jihadistische Hacker mit dem Ziel, beispielsweise Kritische Infrastrukturen zu sabotieren (u.a. den Wasser-, Energie-, Finanz-, Telekommunikations- oder Gesundheitssektor) könnten enormen physischen, ökonomischen sowie sozialen Schaden anrichten, subjektive Sicherheit strategisch reduzieren und so die Schadenswirkung bisheriger Angriffe deutlich übertreffen.

Rechtsextremismus

Lagebild

Auch im Berichtsjahr 2020 stellten rechtsextremistische Aktivitäten eine demokratiegefährdende Tatsache in Österreich dar. Ein potenzielles Risiko für die Störung der öffentlichen Ruhe, Ordnung und Sicherheit war und ist durch rechtsextremistische

Gewalt gegeben. Zu den primären Feindbildern rechtsextremistischer Kreise zählen unter anderem:

- Juden und Muslime sowie deren Einrichtungen;
- der Islam als Religion;
- Islamisten;
- Angehörige der Roma- und Sinti-Minderheit;
- Asylwerber und Migranten;
- Personen, die als „fremd“ wahrgenommen werden;
- Personen, karitative Einrichtungen und andere Organisationen, die sich für asyl- und schutzsuchende Menschen in Österreich einsetzen;
- Aktivisten des linken bis linksextremistischen Spektrums;
- traditionelle Institutionen der Massenmedien;
- die Polizei, speziell im Rahmen von Rechts/Links-Konfrontationen im öffentlichen Raum;
- die Europäische Union sowie
- das demokratische System.

Die von den österreichischen Staatschutzbehörden verwendete Definition von Rechtsextremismus versteht unter diesem Begriff eine Sammelbezeichnung für politische Auffassungen und Bestrebungen – von fremdenfeindlich/rassistisch bis hin zur nationalsozialistischen Wiederbetätigung –, die im Namen der Forderung nach einer von sozialer Ungleichheit geprägten Gesellschaftsordnung die Normen und Regeln eines modernen demokratischen Verfassungsstaates ablehnen und diesen mit Mitteln bzw. Gutheißung oder Inkaufnahme von Gewalt bekämpfen. Der Terminus Rechtsextremismus ergibt sich aus unterschiedlichen gesellschaftlichen Verwendungskontexten und den damit korrespondierenden Interpretationen, mit denen er jeweils bezeichnet wird. Die Befürwortung einer Diktatur, von Islam- und Fremdenfeindlichkeit, Antisemitismus, Chauvinismus, Sozialdarwinismus, Rassismus sowie die Verharmlosung und Relativierung des Nationalsozialismus (Revisionismus), prägen das Weltbild rechtsextremer Ideologen und ideologisierter Gruppierungen/Bewegungen, Netzwerke, Szenen und Milieus. Charakteristisch für rechtsextremistische Einstellungs- und Handlungsmuster ist die Verherrlichung eines „völkischen Nationalismus“ mit deutschnationalen bzw. nationalistisch-konservativen Konzepten. Zentrale Wesensmerkmale rechtsextremistischer Ideologie sind antidemokratische und antipluralistische Gesellschaftsauffassungen bei gleichzeitiger Ablehnung des vorherrschenden (d.h. demokratischen) politischen Systems. In seiner äußersten Steigerungsform kann sich Rechtsextremismus bis hin zum (Rechts-) Terrorismus steigern, um systematisch gegen politische Gegner, gegen Opfergruppen rechtsextremistischer Weltanschauungen und gegen staatliche Institutionen bzw. gegen ihre Repräsentanten vorzugehen.

Die rechtsextremistische Szene in Österreich ist von einer heterogenen Struktur gekennzeichnet und weist in ideologischer Ausrichtung wie auch im äußeren Auftreten kein einheitliches und geschlossenes Erscheinungsbild auf. Verschiedene Akteursgruppen mit unterschiedlicher personeller Stärke und ideologischer Ausrichtung formieren sich um antidemokratische, fremdenfeindliche/rassistische, islamfeindliche, antisemitische und revisionistische Weltbilder, wobei die ideologischen Schwerpunkte variieren können. Rechtsextremistische Akteure, Gruppierungen und Netzwerkkoordinatoren verfolgen unterschiedliche Taktiken und Praktiken zur Zielerreichung. Trotz ihrer ansonsten heterogenen Struktur setzt sich die Szene im Bundesgebiet überwiegend aus männlichen Akteuren zusammen.

Wie schon bei der angespannten Migrationssituation in den Jahren 2015 und 2016 beobachtbar, ließen sich auch im Berichtsjahr 2020 Überschneidungen innerhalb der heimischen rechtsextremistischen Szene (Neonazis, Skinheads, Neue Rechte) feststellen. In jüngster Vergangenheit konnten diese Überschneidungen bei zahlreichen Protestveranstaltungen der COVID-19-Maßnahmengegner zum Teil auch öffentlich wahrgenommen werden. In diesem Kontext lässt die gemeinsame Teilnahme an Kundgebungen von einzelnen Szeneproponenten und Gruppen Rückschlüsse auf oftmals temporär begrenzte, anlass- und themenbezogene, organisationsübergreifende, aber keineswegs institutionalisierte Allianzen bzw. Koalitionen innerhalb des rechtsextremistischen Milieus zu.

COVID-19-Maßnahmen-Kundgebungen

Neurechte Gruppierungen in Österreich nutzten von Anfang an die milieuübergreifenden COVID-19-Maßnahmen-Kundgebungen als Bühne, um ihre Agitationen und Aktionen öffentlichkeitswirksam umzusetzen. Die Aktivisten zeigten von Beginn an Präsenz bei diesen Veranstaltungen und versuchten dem Protest Kampagnencharakter zu verleihen. So traten Aktivisten der Identitäre Bewegung (IBÖ) und der Gruppierung „Die Österreicher“ (DO5) im Demonstrationsgeschehen der COVID-19-Maßnahmengegner oftmals prominent mit Spruchbändern und Plakaten in Erscheinung, um sich selbst als „rechte Bewegung der Straße“ zu inszenieren.

Die Identitäre Bewegung (IBÖ) und „Die Österreicher“ (DO5) sind die bekannteste Vertreter neurechter Gruppierungen in Österreich. Wobei es zwischen der Identitären Bewegung (IBÖ) und „Die Österreicher“ (DO5) große personelle wie auch inhaltliche Überschneidungen gibt.

stock.adobe.com

Eine aus der Vergangenheit bekannte Strategie neurechter Ideologen ist es, Themen und Diskurse mit hoher emotionaler Wirkung aufzugreifen und zu besetzen.[9] Die Handschrift der führenden Ideologen der IBÖ bzw. DO5 wurde im Berichtsjahr 2020 vor allem bei den Protesten gegen die COVID-19-Maßnahmen der Bundesregierung sichtbar. Die Identitäre Bewegung (IBÖ) und „Die Österreicher" (DO5) nutzten das Jahr 2020 strategisch, um sich im emotional geführten Diskurs rund um die COVID-19-Maßnahmen zu positionieren. Dabei gelang es den Neuen Rechten, ihre verschwörungsideologischen Deutungsmuster der Pandemie einer breiteren Bevölkerungsschicht zugänglich zu machen.

Anfänglich wurden seitens der neurechten Gruppierungen Ängste und Unsicherheiten der Bevölkerung geschürt und die COVID-19-Pandemie mit Falschmeldungen über eine bevorstehende nächste „Migrationswelle" vermengt. Anhand der von Führungskadern der Neuen Rechten verbreiteten Propaganda zeigte sich, wie die Pandemie mit der Migrations- und Asylthematik bewusst vermischt, instrumentalisiert und für die eigenen Zwecke gezielt genutzt wurde. In diesem Zusammenhang thematisierten die Neuen Rechten auch die Gefahr eines „Überwachungsstaates". Dabei wurden die COVID-19-Maßnahmen der Regierung scharf kritisiert und zu gemeinsamen Protestkundgebungen gegen die „Virus-Diktatur" aufgerufen. Die Spruchbänder und Verschwörungserzählungen der IBÖ/DO5 wurden somit teilweise zum Slogan der COVID-19-Protestbewegung in Österreich.

Spielte bei den Aktivisten der Neuen Rechten in den vorangegangenen Jahren noch die Kampagne „Der Große Austausch" die zentrale Rolle, so verlagerte sich ihr Fokus im

9 Siehe dazu Verfassungsschutzbericht 2018

Berichtsjahr 2020 auf das Thema „Coronavirus“ und die damit verbundenen Maßnahmen der österreichischen Bundesregierung. Anstelle des „Großen Austausches“ während der Flüchtlingskrise 2015, wurde in der COVID-19-Pandemie 2020 die Theorie „The Great Reset“ zum neuen propagandistischen und verschwörungsideologischen Schwerpunkt neurechter Gruppierungen. Im Zusammenhang mit der Corona-Pandemie gingen prominente Vertreter der Neuen Rechten auf ein Buch mit dem Titel „Covid-19: The Great Reset“ („Covid-19: Der große Umbruch“) ein. Dieses Buch beschreibt unter anderem „wie das neuartige Coronavirus so viel Zerstörung und Leid anrichten konnte und welche Änderungen für eine integrativere, robustere und nachhaltigere Welt erforderlich sind.“ Aus Sicht der Neuen Rechten geht es aber bei diesem Konzept vielmehr um den „perfiden Plan“ der „globalen Eliten“ und „Globalisten“, nach einer inszenierten Zerstörung der bestehenden Verhältnisse, eine „neue Welt“ nach ihren Vorstellungen aufzubauen. Vertreter der Neuen Rechten nutzten die Corona-Demonstrationen im Bundesgebiet, um diese Theorien öffentlichkeitswirksam zu propagieren.

Aus Sicht der Staatsschutzbehörden wird seit Beginn der Pandemie die starke Präsenz von rechtsextremistischen Einzelakteuren und Gruppierungen unter den COVID-19-Maßnahmengegnern als problematisch bewertet (siehe auch Fachbeitrag „Pandemie und Sicherheit“). Aktivisten der IBÖ/DO5 nutzten die Sommermonate 2020 zur Vernetzung mit der damals noch überschaubaren COVID-19-Protestbewegung und prägten im Herbst und Winter mit ihren Spruchbändern aktiv das Protestgeschehen. Im Zuge der COVID-19-Proteste konnten Neurechte Gruppierungen ihren Bekanntheitsgrad unter der am Protest teilnehmenden Bevölkerung ausweiten.

Im Berichtsjahr 2020 spielten das Internet und im Speziellen die Sozialen Medien auch im Zusammenhang mit den COVID-19-Protesten weiterhin eine tragende Rolle. Ihre Funktion ist vielfältig und wird als Kommunikations-, Vernetzungs- und Mobilisierungsinstrument eingesetzt. Besonders in Sozialen Medien versuchten rechtsextremistische Akteure die COVID-19-Pandemie zu nutzen, um eine weitere Polarisierung und Spaltung der Gesellschaft voranzutreiben. Neben gedruckten Publikationen wird von einschlägigen Aktivisten vor allem durch die intensive Nutzung des Internets der Versuch unternommen für die breite Öffentlichkeit einen Gegenpol („alternative Medien“) zu den von ihnen bezeichneten „Mainstream-Medien“ zu etablieren. Die Bemühungen „klassischer“ Social Media-Portale Inhalte und Accounts mit extremistischen Inhalten zu löschen, bringen oftmals nur Verlagerungseffekte mit sich. Daraus resultiert ein Ausweichen auf geschlossene Foren oder andere Kommunikations- und/oder Social Media-Plattformen.

Während in den Jahren vor der Corona-Pandemie die rechtsextremistische Musikszene und ihre Großveranstaltungen mit Festivalcharakter[10] auf internationaler Ebene einen fixen

10 Siehe dazu Verfassungsschutzbericht 2019

Bestandteil der Szene darstellten, mussten aufgrund der Maßnahmen zur Eindämmung des Virus in Europa zahlreiche öffentliche Veranstaltungen abgesagt werden. Darunter fielen auch Festivals, Kampfsportveranstaltungen und Konzerte im rechtsextremistischen Spektrum, die z. B. im benachbarten Ausland stattfinden hätten sollen. Neben der Rekrutierung potenzieller Sympathisanten sowie der propagandistischen und finanziellen Komponente, welche mit diesen Veranstaltungen verbunden ist (Konzertkarten, Merchandise Artikel etc.), dürften auch die ansonsten ebenso wichtigen netzwerk- und szenebildenden Elemente zumindest temporär weggefallen bzw. unterbrochen worden sein.

Einschlägige Bemühungen von rechtsextremistischen Akteuren und Gruppierungen waren auch im Berichtsjahr 2020 Gegenstand von intensiven Ermittlungen, Beobachtungen und Ausgangspunkt für gerichtlich angeordnete Maßnahmen der österreichischen Staatsschutzbehörden. So wurden im Berichtsjahr 2020 unter anderem zahlreiche Hausdurchsuchungen wegen Verdachts des Verbrechens nach dem Verbotsgesetz vollzogen. Bei den Tatverdächtigen konnte zum einen einschlägiges Material mit nationalsozialistischem Hintergrund, elektronische Geräte wie Mobiltelefone, Computer und Datenträger sowie andererseits Waffen, Munition, Sprengstoff und Kriegsmaterial in großem Ausmaß sichergestellt werden.

Statistik

Das Phänomen Rechtsextremismus zeigte sich den österreichischen Sicherheitsbehörden 2020 in Form von Straftaten sowie als politisch-ideologisch motivierte Aggression und Propagandaaktionismus rechtsextremistischer Einzelpersonen und Gruppierungen.

2020 sind den Sicherheitsbehörden in Österreich insgesamt 895 rechtsextremistische, fremdenfeindliche/rassistische, islamfeindliche, antisemitische sowie unspezifische oder sonstige Tathandlungen bekannt geworden, bei denen einschlägige Delikte zur Anzeige gelangten. Eine Tathandlung kann mehrere Delikte mit gesonderten Anzeigen beinhalten. Gegenüber 2019 (954 Tathandlungen) bedeutet dies einen zahlenmäßigen Rückgang um 6,2 Prozent. 622 Tathandlungen, das sind 69,5 Prozent, konnten aufgeklärt werden. 2019 lag die Aufklärungsquote bei 67,6 Prozent.

Im Zusammenhang mit den angeführten Tathandlungen wurden 2020 bundesweit 1.364 Delikte zur Anzeige gebracht, das sind um 18,7 Prozent weniger als im Jahr 2019 (1.678 Delikte).

Anzeigen	2019	2020
Anzeigen nach dem StGB		
Körperverletzung (§ 83 StGB)	14	10
Schwere Körperverletzung (§ 84 StGB)	6	1
Absichtliche schwere Körperverletzung (§ 87 StGB)	1	1
Gefährdung der körperlichen Sicherheit (§ 89 StGB)	1	1
Schwere Nötigung (§ 106 StGB)	0	1
Gefährliche Drohung (§ 107 StGB)	34	30
Fortgesetzte Belästigung im Wege einer Telekommunikation oder eines Computersystems (§ 107c StGB)	0	1
Beleidigung (§ 115 StGB)	4	9
Berechtigung zur Anklage (§ 115 i.V.m. § 117 StGB)	2	3
Sachbeschädigung (§ 125 StGB)	219	186
Schwere Sachbeschädigung (§ 126 StGB)	19	11
Diebstahl (§ 127 StGB)	8	3
Diebstahl durch Einbruch oder mit Waffen (§ 129 StGB)	8	2
Unterschlagung (§ 134 StGB)	0	1
Schwerer Raub (§ 143 StGB)	0	1
Betrug (§ 146 StGB)	2	1
Herabwürdigung religiöser Lehren (§ 188 StGB)	1	3
Störung der Totenruhe (§ 190 StGB)	0	1
Pornographische Darstellungen Minderjähriger (§ 207a StGB)	50	11
Sexuelle Belästigung und öffentliche geschlechtliche Handlungen (§ 218 StGB)	1	2
Urkundenunterdrückung (§ 229 StGB)	1	2
Widerstand gegen die Staatsgewalt (§ 269 StGB)	4	6
Landzwang (§ 275 StGB)	0	1
Aufforderung zu mit Strafe bedrohten Handlungen und Gutheißung mit Strafe bedrohter Handlungen (§ 282 StGB)	8	8
Verhetzung (§ 283 StGB)	169	224
Verleumdung (§ 297 StGB)	2	1
Andere StGB Delikte	27	0
Anzeigen nach dem Verbotsgesetz	1037	801
Anzeigen nach anderen Gesetzen oder Verordnungen		
Abzeichengesetz	2	6

Anzeigen	2019	2020
Art III Abs. 1 Z 3 und Z 4 EGVG	14	1
§ 50 Waffengesetz (WaffG)	19	17
§ 51 Waffengesetz (WaffG)	0	2
Suchtmittelgesetz	18	5
Sicherheitspolizeigesetz	7	6
Pyrotechnikgesetz	0	1
Wiener Landes-Sicherheitsgesetz	0	2
Mediengesetz	1	2
Andere Gesetze oder Verordnungen	6	0
Summe	**1678**	**1364**

Erläuterungen zur Statistik

In folgenden Deliktskategorien wurde ein Anstieg registriert:

- § 115 Beleidigung: 9 Anzeigen (2019: 4)
- § 188 StGB Herabwürdigung religiöser Lehren: 3 Anzeigen (2019: 1)
- § 269 StGB Widerstand gegen die Staatsgewalt: 6 (2019: 4)
- § 283 StGB Verhetzung: 224 Anzeigen (2019: 169)

Zu einem Rückgang kam es in folgenden Deliktskategorien:

- Anzeigen nach dem Verbotsgesetz: 801 Anzeigen (2019: 1.037)
- Körperverletzungsdelikte nach den §§ 83 und 84 StGB: 11 Anzeigen (2019: 20)
- § 107 StGB Gefährliche Drohung: 30 Anzeigen (2019: 34)
- Sachbeschädigungsdelikte nach den §§ 125 oder 126 StGB: 197 Anzeigen (2019: 238)

Österreichweit wurden bei der Bekämpfung rechtsextremistischer Aktivitäten im Jahr 2020 im Rahmen der aufgeklärten Tathandlungen insgesamt 731 Personen durch die Sicherheitsbehörden angezeigt. 62 davon waren Frauen (8,5 Prozent). 2019 wurden 893 Personen (7,3 Prozent davon weiblich) angezeigt. Im Berichtsjahr 2020 wurden insgesamt 200 Jugendliche (27,4 Prozent) zur Anzeige gebracht (2019: 269).

Wegen Körperverletzungsdelikten wurden 2020 im Zusammenhang mit elf einschlägigen Tathandlungen neun Personen (eine davon wegen schwerer Körperverletzung, eine wegen absichtlich schwerer Körperverletzung) angezeigt. 2019 waren es im Rahmen von 21 Tathandlungen 18 Personen.

Durch fremdenfeindlich/rassistisch motivierte Tathandlungen wurden im Jahr 2020 eine (2019: 6), durch islamfeindlich motivierte Tathandlungen keine Person (2019: 0) verletzt. Durch antisemitisch motivierte Tathandlungen kam im Jahr 2020 eine Person zu körperlichen Schäden (2019: 0).

Von den insgesamt 895 bekannt gewordenen Tathandlungen waren

- 697 (77,9 Prozent) rechtsextremistisch,
- 104 (11,6 Prozent) fremdenfeindlich/rassistisch,
- 36 (4 Prozent) antisemitisch und
- 16 (1,8 Prozent) islamfeindlich

motiviert. Bei 42 Tathandlungen (4,7 Prozent) war eine unspezifische oder sonstige Motivlage hinsichtlich der Tatausführung vorhanden.

Von den 30 angezeigten Delikten nach § 107 StGB (Gefährliche Drohung) waren 16 rechtsextremistisch, acht fremdenfeindlich/rassistisch und vier antisemitisch motiviert. Bei zwei Delikten lag den Tathandlungen eine sonstige oder unspezifische Motivlage zugrunde.

Im Jahr 2020 konnten 34 (2019: 18) fremdenfeindliche/rassistische oder rechtsextremistische Tathandlungen der Asyl- bzw. Flüchtlingsthematik zugeordnet werden. Bei all diesen Tathandlungen handelte es sich um einschlägige verbale Agitationen im Internet. Dies bedeutet einen Anstieg um 52,9 Prozent gegenüber dem Vorjahr. Davon konnten 27 Tathandlungen, das sind 79,4 Prozent, aufgeklärt werden.

Von den 895 Tathandlungen fanden 371 (41,5 Prozent) im Internet statt. 2019 lag der Anteil der Internetdelikte bei 34,2 Prozent (326 Tathandlungen).

Bei der Internet-Meldestelle „NS-Wiederbetätigung“ sind im Jahr 2020 insgesamt 3.636 Informationen und Hinweise davon 1.098 relevante[11] Sachverhalte eingegangen (2019: 3.081 Eingänge – 964 relevant).

11 Dabei handelt es sich um staatsschutzrelevante Sachverhalte, um unabhängige Doppel- bzw. Mehrfachmeldungen oder sonstige von Amtswegen zu bearbeitende Anliegen und Hinweise.

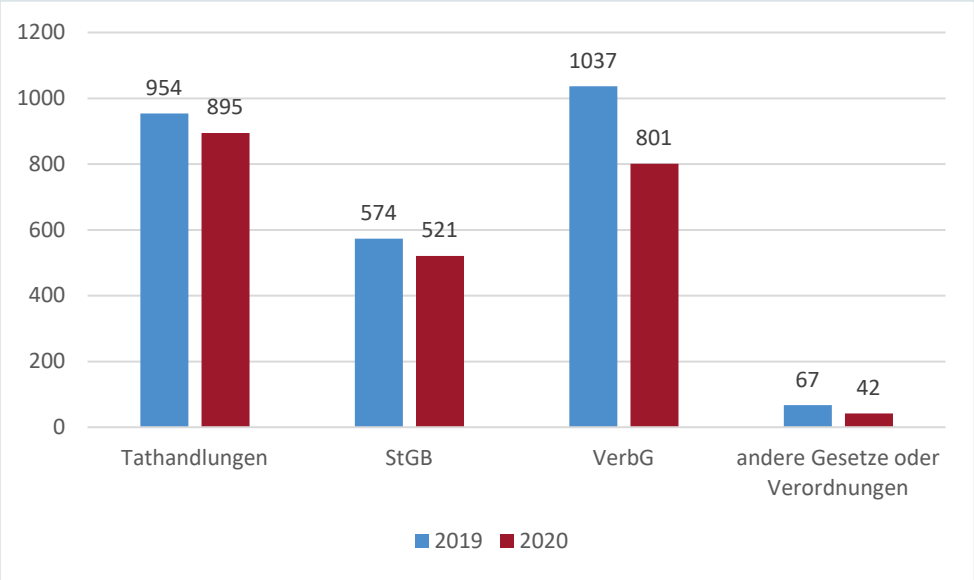


Abbildung: Tathandlungen/ Anzeigen – Vergleich 2019/2020

Trends und Entwicklungen

Aufgrund der Datenlage, der aktuellen Entwicklung und der daraus resultierenden Bewertung kann der Schluss gezogen werden, dass die rechtsextremistische Szene in Österreich im Berichtsjahr 2020 ein staatsschutzrelevantes Gefahrenpotenzial darstellte und ein solches auch weiterhin darstellen wird.

Die jüngsten Entwicklungen im Phänomenbereich Rechtsextremismus legen offen, dass sich eine Konsolidierung der im Berichtjahr 2019 begonnenen personellen und organisatorischen Veränderungen abgezeichnet haben dürfte. Langjährige Führungskader der heimischen organisierten rechtsextremistischen Szene konnten ihre Strukturen und Netzwerke wieder nutzen, um teilweise auch öffentlichkeitswirksam in Erscheinung zu treten. Daneben war es auch neurechten Bewegungen in Österreich möglich, vor allem durch medial inszenierte Kampagnen im Rahmen der COVID-19-Kundgebungen, ihre „Stellung" in der Öffentlichkeit beizubehalten und für eine erhöhte Aufmerksamkeit und Polarisierung zu sorgen.

Bei einem Fortdauern der Corona-Pandemie und der Maßnahmen der österreichischen Bundesregierung zur Eindämmung des Infektionsgeschehens, kann aktuell davon ausgegangen werden, dass Proponenten der heimischen rechtsextremistischen Szene diese Situation auch weiterhin für ihre Bestrebungen nutzen und instrumentalisieren. Dabei können die COVID-19-Maßnahmen-Kundgebungen auch künftig eine geeignete Bühne bieten, um die eigenen antidemokratischen Ziele und Motivlagen einer breiteren Bevölkerungsschicht zugänglich zu machen und Teile des Protestpublikums für ihre Zwecke zu missbrauchen.

Durch das vermehrte Auftreten einschlägiger, teils auch gewaltaffiner bzw. gewalttätiger Personengruppierungen bei Protestveranstaltungen könnte ein zusätzliches, nur schwer kalkulierbares Konfliktpotenzial entstehen. In diesem Zusammenhang wird explizit auf die Brisanz des Spannungsfeldes Rechts-/Linksextremismus hingewiesen, welche besondere Sicherheitsrelevanz birgt und im Rahmen der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit eine herausfordernde Aufgabe für die österreichischen Sicherheitsbehörden darstellt. Es ist evident, dass sich die Gewalt im Kontext Rechts-/Linksextremismus nicht nur gegen den ideologischen Gegner richtet, sondern auch Drittziele (Exekutive, Privatpersonen, öffentliches und privates Eigentum) davon betroffen sein können.

Die Ideologen der Neuen Rechten haben im Berichtsjahr 2020 frühzeitig erkannt, dass sich die COVID-19-Pandemie eignet, um ihre eigene verschwörungserzählerische Weltsicht vom „Großen Austausch“ in den „Great Reset“ - der durch COVID-19 stattfinden soll - zu transformieren. Sowohl beim „Großen Austausch“ als auch beim „Great Reset“ werden dystopische Endzeitszenarien entworfen. Über die Proteste gegen die COVID-19-Maßnahmen konnten die Neuen Rechte schlussendlich neue Bevölkerungsgruppen mit ihrer Propaganda erreichen. Ein Trend der sich auch im kommenden Jahr fortsetzen wird.

Abschließend wird festgehalten, dass das im Phänomenbereich Rechtsextremismus tradierte Narrativ

der „Verdrängung“, „Überfremdung“ und „Unterwanderung des eigenen Volkes“ in der Szene weiterhin als starke Triebfeder genutzt werden wird. Darüber hinaus sind die Themen „Anti-Islam“, „Anti-Multikulturalismus“ sowie die Asyl- und Flüchtlingsthematik auch in Zukunft dazu geeignet, einen zentralen Agitations- und Aktionsschwerpunkt der heimischen rechtsextremistischen Szene in der virtuellen wie auch in der realen Welt darzustellen.

Linksextremismus

Lagebild

Der Phänomenbereich Linksextremismus umfasst in Österreich mehrere staatsschutzrelevante Strömungen. Beobachtungsgegenstand der österreichischen Staatsschutzbehörden sind linksextremistische Positionen, die mit Gewaltakzeptanz und -befürwortung verbunden sind und deren Anhänger für die Durchsetzung ihrer Ideologien und in der Auseinandersetzung mit anderen politischen Weltanschauungen bewusst Gesetzesbrüche einkalkulieren. Die sich daraus ableitenden Aufgabenbereiche umfassen sowohl die Abwehr der von einschlägigen Gruppen ausgehenden Gefahren für die öffentliche Ruhe, Ordnung und Sicherheit, als auch den Schutz des Staates gegen

verfassungsfeindliche Strömungen. Das Ziel der Staatsschutzarbeit ist die Gewährleistung der störungsfreien Funktion der demokratisch-rechtsstaatlichen Einrichtungen.

Organisationen und Gruppierungen

Die linksextreme Szene in Österreich ist durch interne Differenzen und die Spaltung in einen marxistischen/leninistischen/trotzkistischen Bereich und in ein autonom-anarchistisches Spektrum gekennzeichnet.

Die gemeinsame Stoßrichtung der unterschiedlichen linksextremistischen Strömungen – von marxistisch über anarchistisch bis autonom – ist die Beseitigung des bestehenden „bürgerlich-kapitalistischen Systems". Dieses soll entweder durch einen sozialistischen Staat oder durch eine herrschaftsfreie Gesellschaft abgelöst werden. So wie bei anderen in sich geschlossenen Weltbildern, sollen grundlegende demokratische bzw. rechtsstaatliche Regeln durch neue, die individuelle Freiheit einschränkende Normen ersetzt werden, oder – nach dem anarchistischen Prinzip – zu Gunsten einer herrschaftslosen Gesellschaft überhaupt aufgehoben werden.

Linksextremisten thematisieren im Rahmen ihrer Agitations- und Aktionsfelder aktuelle Entwicklungen, benennen politische, wirtschaftliche und gesellschaftliche Missstände, und versuchen, diese für ihre Zwecke zu instrumentalisieren. Auf die Formulierung von konstruktiver Kritik wird verzichtet, Interesse an politischen Reformen wird nicht gezeigt – als Ziel wird einzig und alleine eine vollständige Systemüberwindung angestrebt.

Kommunistische Kaderorganisationen

Marxistisch-leninistische Gruppen stellen ihrer politischen Arbeit das Element des revolutionären Umbruchs voran. Dieser soll durch eine sogenannte politische Avantgarde erfolgen, die in einer revolutionären Kaderpartei organisiert und deren Aufgabe die Heranführung von möglichst breiten Bevölkerungsschichten an die Bewegung ist. Innerhalb der Partei agieren deren Mitglieder nach dem Prinzip des Zentralismus, wonach Beschlüsse der Leitungsgremien strikt zu befolgen und Fraktionsbildungen verboten sind.

Trotzkistische Gruppen sehen sich als Betreiber der „permanenten Revolution", die sich in einer andauernden Weiterentwicklung des Sozialismus manifestiert. Wesentliches Element ihrer politischen Arbeit ist der Entrismus, d.h. das Unterwandern von demokratischen Organisationen wie Parteien oder Gewerkschaften und die damit verbundene Einflussnahme auf deren Politik.

Marxistisch-leninistische und trotzkistische Organisationen agieren in der Regel nicht offen gewalttätig, stehen der Anwendung von Gewalt aber nicht grundsätzlich ablehnend gegenüber. Für den Fall einer revolutionären Situation, wird in der Anwendung von Gewalt ein probates Mittel für den politischen Kampf gesehen.

Autonom-anarchistische Szene

Die autonom-anarchistische Szene in Österreich lehnt feste Strukturen ab und organisiert sich meist in losen Gruppierungen und Plattformen. Aktivitäten und Aktionen werden häufig auf der Ebene bzw. in Form von „Bezugsgruppen" gesetzt. Die sich primär aus dem autonomen Spektrum zusammensetzenden „Bezugsgruppen" finden sich spontan/kurzfristig zu Aktionen zusammen, agieren konspirativ und zeigen oftmals eine Bereitschaft zu Gesetzesbrüchen und Gewaltakten. In Äußerungen und Stellungnahmen von Autonomen wird die „Gewaltfrage" grundsätzlich positiv beantwortet und als „Notwehr" und legitime Handlung gegen das aus ihrer Sicht „repressive" Gewaltmonopol des Staates gedeutet.

„**Autonom**" bedeutet so viel wie „eigenständig" und bezieht sich beim staatsschutzrelevanten Phänomenbereich Linksextremismus vor allem auf das Organisationsverständnis: Autonome lehnen die Integration in eine feste politische Struktur in Gestalt einer Partei oder eines Vereins ab. Demgegenüber plädieren sie für Eigen- und Selbstständigkeit, was sich auch in der Distanz gegenüber formalen Hierarchien und anderen Organisationen artikuliert. Autonome sind Anhänger einer linksextremistischen Subkultur, die mit anarchistischen und marxistisch-leninistischen Ideologiefragmenten in losen Personenzusammenschlüssen aktionistisch und oftmals spontan agieren. Autonome lehnen grundsätzlich die Normen und Regeln eines demokratischen Verfassungsstaates ab und bekämpfen diesen (nicht zuletzt auch mittels Gewalt).

Anarchismus ist eine Sammelbezeichnung für politische Auffassungen und Bestrebungen, die auf die Abschaffung jeglicher Herrschaft von Menschen über Menschen – insbesondere in Gestalt des Staates – ausgerichtet sind. Den unterschiedlich ausgerichteten anarchistischen Strömungen ist die Forderung gemein, den Staat als Herrschaftsinstitution von Menschen über Menschen abschaffen zu wollen – und zwar unabhängig von einer demokratischen oder diktatorischen Ausrichtung. Die Institution des Staates gilt im anarchistischen Selbstverständnis als repressive Zwangsinstanz, die zugunsten einer herrschaftsfreien Gesellschaft aufgelöst oder zerschlagen werden muss.

Im Mittelpunkt des politischen Handelns von Autonomen stehen das Individuum und seine Selbstverwirklichung; jede Form von Fremdbestimmung wird abgelehnt. Folgerichtig besteht aus autonomer Sicht auch kein Bedarf an der Formulierung konkreter

Zielvorgaben. Das zentrale Leitmotiv besteht de facto in der Negierung des Bestehenden. Die inhaltlichen Ausführungen von autonomen „Konzepten“ erschöpfen sich meist in der Formulierung von „Anti-Haltungen“, mit denen Missstände, Ungerechtigkeiten und negative Entwicklungen sichtbar gemacht werden sollen. Konkrete Konzepte zu deren Behebung oder Beseitigung werden aber nicht entwickelt, da im autonomen Politikverständnis einzig die Beseitigung der bestehenden Staats- und Gesellschaftsform als erstrebenswert und zielführend erachtet wird.

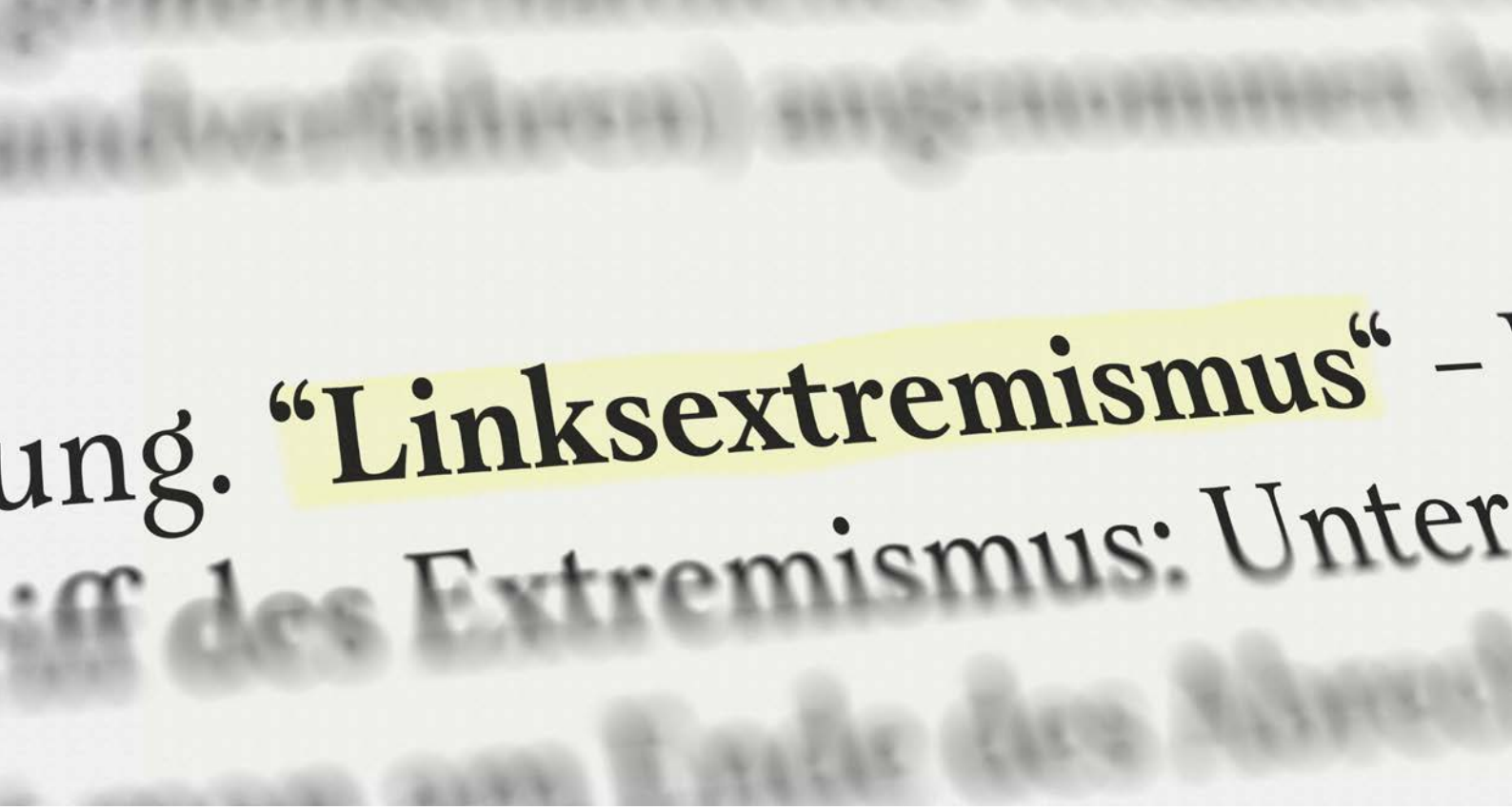
Themen und Aktivitäten linksextremistischer Szenen, Akteure und Gruppierungen

Wie schon in den Vorjahren, stellten auch im Jahr 2020 die autonom-anarchistischen Verbindungen die aktivsten Szenebereiche dar. Die von ihnen gesetzten Aktivitäten fokussierten sich primär auf Aktionen und Agitationen im Zusammenhang mit „Antifaschismus“, „Antirepression“, Flüchtlings- und Asylthemen, Kapitalismus-, Wirtschafts- und Sozialkritik sowie auf die Erlangung von „Freiräumen“. Kundgebungen und Protestaktionen zu diesen Themenbereichen führten auch zu gewalttätigen Handlungen.

Marxistisch-leninistische und trotzkistische Gruppen traten im Hinblick auf die Gefährdung der öffentlichen Ruhe, Ordnung und Sicherheit im Jahr 2020 kaum in Erscheinung. Die von ihnen thematisierten Bereiche konzentrierten sich so wie in den Vorjahren neben „Antifaschismus“ hauptsächlich auf Kapitalismus-, Globalisierungs- und Sozialkritik sowie auf das österreichische Asyl- und Fremdenwesen.

Die seit Jahren bestehenden internen Differenzen, Animositäten und Spaltungen der linksextremistischen Szene in getrennt agierende Spektren, wurden im Jahr 2020 lediglich anlassbezogen und temporär in Form von Kooperationsplattformen überwunden. „Antifaschismus“ sowie Aspekte der Flüchtlings-, Migrations- und Asylpolitik waren erneut Themenbereiche mit relevanten Mobilisierungspotenzialen. Dabei wurden analog zu den Vorjahren nicht nur radikale und extremistische Gruppierungen zum Ziel von Protesten, sondern auch im Parlament vertretene Parteien. Neben diesen „traditionellen“ Aktionsfeldern haben im Jahr 2020 neue Agitations- und Handlungsbereiche zumindest temporär Aktualität erlangt: Klima- und Umweltschutzthematiken, „Black Lives Matter“-Aktivitäten[12] und die COVID-19-Pandemie.

12 Black Lives Matter („Schwarze Leben zählen“) ist eine internationale Bewegung, die innerhalb der afroamerikanischen Gemeinschaft in den USA entstanden ist und sich gegen Gewalt People of Color einsetzt. Black Lives Matter organisiert regelmäßig Proteste gegen die Tötung von Afroamerikanern durch Polizeibeamte und zu breiteren Problemen wie Racial Profiling, Polizeigewalt und Rassismus. Die BLM-Bewegung ist ein dezentralisiertes Netzwerk und hat keine formale Hierarchie.



stock.adobe.com

Linksextreme Aktivisten traten im Jahr 2020 wiederholt bei Protestaktionen gegen deutschnationale Burschenschaften und gegen eine der „Neuen Rechten“ zuordenbaren Gruppierung in Erscheinung. Bei mehreren Veranstaltungen kam es zu Stör- und Blockadeversuchen und in einigen Fällen auch zu Gewalttätigkeiten.

Die COVID-19-Pandemie wurde analog zur internationalen Entwicklung auch von linksextremen Akteuren in Österreich genutzt, um vor allem via Internet und in Sozialen Medien szenetypische Texte, Aufrufe und Mobilisierungsappelle zu verbreiten. Über die Artikulierung szenetypischer Narrative hinausgehende konkrete physische (Tat-) Handlungen – z.B. Schmier-, Spray- und Plakataktionen – wurden nur wenige verübt. Zudem ist evident, dass linksextremistische Akteure, die zu Beginn der Pandemie noch versuchten den Protest gegen die Bundesregierung unter dem Vorwand der Kritik am COVID-19-Maßnahmengesetz mitzubestimmen, zunehmend eine Position als kritische Beobachter der Anti-COVID-19-Sammelbewegungen – insbesondere in Hinblick auf das Agieren von rechtsextremen Kreisen innerhalb dieser Bewegungen – eingenommen haben.

Ungeachtet des Faktums, dass die Mehrzahl der im Jahr 2020 stattgefundenen Demonstrationen und Kundgebungen, die von Organisationen/Exponenten des linksextremen Spektrums organisiert wurden oder an denen Szenevertreter teilgenommen haben, ohne staatspolizeilich relevante Vorfälle abgelaufen sind, wurden im Jahr 2020 wiederholt auch Fälle sowohl von konfrontativer als auch von klandestiner Gewaltausübung[13] durch Exponenten des linksextremen Spektrums registriert.

13 Im gewaltgeneigten Teil der österreichischen linksextremen Szene lassen sich grob zwei unterschiedliche Arten von strategischer Gewaltausübung unterscheiden:

Am 15. Jänner 2020 wurde in Wien ein Mitglied einer deutschnationalen Burschenschaft von zwei linksextremen Aktivisten tätlich angegriffen. Die mutmaßlichen Täter wurden festgenommen und wegen des Verdachts der Körperverletzung angezeigt.

Am 7. März 2020 wurde in Wien von einer der „Neuen Rechten" zuordenbaren Gruppierung eine Veranstaltung abgehalten, die von Exponenten der linksextremen Szene gestört und physisch angegriffen wurde.

Am 19. August 2020 wurde in Wien eine von einer Gruppierung der „Neuen Rechten" organisierte Veranstaltung von Aktivisten des autonomen Szenespektrums attackiert. Vier Exponenten der rechtsextremen Gruppierung wurden durch Schläge und Tritte verletzt.

Objekte und Einrichtungen von im Parlament vertretenen politischen Parteien wurden im Jahr 2020 mehrfach Ziel von Sachbeschädigungen, die aufgrund der Zielauswahl, der Modi Operandi und sonstiger Tatumstände linksextremen Aktivisten zugeordnet werden können:

- In der Nacht zum 19. März 2020 wurden Außenscheiben der ÖVP-Bundesparteizentrale in Wien massiv beschädigt.
- Im August 2020 wurde in Wien ein Fahrzeug der ÖVP Ziel einer Schmieraktion.
- Am 15. September 2020 wurde ein ÖVP-Parteilokal in Wien beschmiert.
- Am 6. November 2020 wurde die Parteizentrale der steirischen FPÖ in Graz mit Farbbeuteln beworfen.

Der gewaltsame Tod des schwarzen US-Amerikaners George Floyd[14] hat in den USA und in weiterer Folge weltweit unter dem Motto „Black Lives Matter" (BLM) stehende Proteste gegen Rassismus und Polizeigewalt ausgelöst. Die in Österreich stattgefundenen BLM-Kundgebungen verliefen grundsätzlich friedlich und gewaltfrei. Bei einigen Protesten bzw. im Gefolge oder im zeitlichen und örtlichen Nahbereich von derartigen Veranstaltungen wurden allerdings teils schwere Gewaltakte – primär in Form von Sachbeschädigungen – verübt. Bei den Tätern handelte es sich zum Teil erwiesenermaßen um Vertreter der linksextremen Szene, zum Teil ist aufgrund der Zielauswahl und der Modi Operandi mit hoher Wahrscheinlichkeit von linksextremen Tätern auszugehen:

- Konfrontative Gewalt: meist Gewalt im Zuge von Protestaktionen und Demonstrationen
- Klandestine Gewalt: verborgen vorbereitete und durchgeführte Gewalttaten (oftmals gegen Sachen, Einrichtungen und Objekte)

14 Die Tötung von George Floyd im Zuge einer gewaltsamen Festnahme durch Polizisten ereignete sich am 25. Mai 2020 in Minneapolis/Minnesota. Ein Video des Vorfalls führte weltweit zu Entsetzen und Empörung.

- Eine am 4. Juni 2020 von zivilgesellschaftlichen Gruppen organisierte und von rund 50.000 Personen (darunter auch Exponenten der linksextremen Szene) besuchte BLM-Kundgebung in Wien verlief weitestgehend ohne staatspolizeilich relevante Vorfälle. An der Fassade sowie an Türen der Karlskirche wurden allerdings diverse Vandalismusakte und Beschmierungen verübt, die zum Teil von Exponenten der linksextremen Szene bzw. von Tätern mit linksextremen Tatmotiven begangen worden sein dürften.
- Eine von zivilgesellschaftlichen Gruppen organisierte Kundgebung am 5. Juni 2020 in Wien mit rund 8.500 Teilnehmern verlief grundsätzlich friedlich und ruhig. Im Zuge einer von Aktivisten der „Neuen Rechten" gesetzten Stör- bzw. Provokationsaktion kam es zu physischen Zusammenstößen zwischen rechtsextremen Störern und Exponenten linksextremer Gruppierungen. Darüber hinaus wurden während der Kundgebung Polizeikräfte und Polizeifahrzeuge von linksextremen Aktivisten mit Flaschen und pyrotechnischen Gegenständen beworfen.

Im Zeitraum vom 2. bis 10. Juni 2020 wurden in Wien zahlreiche Sachbeschädigungen – neben diversen Schmieraktionen auch Brandstiftungen – an Gebäuden, öffentlichen Einrichtungen und Objekten sowie an Fahrzeugen der Polizei verübt, die einen direkten oder indirekten Bezug zur BLM-Thematik aufwiesen und zum Teil erwiesenermaßen und zum Teil mit hoher Wahrscheinlichkeit von Exponenten der linksextremen Szene bzw. von Tätern mit linksextremen Tatmotiven begangen wurden:

- In der Nacht zum 3. Juni 2020 wurden ein Amtsgebäude und ein Polizeiauto beschmiert.
- In der Nacht zum 8. Juni 2020 wurde die Windschutzscheibe eines abgestellten Polizeifahrzeuges eingeschlagen.
- Am 8. Juni 2020 wurde ein Polizeifahrzeug durch Deponierung eines Brandbeschleunigers auf einem Reifen in Brand gesetzt und schwer beschädigt.[15]
- In der Nacht zum 10. Juni 2020 wurde ein Polizeiauto unter Verwendung eines Brandbeschleunigers in Brand gesetzt und schwer beschädigt.

Im Zusammenhang mit den im Juni 2020 stattgefundenen BLM-Demonstrationen und -Protestaktionen wurden in Wien, Graz und Hartberg Denkmäler von historischen Persönlichkeiten, deren ehrende Würdigung aufgrund ihrer antisemitischen/rassistischen

15 In einem Bekennerschreiben auf der Onlineplattform emrawi.org wurden die Beschädigungen der Polizeifahrzeuge am 8. Juni 2020 thematisiert (die Plattform https://emrawi.org/ ist eine anonymisierte Homepage, die in mehreren Sprachen über linksextreme Aktionen in Europa berichtet).

Einstellungen, Äußerungen und Positionierungen bzw. ihrer evidenten NS-Sympathien kritisch bewertet werden, beschmiert und mit schriftlichen Kommentaren versehen.

Internationale Verbindungen

Die österreichische linksextreme Szene verfügt über diverse Auslandskontakte. Die intensivsten Beziehungen gibt es nach Deutschland und in geringerem Maße in andere (Nachbar-)Länder. Die internationalen Verbindungen weisen allerdings kein stabiles und strukturiertes Netzwerk auf, sondern basieren primär auf Einzelkontakten.

Die Beteiligung von österreichischen Szeneangehörigen an Aktionen im Ausland bewegt sich seit Jahren auf eher niedrigem Niveau und überschreitet in quantitativer Hinsicht meist kaum Kleinstgruppenstärke.

Ausländische Linksextremisten treten in Österreich eher selten in Erscheinung, was primär auf das Fehlen von relevanten Veranstaltungen in Österreich und die organisatorischen Schwächen der österreichischen Szene zurückzuführen ist.

Kommunikation und Medien

Um ihre Botschaften zu verbreiten, ihre Anliegen zu propagieren und ihre Ziele zu erreichen, nutzen die Exponenten und Gruppierungen der österreichischen linksextremen Szene ein breites Spektrum – von Aufklebern, Flugblättern, Druckwerken über Diskussionsveranstaltungen, Demonstrationen und aktionistischen Handlungen bis hin zu den vielfältigen Mitteln und Möglichkeiten digitaler Kommunikationstechnologien.

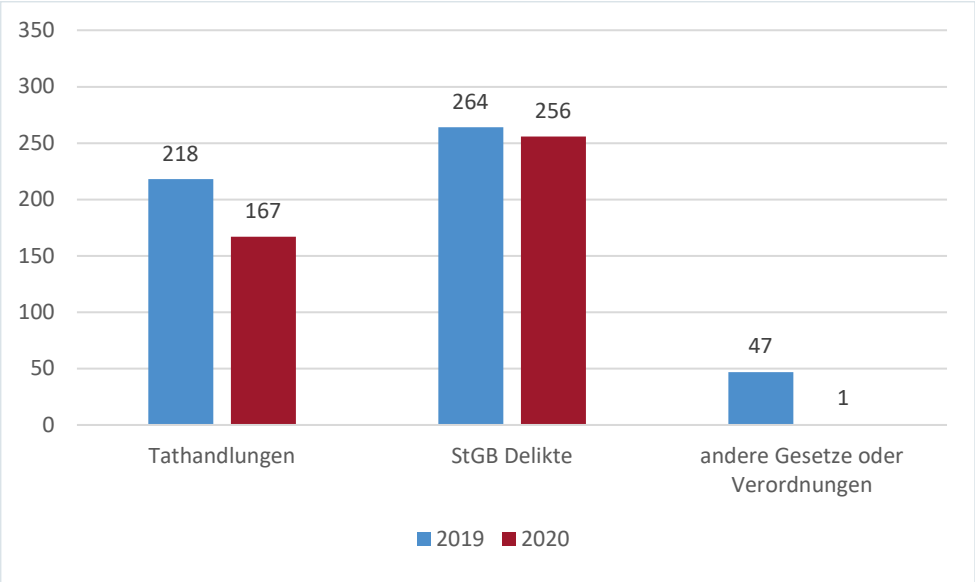
Die sich ständig weiterentwickelnden Möglichkeiten des Internets und die vielfältigen Nutzungsfelder von sozialen Medien sind ideale Instrumente für die linksextreme Kampagnenarbeit und die Diskussion zentraler Anliegen und Agitationsschwerpunkte. Die unterschiedlichen Plattformen, Messenger-Dienste, Blogs und Foren werden genutzt, um sich zu vernetzen, schnell Informationen im In- und Ausland auszutauschen, zu mobilisieren und Aktionen zu koordinieren.

Statistik

Im Vergleich zum Vorjahr zeigten die Straftaten, die linksextremistischen Gruppierungen bzw. Tätern zugerechnet werden konnten, einen rückläufigen Trend.

2020 sind in Österreich insgesamt 167 Tathandlungen mit erwiesenen oder vermuteten linksextremen Tatmotiven bekannt geworden (2019: 218 Tathandlungen), wobei eine Tathandlung mehrere Delikte mit gesonderten Anzeigen beinhalten kann. 12 Tathandlungen, das sind 7,2 Prozent, konnten aufgeklärt werden (Aufklärungsquote

2019: 11,5 Prozent). Im Zusammenhang mit den angeführten Tathandlungen wurden bundesweit 257 Anzeigen (2019: 311 Anzeigen), davon 256 nach dem Strafgesetzbuch (StGB)[16], erstattet. Im Zuge der Bekämpfung linksextremer Aktivitäten wurden im Berichtsjahr insgesamt 38 Personen angezeigt (2019: 72), davon 8 Frauen (2019: 29) und 5 Jugendliche (2019: 3).



Tathandlungen/Anzeigen – Vergleich 2019/2020

Ein Vergleich der Jahre 2019 und 2020 zeigt einen Rückgang sowohl der einschlägigen Tathandlungen (– 23,4 Prozent) als auch der im Zusammenhang mit diesen Tathandlungen erstatteten Anzeigen (– 17,4 Prozent).

Der in den Jahren 2018 und 2019 gegebene Hotspot-Charakter der Bundesländer Wien, Salzburg, Tirol und Steiermark war auch im Jahr 2020 evident:

- Wien: 67 Tathandlungen (40,1 Prozent aller linksextrem motivierten Tathandlungen) und 137 Anzeigen (53,3 Prozent aller Anzeigen)
- Salzburg: 29 Tathandlungen (17,4 Prozent) und 37 Anzeigen (14,4 Prozent)
- Tirol: 25 Tathandlungen (15,0 Prozent) und 29 Anzeigen (11,3 Prozent)
- Steiermark: 24 Tathandlungen (14,4 Prozent) und 27 Anzeigen (10,5 Prozent)

16 Von den 256 Anzeigen nach dem Strafgesetzbuch entfiel die überwiegende Mehrheit auf Sachbeschädigungen (145 Anzeigen nach § 125 StGB und 31 Anzeigen nach § 126 StGB).

Anzeigen	2019	2020
Anzeigen nach dem StGB		
Körperverletzung (§ 83 StGB)	2	12
Schwere Körperverletzung (§ 84 StGB)	5	21
Gefährdung der körperlichen Sicherheit (§ 89 StGB)	1	1
Raufhandel (§ 91 StGB)	0	21
Nötigung (§ 105 StGB)	0	1
Schwere Nötigung (§ 106 StGB)	0	4
Gefährliche Drohung (§ 107 StGB)	4	2
Beleidigung (§ 115 StGB)	1	2
Berechtigung zur Anklage (§ 117 StGB)	0	2
Sachbeschädigung (§ 125 StGB)	194	145
Schwere Sachbeschädigung (§ 126 StGB)	19	31
Diebstahl (§ 127 StGB)	12	1
Brandstiftung (§ 169 StGB)	3	5
Vorsätzliche Gefährdung von Menschen durch übertragbare Krankheiten (§ 178 StGB)	0	1
Widerstand gegen die Staatsgewalt (§ 269 StGB)	5	1
Aufforderung zu mit Strafe bedrohten Handlungen und Gutheißung mit Strafe bedrohter Handlungen (§ 282 StGB)	3	3
Verhetzung (§ 283 StGB)	0	3
Sonstige StGB Delikte	15	0
Anzeigen nach anderen Gesetzen/Verordnungen		
Waffengesetz (§ 50)	0	1
Sonstige Gesetze/Verordnungen (z.B. Versammlungsgesetz, Sicherheitspolizeigesetz, Pyrotechnikgesetz)	47	0
Summe	311	257

Trends und Entwicklungen

Im Phänomenbereich Linksextremismus sind in näherer Zukunft keine substantiellen Änderungen erwartbar. Festzuhalten ist allerdings, dass Aktivitäten und Mobilisierungspotenziale der österreichischen Szene stark von aktuellen politischen, wirtschaftlichen und gesellschaftlichen Entwicklungen und Ereignissen – sowohl auf nationaler als auch auf internationaler Ebene – beeinflusst werden.

Es ist davon auszugehen, dass auch weiterhin das Aktionsfeld „Antifaschismus“ ein das gesamte linksextreme Spektrum umfassendes Mobilisierungspotenzial besitzen wird. Sofern allfällige antifaschistische (Protest-)Kundgebungen auf Exponenten der inländischen Szene beschränkt bleiben, sind in quantitativer Hinsicht überschaubare Teilnehmerzahlen zu erwarten.

Darüber hinaus ist erwartbar, dass die in jüngerer Zeit relevanten Themenfelder – zu nennen sind v.a. die COVID-19-Pandemie, die Flüchtlingsproblematik, die Klimakrise, die Kurdenthematik und „Black Lives Matter“-Aktivitäten – von der linksextremen Szene weiterhin in ihrem Sinn interpretiert und instrumentalisiert werden. Das diesbezüglich denkbare bzw. mögliche Handlungsspektrum umfasst neben gewaltfreien Aktivitätsformen grundsätzlich auch gewalttätige Manifestationsformen.[17]

Bedingt durch die in quantitativer Hinsicht eher kleine österreichische Szene, die evidenten organisatorischen Schwächen sowie aufgrund des Umstandes, dass internationale Veranstaltungen und sonstige Anlässe für großangelegte und erfolgversprechende Mobilisierungskampagnen in Österreich in der Regel fehlen, dürfte das Mobilisierungspotenzial des linksextremen Spektrums in personeller Hinsicht auch weiterhin beschränkt bleiben.

Das linksextreme Gewaltpotenzial wird sich mit hoher Wahrscheinlichkeit weiterhin im autonom-anarchistischen Spektrum konzentrieren. Zum Ausleben ihrer Gewaltbereitschaft benötigen diese Kreise erfahrungsgemäß ein schützendes Umfeld (z.B. eine Großdemonstration).[18]

Der Linksextremismus stellt gegenwärtig keine ernsthafte Gefahr für die Funktions- und Handlungsfähigkeit des Staates bzw. der Verfassung dar. Für die öffentliche Ruhe,

---

17 Insbesondere im Zusammenhang mit den erwartbaren mittel- und langfristigen politischen, wirtschaftlichen und sozialen Auswirkungen und Folgen der Corona-Krise (Stichwort Arbeitslosigkeit) und der anzunehmenden weiteren bzw. intensivierten Thematisierung der Corona-Thematik durch Exponenten/Gruppierungen/Parteien aus dem Bereich des rechtsextremen Spektrums, ist für die Zukunft eine Wiederaufnahme bzw. eine erneute Priorisierung des „Themenfeldes Corona“ als mögliches Szenario in Betracht zu ziehen. Seitens linksextremer Akteure sind in diesem Zusammenhang neben Internet- und Social-Media-Aktivitäten primär per se nicht gewalttätige Protestmanifestationen bzw. aktionistische Handlungen und Formen des zivilen Ungehorsams (z.B. Blockadeaktionen) in Betracht zu ziehen. Neben gewaltfreien Aktionsformen sind aber auch Aktivitäten in Form von „direkten Aktionen“ (z.B. Sachbeschädigungen an Einrichtungen und Objekten) als mögliche Handlungsszenarien zu bewerten.

18 Neben Straßenmilitanz im Zuge beziehungsweise am Rande oder nach dem offiziellen Ende von Demonstrationen sind auch klandestin vorbereitete und durchgeführte Gewalttaten durch Klein- und Kleinstgruppierungen als mögliche Szenarien in Betracht zu ziehen.

Ordnung und Sicherheit sind Teilbereiche des linksextremen Spektrums jedoch – temporär und anlassbezogen – als Risiko zu bewerten.

Nachrichtendienste und Spionageabwehr

Lagebild

Nachrichtendienste sowie weitere staatliche und staatsnahe Organisationen sind verantwortlich für geheime Beschaffungsvorgänge und Einflussnahmen im Ausland. Österreich ist nach wie vor Operationsgebiet solcher Akteure. Dazu tragen seine EU-Mitgliedschaft, der Sitz mehrerer internationaler Organisationen, seine Unternehmenslandschaft und ein starker Forschungsstandort, aber nicht zuletzt auch die günstige Gesetzeslage bei. Ebenso geraten die aus autoritären Herkunftsländern stammenden Diasporagemeinden Österreichs immer mehr in den Fokus nachrichtendienstlicher Organisationen. Auch vor nachrichtendienstlicher Aktivität aus dem virtuellen Raum, wie Cyberangriffen oder der Verbreitung von Desinformation bleibt Österreich nicht verschont.

Die politischen Zielsetzungen der jeweiligen ausländischen Regierungen geben die Schwerpunkte der Arbeit ihrer Nachrichtendienste vor. Je nachdem können nachrichtendienstliche Aktionen politischen, wirtschaftlichen, (technisch-) wissenschaftlichen oder militärischen Interessen dienen. Für die Aufklärung von besonderem Interesse sind die österreichische Haltung zu Fragen der Außen-, Sicherheits- und zusehends der Gesundheitpolitik. Je einflussreicher und hegemonialer Staaten im Bereich der internationalen Politik sind, umso mehr tendieren sie dazu, ihre im Ausland aktiven Nachrichtendienste nicht nur mit der Ausspähung, sondern auch mit der Beeinflussung der Entwicklungen anderer Staaten zu beauftragen. Ansatzpunkte für derartige Maßnahmen sind vor allem politische Entscheidungsträger oder Beamte in Schlüsselpositionen.

Eine große Anzahl von ausländischen Nachrichtendienstoffizieren wird in Österreich nach wie vor unter der Tarnung sogenannter Legalresidenturen wie Botschaften, Konsulaten und internationalen Organisationen tätig. Hinzu kommen halboffizielle Einrichtungen – beispielsweise Fluggesellschaften, Presseagenturen, Vereine, Kulturzentren, aber auch Firmenniederlassungen –, die der nachrichtendienstlichen Abdeckung dienen können. Der Verantwortungsbereich von in Österreich stationierten Nachrichtendienstoffizieren soll sich neben dem Bundesgebiet auch auf andere Länder der Europäischen Union erstrecken und so – im Auftrag der jeweiligen Regierung – auch eine Kontrolle der Botschaftsangehörigen und anderer Staatsbürger im Ausland ermöglichen. Auch kleinere autoritäre Staaten mit potenten Nachrichtendiensten nehmen fallweise Einfluss auf ihre Staatsbürger im Ausland und verstoßen dabei gegen das Recht des Gastlandes. Dies geht

bis zu unfreiwilligen Außerlandesbringungen oder sogar Kidnapping von Asylwerbern, in einzelnen Fällen zu Anschlagsversuchen, wie Vorkommnisse in anderen EU-Staaten gezeigt haben.

Wirtschaftsspionage und andere Formen des Wissensabflusses

Informationen im Bereich von Wirtschaft, Wissenschaft und Technik dringen durch Spionage, jedoch auch durch legale Methoden aus Österreich ins Ausland. Forschungs- und Bildungseinrichtungen sowie innovative Unternehmen bergen Schlüsseltechnologien und Hidden Champions[19]. Sie alle sind potenzielle Ziele von Ausspähung. Die Faktoren Mensch und Technik stellen dabei gleichermaßen ein Risiko dar.

So erfolgt Spionage unter Ausnützung von Sicherheitslücken in IT-Systemen aber auch nach wie vor auf konventionellen Wegen. Dabei kommt es zur Anwerbung von Insidern, sowohl auf persönlicher Ebene als auch in sozialen Netzen. Die enge Kooperation des BVT mit Wirtschaft, Wirtschaftsverbänden und Hochschulen bildet den Kern im Kampf gegen diese Wirtschafts- und Industriespionage[20]. Im Vordergrund stehen dabei Vortragstätigkeiten in denen auf Spionagemethoden und geeignete Schutzmaßnahmen eingegangen wird. Erfahrungen zeigten, dass sich dahingehend sensibilisierte Mitarbeiter der Gefahren weitaus bewusster sind. Schaden kann somit häufig abgewendet und Wirtschaftsgeheimnisse gewahrt werden.

Bedenklich stimmen jedoch legale Formen des Wissensabflusses. Dazu zählt beispielsweise die Rekrutierung hochqualifizierter Wissenschaftler unter dem Deckmantel von Stipendien oder Preisen, um sie – zumindest temporär – an Forschungsprojekten im Ausland zu beteiligen, wo sie ihre Expertise – gänzlich ohne Spionage – vor Ort abliefern. Auch bei Veräußerungen von Schlüsseltechnologie-Unternehmen wird keine strafrechtliche Schwelle überschritten. Solch massiver Wissensabfluss schwächt die österreichische Wirtschaft potenziell jedoch zumindest auf zweierlei Arten. Einerseits bewirkt der Abfluss des Knowhows eine Einbuße des Wettbewerbsvorteils, andererseits öffnet der unternehmerische Kontrollverlust das Tor für mögliche staatliche Einflußnahme. Diese Vorgangsweise erstreckt sich in Österreich etwa auf Luftfahrtindustrie sowie Automobil- und Leiterhersteller. Mehrheitliche Veräußerungen österreichischer Betriebe an fremde staatseigene Unternehmen, die selbst mit politischen Kadern durchsetzt sind, scheinen daher problematisch – umso mehr, wenn es sich dabei um Rüstungsunternehmen handelt.

---

19 Einige Klein- und mittelständische Unternehmen dominieren Marktsegmente oder ganze Branchen ohne auf eine offensive Kommunikationspolitik setzen zu müssen und sind der breiten Öffentlichkeit oft nicht bekannt. Sie werden daher „heimliche Meister (Hidden Champions)“ genannt.

20 *Wirtschaftsspionage* geht von fremden Staaten aus, während man bei konkurrierenden Unternehmen von *Industriespionage* spricht.

Nachrichtendienste und Zivilgesellschaft

Nachrichtendienste und andere staatliche Akteure trachten danach, in Österreich etablierte Diasporagemeinden zu unterwandern. Dies dient einerseits dazu, Regimekritiker im Ausland auszuspähen und gegebenenfalls unter Druck setzen zu können; andererseits dazu, die Diaspora selbst für nachrichtendienstliche Zwecke zu instrumentalisieren oder für politische Ziele zu mobilisieren. Solche Interaktionen ließen sich in Österreich bisher etwa in der iranischen und türkischen, zusehends aber auch der chinesischen Gemeinde beobachten. In diese Arbeit sind auch diplomatische Vertretungen, Vereine, Bildungseinrichtungen und Nachrichtenagenturen eingebunden.

Wie stark die Unterwanderung von Diasporagemeinden in Österreich sein kann, zeigten beispielsweise die Ausschreitungen in Favoriten im Sommer 2020. Eine unmittelbare Steuerung der Proteste durch ausländische Nachrichtendienste und staatliche Akteure konnte jedoch nicht nachgewiesen werden. Allerdings wurde deutlich, wie hoch das Mobilisierungspotential, insbesondere bei der vulnerableren, jüngeren Generation, ist, und wie schnell sich importierte, grundsätzlich innerhalb bzw. zwischen den Diasporagemeinden ausgetragenen Konflikte über die Diasporagrenzen hinaus entwickeln und zu Stimmungseskalationen, Provokationen und Gewaltausbrüchen führen können. Die durch diese Ereignisse erzeugten Unruhen zogen medial die Aufmerksamkeit auf sich und führten in weiterer Folge auch zur Polarisierung in der österreichischen Gesellschaft hinsichtlich der betroffenen Diasporagemeinden.

stock.adobe.com

Aber auch die allgemeine Gesellschaft Österreichs ist Ziel staatlicher Beeinflussung und Ausspähung. Versuche der Einflussnahme durch ausländische Nachrichtendienste dienen dem Zweck der Destabilisierung eines funktionierenden Staates, der Schaffung von Unruhen 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. Zudem führen Spionageangriffe zu Spannungsverhältnissen und gefährden letztlich das notwendige zwischenstaatliche Vertrauen.

In den vergangenen Jahren konnten in verschiedenen gesellschaftlichen Bereichen Anwerbungsversuche durch ausländische Nachrichtendienste festgestellt werden. Neben dem Versuch, mit Hilfe von menschlichen Quellen an vertrauliche bzw. geheime Informationen zu gelangen[21], haben nachrichtendienstliche Aktionen zum Zwecke der Einflussnahme auf staatliche Entscheidungs- und Machtstrukturen an Relevanz gewonnen.

Trends und Entwicklungen

Nachrichtendienstliches Personal beteiligt sich auch an der Beschaffung sanktionierter Güter und Devisen, sowie von Waffen, Dual-Use-Gütern[22] und proliferationsrelevantem Material[23]. Der Iran hat sich nach dem Austritt der Vereinigten Staaten aus dem Atomabkommen und der Tötung einiger Schlüsselfiguren selbst aus dem Abkommen zurückgezogen und begann mit der Anreicherung von waffenfähigem Spaltmaterial. Ähnliches gilt für die Demokratische Volksrepublik Korea, die bereits über Kernwaffen verfügte, und nach einer Zeit der Entspannung, die den Olympischen Winterspielen von 2018 folgte, nun wieder ihr Raketenprogramm vorantreibt. Da diese und weitere Staaten auch unter einem allgemein hohen Sanktionsdruck stehen, ist von geheimen Beschaffungsversuchen im Ausland – daher auch in Österreich – durch Nachrichtendienste wieder vermehrt auszugehen.

Auch an Cyberangriffen sind häufig Nachrichtendienste beteiligt. Einige Dienste betreiben darauf spezialisierte Abteilungen im Herkunftsland oder sicheren Drittländern, von wo aus Störangriffe (*Denial of Service Attacks*) – wie auf das BMEIA Anfang 2020 – gestartet werden oder *Ransomware*[24] verteilt wird, um Devisen zu lukrieren. Aber auch operative Teams in Europa dringen vor Ort physisch in IT-Systeme ein, um sich Zugang zu geheimen Informationen zu verschaffen.

---

21 Diese klassische Spionageform wird als *Human Intelligence (HUMINT)* bezeichnet.

22 Zahlreiche Produkte und Technologien können neben ihrer friedlichen Verwendung auch für militärische Zwecke genutzt werden, weshalb ihre Ausfuhr reglementiert ist.

23 Dazu zählen das Material zur Herstellung von Massenvernichtungswaffen und deren Trägersystemen sowie das erforderliche Knowhow.

24 Einer der größten und bekanntesten Ransomware-Abgriffe der letzten Jahre, hinter denen ein staatlicher Nachrichtendienst vermutet wird, war die Schadsoftware *WannaCry*.

Das Streuen von Fake-News und andere Desinformationskampagnen sind nicht auf extremistische Gruppierungen beschränkt, sondern dienen auch staatlichen Akteuren zur Einflussnahme und werden ebenfalls überwiegend auf der Cyber-Ebene betrieben. Insbesondere vor anstehenden Wahlen sind solche Versuche zu erwarten. Das Jahr 2020 war geprägt von falschen Informationen über das Virus SARS-CoV-2, insbesondere seinem Ursprung. Mit der Fertigstellung der ersten Impfstoffe begann erneut eine Welle von Falschmeldungen, die immer noch anhält.

Cyber-Sicherheit

Lagebild

Der Berichtszeitraum 2020 begann mit einem Cyber-Sicherheitsvorfall in einer verfassungsmäßigen Einrichtung, der es zum ersten Mal seit in Kraft treten des NISG notwendig machte, eine Cyberkrise festzustellen. Es wurde ein Angriff auf das Computernetzwerk des österreichischen Außenministeriums (BMEIA) detektiert und es war damit einem Akteur gelungen, das BMEIA-Netzwerk zu kompromittieren. Nach Bekanntwerden des Angriffs zum Jahreswechsel 2019/20 durch einen anhand von Sicherheitssystemen registrierten verdächtigen Datenverkehr, wurde unverzüglich eine erste Beurteilung durchgeführt und es wurden Gegenmaßnahmen mit dementsprechenden Sicherheitsvorkehrungen eingeleitet. Basierend auf fundierten Analysen des BMEIA gemeinsam mit dem BVT, wurde der IKDOK- und der CKM-Ausschuss am 4. Jänner 2020 einberufen. In weiterer Folge wurde ein Einsatzstab aus BMI, BMLV, BKA (inkl. AT-GovCERT) und BMEIA gebildet, um etwaigen Schaden zu minimieren und den Angriff zu beenden. Dank raschen Erkennens und effektiver interministerieller Zusammenarbeit konnte der Angriff unter Verantwortung des BMEIA Anfang Februar 2020 abgewehrt und eine Bereinigung des Netzwerkes ohne bleibende Schäden durchgeführt werden. Es wurde zudem auch eine österreichische Cyber-Sicherheitsfirma durch das BMEIA zugezogen. Der Angriff und die durch den Akteur gezeigten Verhaltensmuster (TTP; Tactics, Techniques and Procedures (TTP)) kennzeichnen einen Advanced Persistent Threat (APT). Ein strafrechtliches Ermittlungsverfahren ist anhängig. Im Zuge des Cybervorfalls wurden zahlreiche Maßnahmen eingeführt, die die Resilienz des BMEIA-Netzwerks nachhaltig verstärkt haben.

Das vorrangige Ziel von APTs ist die Beschaffung von Informationen im Kontext von Wirtschafts- und Industriespionage, oder wie im Fall des BMEIA, die politisch motivierte Ausspähung. Darüber hinaus erlauben APTs den Angreifern Computernetzwerke in Verwaltung, Produktions- und Lieferketten zu sabotieren. Dies kann bis zur vollständigen Unbrauchbarkeit der Systeme und zu Reputationsverlust führen.

COVID-19 im Cyber-Raum

Die Ausrufung einer Gesundheits-Pandemie im Frühjahr 2020, kurz nach Beendigung der zuvor angeführten Cyber-Krise, führte weltweit nicht nur zu einem massiven Anstieg von Phishing- und Betrugsversuchen mit Pandemie-Ködern als Event based Social Engineering, sondern auch zu einem Absenken von Perimeter-Cyber-Sicherheit in Unternehmen und anderen Einrichtungen. Dieses Absenken war oftmals notwendig um den massiv erhöhten Bedarf an Teleworking/Homeoffice, entstanden durch die Einschränkung der Bewegungsfreiheit aufgrund von Ausgangssperren (Lockdowns), zu ermöglichen. Auch kam es vor allem zu Beginn der Krise zu Störungen in Teleworking-Lieferketten (Cyber Supply Chain) von IT-Systemen, bedingt durch die massive Zunahme von Heimarbeitsplätzen (Homeoffice/Teleworking) und den daraus resultierenden notwendigen Beschaffungen.

Unternehmen waren zudem oftmals gezwungen, ihre eigenen Cyber-Sicherheitsbarrieren abzusenken, um den Remote-Zugriff von außerhalb für ihre Angestellten und Bediensteten zu ermöglichen oder E-Mail-Systeme über das Internet erreichbar zu machen. Dies führte zwangsläufig zu einer enormen Vergrößerung der Angriffsfläche und somit neuer Angriffsvektoren über meist private IKT, welche nun mit organisationsinterner IKT verbunden wurde.

Ebenfalls führte das Streben und die damit verbundenen nationalstaatlichen „Wettläufe“ inklusive medialer Berichterstattung bezüglich COVID-19-Impfstoffforschung zu erhöhtem Interesse nicht nur in der Öffentlichkeit und bei Cyber-Kriminellen, sondern auch bei wirtschaftlichen oder staatlichen Konkurrenten. Es wurden zahlreiche Warnungen von Sicherheitsbehörden hinsichtlich Cyber-Spionageaktivitäten ausgegeben, so auch durch das BVT, wo zusätzlich noch Sensibilisierungsgespräche bei Unternehmen geführt wurden. Die Bedrohungslage wurde durch eine fast zeitgleich bekannt gewordenen Sicherheitslücke in RDP-Gateways und einem Remote Log On Protokoll verschärft.

Im Berichtszeitraum kam es in diesem Zusammenhang allerdings in Österreich zu keinen schwerwiegenden Cyber-Sicherherheitsvorfällen in kritischen Infrastrukturen oder Einrichtungen der öffentlichen Verwaltung. Dieser erfreuliche Umstand sollte allerdings nicht zum Anlass genommen werden, weiterhin mit diesem abgesenkten Sicherheitsniveau zu operieren, nur weil es „funktioniert“.

Das österreichische Festnetz und die Mobilnetze hielten nach Angaben der RTR dem Stresstest durch Corona weitgehend stand. Im Zusammenhang mit der COVID-19-Krise und der zu Beginn forcierten Ausrollung einer Kontakt-Nachverfolgungs-Software für Smartphones – und in weiterer Folge durch das Rote Kreuz als Rot-Kreuz-App –, wurde durch den IKDOK eine Bedrohungsanalyse und ein Anforderungskatalog für Covid-19 Contact Tracing Mobile Apps erarbeitet und dem Bundesministerium für Soziales,

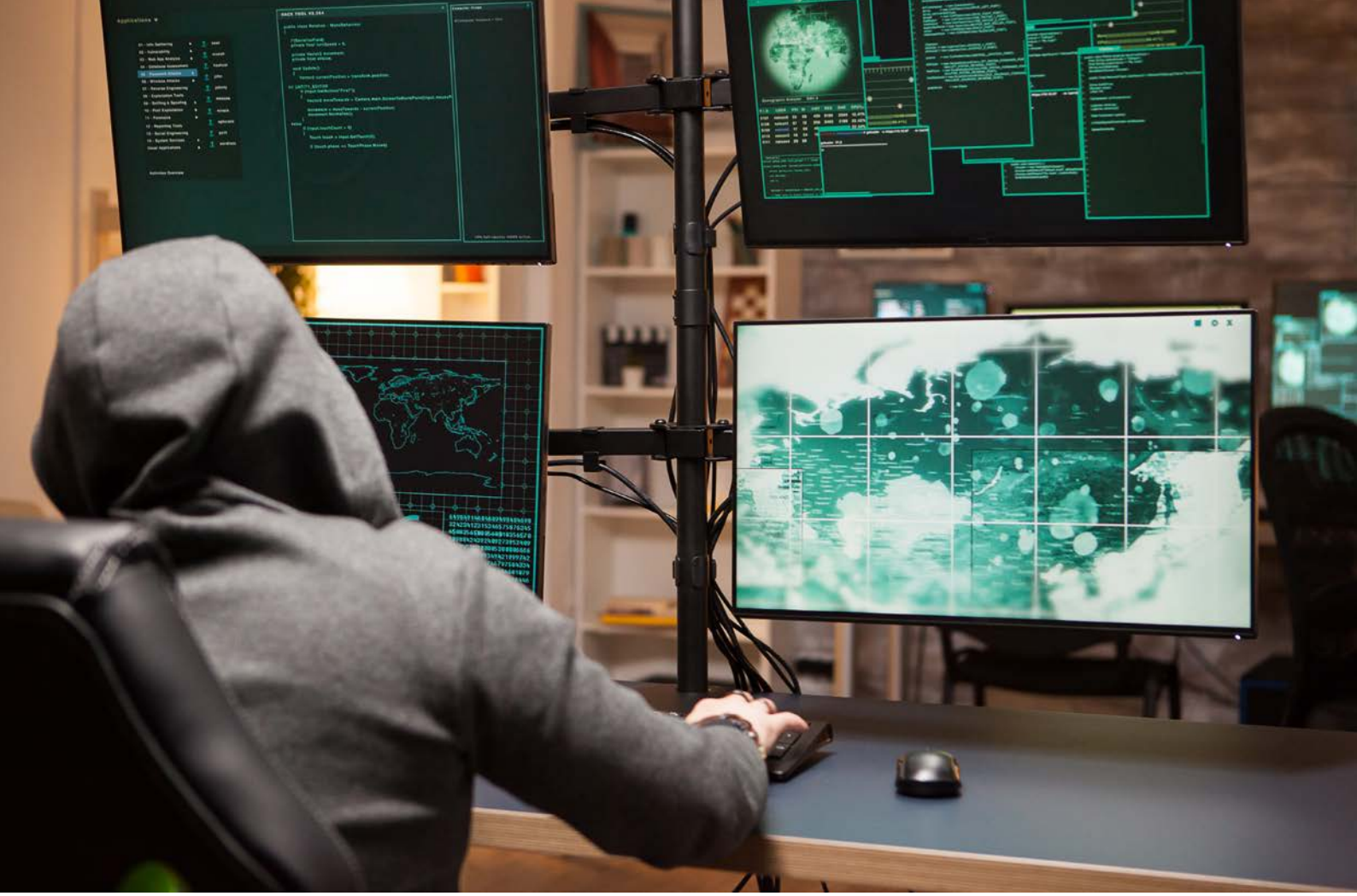
Gesundheit, Pflege und Konsumentenschutz (BMSGPK) zur weiteren Verwendung zur Verfügung gestellt.

Der zu Beginn durch Cyber-Kriminelle ausgerufene weltweite „Verzicht", Organisationen aus dem Gesundheitsbereich gezielt anzugreifen, wurde nicht von allen eingehalten und kann mittlerweile als obsolet angesehen werden. International waren einige Angriffe auf Krankenhäuser zu verzeichnen, wobei es sich eher nicht um gezielte Angriffe gehandelt haben dürfte, wie das Beispiel der Uni-Klinik in Düsseldorf veranschaulicht. Die Krankenhausbetreiber erhielten die Schlüssel zur Entschlüsselung der Daten, ohne Lösegeld dafür zu bezahlen. In Österreich waren jedoch keine Angriffe mit Ransomware auf Gesundheiteinrichtungen zu verzeichnen.

Ransomware: Als Ransomware werden Schadprogramme bezeichnet, die speziell dafür entwickelt wurden, den Zugriff auf Daten und Computersysteme einzuschränken bzw. zu verhindern. Sobald ein System mit der Schadsoftware infiziert ist, werden die Daten darauf verschlüsselt, sodass von den rechtmäßigen Nutzern nicht mehr darauf zugegriffen werden kann. Von der Verschlüsselung sind auch externe Datenträger und Netzlaufwerke betroffen. Sofern die Daten nicht vorsorglich mit einem Backup gesichert wurden, sind diese verloren, wenn nicht innerhalb einer bestimmten Zeit ein „Lösegeld" (engl. Ransom) dafür bezahlt wird.

Digitale Wegelagerei

Die Bedrohungen durch Ransomware oder mittels DDoS (Distributed Denial of Service) blieben im Berichtszeitraum weiter hoch. Vor allem bei Ransmware gab es laut einem Bericht von Fortinet weltweit eine Versiebenfachung von Angriffen im zweiten Halbjahr des Berichtszeitraums. Dieser Trend machte sich auch in Österreich bemerkbar. Zudem wurden die Angriffe gezielter und um jeweils eine Facette bereichert. So fordern nun Täter einerseits nicht mehr „nur" Lösegeld für Entschlüsselung, sondern drohen nun auch mit der Veröffentlichung von im Zuge des Ransomware-Angriffs erbeuteter Daten. Waren DDoS-Angriffe das Mittel zum Zweck, wurde mit weiteren, erheblich stärkeren DDoS-Angriffen zur Lahmlegung der „internet facing" IT-Infrastruktur gedroht, sollte bei diesem ersten „Warnschuss", mit gleichzeitigem Eingang einer entsprechenden Erpresser-E-Mail, nicht „Schutzgeld" in Form von Kryptowährung bezahlt werden. Es folgten aber unmittelbar nach Verstreichen der knapp gesetzten Frist keine weiteren Angriffe. Gegen Ende des Berichtsjahres wurden aber Unternehmen, welche auf den ersten Erpressungsversuch in den Vormonaten nicht eingegangen waren, erneut, mit Bezug auf den ersten, angegriffen. In einigen Fällen handelte es sich um Trittbrettfahrer, die in den Erpresserschreiben Namen bekannter Tätergruppen (u.a. Fancy Bear, Lazarus)



stock.adobe.com

verwendeten, um ihren Ansinnen mehr Glaubwürdigkeit und Nachdruck zu verleihen. National wie international kam es zu mehreren Wellen solcher erpresserischen DDoS-Angriffe, vor allem im Banken- und Finanzsektor und auf Internet Service Provider (ISP) im Sektor der digitalen Infrastruktur. Dieses Phänomen tritt weltweit und zunehmend auch in unterschiedlichen Sektoren auf, oftmals mit identen Erpesserschreiben. Lediglich die Adressen der Kryptowährungen (oftmals Bitcoin) und die Absender-Email-Adressen variieren. Es ist jedoch nicht ersichtlich, ob es sich dabei um nur eine Tätergruppe handelt oder mehrere Tätergruppen aktiv sind. Die Form der digitalen Wegelagerei wird durch die zunehmende Vernetzung und die Einbindung von meist gering gesichertern Computern oder IoTs in Bot-Netze einen weiter ansteigenden Trend erfahren.

Beim Phänomen Ransomware, das im Berichtszeitraum große Schäden verursachte, wird die Angst der Opfer ausgenützt, dass Daten aus dem befallenen Computernetzwerk veröffentlicht werden könnten. Die Täter erhoffen sich dadurch eine gesteigerte „Motivation“ des Opfers zur Bezahlung des geforderten Lösegelds. Die Höhe des geforderten Lösegelds bemisst sich häufig an der finanziellen Situation des Opfers, welche meist durch Recherche in offenen Quellen beurteilt wird. Als Angriffsvektor dient hier in den meisten Fällen ein mit Schadcode verseuchtes MS-Office-Dokument als Anhang zu einem E-Mail, welches mittels der Methode des Social Engineering an den Empfänger, gezielt oder als Spam, versandt wird.

Auswahl an kritischen Schwachstellen im Berichtszeitraum

Zahlreiche neu entdeckte und auch veröffentlichte Schwachstellen hielten im Berichtszeitraum die Risiken für Unternehmen und verfassungsmäßige Einrichtungen mit Abhängigkeiten von Cloud-Infrastrukturen, Remote-Zugängen für Teleworking und bei digitalen Lieferketten (Cyber Supply Chain) auf entsprechend hohem Niveau. Das Risiko wurde durch die Vergrößerung der Angriffsfläche durch die starke, notgedrungene Zunahme von Teleworking massiv erhöht, da gleich zu Beginn des Berichtszeitraums, und somit zu Beginn der COVID-19 Krise, kritische Schwachstellen bei Hard- und Software für Fernzugänge (Remote Desktop Verbindungen) bekannt wurden.

Cyber Supply Chain

Gegen Jahresende 2020 wurde ein Cyber-Sicherheitsvorfall bekannt, welcher die Abhängigkeit innerhalb der Cyber Supply Chain und deren Verwundbarkeit dramatisch offenlegte. Der mutmaßlich initiale Vorfall ereignete sich bei einem US-amerikanischen Unternehmen, welches im Bereich von Software-Lösungen für Computer-Netzwerkverwaltung tätig ist – SolarWinds. In der Folge des erfolgreichen Angriffs wurde durch die Täterschaft das Software-Produkt Orion von SolarWinds innerhalb der unternehmenseigenen Infrastruktur kompromittiert. Da diese Software auch von US- Regierungsbehörden sowie dem Großteil der Fortune-500-Unternehmen und auch international eingesetzt wird, wurde umgehend nach Bekanntwerden des Vorfalls eine Notfallwarnung durch die US-Cyber-Sicherheitsbehörde CISA ausgesprochen, die eine sofortige Einstellung der Nutzung der Plattform empfahl. Nachfolgende Attacken unter anderem auf das US-Finanzministerium und die Telekommunikationsbehörde NTIA, die zum US-Handelsministerium gehört, sind bereits evident. In Österreich ist diese Software-Plattform wenig verbreitet und wird in keinem kritischen Sektor eingesetzt. Wie kam es zu diesem Cyber-Sicherheitsvorfall mit großer Auswirkung?

Einem Angreifer war es bereits im Herbst 2019 gelungen, in das Unternehmensnetzwerk von SolarWinds einzudringen und in Folge dessen die Software-Update-Infrastruktur zu kompromittieren. Kunden, welche Updates des in ihrer Integrität verletzten, aber mit der Signatur von SolarWinds versehenen Software-Produkts Orion herunterluden und installierten (es kam auf Grund der gültigen Signatur aus vertrauter Quelle), erhielten auch eine Backdoor, welche der Angreifer im Update implementiert hatte. Der Angreifer hat(te) somit potenziell Zugriff auf diese IT-Infrastrukturen. Eine erste Schadensanalyse durch SolarWinds ergab 18.000 potentielle Opfer des Supply Chain-Angriffs, darunter auch einige österreichische Unternehmen, aber keine verfassungsmäßigen Einrichtungen oder kritische Infrastrukturen. Einige Kunden von SolarWinds waren bereits mutmaßliche Opfer, darunter – mit Stand Februar 2021 – neun US-Behörden und über 100 private Unternehmen (wie Microsoft, Cisco, Intel, NVIDIA und das Cyber-Sicherheitsunternehmen FireEye, welches als erstes den Vorfall öffentlich bekannt machte). Eine abschließende

Schadensanalyse ist zum Zeitpunkt der Erstellung dieses Berichts noch nicht abgeschlossen.

Supply Chain-Angriff: Ein Supply Chain-Angriff bezeichnet einen Angriff auf die Lieferkette eines potentiellen Opfers. Oft ist es Angreifern aus verschiedenen Gründen nicht möglich, bestimmte Ziele direkt anzugreifen. In solchen Fällen kommt es vor, dass stattdessen eine Organisation in der Lieferkette des eigentlichen Ziels angegriffen wird. So wurden bei dem in diesem Bericht angeführten SolarWinds-Vorfall nicht die eigentlichen Ziele (z.B. US-Behördenorganisationen) angegriffen, sondern eine Firma, die Netzwerk-Management-Software für die Behördenorganisationen herstellt. Über die normale Update-Funktionalität dieser Software wurden dann mit Schadcode versehene Programmteile in die Systeme der eigentlichen Ziele eingeschleust

Backdoor: Im Bereich der Cybersicherheit bezeichnet der Begriff Backdoor (Hintertüre) ein Programm, das es Benutzern ermöglicht, unter Umgehung der vorgesehenen Authentifizierungsmechanismen, direkten Zugang zu einem Computersystem zu erlangen. Oft werden im Zuge eines Angriffs auf ein Computersystem Backdoors auf dem angegriffenen System installiert, die es dem Angreifer ermöglichen, auch nach dem eigentlichen Angriff jederzeit wieder unbemerkt Zugriff auf das System zu erlangen.

Ein weiterer schwerwiegender Cyber-Sicherheitsvorfall ereignete sich beim Unternehmen Software AG, dem zweitgrößten Softwareunternehmen Deutschlands. Dieses wurde Anfang Oktober 2020 Opfer eines Cyber-Erpressungsangriffes mittels Ransomware. Bei dem Angriff wurden nicht nur die Daten im Unternehmensnetzwerk unbrauchbar gemacht, sondern auch zuvor aus dem System entwendet und zum Angriff auf Kunden der Software AG genutzt. Außergewöhnlich und brisant ist dieser Fall dahingehend, da die Software AG auch Produkte für sogenannte operating Technology (OT, ~Industrie 4.0, Produktions-IT) anbietet und daher Fernwartungszugänge zu dieser, oftmals bei Kunden im Einsatz befindlichen Technologie, bestehen. Die Täterschaft des Angriffs auf die Software AG verfügt nun möglicherweise auch über die Zugangsdaten zu Systemen bei deren Kunden. Auf der im TOR-Netzwerk befindlichen Plattform, die für die Veröffentlichung der erbeuteten Daten genutzt wurde, befanden sich auch Daten österreichischer Unternehmen. Diese wurden durch ein zeitnahes Warnschreiben des IKDOK darüber in Kenntnis gesetzt und Mitigationsmöglichkeiten in selbigem Schreiben bereit gestellt.

Zahlreiche Cyber-Sicherheitsvorfälle gab es im Berichtszeitraum auch bei cloudbasierten Datenbanken und Speichern. Diese Vorfälle haben gezeigt, dass solche Systeme (u.a. Amazon S3 Buckets, Redis, Elasticsearch, MongoDB) von Angreifern systematisch gesucht, entdeckt und anschließend angegriffen werden. In diesem Zusammenhang sollte auch der SolarWinds-Vorfall beurteilt werden. Entsprechende Warnungen wurden im Rahmen des IKDOK ausgesprochen.

Schadcode

Auch EMOTET wurde nach einer mehrmonatigen Pause im Sommer des Berichtszeitraums wieder aktiv. Es kam zu neuen weltweiten Malspam-Wellen. Die Fähigkeiten der Schadsoftware wurden in dieser Pause ebenfalls weiterentwickelt. So kann EMOTET, nachdem er am Opfersystem aktiv geworden ist, weitere Schadcode-Module wie Ransomware (RYUK, Megacortex oder Bitpayment) oder diverse (Banking)Trojaner wie Dridex, Ursnif, ICEDID, Qbot oder Trickbot automatisch nachladen. Tools zur Datenextraktion/Datendiebstahl oder Software zur Einbindung des befallenen Systems in ein Bot-Netzwerk wurden ebenfalls in den Funktionsempfang aufgenommen. Eine der zentralen Schutzmaßnahmen gegen EMOTET ist es, Microsoft Office das Ausführen von Makros zu verbieten oder nur vertrauenswürdige, signierte Makros zu erlauben. Office-Dokumente mit Makros stellen das gleiche Sicherheitsrisiko dar wie z.B. EXE-Dateien. EMOTET verwendet eine ausgefeilte Social Engineering-Methode um sich zu verbreiten, in dem es sich in bestehende E-Mail-Kommunikation einklinkt und so das Opfer mit Bezug auf eine legitime E-Mail Kommunikation zu täuschen versucht. Auch hier wurden im Rahmen des IKDOK entsprechende Informationen aufgearbeitet und verteilt sowie durch das BVT zahlreiche Awarenss-Schulungen zu Cyber-Sicherheit durchgeführt.

Daten-Lecks

Auch in diesem Jahr kam es wieder zu zahlreichen Veröffentlichungen (Data Leaks) von entwendeten Zugangsdaten (meist User Credentials), jedoch nicht nur im Zusammenhang mit oben angeführter Ransomware, von denen auch Domänen verfassungsmäßiger Einrichtungen betroffen waren. So waren beispielsweise bei der IT-Sicherheits-Trainingsfirma SANS persönliche Daten, auch von österreichischen Kunden, betroffen. Wie schon in den voranstehenden Punkten Ransomware, DDoS und andere Schadcodes angeführt, ist die Drohung und oftmals durchgeführte (teilweise) Veröffentlichung von erbeuteten Daten eine Erweiterung des Geschäftsmodells von Cyber-Kriminellen geworden, um ihren Forderungen mehr Nachdruck zu verleihen. Betroffen sind dabei nicht nur das primäre Opfer selbst, sondern auch dessen Partner in der Cyber Supply Chain. Hier ist vor allem der bereits zuvor angeführte Cyber-Sicherheitsvorfall beim

Unternehmen Software AG zu sehen, in dessen Folge die Kunden des Unternehmens angegriffen bzw. kontaktiert wurden. Auch kamen der Gebühren Info Service GmbH (GIS) Daten abhanden und wurden im Internet zum Verkauf angeboten.

Das BVT und der IKDOK agierten auch hier prokativ im Rahmen seiner Möglichkeiten und informierte Betroffene.

2
Fachbeiträge

Schutz der obersten Organe und verfassungsmäßigen Einrichtungen – Bedrohungslage 2020

Das Handeln der durch die Verfassung eingerichteten obersten politischen Funktionsträgerinnen und Funktionsträger des Staates steht tagtäglich im Blickpunkt des öffentlichen Interesses. Neben des im demokratiepolitischen Sinn legitimen Diskursverhaltens sowie des Vorbringens konträrer Ansichten unter Berücksichtigung rechtsstaatlicher Prinzipien, bieten politische Entscheidungen und Äußerungen von Obersten Organen aber naturgemäß auch eine große Projektionsfläche als lohnenswertes Angriffsziel für Polemik, Agitation sowie tätlichen Aktionismus. Um den kontinuierlichen Fortbestand der Handlungs- und Funktionsfähigkeit unserer demokratischen Grundordnung zu ermöglichen, obliegt dem Bundesamt für Verfassungsschutz und Terrorismusbekämpfung im Zusammenwirken mit den Landesämtern für Verfassungsschutz und Terrorismusbekämpfung der besondere Schutz der Obersten Organe und Verfassungsmäßigen Einrichtungen.

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 bzw. politische Absichten. Das Drohgeschehen des Jahres 2020 wurde maßgeblich von den Themen der Covid19-Maßnahmengesetzgebung sowie dem Terrorattentat in der Wiener Innenstadt bzw. den darauffolgenden politischen Statements bestimmt.

Seit Beginn des zweiten Lock-Downs hat sich diese regierungskritische Agitation sowohl quantitativ als auch qualitativ verstärkt und radikalisiert, weshalb Eskalationen in Form von Aktionismus, Protesten, Drohungen und Ausschreitungen im Nahebereich von Regierungsgebäuden als plausible und mögliche Reaktionen und Risiken erscheinen. Am Rande bot aber auch die Reaktion der Politik auf den öffentlich ausgetragenen Konflikt zwischen Kurden und Türken genügend Anlass für dementsprechend emotionsgeladene Polemik und Agitation gegenüber politischen Repräsentantinnen und Repräsentanten. In diesem Zusammenhang überraschte es wenig, dass im Berichtsjahr vorwiegend all jene mit diesen Themenbereichen befassten Politikerinnen und Politiker und Behörden als favorisiertes Adressatenziel 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 insgesamt 309 bekannt gewordenen Eingaben wiesen 54 Fälle den strafrechtlich relevanten Tatbestand einer gefährlichen Drohung auf.

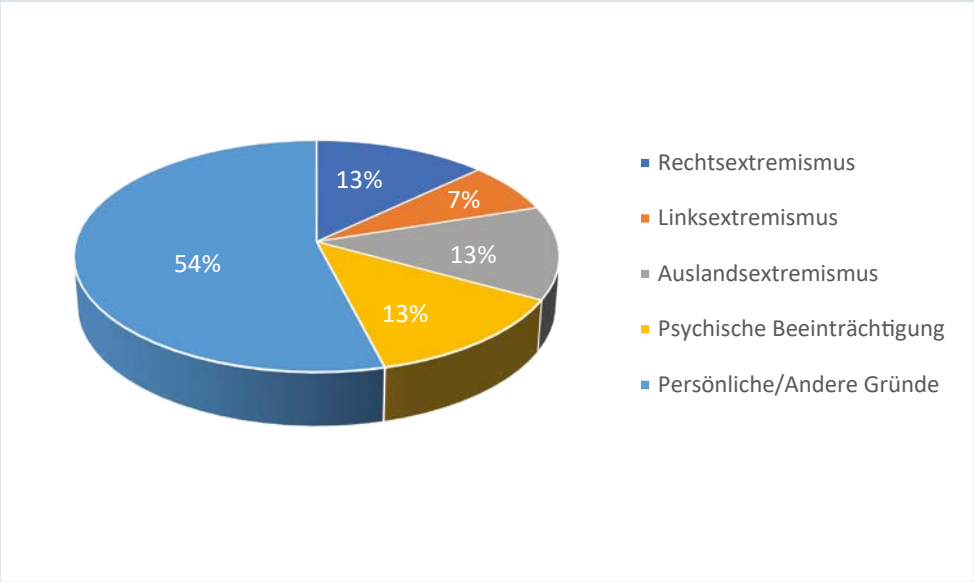


Abbildung: Prozentuelle Verteilung der Motivlagen

Die Abbildung stellt die Verteilung der Drohungsinhalte nach der Motivlage dar. Wie dem Kreisdiagramm zu entnehmen ist, entfällt der größte Anteil mit 29 Deliktsfällen (54 Prozent) auf das Motiv „Persönliche/Andere Gründe“, was vorwiegend damit begründet ist, dass unter dieser Motivlage auch sämtliche Drohungen zum Thema Corona-Maßnahmenkritik subsumiert sind. Die Bereiche „Rechtsextremismus“, „Auslandsextremismus“ und „Psychische Beeinträchtigung“ verfügen mit jeweils sieben Deliktsfällen (13 Prozent) über gleich hohe Anteile. Der Sektor „Linksextremismus“ stellt mit vier Deliktsfällen (7 Prozent) den geringsten Anteil dar. Während 33 dieser Drohungen via Social-Media-Plattformen als öffentlich einsehbarer Kommentar oder mittels persönlicher Nachricht getätigt wurden, wurden 13 Drohungen per Mail versendet, die restlichen Drohungen erfolgten in Briefform oder als Telefonanruf. Es konnten bislang mehr als zwei Drittel aller registrierten Drohungen geklärt werden, wovon 29 männliche und neun weibliche Personen als Verfasser einer Drohung ausgeforscht wurden. Die verbleibenden Fälle waren zum Zeitpunkt dieser Berichtslegung noch Gegenstand laufender Ermittlungen.

Obwohl die Intensität an schriftlichen Eingaben im Jahr 2020 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 oder die physische Integrität von Objekten verfassungsmäßiger Einrichtungen bedeutet hätten. Nichtsdestotrotz ist es Aktivisten in drei Fällen gelungen, nach widerrechtlichem Eindringen in mittels Barrieren umfriedete Baustellenbereiche auf Fassadengerüste zu klettern und Transparente anzubringen. Eine mit einer Machete bewaffnete Person, die im Regierungsviertel mit der Intention erschienen war, im Nationalrat über ihre coronabedingt prekäre finanzielle Lage sprechen zu wollen, konnte durch aufmerksames Agieren eines Zeugen sowie der professionellen Intervention der alarmierten Exekutivkräfte zeitnah festgenommen werden. Ein weiterer Intrusionsversuch

in ein Regierungsgebäude mit der Absicht einer persönlichen Kontaktaufnahme mit einem Obersten Organ, konnte ebenso durch umsichtiges Verhalten der vor Ort eingesetzten Sicherheitskräfte frühzeitig unterbunden werden. Diese Vorfälle bilden eine wichtige Grundlage zur regelmäßigen Evaluierung und zweckmäßigen Adaptierung von Sicherheitsmaßnahmen bei verfassungsmäßigen Einrichtungen.

Unmittelbar nach Amtsantritt eines Obersten Organs wird nach Bedarf eine Sicherheitsberatung durchgeführt. Das Beratungsangebot umfasst dabei sämtliche, die jeweilige Person betreffende sicherheitsrelevante Themen, wie beispielsweise allgemeine Verhaltensempfehlungen, die sichere Nutzung von Kommunikationsmedien, die Sicherheit im privaten Umfeld, am Arbeitsplatz und am Arbeitsweg, Awareness bei Dienstreisen und Auslandsaufenthalten, den Umgang mit verdächtigen Postsendungen, das Verhalten bei Drohungen, Ratschläge gegen Ausspähung und vieles mehr. Im Berichtsjahr fanden sieben Sicherheitsberatungen bei Obersten Organen statt. Im Anschluss daran erfolgten bei zwei Privatwohnsitzen und zwei Amtssitzen objektschutztechnische Evaluierungen zur Identifikation allfälliger Sicherheitsmängel. Die daraus gewonnenen Erkenntnisse fanden Eingang in vier im Berichtsjahr erstellte Sicherheitskonzepte, die neben objektspezifischen Risikoanalysen verschiedenartige Handlungsempfehlungen für technische, organisatorische und personelle Sicherheitsmaßnahmen veranschaulichen. Das Aufzeigen existenter Sicherheitslücken bildet die Basis zur Optimierung des Widerstandszeitwertes der jeweiligen Immobilie. Dadurch wird das Gefährdungspotenzial für den jeweiligen politischen Funktionsträger und sein privates oder berufliches Umfeld vermindert. Bei Bedarf werden zudem auch bestehende Sicherheitskonzepte für verfassungsmäßige Einrichtungen von privaten Sicherheitsdienstleistern auf ihre Plausibilität und ihren Wirkungsgrad evaluiert, was im Berichtszeitraum mehrmals im Zuge von Objektbegehungen von den bedarfstragenden Sicherheitsverantwortlichen in Anspruch genommen wurde.

Unter Berücksichtigung der jeweils vorhandenen staatsschutzrelevanten Phänomenbereiche, der aktuellen innen- und außenpolitischen Vorgänge im Zusammenhang mit dem jeweiligen Obersten Organ sowie der allgemeinen Gefährdungslage Österreichs, werden regelmäßig Gefährdungseinschätzungen erstellt. Das darin beinhaltete einheitliche Analyseverfahren bildet die Grundlage für die gefährdungsbezogene Auswahl an sicherheitspolizeilichen Personen- und Objektschutzmaßnahmen, die in unterschiedlichster Ausprägung im Rahmen der gesetzlichen Befugnisse zur Anwendung kommen.

Wissens- und Erfahrungsaustausch in Sicherheitsangelegenheiten ist für die generelle Erhöhung des Resilienzniveaus innerhalb einer aus mehreren homogen agierenden Teilnehmerinnen und Teilnehmern bestehenden Gruppierung als unerlässlich anzusehen. Daher veranstaltet das BVT periodisch wiederkehrende Tagungen mit den Sicherheitsverantwortlichen der Verfassungsmäßigen Einrichtungen, die Gelegenheit zum Diskurs über neu entstandene Gefährdungspotenziale und zur Erörterung

von Möglichkeiten zur Minimierung daraus entstehender Sicherheitsrisiken bieten. Pandemiebedingt wurde 2020 statt einer Präsenzveranstaltung eine Videokonferenz abgehalten. Darüber hinaus fanden mehrere anlassbezogene bilaterale Gespräche mit den Sicherheitsverantwortlichen statt, woraus mitunter schriftliche Sicherheitsempfehlungen in Bezug auf Personen- oder Objektschutzmaßnahmen resultierten. Hinsichtlich abstrakt drohender Sicherheitsrisiken und potentiell aufkeimender Gefährdungspotentiale, wie z.B. bevorstehende Ereignisse, welche die Regelbetriebstätigkeit beeinflussen könnten, werden die Verfassungsmäßigen Einrichtungen im Sinne einer Frühwarnsystematik zeitnah informiert.

Wesentlicher Baustein eines umfassenden Sicherheits- und Bedrohungsmanagements für Oberste Organe und Verfassungsmäßige Einrichtungen ist die Verfolgung eines holistischen Ansatzes. Dieser fand in einem 2020 durchgeführten Projekt zur Identifizierung des Verbesserungspotentials in Fragen der baulichen/technischen Gegebenheiten, der Drohnenabwehr sowie der personellen Objektschutzmaßnahmen Niederschlag. Sicherheitsmaßnahmen sind als Immunsystem der Handlungsfähigkeit von obersten Staatsorganen und verfassungsmäßigen Vertretungskörpern zu verstehen. Daher unterliegen Maßnahmen zur kontinuierlichen Stärkung dieses Immunsystems der Notwendigkeit einer fortwährenden Prüfung auf Plausibilität und Effektivität, um den Anforderungen dynamisch wechselnder Bedrohungsarten gerecht werden zu können.

Schutz kritischer Infrastruktur im Rahmen der Covid-19-Pandemie

Österreich ist als hochentwickeltes Wirtschaftsland substanziell vom kontinuierlichen Funktionieren seiner kritischen Infrastruktur abhängig. Da temporäre Störungen oder längerfristige Ausfälle kritischer Infrastrukturen unmittelbare Auswirkungen auf die Wirtschaft und die Bevölkerung zur Folge hätten, ist die Versorgung mit wesentlichen Dienstleistungen und Gütern größtmöglich sicherzustellen.

Als kritische Infrastruktur gelten unter anderem Betreiber und Anbieter von Produkten und Dienstleistungen aus den Sektoren Energie, Gesundheit, Hilfs- und Einsatzkräfte, Transport, Finanzen, Wasser, Informations- und Kommunikationstechnologien, Lebensmittel, chemische Industrie, Sozial- und Verteilsysteme sowie verfassungsmäßige Einrichtungen und Forschungseinrichtungen.

Im gesamtstaatlichen Zusammenhang obliegt die Umsetzung zur Erhöhung der Resilienz und Sicherheit für kritische Infrastrukturen in strategischer Hinsicht dem Bundeskanzleramt und dem Bundesministerium für Inneres. In Bezug auf die operative Umsetzung koordiniert das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) gemeinsam mit

den Landesämtern für Verfassungsschutz und Terrorismusbekämpfung (LVT) Maßnahmen zur Erhöhung der Sicherheit und des Schutzes dieser Einrichtungen.

Vor dem Hintergrund einer anhaltenden Bedrohung durch terroristische Anschläge sowie den seit Februar 2020 in Österreich spürbaren Auswirkungen der COVID-19-Pandemie, kam dem Schutz kritischer Infrastruktur im Jahr 2020 ganz besondere Bedeutung zu.

Das BVT setzte hierbei in der Pandemiebekämpfung und im Zusammenhang mit dem Schutz kritischer Infrastruktur insofern Aktivitäten, als durch vorbeugende Maßnahmen, die sich insbesondere in rascher Information und Kooperation mit Unternehmen niederschlug, ein Ausfall bzw. eine Unterbrechung der für die Bevölkerung so wichtigen Dienste verhindert werden sollte.

Entwicklung der Kriminalität und Gefährdungslage für kritische Infrastrukturen im Kontext der COVID-19-Pandemie

International betrachtet beeinflusste die COVID-19-Pandemie seit ihrem Beginn auf unterschiedliche Weise die Bedrohungslage von kritischen Infrastrukturen. Neben kriminellen Motivlagen richteten sich im Berichtsjahr ideologisch motivierte Agitationen und auch staatliche Angreifer gegen Betreiber kritischer Infrastrukturen.

Kriminelle Kreise nutzten weltweit die Pandemie als Möglichkeit für „neue Geschäftsbereiche", insbesondere in den Kriminalitätsfeldern Fälschung und (Online-) Betrug.

Unterschiedliche **ideologisch motivierte Gefährderszenen** machten sich die COVID-19-Krise von Anbeginn an zu Nutze, um die jeweils eigene Agenda voranzutreiben und um zu rekrutieren. Angriffe **staatlicher Akteur**e standen im Zusammenhang mit der Entwicklung von COVID-19-Impfstoffen.

Diese internationalen Entwicklungen erhöhten auch das diesbezügliche Gefährdungspotential in Österreich, da sie als zumindest abstrakte Gefährdungslagen für inländische Einrichtungen zu bewerten waren.

Im Bereich der **Pharmaindustrie bzw. im Gesundheitssektor** generell war die steigende Gefahr von Diebstählen und Einbrüchen in Apotheken, bei Ärzten und Lagerstandorten zu erkennen, die sich am Beginn der Pandemie auf medizinische Güter zur Bekämpfung der Pandemie (Schutzausrüstung, Testkits etc.) richtete. In Österreich wurden einzelne Diebstähle – unter anderem von Schutzmasken sowie sonstigen medizinischen Gütern – bekannt. Ebenso wurden verstärkt gefälschte und minderwertige Gesundheitsprodukte online angeboten, wobei auch Pharmaziebetriebe zu den Betrugsopfern zählten.

Im Herbst 2020 ergaben sich aus den näher rückenden COVID-19-Impfungen potenzielle Gefährdungen für den Pharmaziesektor. Von Interpol wurden Diebstähle, Lagereinbrüche, Überfälle auf Impfstofftransporte und Korruption als realistische Szenarien bezeichnet, ebenso war mit Impfstofffälschungen zu rechnen. Neben kriminellen Motiven richtete sich auch die ideologische motivierte Szene gegen diese Einrichtungen. COVID-19-Maßnahmengegner mussten als potenzielles Risiko für oben genannte Anlagen mitbetrachtet werden, wobei der Aktionismus von Brandanschlägen, Sabotageakten bis hin zu Körperverletzungen reichen konnte. Diese Gefahr galt ebenso für Einrichtungen für COVID-19-Testungen, wie die zahlreich in Österreich eingerichteten Teststraßen.

Darüber hinaus wurde von unterschiedlichen ideologischen Gruppierungen international in Online-Foren die vorsätzliche Ansteckung ua. von medizinischem Personal sowie die Zerstörung wichtiger (Gesundheits-)Infrastruktureinrichtungen zur Sabotage des öffentlichen Gesundheitswesens diskutiert, um die angestrebte Systemänderung zu erreichen.

Im Sektor der **Lebensmittelversorgung** berichteten internationale Medien am Beginn der Krise von einzelnen bewaffneten Überfällen auf Lebensmitteltransporte sowie über eine Steigerung von Einbruchsdiebstählen in Supermärkten, von denen Österreich nicht betroffen war. In Nachbarländern Österreichs nutzten Linksextremisten die in der Bevölkerung verbreitete Angst von Versorgungsengpässen und riefen zu Plünderungen auf, vereinzelt waren darin auch Aufrufe zur Störung des gesamten Systems (z.B. durch Angriffe auf die Energieversorgung einzelner Unternehmen) enthalten. Internationale extremistische/terroristische Gruppierungen unterschiedlicher ideologischer Ausrichtung thematisierten auch den Einsatz von COVID-19 als Waffe, unter anderem durch Kontaminierung von Lebensmitteln (durch Ablecken von Obst und Gemüse in Supermärkten).

Bezugnehmend auf den Sektor der **Forschungseinrichtungen** erhöhte die Verlagerung von Besprechungen/Konferenzen in virtuelle Räume das Risiko der Ausspähung. Forschungsergebnisse, Erfindungen und Innovationen sind grundsätzlich ein attraktives Ziel für Spionageaktivitäten und rückten so stärker in den Fokus von Cyberkriminellen. Im Mai 2020 stoppten mehrere europäische Hochleistungszentren unter Verweis auf Sicherheitsprobleme den Zugriff auf ihre Rechenkapazitäten. Es wurde vermutet, dass hinter den Cyberangriffen Spionageaktivitäten gegen Forschungszentren stünden, um an Forschungsdaten zum Corona-Virus zu gelangen. Bei einem Hackerangriff auf die Europäische Arzneimittelbehörde (EMA) wurde nach Angaben von Biontech und Pfizer auf Dokumente zum Corona-Virus-Impfstoff der Pharmakonzerne zugegriffen.

Forschungseinrichtungen standen aber auch im Fokus physischer Angriffe. Im Oktober 2020 kam es zu einem Brandanschlag auf ein Gebäude des Robert Koch-Instituts in Berlin, einer der wichtigsten Forschungseinrichtungen in Deutschland zu COVID-19. Im

April 2020 wurde in Berlin ein Versorgungs- bzw. Telekommunikationskabel in Brand gesteckt, wobei sich eine linksextremistische Gruppe „zur Sabotage einer Datenleitung zum Heinrich-Hertz-Institut“ bekannte, um der so genannten Corona-App, „die eine Aufweichung der Grundrechte bedeute, eine Absage zu erteilen“.

Im Sektor **Finanzen** standen am Beginn des ersten Lockdowns Befürchtungen eines „Banken-Runs“, bei dem Bürgerinnen und Bürger Bargeld in großem Ausmaß von ihren Konten beheben und zu Hause deponieren könnten. Auch wenn eine Steigerung in Bargeldabhebungen erkennbar war, verwirklichte sich dieses Risiko schlussendlich nicht. In linksextremistischen Internetportalen im Ausland wurden kapitalismuskritische Aufrufe verbreitet, die sich insbesondere gegen Banken richteten.

Der Bereich der **Informations- und Kommunikationstechnologien (IKT)** war insbesondere durch Verschwörungstheorien betroffen, die einen Zusammenhang zwischen der 5G-Technologie und dem Ausbruch der Pandemie in Wuhan (China) herzustellen versuchten. Seit Ausbruch der Pandemie kam es in Europa (u.a. Niederlanden, Großbritannien, Irland und Zypern) zu insgesamt mehr als einhundert Brandanschlägen auf Mobilfunksendemasten. Eine klare Motivlage zeigte sich dabei nicht. Europäische Sicherheitsbehörden gingen davon aus, dass zum Teil rechtsextremistisch als auch linksextremistisch motivierte Tätergruppen, aber auch solche aus dem verschwörungstheoretischen Phänomenbereich und aus der Zivilgesellschaft, hinter den Anschlägen standen. In diesem Zusammenhang wurden auch deutschsprachige Anleitungen zur Zerstörung von 5G-Sendeeinrichtungen durch französische Anarchisten bekannt.

In Österreich hatte die „5G=COVID-19“-Verschwörungstheorie im Phänomenbereich der staatsfeindlichen Verbindungen ihren Ursprung. In Sozialen Medien wurden aus diesen Kreisen Veröffentlichungen gegen den Bau von „5G-Masten“ verbreitet. In Tirol wurde der Schriftzug „Corona = 5G!“ mehrmals auf einem Gehsteig mit Kreide geschrieben festgestellt. Im März kam es zu drei Brandanschlägen auf Wavenet-Masten in Niederösterreich. Die Täter stammten aus dem Drogenmilieu, als Motiv nannten sie die Schädlichkeit von Sendemasten für die Gesundheit. Im Juni erfolgte neuerlich ein Brandanschlag gegen einen Mobilfunk-Sendemast in Niederösterreich, Hinweise auf eine bestimmte Motivlage bestanden nicht. Im September kam es in Tirol zu einem Anschlag auf einen Sendemast durch Abschneiden mehrerer Glasfaser- und Stromkabel und zur Beschmierung von Schaltkästen mit den Schriftzügen „STOP 5G“ und „5G KILLS!“.

Auf einer Social-Media-Plattform wurde im Oktober die Möglichkeit von österreichweiten, zeitgleich durchgeführten Anschlägen auf 5G-Masten thematisiert und konkrete Überlegungen zum möglichen diesbezüglichen Modus Operandi diskutiert. Gründerin und Administratorin der gegenständlichen Telegram-Gruppe war eine einschlägig bekannte Aktivistin aus der Verschwörungstheoretiker- bzw. Corona-Maßnahmengegnerszene.

stock.adobe.com

Aggressionen der Corona-Maßnahmengegnerszene richteten sich im Laufe des Jahres auch zunehmend gegen den ORF, der als „Systemmedium“ dem Feindbild Regierung zugeordnet wurde und so in den Fokus dieser Gruppierungen geriet.

In Bezug auf den **Transport-/Verkehrssektor** wurde in einschlägigen Social-Media-Kanälen im Dezember 2020 ein aus der internationalen Corona-Maßnahmengegnerschaft stammender Flyer mit einem gegen einen Lockdown gerichteten Aufruf zu einem europaweiten „Blockdown“ veröffentlicht. Darin wurde angekündigt, dass es in der Zeit vom 20. bis 31. Dezember 2020 zu temporären Blockademaßnahmen von zentralen Infrastruktur- und Verkehrsknotenpunkten mittels Großfahrzeugen kommen solle, wobei sich dazu in Österreich keine öffentlichkeitswirksamen Tathandlungen ergaben.

Zusammenfassend lässt sich feststellen, dass sich die internationale Kriminalitätsentwicklung im Kontext mit COVID-19 in Österreich nur in geringem Ausmaß in Form von kriminell motivierten Tathandlungen gegen kritische Infrastrukturen niederschlug. Die pandemiebezogene Bedrohungslage durch weltanschaulich motivierte Gefährdergruppen blieb in Österreich für Unternehmen im Jahr 2020 im internationalen Vergleich ebenso gering.

Organisatorische Herausforderungen für Betreiber kritischer Infrastruktur

Neben den genannten kriminellen und intentionalen Risiken bestanden im Zusammenhang mit der Pandemie auch eine Vielzahl organisatorischer Herausforderungen, die sich zumeist sehr dynamisch und kurzfristig in der möglichen Reaktionszeit stellten.

Eine Problemstellung lag häufig in der vorab fehlenden Erfassung der Pandemie als mögliches Risiko für die Dienstleistungserbringung des Unternehmens. Die Durchführung eines angemessenen **Risikomanagements** ist eine Kernaufgabe von Organisationen, insbesondere von Betrieben kritischer Infrastruktur. Hierbei sollen für das Unternehmen

relevante Risiken identifiziert und Maßnahmen gesetzt werden, die zu einer Reduzierung möglicher Eintrittswahrscheinlichkeiten und/oder Auswirkungen dieser Risiken beitragen. Auf das Risiko einer Pandemie inkl. der damit verbundenen Folgen wurde häufig nicht Bedacht genommen bzw. wurde dieses im Rahmen der Entwicklung möglicher Strategien zur Aufrechterhaltung des Betriebes vorab selten berücksichtigt. Dies führte dazu, dass Maßnahmen schlussendlich sehr kurzfristig entschieden und umgesetzt werden mussten. Ein umfassendes, alle denkbaren Szenarien berücksichtigendes und verschiedenste Stakeholder einzubeziehendes Risikomanagement sowie eine Erhöhung der Durchführungszyklen können in diesem Zusammenhang künftig von Vorteil sein.

Neben dem Risikomanagement ist auch ein gut vorbereitetes **Krisenmanagement** bzw. Business Continuity Management elementar für die Gewährleistung der Unternehmensleistung in Krisenszenarien. Wenngleich eine Vielzahl der Unternehmen sehr gut auf Krisen vorbereitet waren, ist es für Betreiber herausfordernd, Krisenmanagementstrukturen im Unternehmen rechtzeitig hochzufahren, Aufgaben und Entscheidungskompetenzen klar zu verteilen und nach innen und außen rasch und effizient zu kommunizieren.

Viele Unternehmen reagierten bereits im Frühling 2020 mit der Einführung weitgehender **Home-Office-Regelungen**, um die Risiken der Ansteckungen im Betrieb auf ein Minimum zu reduzieren. Dazu mussten Mitarbeiterinnen und Mitarbeiter in großem Umfang mit technischem Equipment (z.B. Laptops) ausgestattet sowie im Unternehmen die technische Infrastruktur angepasst/eingerichtet werden, um den einwandfreien Betrieb auch in dieser veränderten Arbeitswelt aufrechterhalten zu können. Mit diesem Umdenken einher ging der Umstieg auf Videokonferenzen, die wohl auch in Zukunft in der Arbeitswelt verhaftet bleiben werden.

Da insbesondere bei Betreibern kritischer Infrastruktur Home-Office-Möglichkeiten nur begrenzt möglich sind – man denke an den öffentlichen Verkehr, die Leitstellen der Energieversorgung, die Lebensmittelversorgung oder den Krankenhausbetrieb –, mussten vielfach veränderte **Betriebskonzepte** im Unternehmen umgesetzt werden. Dabei wurden unterschiedliche Vorgehensweisen – wie die Trennung der Teams in zwei Gruppen oder auf so genanntes „Schlüsselpersonal" reduzierte Anwesenheit – verfolgt. Hier zeigte sich insbesondere die elementare Rolle einer Business Impact Analyse, d.h. der Identifizierung essentieller Abläufe und Prozesse, für die ein durchgehender Betrieb unbedingt notwendig sein muss.

Für jene Mitarbeiterinnen und Mitarbeiter, deren Anwesenheit am Arbeitsplatz weiterhin erforderlich war, entstanden vielfach Problemstellungen durch **Beschränkungen des Pendlerverkehrs im In- und Ausland**. Einerseits kam es zu Beschränkungen des Personenverkehrs aus Nachbarstaaten nach Österreich bzw. in die umgekehrte Richtung, wobei jedoch in nahezu allen Fällen Ausnahmen für den Pendlerinnen- und Pendlerverkehr

geregelt wurden. Ebenso kam es zu Schwierigkeiten bei der Ein- und Ausreise im nationalen Verkehr (bezirks- bzw. bundesländerübergreifend), wobei in vielen Fällen Bestätigungen des Arbeitgebers aus systemrelevantem Unternehmen ausreichten, um den Arbeitsort erreichen zu können.

Durch **Einberufung der Miliz sowie Verlängerung des Zivil-/Präsenzdienstes** im Frühjahr 2020 bestand in einigen Fällen die Gefahr, dass in der damaligen Situation dringend notwendiges Schlüsselpersonal von Betreibern kritischer Infrastruktur in den Unternehmen für einige Monate nicht mehr zur Verfügung stehen könnte. Dementsprechend fanden Ausnahmeregelungen Anwendung, sodass in begründeten Fällen einer Einberufung/Verlängerung nicht Folge geleistet werden musste.

In Bezug auf die **Logistik** innerhalb der kritischen Infrastruktur wurde das Risiko der „Just-in-time"-Lieferketten schlagend. Durch Verzögerungen im Warenverkehr – insbesondere durch Einführung von Grenzkontrollen – konnten in manchen Fällen relevante Ersatzteile, Ressourcen oder Güter nicht rechtzeitig geliefert werden. Durch ein durchzuführendes Supply Chain Management sowie ausreichende Bevorratung kann dieses Risiko im Vorfeld minimiert werden.

Präventionsmaßnahmen durch das BVT im Rahmen des Schutzes kritischer Infrastruktur

Die für den Schutz kritischer Infrastruktur zuständige Organisationseinheit im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung setzte während der COVID-19-Pandemie vorbeugende Maßnahmen, um das Funktionieren kritischer Infrastrukturen weiterhin zu gewährleisten.

Einerseits wurden Betreiber aus möglicherweise betroffenen Infrastruktursektoren von den Staatsschutzbehörden von Bedrohungen und Gefahren, die sich aus kriminellen oder ideologischen Motiven ergaben, laufend informiert. Wo es erforderlich war, wurden zusätzlich entsprechende sicherheitspolizeiliche Schutzmaßnahmen gesetzt.

Außerdem ging der vorbeugende Schutz während der Pandemie mit weitreichender, proaktiver Kommunikation und Interaktion mit den betroffenen Unternehmen einher, um diesen jenen Stand an Information zur Verfügung zu stellen, die diesen zur weiteren Gewährleistung der für die Daseinsvorsorge so wesentlichen Dienstleistungen benötigten.

Durch das BVT wurde dazu eine eigene Kontaktstelle im SKKM-Koordinationsstab COVID-19 im BMI eingerichtet, an die sich Unternehmen jederzeit mit Fragen wenden und von der im Berichtszeitraum insgesamt über 1.700 Anfragen beantwortet werden konnten. Am Beginn der Krise erfolgte außerdem die Organisation einer großen Informationsveranstaltung unter Einbeziehung der wichtigsten einhundert Infrastrukturbetreiber Österreichs sowie

hochrangiger Vertreter des Bundesministeriums für Inneres, des Bundesministeriums für Soziales, Gesundheit, Pflege und Konsumentenschutz, des Bundesministeriums für europäische und internationale Angelegenheiten sowie des Bundesministeriums für Arbeit, um wichtige Anliegen der Unternehmen in diesem Kreis besprechen und lösen zu können.

Nahezu täglich wurden über einen alle Sicherheits- und Krisenmanagementbeauftragten der kritischen Infrastrukturen umfassenden Verteiler, Änderungen in der Rechtslage (neue Verordnungen oder Gesetze), Änderungen in Impf- oder Teststrategien sowie Handlungsempfehlungen zum unternehmensinternen Umgang mit der COVID-19-Pandemie verteilt.

Ebenso erhielten die auf der offiziellen Liste kritischer Infrastruktur („ACI-Liste“) erfassten Unternehmen auf Nachfrage Bestätigungen, die ihre Mitarbeiterinnen und Mitarbeiter im Pendlerverkehr sowie im grenzüberschreitenden Warenverkehr teilweise benötigten.

Auch der Informationsaustausch in die andere Richtung erwies sich als relevant für die Behörden. Eingehende Informationen über aktuelle Herausforderungen und Probleme von Unternehmen konnten für zielgerichtete und umsetzbare Bestimmungen in den zahlreichen Verordnungen und Gesetzen in Zusammenhang mit COVID-19 genutzt werden.

Zusammenfassend ließ sich feststellen, dass das bereits bestehende Kooperations- und Vertrauensverhältnis zwischen Betreibern kritischer Infrastruktur und dem BVT im dynamischen Krisengeschehen unabdingbar war, um in der Daseinsvorsorge entstehende Probleme rasch und effizient lösen zu können.

Gesamtgesellschaftlicher Ansatz in der Extremismusprävention und Deradikalisierungsarbeit- das BNED

Extremismus in all seinen Erscheinungsformen stellt eine konstante Bedrohung für den demokratischen Rechtsstaat dar. Für die Identifikation und Umsetzung von geeigneten Gegenmaßnahmen ist ein gesamtstaatlicher Lösungsansatz geboten. Präventions- und Deradikalisierungsmaßnahmen spielen dabei eine entscheidende Rolle und müssen in Österreich gestärkt werden. Um dieser Bedrohung gesamtgesellschaftlich entgegenzutreten, wurde im Jahr 2017 das „Bundesweite Netzwerk Extremismusprävention und Deradikalisierung“ (BNED) gegründet.

Unter Koordination des Bundesministeriums für Inneres (BMI) stimmen sich seither Vertreterinnen und Vertreter aus Ministerien, Bundesländern, der Zivilgesellschaft, dem

BNED

Bundesweites
Netzwerk
Extremismus-
prävention und
Deradikalisierung

Österreichische Strategie Extremismusprävention und Deradikalisierung

Städte- und dem Gemeindebund sowie anlassbezogen Expertinnen und Experten aus Wissenschaft und Forschung in regelmäßigen Abständen zu strategischen Aspekten von Extremismusprävention und Deradikalisierung in Österreich ab. Das Netzwerk versteht sich dabei als zentrales strategisches und politikberatendes Gremium zur gesamtstaatlichen Auseinandersetzung mit Extremismusprävention und Deradikalisierung in Österreich. Es soll als wichtiges Früherkennungsinstrument dienen, in welchem Wissen generiert, gebündelt und verwertet wird.

Als qualitativ hochwertiges Beratungsgremium soll das BNED die Politik und Entscheidungsträger mit strategischen Handlungsempfehlungen, „Policy Paper“ und sonstigen relevanten Informationen unterstützen. Durch die Anerkennung des BNED am 8. Juli 2020 durch den Ministerratsvortrag wurde ein Meilenstein in der gesamtgesellschaftlichen Extremismusprävention und Deradikalisierung gesetzt. Das BNED ist somit als überparteiliches, sachlich objektives und unvoreingenommenes Gremium aus Expertinnen und Experten anerkannt.

Das Jahr 2020 stand auch im Zeichen der Weiterentwicklung und Professionalisierung des BNED. Im Rahmen einer Arbeitsklausur wurden mit den Netzwerkmitgliedern partizipativ die Eckpfeiler der künftigen Arbeitsmethodik und Struktur identifiziert und weiterentwickelt. Daraus folgend wurde ein „Mission Statement“ erstellt, in dem die Ziele, die Aufgaben sowie die strukturierte Arbeitsweise des BNED abgebildet wurden und die als strategischer Rahmen für die zukünftigen Netzwerkarbeiten des BNED dienen sollen.

Das Netzwerk hat demzufolge zur Aufgabe:

- Einzelmaßnahmen der Extremismusprävention und Deradikalisierung zu bündeln,
- den fachlichen und interdisziplinären Austausch zu bundesweiten Maßnahmen im Bereich Extremismusprävention und Deradikalisierung voranzutreiben,
- geeignete Interventionsmaßnahmen zu identifizieren sowie
- Handlungsempfehlungen, Strategien, Aktionspläne etc. zu aktuellen Themen der Extremismusprävention und Deradikalisierung zu erstellen.

Um sich inhaltlich mehr drängenden Themen der Extremismusprävention widmen und schneller auf neue Phänomene reagieren zu können, einigte man sich auf die Einsetzung von themenbezogenen Arbeitsgruppen. Zur Umsetzung der Arbeitsgruppen wurden Netzwerktätigkeiten von internationalen Institutionen auf ihre Umsetzbarkeit überprüft und teilweise Anleihe genommen. Folgende vier Arbeitsgruppen wurden von den Mitgliedern des BNED auf Grund der Dringlichkeit und Aktualität vorgeschlagen und etabliert:

- AG „Antisemitismus“

Die jüngsten antisemitisch motivierten Vorfälle im deutschsprachigen Raum erforderten einen besonderen Fokus auf dieses breite Phänomen, das vom rechtsextremistischen bis zum islamistischen Spektrum reicht.

- AG „Verschwörungstheorien“

Als Reaktion auf die zunehmenden Verschwörungstheorien und die vermehrt verschwörerischen Überzeugungen und Ideen in der österreichischen Gesellschaft und weltweit, insbesondere seit der COVID-19-Krise, die sich als Vorläufer einer etwaigen Radikalisierung zeigen können, wurde eine Arbeitsgruppe gegründet, um politische Empfehlungen und Expertisen zu entwickeln, die dazu beitragen sollen, Verschwörungstheorien wirksam zu verhindern und ihnen entgegenzuwirken.

- AG „Regionale Netzwerke in den Bundesländern“

Da der Bedarf an der Etablierung von lokalen Netzwerkstrukturen besteht, um Extremismusprävention und Deradikalisierung strukturell und gesamtgesellschaftlich zu begegnen, wurde dafür eine Arbeitsgruppe gegründet.

- AG „Nationaler Aktionsplan Extremismusprävention und Deradikalisierung“

Diese Arbeitsgruppe setzt sich mit der Entwicklung des Nationalen Aktionsplans auseinander.

Neben den üblichen Aktivitäten des nationalen Netzwerks wird es mit dieser neuen Arbeitsstruktur für Stakeholder möglich sein, mit einem vielfältigen Repertoire an Fachwissen und beruflichem Hintergrund, Themen der Extremismusprävention und Deradikalisierung stärker zu betonen, indem politische Empfehlungen formuliert und gleichzeitig an anderen relevanten Ergebnissen gearbeitet wird. Darüber hinaus wird der Aufbau einer behördenübergreifenden Zusammenarbeit innerhalb und außerhalb der Grenzen der Bundesländer zu einem strategischen Gesamtnetzwerk führen. Die vielfältigen Strukturen der Kommunikation und des Wissenstransfers ermöglichen es, Probleme des gewalttätigen Extremismus auf verschiedenen Ebenen zu bearbeiten.

Ein koordiniertes Ausstiegs- und De-Radikalisierungsprogramm in Österreich – Projekt KOMPASS

Aufgrund der europaweiten Bedrohung von Radikalisierung und Rekrutierung entlang des politisch, religiös oder weltanschaulich motivierten Extremismus, steht das BMI zunehmend vor neuen Aufgaben zur Wahrung der inneren Sicherheit Österreichs. Gerade in Zeiten der Krise, wie wir sie auch durch COVID-19 erleben, erfahren extremistische Ideologien jeder Form mehr Aufwind und stellen eine Herausforderung für die demokratische Gesellschaftsordnung dar. Mehr denn je bedarf es einer auf den Bedürfnissen der aktuellen Entwicklungen angepassten Möglichkeit der Ausstiegsarbeit, um Extremismus effektiv und nachhaltig begegnen zu können. Unter Berücksichtigung der Empfehlungen und abgeleitet von der wissenschaftlichen Evaluierung des einjährigen Pilotprojektes (2017-2018), wurde mit 1. September 2020 ein österreichisches koordiniertes Ausstiegsprogramm etabliert.

Mit der Einführung des österreichischen Ausstiegs- und Deradikalisierungsprogrammes erfolgte die Beauftragung des Vereins NEUSTART zur Umsetzung der gesamtstaatlich koordinierten Ausstiegs- und Deradikalisierungsarbeit. Ziel des Projektes KOMPASS ist die Distanzierung einer radikalisierten Person von einer extremistischen Ideologie und die Ermöglichung der Resozialisierung. Somit soll das Risiko, welches von einer radikalisierten/extremistisch-ideologisierten Person ausgehen kann, für die Gesellschaft verringert werden. Im 21-monatigen Projektzeitraum des Projektes KOMPASS werden alle Formen des Extremismus mitberücksichtigt. Durch engmaschige und individuelle Betreuungsmaßnahmen soll auf Alternativen zu extremistischen Ideologien abgezielt und weitere Radikalisierung verhindert werden. Die Zielgruppe umfasst nicht nur bereits straffällige Personen nach der Haftentlassung, sondern auch jene Personen, die den Absprung von einer extremistischen Ideologie schaffen wollen. Als wesentliches Merkmal gilt, dass diese Personen die freiwillige Entscheidung getroffen haben müssen, sich schrittweise von extremistischen Weltanschauungen und Gruppen zu lösen und sich in die liberale, demokratische Gesellschaft re-integrieren zu wollen. Der Verein NEUSTART, der als koordinierende Stelle agiert, verfügt über jahrzehntelange Erfahrung im Bereich des Übergangsmanagements zwischen Haft und Freiheit sowie bei der Reintegration

und Resozialisierung von Personen. Neben dem Verein NEUSTART wird zusätzlich anlassbezogen die Expertise von spezialisierten Organisationen herangezogen, die mit unterschiedlichen Methoden mit Klientinnen und Klienten arbeiten und damit bereits sehr gute Erfolge verzeichnen konnten.

Ein weiterer Meilenstein für die nationale Extremismusprävention- und Deradikalisierungsarbeit unter der Federführung des BMI ist die gesetzliche Verankerung von sicherheitspolizeilichen Fallkonferenzen, die seit dem 1. Januar 2020 durchgeführt werden konnten. Mit der Einführung dieses Rechtsinstruments ist es nun möglich, durch Informationsaustausch zwischen den zuständigen Behörden und Institutionen koordinierte Maßnahmen zur Verhinderung von Straftaten zu treffen. Auf Basis einer Gefährdungseinschätzung und Sicherheitsplanung können somit unter der Leitung der Sicherheitsbehörde besondere Schutzmaßnahmen für Hochrisikofälle des gewaltbereiten Extremismus oder Fälle mit mittlerem Risiko, je nach Gefährdungsgrad, erarbeitet und zum Schutze der Allgemeinheit umgesetzt werden. Dies geschieht in enger Zusammenarbeit mit jenen Behörden und Einrichtungen, die mit dem Vollzug öffentlicher Aufgaben – insbesondere zum Schutz vor bzw. der Vorbeugung von Gewalt sowie der Betreuung von Menschen – betraut sind. Sicherheitspolizeiliche Fallkonferenzen dieser Art wurden infolgedessen im nationalen Ausstiegsprogramm KOMPASS schon mehrmals als Rechtsinstrument eingesetzt, bevor die Arbeit mit den ausstiegswilligen Klientinnen und Klienten begonnen wurde und individuell zugeschnittene Maßnahmen gesetzt wurden.

Kooperation der Ausstiegsarbeit auf EU-Ebene - Projekt EXIT Europe

Die Sicherheitsbehörden haben in den letzten Jahren verstärkt bundesweite Maßnahmen im Bereich Extremismusprävention und Deradikalisierung gesetzt, um gegen alle Formen des Extremismus vorzugehen. Dabei orientierte man sich am gesamtgesellschaftlichen Ansatz. Eine weitere Maßnahme ist das Projekt EXIT Europe unter der Koordination des BVT, das im Jahr 2019 angelaufen ist, mit dem Ziel der gemeinsamen Etablierung evidenzbasierter und praxisorientierter Ausstiegsprogramme zur Professionalisierung und qualitativen Aufwertung der europaweiten Ausstiegs- und Deradikalisierungsarbeit. Zunächst wurde ein Trainingshandbuch für Ausstiegs- und Distanzierungsarbeit entwickelt. Die Methoden im Handbuch bauten auf die Fachkenntnisse und das Praxiswissen von internationalen Akteuren der Zivilgesellschaft sowie auf die methodische Vorgehensweise aus der Pilotphase des Österreichischen Ausstiegsprogramms auf. Praktikerinnen und Praktiker wurden auf Basis dieses Handbuchs für Ausstiegs- und Distanzierungsarbeit aus dem gewaltbereiten Extremismus ausgebildet. Zugleich wurden sie mit qualitativ hochwertigen Instrumenten ausgestattet, um neben Österreich Ausstiegsprogramme in vier weiteren operativen Partnerländern Europas zu etablieren, denen es in weiten Teilen an Ressourcen oder Strukturen für koordinierte Deradikalisierungs- und Distanzierungsarbeit fehlt: Deutschland, Frankreich, Italien und die Slowakei. Nach dem Vorbildmodell des vom BVT koordinierten „Bundesweiten Netzwerks Extremismusprävention und

Deradikalisierung“ (BNED) wurden in den involvierten Ländern darüber hinaus lokale bzw. nationale Netzwerke aufgebaut, um zielgerichtete Maßnahmen für ausstiegswillige Personen zu setzen. Ähnlich wie in Österreich konnten mit einer gesamtgesellschaftlichen Kooperation zwischen Zivilgesellschaft, Sicherheitsbehörden und den Einrichtungen, die für diese Personen besonders relevant sind, individuelle Bedürfnisse weitgehend abgedeckt und Unterstützungsangebote auf sie zugeschnitten werden, die ihnen neue Perspektiven bieten und den Ausstieg erleichtern. Dabei fokussiert EXIT Europe auf alle Formen des gewaltbereiten Extremismus und bezieht lokale Kontexte der Partnerländer mit ein, da extremistische Ideologien je nach Land unterschiedlich stark auftreten. Ebenfalls berücksichtigt werden Schlüsselelemente der psychosozialen Betreuung und ideologischen Dekonstruktionsarbeit. Auf diese Weise wurden stabile Strukturen geschaffen, um nachhaltige Rehabilitierungs- und Reintegrationsmaßnahmen auch nach Projektende zu gewährleisten. Das Potential von EXIT Europe liegt darin, durch einen intensiven Austausch über die Entwicklungen, Wirkung und Erfolge von Ausstiegsarbeit mit den Projektländern, aber auch durch eine kontinuierliche Evaluierung und Qualitätskontrolle während der Projektlaufzeit, zur Professionalisierung der europaweiten Deradikalisierungsarbeit beizutragen.

Pandemie und Sicherheit

Am 25. Februar 2020 wurden die ersten zwei COVID-19-Fälle in Österreich registriert. Nicht ganz ein Monat später, am 11. März 2020, erklärte die Weltgesundheitsorganisation (WHO) COVID-19 zur weltweiten Pandemie. Es sollte ein Jahr mit weitreichenden Veränderungen alltäglicher Routinen und wirtschaftlicher Abläufe folgen. Aus der Perspektive der österreichischen Staatsschutzbehörden hat die Pandemie auch nicht vor den Phänomenbereichen Halt gemacht, deren Erforschung und Bekämpfung sich der Staatsschutz widmet.

Die gesundheitlichen, wirtschaftlichen, sozialen und psychologischen Folgen der Pandemie hatten nicht nur Auswirkungen auf das gesellschaftliche Zusammenleben in Österreich. Das Jahr 2020 brachte viele Veränderungen und viele Unsicherheiten mit sich. Kurzarbeit, ein möglicher Verlust des Arbeitsplatzes, die Sorge vor den möglicherweise schweren Folgen einer Erkrankung mit COVID-19, die Sorge um die eigene Zukunft, aber auch um die Perspektiven von Angehörigen und Freunden, schafften einen gesellschaftlichen Zustand, in dem das eigene Leben zunehmend von der Pandemie bestimmt zu werden scheint.

Für staatsschutzrelevante Gruppierungen ist diese Entwicklung Nährboden, um die eigenen extremistischen Botschaften breiter in die Bevölkerung streuen zu können. Extremistische Gruppierungen reflektierten von Beginn an auf die Pandemieentwicklung.

In der ersten Phase der Pandemie wurde dies zunächst in der propagandistischen Verarbeitung von COVID-19 deutlich.

Pandemie und Propaganda

Verschiedenste, teilweise auch halbstaatliche, Akteure haben zu Beginn der Pandemie die unterschiedlichsten Erklärungen über den Ursprung des Sars-CoV-2-Virus verbreitet.

Islamistische Terrororganisationen deuteten die Pandemie in der eigenen propagandistischen Kommunikation als eine „Strafe Gottes für die Kreuzfahrernationen". Mit dem Begriff Kreuzfahrernationen wird von islamistischen Terrororganisationen ein altbekanntes Feindbild, die westliche Staatengemeinschaft, adressiert.

Linksextremistische Gruppierungen sahen Anfang 2020 in ihrer propagandistischen Deutung des Geschehens das Ende der „kapitalistischen Weltordnung" gekommen.

Für die Anhänger staatsfeindlicher Verbindungen wurden, die bereits vor der Pandemie verbreiteten Verschwörungserzählungen, von einem konspirativ agierenden „Tiefen Staat", der die gesamte Menschheit ins Verderben führen wird, nun Wirklichkeit. Diese Verschwörungserzählungen, vor allem jene von QAnon, intensivierten sich im Verlauf der Pandemie und haben auch in Österreich an Reichweite gewonnen.

QAnon – Ein verschwörungsideologisches Baukastensystem zur Erklärung der Welt in der Pandemie

Bei QAnon handelt es sich um eine 2017 in den USA entstandene, Verschwörungsideologien verbreitende Bewegung. Ihre Bezeichnung setzt sich aus dem Benutzernamen „Q" eines Users auf einer einschlägigen US-amerikanischen Onlineplattform und dem Wort „Anonymous" zusammen. Anhänger dieser Bewegung glauben in den USA unter anderem an einen „Kampf" gegen den „tiefen Staat" – einem verschwörerischen Netzwerk aus Politikern, Bürokraten, Behörden und Medien, welches die USA kontrolliert.

In Österreich werden die verschwörungsideologischen Erzählungen von QAnon ab März 2020 immer populärer. Zunächst ausgehend von Diskussionen in Sozialen Medien finden sich ab April 2020 die ersten Protestteilnehmer an den Demonstrationen gegen die COVID-19-Maßnahmengesetzgebung mit Symbolen der QAnon-Bewegung ein.

COVID-19 wird sehr schnell in das weltverschwörerische Ideologiegebilde von QAnon aufgenommen. Vor allem Falschmeldungen im Zusammenhang mit der

damals in Entwicklung befindlichen COVID-19-Impfung werden schon sehr früh im Jahr 2020 in die Welt gesetzt.

Die verschwörungsideologische Weltsicht von QAnon überbetont einen „Erweckungsmoment". Die Anhänger von QAnon sind „Erwachte", welche die vermeintliche Weltverschwörung ausgehend vom „Tiefen Staat" nun klarer sehen. Dieser „Erweckungsmoment" ist zentraler Bestandteil vieler Ideologien von extremistischen oder radikalen Gruppierungen und dient zur Abgrenzung von der restlichen Bevölkerung und den expliziten Feindbildern der Bewegung. Feindbild von QAnon ist der Staat. Genau jener Staat, der in der COVID-19-Pandemie wahrnehmbar in den Alltag der Menschen eingreifen wird, um die Ausbreitung der Pandemie zurückzudrängen. Die Erzählung vom „Tiefen Staat" ist jedoch keine genuine Erfindung von QAnon. Rechtsextremistische Gruppierungen hantieren mit diesem Begriff, der oft auch antisemitisch konnotiert wird, seit vielen Jahren.

Rechtsextremistische Gruppierungen, vor allem jene aus dem deutschsprachigen Raum, verhielten sich zu Beginn der Pandemie taktisch differenzierter als andere Gruppierungen. Zentrale Aktivisten der sogenannten „Neuen Rechten" stellten sich anfangs noch hinter die Maßnahmen zur Eindämmung des Infektionsgeschehens. Erst mit dem Entstehen einer Protestbewegung im April 2020 erfolgte eine radikale Strategieänderung neurechter Akteure. So wurde ihr Hauptthemenfokus von Migration auf die Kritik der Corona-Maßnahmen umgelenkt beziehungsweise ergänzt.

Pandemie und Protest

Am 16. März 2020 trat der erste Lockdown während der COVID-19-Pandemie in Kraft. Es dauerte knapp ein Monat, bis sich die ersten Proteste gegen die Maßnahmen zur Eindämmung der Pandemie formieren sollten. Am 24. April 2020 fand der erste Protest in Wien statt. Bereits bei dieser ersten Protestkundgebung fanden sich Aktivisten aus der rechtsextremistischen Szene ein. Allen voran Vertreter der sogenannten Neuen Rechten. Während sich viele Aktivisten dieser Protestbewegung im Verlauf des Jahres nach und nach aus dem Protestgeschehen zurückgezogen hatten, blieb die Beteiligung von rechtsextremistischen Gruppierungen und Einzelakteuren über die Monate hinweg aufrecht. In ihren ersten propagandistischen Aussendungen im März 2020 pflichteten Aktivisten der Neuen Rechten noch den Maßnahmen der Bundesregierung bei. Schließlich

galt es mit dem Virus einen „neuen Feind“ von außen zu bekämpfen. Im weiteren Verlauf der Pandemie erkannten rechtsextremistische Netzwerke jedoch relativ rasch, dass sich der vordergründige Protest gegen die Maßnahmen wohl auch zu einem Protest gegen den Staat und seine demokratisch legitimierten Institutionen umlenken lassen wird können.

Pandemie und Radikalisierung

Nahezu alle Staaten der Welt haben zu unterschiedlichen Zeitpunkten im Verlauf des Jahres 2020 Maßnahmen zur Eindämmung der Pandemie ergriffen. Diese Maßnahmen zum Schutz der Allgemeinheit wurden individuell unterschiedlich erlebt. Ein sozialpsychologischer Effekt der sich zeitverzögert eingestellt hat, war, dass der Staat selbst nun als handlungsmächtiger Akteur in das tägliche Leben der Bürgerinnen und Bürger eingreift.

Die Pandemie verlangsamte zunächst den Prozess des Strukturwandels, der in allen postindustriellen Gesellschaften seit den 1970er Jahren zu beobachten ist. Dieser Strukturwandel, von modernen Gesellschaften, die von der industriellen Produktion geprägt sind, hin zu spätmodernen Dienstleistungs- und Wissensgesellschaften, ist auch mit einem kontinuierlichen Rückgang des staatlichen Einflusses auf die Wirtschaftsentwicklung und das alltägliche Leben der Menschen gekennzeichnet. Dies erklärt bis zu einem gewissen Grad, warum in manchen Teilen der Bevölkerung die von der Politik sehr weitreichenden Sicherungsmaßnahmen zur Pandemiebekämpfung als Bevormundung und Einmischung in ihre wirtschaftlichen und privaten Sphären empfunden wurden. Vor diesem Hintergrund konnten Leugner, Skeptiker und Extremisten die dafür charakteristische Stimmung der Ungewissheit einfach manipulieren und für ihre Ideologie instrumentalisieren. Die Neuheit der Virusbekämpfungsform mit Maßnahmen des Lockdowns (inklusive Reise- und Bewegungseinschränkungen) sowie die dynamische Komplexität der Virusverbreitung steigerte zeitgleich Verschwörungserzählungen bezüglich des Ursprungs des Virus aber auch gegen Experten und Politiker. Die Ungewissheit der (wirtschaftlichen) Zukunft und der Vertrauensverlust in die Notwendigkeit und Wirksamkeit der Maßnahmen hinsichtlich ihrer Verhältnismäßigkeit, sind zentrale Mobilisierungsfaktoren für einige Bevölkerungsgruppen, welche ihren Unmut darüber in der Öffentlichkeit artikulierten.

Schnell war zu beobachten, dass die unmittelbare Betroffenheit – einerseits die einer Infektion und Krankheit, andererseits von den behördlichen Eindämmungsmaßnahmen – viele Bevölkerungsschichten zunehmend emotionalisierte und teils radikalisierte. Extremisten unterschiedlichster Provenienz griffen diese diffusen Krisenängste auf, um diese in einfache unterkomplexe Antworten zu konvertieren. Für viele waren ideologisch grundierte Meinungen und einfache „Lösungsvorschläge“ in Internetforen und anderen Teilöffentlichkeiten im Internet nicht leicht dechiffrierbar und führten zu einer massiven Verbreitung von Desinformationen.

Insbesondere offen gewaltbefürwortende Extremisten standen in den letzten Dekaden vor dem Problem, eine breite und nachhaltige Mobilisierungsbasis für ihre demokratiezersetzenden Ideologien und „Umsturzpläne“ sicher zu stellen. Das Gewaltmoment oder die Teilnahme von bekannten Extremisten bei Demonstrationen und Straßenprotesten wirkte für viele Teile der Bevölkerung abschreckend und führte oft zur frühzeitigen Beendigung von sozialen Bewegungen.

Pandemie und Kritik

Die junge Protestbewegung, die sich zu Beginn des Jahres noch unter dem Blickwinkel der Kritik am COVID-19-Maßnahmengesetz formierte, änderte gegen Jahresende ihre strategische Ausrichtung. Dominierten anfänglich noch die Kritik an Abstandsregeln und das Tragen von MNS-Masken die Redebeiträge bei Demonstrationen, verlagerte sich die thematische Schwerpunktsetzung der Bewegung auf eine allgemeine regierungskritische Linie. Die Protestbewegung selbst ist in vielerlei Hinsicht als postmoderne Bewegung zu charakterisieren. Postmodern in dem Sinn, dass kein gemeinsamer Wertekanon geteilt wird, die Protestteilnehmer aus unterschiedlichsten Bevölkerungsteilen stammen und unterschiedliche soziodemographische Merkmale aufweisen. Vereint werden diese Kritiker unter der einfachen Formel „Ich bin dagegen“. Wie die Pandemie tatsächlich überwunden werden soll, wird kaum behandelt. Fraglich bleibt, ob diese Grundhaltung des Dagegenseins die Pandemie überdauern wird und die Proteststeilnehmer, die sich im Kontext der Proteste während der Pandemie radikalisiert haben, ihrer Ablehnung gegen den Staat zukünftig neue Ausdrucksformen verleihen werden.

stock.adobe.com

Pandemie und Symbolik

Auf den Demonstrationen gegen die COVID-19-Maßnahmen der Bundesregierung dominieren Österreichfahnen das Straßenbild. Dennoch finden sich noch einige andere Symbole, die auch medial für Aufsehen sorgten. Für Aktivisten, die sich vorab im Internet tiefer in die verschwörungsideologische Weltsicht von QAnon begeben haben, gilt es ein „diktatorisches Politsystem", den sogenannten „Tiefen Staat" zu bekämpfen. Mit der „Baukastenideologie" von QAnon kann jeder zum „Erleuchteten Aktivisten" und „Kämpfer gegen das System" werden. Die ersten QAnon-Symbole wurden bereits im April 2020 auf Demonstrationen gegen die COVID-19-Gesetzgebung registriert.

Für Sympathisanten der Neuen Rechten ist ein Kampf gegen den „Great Reset" ein mögliches Motiv des Protests. Auch bei der verschwörungsideologischen Umdeutung des Buches „The Great Reset" – einer Publikation die ursprünglich vom Weltwirtschaftsforum (WEF) vorangetrieben wurde – ist, aus Sicht der Neuen Rechten, ein zwielichtig agierender Staat der Feind der Menschheit und muss bekämpft werden. Vereint werden diese unterschiedlichen Motivlagen unter der einfachen Formel „Ich bin dagegen".

Vieles bei dieser jungen Protestbewegung mag für den außenstehenden Betrachter widersprüchlich oder manchmal auch skurril anmuten. Etwa, warum neben der Österreichfahne, die schwarz-weiß-roten Flagge des deutschen Kaiserreichs (1871-1918), QAnon-Symboliken oder Fahnen aus dem US-Wahlkampf der republikanischen Partei im Jahr 2020 durch die Straßen Wiens getragen werden. Für die Aktivisten der Bewegung drücken diese Symbole vielmehr den gemeinsamen Sinn „Ich bin dagegen" aus und sind weniger Ausdruck eines geteilten, kollektiven politischen und ideologischen Wertekanons.

Die Gefahr für die Innere Sicherheit des Landes liegt im Radikalisierungspotenzial dieses Dagegenseins, das durch die verschwörungsideologischen Erzählungen von rechtsextremistischen Gruppierungen oder auch von QAnon instrumentalisiert und demokratiefeindlich eingesetzt wird.

Pandemie und Konflikt

Die dynamischen Ereignisse und volatilen Entwicklungen des Jahres 2020 haben alle gesellschaftliche Bereiche in unterschiedlichsten Ausprägungen beeindruckt und vor einzigartige Herausforderungen gestellt. Auch für die Staatsschutzbehörden war in den relevanten Phänomenbereichen ein beschleunigter Wandel erkennbar. So war nicht nur ein gesteigertes Aggressionspotenzial auf den Straßen und im Internet feststellbar, sondern auch eine Ausweitung der Erreichbarkeit von potenziellen Sympathisanten, welche über wenig Protesterfahrungen verfügten. Die „klassischen" Konfrontationslinien von rechten bis rechtsextremen Protesten gegen linke bis linksextreme Gruppierungen, wurden um weitere Facetten und Konfrontationsherde erweitert. Auffällig an diesen Entwicklungen ist die heterogene Zusammensetzung der Protestteilnehmer. Diese reicht

von Personen, die unmittelbar von den wirtschaftlichen Folgen der Pandemie betroffen sind, über Wirtschaftstreibende der Mittelschicht bis hin zu Bürgerinnen und Bürger. Problematisch erscheint der Umstand, dass diese heterogene Protestbewegung unter der Begleitung von extremistischen Mobilisierungsstrategen zum Protest aufgerufen wird.

Auffällig an diesen Entwicklungen ist die heterogene Zusammensetzung der Mobilisierungsmassen von unmittelbar Betroffenen, Wirtschaftstreibenden der Mittelschicht, besorgten Bürgerinnen und Bürgern, welche unter der Begleitung von extremistischen Mobilisierungsstrategen „mitgenommen" werden.

Wann die Pandemie letztendlich beendet sein wird, vermag zu Jahresbeginn 2021 niemand seriös abzuschätzen. Mit Ende der Pandemie wird sich diese junge Protestbewegung auch thematisch transformieren müssen.

Was sich aber aus Sicht der österreichischen Staatsschutzbehörden schon Ende 2020 abzeichnet, ist, dass die Entwicklung rund um die COVID-19-Pandemie auch neue Formen der radikalen Ablehnung staatlicher Strukturen beschleunigt hat.

Unter den Anhängern staatsfeindlicher Verbindungen hatten beispielsweise die „Erwachungsmomente" der QAnon-Verschwörungsideologie bereits vor der Corona-Pandemie eine überschaubare Anhängerschaft in Österreich gefunden. Die verschwörungsideologischen Erzählungen wurden nicht zuletzt über Soziale Medien, die zur Organisation des Protests auf der Straße genutzt werden, in der Pandemie breiten Teilen der österreichischen Gesellschaft zugänglich.

Der Kern der besorgniserregenden Entwicklungstrends im Kontext der Corona-Pandemie ist der Umstand, dass eine demokratiefeindliche Spaltung von Extremisten nachhaltig zu gewaltbereiten Massenmobilisierung führen kann.

Die Pandemie scheint die soziale Ungleichheit im Land eher zu verstärken. Wachsende soziale Ungleichheit kann auch immer ein Nährboden für die extremistischen Ränder der Gesellschaft sein. Eine Trendentwicklung der letzten Jahre, wonach diese extremistischen Ränder stärker um Zulauf bemüht sind, könnte sich durch die Pandemie somit fortsetzen.

Der Cyber-Raum und seine Auswirkung auf die Resilienz Österreichs

Durch die seit Beginn des Berichtszeitraums herrschenden Krisen ist ein Thema in den Fokus gerückt, welches zuvor eher ein Schattendasein führte und nur im Zusammenhang mit "Blackout-Szenarien" zur Sprache kam: Resilienz – also die Fähigkeit, auch bei

Teilausfall eines Systems noch ein gefordertes Maß an Funktionalität dieses Systems gewährleisten zu können und nicht zu versagen.

Es wurde sichtbar, dass es auch ohne Blackout, beispielsweise durch geopolitische Entwicklungen wie Handelskonflikte oder Sanktionen-Regimen, politische Änderungen im jeweiligen Bereitsteller-Staat[25], (Natur-)Katastrophen, „technische Probleme“[26] oder eben Gesundheits-Pandemien zu Einschränkungen oder den kompletten Abbruch der (Internet-)Verbindung, den “Lebensadern” in denen das neue “Öl” in Form von Daten fließt, kommen kann. Dies geschieht, wenn die fünfte Domäne, der Cyber-Raum, Teil eines Konfliktes wird und Einschränkungen im Personen-, Waren- und Dienstleistungsverkehr stattfinden, Auswirkungen einer Naturkatastrophe die Infrastruktur beschädigen (u.a. Unterseekabel durchtrennt werden oder Infrastruktur (~Serverfarmen) in der Nähe der Katastrophe loziert sind) oder eine schlichte Fehlbedienung vorliegt.

„Die Wirtschaft ist im Hinblick auf ihre technische Weiterentwicklung und Effizienz ihrer internen Geschäftsprozesse zunehmend von einer funktionierenden digitalen Infrastruktur abhängig. Für die öffentliche Verwaltung ist das Internet eine unverzichtbare Grundlage geworden, ihre Dienstleistungen über den traditionellen Weg hinaus einer breiten Öffentlichkeit zugänglich zu machen. Angriffe aus dem Cyber-Raum sind eine unmittelbare Gefahr für die Sicherheit und das Funktionieren von Staat, Wirtschaft, Wissenschaft und Gesellschaft. Sie können unser tägliches Leben schwerwiegend beeinträchtigen“.[27]

Diese einleitenden Worte zur Österreichischen Strategie für Cyber-Sicherheit (ÖSCS) aus dem Jahr 2013 legen bereits deutlich dar, dass der Cyber-Raum eine unverzichtbare Grundlage zur Funktion des Staates darstellt. Diese Feststellung gilt heute mehr denn je und nicht nur in Bezug auf Cyber-Angriffe, denn seit damals hat sich durch technologische Neu- und Weiterentwicklungen bei Verfügbarkeit, Geschwindigkeit und Angeboten, durch Änderungen sozialer Verhaltensweisen (z.B. Nutzung von Social Media und digitaler Konsum) und Anpassungen gesellschaftspolitischer Prozesse (digitale Verwaltung, Kommunikation, Produktions- und Logistikprozesse) bei der Nutzung des Cyber-Raums, die Abhängigkeit von dieser Grundlage weiter gesteigert. Schlagworte wie Big Data, Cloud Computing, Smart Cities, Industrie 4.0, Smart Precision Livestock Farming[28], autonomes Fahren oder Internet of (Every)Things (IoT) sind allgegenwärtig. Als zusätzlicher Beschleuniger dieser Entwicklung, vor allem hinsichtlich

25 Vgl. https://www.derstandard.at/story/2000119709760/internetzensur-in-belarus-wien-mischt-sich-nicht-in-die-geschaefte

26 Siehe https://futurezone.at/digital-life/weltweite-ausfaelle-bei-microsoft-outlook-und-teams-betroffen/401047324. 30.09.2020

27 https://www.bmi.gv.at/504/files/130416_strategie_cybersicherheit_WEB.pdf, Seite 4, 18.09.2020

28 Siehe https://www.innovationfarm.at, 12.10.2020

der fast bedingungslosen Akzeptanz und Nutzung von Telekonferenz-Produkten als Führungsinstrument, Cloud basierten Dienstleistungen wie Kollaborationsplattformen, Messenger Diensten und Telearbeit und der Abkehr von Datenschutzbedenken, kann die gegenwärtige COVID-19-Krise gesehen werden. „Cyber" ist daher neben Energie zum entscheidenden Beurteilungsfaktor zur Erreichung einer entsprechenden Versorgungsresilienz im Staatsganzen geworden, da „Cyber" nicht nur technologiebedingt von Vulnerabilitäten nicht verschont ist.

Abgesehen von absichtlich herbeigeführten Cyber-Angriffen mit kriminellem, extremistischem, terroristischem oder politischem Motiv, ist die möglich gewordene Beeinträchtigung oder Unterbrechung der Verfügbarkeit von Geräten und Services im Netzwerk eine Bedrohung. Diese Bedrohung wird durch eine zeitkritische und nicht redundante Ausführung von Lieferketten (Supply Chain) heutiger Organisationen verstärkt. Unabhängig von einzelnen Ursachen einer etwaigen Unterbrechung, geht mit dieser Bedrohung bei längerer Dauer der Nicht-Verfügbarkeit eine massive Einschränkung einher, wenn Arbeits-, Produktions-, Geschäfts- oder Verwaltungsprozesse auf permanente Verfügbarkeit hinsichtlich Konnektivität angewiesen sind. Mit Unterbrechung der Konnektivität ist nicht nur die physische Unterbrechung durch Zerstörung, technisches Gebrechen (kein Ersatz vorhanden) oder „Abstecken" gemeint, sondern auch der Zugriff innerhalb eines Netzwerks auf notwendige Online-Ressourcen wie beispielsweise Cloud-Services (u.a. E-Mail-Services, Datenspeicher), Video-Konferenz-Lösungen, Online-Kollaborationsplattformen oder Software-as-a-Service (SaaS: z.B. Office365), Platform as a Service (PaaS) oder Infrastructure as a Service (IaaS) bei an sich funktionierender Technik. Auch Online-Prüfungen in Echtzeit von Software-Lizenzen[29] oder Herstellersignaturen von installierter Software beim Start eines Programms[30], Remote Desktop-Verbindungen für Teleworking, IoT-Lösungen (z.B. Sicherheitskameras mit Google-Login), Telebanking oder Verkaufs- oder Informationsportale können bei eigentlich intakter Infrastruktur unterbrochen werden und so deren Funktionsumfang eingeschränkt oder die Verwendung verhindert werden. Dies kann bei längerer Dauer zu einer Krise in einer anderen Krise führen, wenn kein "Plan B" ohne vernetzte IKT besteht und auf benötigte und eigentlich vorhandene Ressourcen zur Bewältigung einer Krise nicht zurückgegriffen werden kann.

29 Eine lokale Installation von MS Office beispielsweise nimmt regelmäßig und automatisch eine Verbindung mit dem Linzenz-Server auf. Nach nicht erfolgter erfolgreicher Prüfung steht nur eine eingeschränkte Funktionalität im gesamten lokal installierten Office Paket zur Verfügung

30 Siehe "Apples Image beim Datenschutz angekratzt", https://orf.at/stories/3190927/, 25.11.2020

Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) und Infrastructure-as-a-Service (IaaS):
Die Begriffe beschreiben alternative Nutzungsarten von Hard- und Software. Bei **Software-as-a-Service (SaaS)** wird sowohl die Software, als auch die darunterliegende Hardware von einem externen Unternehmen betrieben und gegen Entgelt den diesbezüglichen Kunden angeboten. Die Nutzung solcher Software durch den SaaS-Kunden erfolgt in der Regel über einen normalen Webbrowser.

Im Unterschied dazu wird den Kunden bei **Platform-as-a-Service (PaaS)** eine vollständige Entwicklungsumgebung für die Erstellung von Software (insbesondere Webanwendungen) zur Verfügung gestellt. Damit kann eine Entwicklung ohne Anschaffung und Einrichtung einer eigenen Entwicklungsumgebung durchgeführt werden.

Unter **Infrastructure-as-a-Service (IaaS)** versteht man schließlich die Anmietung von Hardware (insbesondere Serverinfrastruktur) bei einem externen Anbieter und die Nutzung dieser Infrastruktur über das Internet. Dadurch können hohe Investitionen in eigene Infrastruktur sowie der laufende Wartungsaufwand ausgelagert werden.

Die Dominanz einiger weniger Unternehmen, angesiedelt zusätzlich im selben Wirtschaftraum, bei der Bereitstellung von systemrelevanter Soft- und Hardware sowie dem Betrieb von digitalen Serviceleistungen und digitaler Infrastruktur, stellt ein nicht zu unterschätzendes Risiko, dar. So liegt die Abhängigkeit in Österreich bei Betriebssystemen[31] von *Microsoft* (Windows-Familie) bei mehr als 70 Prozent, von OS X (*Apple*) bei 20 Prozent, mit 3,16 Prozent bei *Android* (*Google*) und mit 2,93 Prozent bei iOS (*Apple*), was in Summe einen Marktanteil von mehr als 97 Prozent in Österreich bedeutet und 100 Prozent US-Firmen darstellt. Hier handelt es sich allerdings „nur" um Betriebssysteme. Anwendersoftware wie *Microsoft Office365*[32] wird beispielsweise gemäß einer Studie (Herbst 2019) im Auftrag des deutschen Bundesinnenministeriums in 96 Prozent aller (deutschen) Bundesbehörden verwendet[33]. Für Österreich liegen hierzu keine Zahlen auf. Microsoftprodukte sind in der öffentlichen Verwaltung jedoch Standard, wie etwa auch *SAP*[34]. Zum Betrieb der Hardware, auf welcher dann das Betriebssystem

31 https://de.statista.com/statistik/daten/studie/431623/umfrage/marktanteile-der-betriebssysteme-in-oesterreich/, 22.09.2020
32 *https://de.statista.com/statistik/daten/studie/431623/umfrage/marktanteile-der-betriebssysteme-in-oesterreich/*, 22.09.2020
33 Vgl. Spiegel 38 2020, e-Paper, , Seite 23
34 SAP läuft auf Oracle-Datenbanksystemen

läuft, ist sogenannte Firmware notwendig. Diese stellt die Kommunikation der jeweiligen Bauteile, beispielweise auf einem Motherboard, mit dem Betriebssystem sicher. Hardware kommt fast ausschließlich aus China, so auch die dazugehörige Firmware, welche unter anderem von Firmen wie der Hon Hai Technology Group, besser bekannt als *Foxconn*[35], produziert wird.

Diese „quasi" Monokette gilt auch für Clouddienste (Infrastructure as a Serivce; IaaS) bei denen US-Unternehmen wie *Amazon Web Service* (AWS, *aws.amazon.com*) mit 32,06 Prozent, *Microsoft* (*Azur*) mit 16,9 Prozent und *Google Cloud*[36] (Google Compute Engine, GCE) mit 6,9 Prozent in Summe mehr als 57 Prozent der weltweiten derzeitigen Kapazität bereitstellen[37]. Es wird prognostiziert, dass das Wachstum bei Cloudgeschäften von 182,4 Mrd US-Dollar im Jahr 2018 auf 331,2 Mrd US-Dollar im Jahr 2020, vor allem durch die COVID-19-Krise beschleunigt wird[38]. Auch Dropbox (US-Unternehmen) wird beispielsweise bei AWS gehostet. Ebenso ist durch *Telefonica Deutschland* geplant, die sogenannten Campus-Netze ihres zukünftigen 5G-Netzes in der AWS-Cloudinfrastruktur zu betreiben. Eine zumindest "europäische Cloud" existiert bis dato noch nicht.

In Österreich nutzen gemäß Statisik Austria, mit 14. Oktober 2020, bereits rund vier von zehn Unternehmen ab zehn Beschäftigten Cloud Services. Die Nutzung von Cloud Services nimmt mit der Unternehmensgröße zu. Während nur 36 Prozent der kleinen Unternehmen (10 bis 49 Beschäftigte) Cloud Services in Anspruch nehmen, sind es bei mittelgroßen Unternehmen (50 bis 249 Beschäftigte) knapp die Hälfte (49 Prozent) und bei großen Unternehmen (250 und mehr Beschäftigte) 66 Prozent. Innerhalb der vergangenen sechs Jahre hat sich die Nutzung von Cloud Services in österreichischen Unternehmen verdreifacht (2014: 12 Prozent; 2020: 38 Prozent). Speziell kleine Unternehmen weisen eine hohe Steigerungsrate auf (+260 Prozent; mittelgroße Unternehmen +188 Prozent; große Unternehmen +175 Prozent). Neben der gesteigerten Verbreitung von Cloud Services bei Unternehmen, hat sich gemäß Statistik Austria auch die Intensität der Nutzung etwas erhöht. Hat ein Unternehmen 2014 durchschnittlich 2,4 kostenpflichtige Cloud Services genutzt, so sind es 2020 bereits 2,8 Dienste, die ein Unternehmen über Internet verwendet[39].

---

35 Großkunden von Foxconn: Acer, Amazon, Apple, Cisco, Dell, Google, Huawei, Hewlett-Packard, IBM, Intel, Lenovo, Microsoft, Motorola, Nintendo, Nokia, Sony, Toshiba, Vizio, Samsung. Foxconn plant auch die Verlagerung der Produktion nach Mexico, Indien oder Vietnam

36 https://www.netzwoche.ch/news/2020-08-20/google-kaempft-mit-ausfaellen-gmail-und-google-drive-betroffen, 22.09.2020

37 https://futurezone.at/b2b/amazon-web-services-eroeffnet-buero-in-wien/400758822, 22.09.2020

38 Vgl. https://www.heise.de/hintergrund/Cloud-Bursting-platzt-die-Private-Cloud-ist-die-Public-Cloud-zur-Stelle-4968960.html, 25.11.2020

39 Siehe https://www.statistik.at/web_de/presse/124512.html, 05.03.2021

Bei Apps für Smartphones sieht es etwas anders aus. So haben in Österreich Mobil-Geräte mit iOS (Apple) oder Android (Google) einen Marktanteil von nahezu 100 Prozent. Apple beispielsweise entscheidet alleine, ob eine App in den App-Store aufgenommen oder daraus entfernt wird. Aus Google-Play werden häufig Apps entfernt, welche durch Sicherheitsforscher als bedenklich betreffend Datenschutz oder auf Grund von massiven Sicherheitslücken angemahnt wurden. Das hat Auswirkungen auf das eigene Geschäftsmodell oder Verwaltungprozesse, wenn beispielsweise der Verkauf von Dienstleistung oder der Zugang zu Daten, welche zumeist in einer Cloud liegen, über eine dieser Apps läuft und diese App, aus welchen Gründen auch immer, nicht mehr in der Apple- oder Android-Welt funktioniert. In diesem Zusammenhang müssen auch die sogenannten "Corona-Tracing Apps" oder, sich bereits abzeichnend, digitale Impfpässe oder "Freiheits-Pässe" angesprochen werden, welche ausschließlich auf Smartphones mit Apple- oder Google-Betriebssystem betrieben werden sollen.

Es kann jedoch eine Software (App) durch ein Update auch zur Malware werden[40] oder Software eine Abhängigkeit schaffen, die die Eigenständigkeit von Unternehmen gefährden kann, wie es der Vorstandsvorsitzende der Volkswagen AG, Herbert Diess, in einem Interview mit der Zeitschrift Businessinsider vor kurzem ausgesprochen hat[41]. Diese Abhängigkeit ist nicht nur auf Unternehmen beschränkt, sondern greift auch in die Funktionsfähigkeit eines Staates massiv ein.

Verschärfend kommt bei IaaS, PaaS, SaaS und digitalen Serviceleistungen[42] hinzu, dass hier keine „Lager" angelegt werden oder binnen kurzer Zeit Substitute beigeschafft oder produziert bzw. programmiert werden können. Zusätzlich führt ein Ausfall der Internet-Infrastruktur, über den die genannten Dienste erbracht werden, zu einem Ausfall dieser Dienste. – vom Betreiber der notwendigen Internet-Infrastruktur (ISP) abgesehen, über den das Service dann werden soll.

Handelskonflikte wie derzeit zwischen den USA und China zeigen die entstandene Abhängigkeit in der „globalisierten" Cyber Supply Chain. Am Beispiel HUAWEI wird das in einem Artikel in der Wochenzeitung *Die Zeit* veranschaulicht. Unter dem Titel „*Angriff mit dem Skalpell*"[43] wird beschrieben, welche große Auswirkung die von der breiten Öffentlichkeit im wesentlichen unbemerkte Sanktionsmaßnahme der USA durch

---

40 Siehe https://www.heise.de/news/Von-Google-Play-entfernt-Beliebter-Barcode-Scanner-wurde-nach-Update-zu-Malware-5049530.html, 09.02.2021

41 Siehe https://www.businessinsider.de/wirtschaft/vw-chef-diess-in-sorge-um-souveraenitaet-des-gesamten-konzerns-wenn-wir-unabhaengig-bleiben-wollen-muessen-wir-software-im-auto-selbst-entwickeln-b/, 09.02.2021

42 Das betrifft auch die Echtzeit-Lizenzprüfung bei Start der Anwendung welche online erfolgt.

43 Siehe https://www.zeit.de/2020/23/huawei-usa-china-sanktionen-handelskonflikt-smartphones-halbleiter, 12.02.2021

stock.adobe.com

Exportbeschränkungen von Technologie nach China bedeutet, deren Konsequenzen auch unmittelbar in Europa beim geplanten Aufbau von 5G-Infrastruktur zu spüren sein werden. Denn Know-how der USA bei der Produktion von Halbleitern in 5 Nano-Meter-Technologie ist das Ziel der Beschränkung. Diese Technologie ist jedoch für chinesische Unternehmen essentiell, um bei der Produktion von Hardware-Komponenten für den 5G-Ausbau konkurrenzfähig zu bleiben. China verfügt derzeit, nach Informationen in selbigem Bericht, nur über die Fähigkeit zur Produktion von Halbleitern im 12 Nano-Meter-Bereich. Technologischer Rückstand in Kombination mit Konkurrenzkampf war immer schon ein Treiber für Spionage und ist es besonders im Ökosystem Cyber-Raum, wie durch in der Vergangenheit bekannt gewordene Cyber-Spionage-Angriffe auf US-Rüstungsprogramme belegt werden kann[44].

Auch das von den USA vor kurzem initiierte „Clean Network Programm“[45] sieht vor, dass nur sogenannte Clean Carrier, Clean Stores, Clean Apps, Clean Clouds, Clean Cables, Clean Paths verwendet werden dürfen, um Bedrohungen für Datenschutz, Sicherheit, Menschenrechte und Zusammenarbeit (im Sinne „westlicher“ Werte) von „bösartigen,

44 U.a. https://www.reuters.com/article/usa-fighter-hacking-idUSL2N0EV0T320130619, 12.02.2021

45 https://www.state.gov/the-clean-network/, 23.09.2020

autoritären“ Regimen zu begegnen. China hat daraufhin eine Gegeninitiative unter dem Namen „Global Data Security Initiative“[46] gestartet. Beiden Initiativen ist grundsätzlich eigen, dass jeweils nur Technologie aus der eigenen Einflusssphäre, USA oder China, verwendet werden darf. Eine Vermischung von Technologie schließt sich somit eigentlich aus und dies wird Europa beim geplanten Ausbau der 5G-Infrastruktur vor interessante Herausforderungen stellen. Auf der Ebene von Unternehmen oder Bürgern bedeuten dies, dass sich beispielsweise ein Huawei-Mobiltelefon zukünftig mit eigenem Betriebssystem auf Grund von US-Sanktionen möglicherweise nicht mit Services von US-Anbietern verbinden wird können. Diese Entwicklung hat auch Auswirkungen auf die eigenen Supply Chain, denn alle Partner entlang dieser Supply Chain werden sich für eine Seite entscheiden müssen. Das stellt mit Sicherheit eine große Herausforderung dar, da zur gegenwärtigen Infrastruktur oftmals parallel eine neue „reine“ aufgebaut und betrieben werden müsste. Aktuell geht man in den USA bereits so weit, dass Unternehmen (Anmerkung: egal wo auf der Welt diese beheimatet sind), welche Opfer einer Ransomware-Erpressung sind und dieser durch Bezahlung des Lösegelds an Cyber-Kriminelle nachgeben, möglicherweise als „Sanktionsbrecher“ sanktioniert werden. Das Verbot richtet sich nicht nur an das zahlende Opfer, sondern auch an zahlende Versicherungen. Hinzu kommen Finanzdienstleister, die solche Transaktionen ermöglichen und sonstige Dritte, die daran beteiligt sind oder dazu beitragen - etwa IT-Sicherheitsfirmen oder IT-Forensiker.[47] US-Unternehmen dürfen bekanntlich keine Geschäftsbeziehungen mit „Sanktionsbrechern“ haben oder eingehen, um nicht selbst sanktioniert zu werden.

Die schon derzeit bestehenden Abhängigkeiten österreichischer Digitalisierung bergen ein hohes Risiko mit einer nicht zu geringen Eintrittswahrscheinlichkeit für die Versorgungsresilienz Österreichs. Der hier zu Lande parallel laufende, stark ansteigende Trend zur Digitalisierung durch Outsourcing[48], Cloud Computing und Einbindung von Automatisierungstechnik in das Internet zum Zweck der Kostensenkung, beschleunigt durch die gegenwärtige COVID-19-Krise, konterkariert in Wahrheit nicht nur Cyber-Sicherheit sondern die gesamtstaatlich geforderte Versorgungsresilienz. Denn Versorgungsresilienz hat das Ziel, die permanente, vor allem autarke Versorgungssicherheit der österreichischen Bevölkerung durch strategische Bevorratung/Lagerhalterhaltung und nationale/regionale Produktion zu gewährleisten. Wenn aber Verwaltungs- und Produktionsprozesse zur Aufrechterhaltung eines funktionierenden Staatsganzen von einer gobalen Monokette unmittelbar abhängig sind, ist diese Versorgungsresilienz nur schwer zu erreichen.

---

46 https://www.insurancejournal.com/news/international/2020/09/10/581955.htm, 23.09.2020

47 Siehe https://www.heise.de/news/Ransomware-Wer-in-den-USA-Loesegeld-zahlt-koennte-selbst-im-Knast-landen-4918239.html, 12.11.2020

48 Siehe https://www.diepresse.com/5874273/krise-mit-happy-end, 01.10.2020

Um mit den Worten des australischen Chief of Home Affairs *Mike Pezzullo* zu schließen: „Cyber must be part of all-hazards national resilience“.[49]

Technologie-Souverenität mit Fokus auf “digitaler” Souverenität, mit welcher sich unter anderem auch der Rat für Forschungs- und Technologieentwicklung in Österreich (Austrian Council) befasst, wird auch im staatlichen Krisen- und Katastrophen-Management (SKKM) behandelt. Zu Beginn der COVID-19 Krise wurde in Österreich der Bedarf erkannt, den Versorgungsbereich über das Gesundheitswesen hinaus zu koordinieren. Diese Koordination erfolgt seitdem im SKKM-Koordinationsstab. Dieser Stab gab in weiterer Folge den Auftrag zur Etablierung einer Task Force Krisen-Bedarfsdeckung (TF KBD), an welcher auch das BVT (Fachbereiche Schutz kritischer Infrastrukturen und Cyber Sicherheit) teilnimmt und Expertise einfließen lässt. Ziel und Auftrag dieser TF KBD ist es, die gesamte Versorgungslage der Republik Österreich strategisch und operativ begleitend und koordinierend zu unterstützen. Im Rahmen dieser Task Force wurde gegen Ende des Berichtszeitraum dieses Berichts das *Arbeitspapier Grundlagen Versorgungsresilienz* publiziert, in dem die Aspekte des Cyber-Raums auf die Resilienz Österreichs thematisiert werden.

Die Operative NIS-Behörde im BVT

Das Ziel des seit Ende 2018 in Kraft getretenen Netz- und Informationssystem-sicherheitsgesetzes (NISG) ist es ein hohes Sicherheitsniveau von Netz- und Informationssystemen zu erreichen und sicherzustellen. In der Abteilung II/BVT/5 (Cybersicherheit) werden die Aufgaben der operativen NIS-Behörde wahrgenommen.

Mit dem NISG werden erstmalig in puncto Cyber-Sicherheit konkrete Vorgaben für die bzgl. Versorgungssicherheit wichtigen Unternehmen - **Betreiber wesentlicher Dienste (BwD)** und **Anbieter digitaler Dienste (AdD)** - sowie **Einrichtungen der öffentlichen Verwaltung** getroffen. Diese Adressaten des NISG sind verpflichtet, technische und organisatorische Sicherheitsvorkehrungen zu treffen und Sicherheitsvorfälle zu melden.

Weitere Adressaten des NISG sind unter anderem **Computernotfallteams**. Folgende drei Computernotfallteams wurden bereits seitens des Bundeskanzleramts (in Abstimmung mit dem BMI) identifiziert und festgestellt:

- Nationales Computernotfallteam: cert.at
- Computernotfallteam der Öffentlichen Verwaltung: GovCERT
- Computernotfallteam für den Sektor Energie: AEC (Austrian Energy CERT)

---

49 Siehe https://www.zdnet.com/article/cyber-must-be-part-of-all-hazards-national-resilience-home-affairs-chief/#ftag=RSSbaffb68, 19.10.2020

Computernotfallteams sind Ansprechpartner für IKT-Sicherheit auf nationaler Ebene. CERT.at vernetzt andere CERTS und „CSIRTs“ (Computer Security Incident Response Teams) von Unternehmen oder Institutionen. Es werden Warnungen, Tipps und Hilfestellungen zur Verfügung gestellt. Neben der Funktion als Informationsdrehscheibe liegt der Schwerpunkt eines CERT darin, erste Hilfe zu leisten und Notfallmaßnahmen bei Sicherheitsvorfällen einzuleiten.

Aufgaben des BMI (§ 5 NISG)

§ 5. (1) Dem Bundesminister für Inneres kommen folgende operative zentrale Aufgaben zu:

1. Betrieb einer **zentralen Anlaufstelle (SPOC)** …
2. organisatorische **Leitung** der Koordinierungsstrukturen **IKDOK und OpKoord**…
3. **Entgegennahme und Analyse von Meldungen** über Risiken, Vorfälle oder Sicherheitsvorfälle, **regelmäßige Erstellung eines diesbezüglichen Lagebildes** und **Weiterleitung der Meldungen sowie des Lagebildes** und **zusätzlicher relevanter Informationen** an inländische Behörden oder Stellen …
4. **Erstellung und Weitergabe** von zur Gewährleistung der Sicherheit von Netz- und Informationssystemen relevanten Informationen zur **Vorbeugung** von Sicherheitsvorfällen
5. **Überprüfung der Sicherheitsvorkehrungen** und die **Einhaltung der Meldepflichten**
6. **Feststellung und Überprüfung** der **qualifizierten Stellen**…
7. **Unterrichtung der Öffentlichkeit** über einzelne Sicherheitsvorfälle…
8. **Leitung und Koordination des Cyberkrisenmanagements** auf operativer Ebene…

BwD sind öffentliche oder private Einrichtungen aus den Bereichen Energie, Verkehr, Finanzmarktinfrastruktur, Bankwesen, Trinkwasserversorgung, Gesundheitswesen und digitale Infrastruktur. Das Bundeskanzleramt (BKA) ermittelt für jeden Sektor diese Betreiber wesentlicher Dienste basierend auf Schwellwerten, welche in der NIS-Verordnung (NISV) geregelt sind. Bis dato wurden rund **100 Unternehmen** als **BwD** ermittelt. Die ermittelten Unternehmen müssen mindestens alle drei Jahre nach Zustellung des Bescheids einen Nachweis über entsprechende Sicherheitsvorkehrungen für die eigenen Netz- und Informationssysteme der operativen NIS-Behörde im BMI erbringen. Solche Überprüfungen werden durch qualifizierte Stellen durchgeführt. Anforderungen an diese Unternehmen sind in der Qualifizierte Stellen Verordnung

(QuaSteV) des BMI geregelt. Darüber hinaus ist das BMI ermächtigt, die Einhaltung der Anforderungen im Rahmen einer Einschau in die NIS- bzw. IKT-Systeme der Adressaten des NISG zu überprüfen.

Zwei der im NISG definierten Sektoren haben 2020 **sektorspezifische Sicherheitsvorkehrungen (3SV)** eingebracht, welche im Rahmen von Feststellungsverfahren der operativen NIS-Behörde bearbeitet werden. Neben dem Kerninhalt der Sicherheitsmaßnamen/-vorkehrungen können Anwendungsbereiche sowie Spezifika des Sektors innerhalb eines solchen 3SV dargestellt werden. Hierzu zählen bspw. sektorspezifische Gefährdungen, die Risiko- und Business Impact Analyse beeinflussen, und Glossare, die die Begriffsbestimmungen der NIS-Rechtsnormen berücksichtigen.

Durch die laufende Identifizierung von BwD durch das BKA im Jahr 2020 ergaben sich diverse behördliche Aufgaben, welche durch die operative NIS-Behörde zu vollziehen waren. Die Überprüfung und Herstellung der gesicherten Kommunikationsfähigkeit mit den Kontaktstellen der Betreiber wesentlicher Dienste und qualifizierten Stellen wurde und wird mit oberster Priorität durchgeführt und behandelt.

Des Weiteren wurden 2019 und 2020 bereits etliche Feststellungsverfahren mit Unternehmen (Qualifizierte Stellen) bzgl. der Prüfung von Vorgaben zu Sicherheitsvorkehrungen/-maßnahmen bei BwD gem. NISG/QuaSteV geführt. Mit Ende 2020 sind rund **20 Unternehmen** als **qualifizierte Stellen** festgestellt.

Im Jahr 2020 wurden ebenfalls bereits organisatorische sowie technische Überprüfungsberichte von Sicherheitsvorkehrungen/-maßnahmen seitens einiger BwD bei der operative NIS Behörde eingebracht, welche formal sowie inhaltlich angenommen und analysiert werden konnten. Inhaltliche Stellungnahmen diesbezüglich wurden übermittelt, um die Sichtweise der operativen NIS-Behörde bzgl. der dargelegten Überprüfungsergebnisse darzulegen und zu kommunizieren.

stock.adobe.com

Bei **AdD** handelt es sich um Unternehmen, die einen Online-Marktplatz, eine Online-Suchmaschine oder einen „Cloud-Computing-Dienst“ anbieten. Von der Regelung für diese sind Kleinunternehmen, die weniger als 50 Mitarbeiterinnen und Mitarbeiter beschäftigen oder deren jährlicher Umsatz weniger als zehn Millionen Euro beträgt, ausgenommen. Im Unterschied zu den BwD entfällt bei den AdD eine gesonderte Ermittlung durch Bescheid.

Bei Auftreten eines Sicherheitsvorfalles trifft die Adressaten des NISG eine Meldepflicht. Die Unternehmen müssen unverzüglich Meldung an das nationale oder, falls vorhanden, an das sektorspezifische Computernotfallteam erstatten. Zusätzliche Details und Informationen zum Sicherheitsvorfall müssen nach den Erstmaßnahmen bzw. der Erstmeldung nachgereicht werden. Die beim Computernotfallteam einlangenden Pflichtmeldungen sind in weiterer Folge unverzüglich an die operative NIS-Behörde weiterzuleiten. Neben der Meldepflicht gibt es auch die Möglichkeit für Unternehmen und Bürgern freiwillige Meldungen abzusetzen. Diese werden, wenn nicht explizit seitens des Einmelders gewünscht, in aggregierter und anonymisierter Form an die operative NIS-Behörde durch die Computernotfallteams weitergeleitet. Im Jahr 2020 sind **36 NIS-Meldungen** (Pflichtmeldungen sowie freiwillige Meldungen) bei der operativen NIS-Behörde eingegangen. Weitere aggregierte anonymisierte freiwillige Meldungen wurden und werden im Rahmen der IKDOK/OpKoord-Lagebildsitzungen thematisiert und in den periodischen sowie anlassbezogen Lagenbildern verarbeitet.

Um Sicherheitsvorfällen entgegenzuwirken und auf diese reagieren zu können, ist eine enge Zusammenarbeit innerhalb des „IKDOK“ (Innerer Kreis der Operativen Koordinierung) sowie der „Opkoord“ (Operative Koordinierung) notwendig. Der IKDOK setzt sich aus Vertreterinnen und Vertretern des BMI, des BMLV, des BKA und des BMEIA zusammen. In der Opkoord kommen anlassbezogen der IKDOK, die Computernotfallteams sowie Vertreter von Unternehmen der kritischen Infrastruktur zusammen.

Sanktionen

Sollten die vom NISG betroffenen Unternehmen gegen die Meldepflicht, die Umsetzung von Sicherheitsvorkehrungen oder die Mitwirkungspflicht verstoßen, müssen sie mit verwaltungsstrafrechtlichen Sanktionen rechnen. Der Bundesminister für Inneres kann die Umsetzung von Sicherheitsvorkehrungen mittels Bescheid anordnen.

Die Verwaltungsstrafen bei derartigen Verstößen können bis zu 50.000 Euro, im Wiederholungsfall bis zu 100.000 Euro ausmachen. Zuständig für das Verwaltungsstrafverfahren ist die jeweilige Bezirksverwaltungsbehörde.

Laufende Arbeiten im Rahmen diverser NIS-Projekte im NIS-Umsetzungsprogramm des BMI sollen sicherstellen, dass das BMI sowohl als Behörde als auch als Adressat des Gesetzes den Anforderungen des NISG entspricht.

Neben laufenden interministeriellen sowie europäischen Arbeiten und Abstimmungen - u.a. im 2020 neu ins Leben gerufenen CyCLONe-Netzwerk operativer Behörden im Bereich Cybersicherheit der EU-Mitgliedsstaaten - wurde auch Ende 2020 eine detaillierte Sichtung und Stellungnahme zum Textvorschlag der europäischen Kommission zu NIS RL 2.0 vorgenommen, um die Auswirkungen auf die österreichische Cybersicherheitslandschaft (Wirtschaft, Staatliche Strukturen, Behörden etc.) zu analysieren und abzuschätzen

CyCLONe - Cyber Crises Liaison Organisation Network

Ziel des CyCLONe ist eine effiziente Vorgehensweise bei großflächigen Cybersicherheitsvorfällen und -krisen in der Europäischen Union. Daher soll CyCLONe vorrangig eine operative Verknüpfung zwischen politischer (Integrated Political Crisis Response (IPCR) – Krisenreaktionsmechanismus der EU) und technischer (CSIRTs-Netzwerk - Netzwerk der nationalen Computer Notfallteams auf EU-Ebene) Ebene ermöglichen und ebendiese verbessern. Dies soll durch die Etablierung eines Netzwerkes zur Kooperation zuständiger nationaler Behörden bei Cybervorfällen und –krise erreicht werden.

Aufgaben, welche im Rahmen des CyCLONe wahrgenommen werden müssen, sind unter anderem:

1. Erstellung von **Lagebildern** (regelmäßige Berichte zur Einschätzung der Situation auf EU-Ebene, Ad-hoc-Berichte bei großflächigen Cybersicherheitsvorfällen).
2. **Koordination** des **Krisenmanagements**
3. **Unterstützung** für **politische Entscheidungen** – auf nationaler wie europäischer Ebene
4. **Vorlagen** und **Tools** zur **Kommunikation** auf operativer sowie zu politischer und technischer Ebene werden bzw. sind teilweise bereits bereitgestellt.

Um die Resilienz Europas zu bewahren, sieht die Europäische Kommission (EK) die Notwendigkeit die NIS-Richtlinie zu überholen und legte am 15. Dezember 2020 im Rahmen eines größeren Cybersicherheitspakets einen **Vorschlag** für eine **NIS-RL 2.0** vor. Die NIS-RL 2.0 muss in einem größeren Kontext der Verbesserung der Widerstandsfähigkeit

und der Reaktionsfähigkeit bei Vorfällen im öffentlichen und privaten Bereich gesehen werden und ist ein Baustein in einem Gefüge (Cybersicherheitsstrategie, SKI etc.), das Europa für das digitale Zeitalter fit machen soll.

Unter anderem sind sowohl der Ausbau von Cyber-Fähigkeiten in der EU, eine erweiterte Kooperation auf EU-Ebene, eine deutliche Erweiterung des Adressatenkreises der NIS-Richtlinie sowie neue und erweiterte Vorgaben im Bereich des Cybersicherheitsrisikomangement im Textvorschlag vorgesehen.

2021 wird der Textvorschlag zu NIS-RL 2.0 auf europäischer Ebene gesichtet und verhandelt. Abzusehen ist jedoch, dass in Österreich Herausforderungen auf behördlicher Ebene zukünftig sowohl im Personal als auch im Sachressourcenbereich erheblich sein werden, um den Vorgaben der europäischen Regelwerke im Cyber-Bereich zu entsprechen.

3 General Situation Report

Islamist extremism and terrorism

As in previous years, Islamist extremism has continued to pose an increased threat to Austria in 2020. It was primarily Salafist and Jihadist actors, who have played a significant role in this context and who have had a major influence on developments in this field. The appeal exerted by extremist and terrorist ideology remains strong, which makes for continuous mobilisation and popularity. In addition, unresolved political conflicts in the Middle East and in North Africa also play a role in this context.

The greatest threat for Austria was not posed by actual groups, but by individuals who were rather loosely affiliated or by single perpetrators who only felt ideologically inspired. Local Islamist structures and networks belonging to the home-grown terrorist scene that mainly recruit from second or third generation immigrants or from converts to Islam have remained of particular relevance for the security situation. The level of threat reached its peak on 2 November 2020, when a 20-year-old Austrian-born perpetrator killed four people and injured several others in the course of a terrorist attack in downtown Vienna. The attacker had moved in circles of IS sympathisers and had formed part of the environment of Jihad travellers (Foreign Terrorist Fighters, FTF).

In the past years, the presence of such Jihad travellers willing to leave the country has had a major influence on the security situation in Austria and across Europe. Owing to their military training and combat experience as well as their assumed brutality, it may be expected that members of this group of people pose a highly elevated threat potential. Despite the fact that overall numbers are comparatively low, Islamist and especially Salafist and Jihadist ideologies continue to be attractive and therefore the religious and political narrative of a global caliphate is likely to persist.

Therefore, there is also a high risk of single perpetrators carrying out attacks based on Islamist motives in Austria. To make matters worse, the potential economic consequences of the long-lasting COVID-19 measures might have a disintegrating effect on individuals already living on the margins of society. In addition, measures taken by the security authorities were targeted at legalistic Islamist networks. Generally, such networks act in a non-violent way, however, in the long term, they may contribute to the polarisation of society and to further radicalisation. This has shown to be true in the course of ideological conflicts concerning identity, society and freedom of opinion, one example being the incident following the publication of a caricature of Mohammed by the magazine Charlie Hebdo in France..

Right-wing-extremism

The right-wing extremist scene in Austria is heterogeneous in structure. If you consider its ideology and external appearance, it becomes clear that it is not a uniform and closed entity.

Various groups of players who differ in numbers and ideological orientation emerge around anti-democratic, xenophobic, racist, Islamophobic, anti-Semitic and revisionist worldviews, while their ideological focusses may vary. Right-wing extremist protagonists, groups and coordinators of networks use different tactics and methods to reach their aims. Despite its otherwise heterogeneous structure, the Austrian scene mainly consists of male protagonists. Right-wing extremist violence has entailed a potential risk of disturbing public peace, order and security.

Ever since demonstrations against COVID-19 measures started in Austria, individual activists and groups from the right-wing extremist scene have tried to take advantage of these protests to instrumentalise them for their anti-democratic goals. The Corona crisis and the respective COVID-19 measures taken by the Austrian federal government turned out to be central issues within the Austrian right-wing extremist scene in 2020. Furthermore, enemy stereotypes such as foreigners and members of minorities, which have existed for quite some time, were maintained and reinforced. Moreover, it was found that conspiracy theories and fake news were spread and agitations and actions criticising the government were carried out. Since the beginning of the pandemic, individual actors and groups of the right-wing extremist scene have made a strong presence among opponents of COVID-19 measures, which has been considered problematic by the Austrian state protection authorities.

In 2020, the Austrian security authorities registered a total of 895 right-wing extremist, xenophobic, racist, Islamophobic, anti-Semitic and unspecific or other criminal acts, in the course of which relevant offences were reported to the authorities. One criminal act may comprise several offences, which are separately reported to the authorities. Compared to 2019 (954 offences), the number decreased by 6.2 %. Out of these, 622 criminal acts (69.5 %) were successfully investigated. In 2019, the rate of successfully solved cases amounted to 67.6 %. In connection to the criminal offences mentioned, 1,364 offences were reported in Austria in 2020, which is 18.7 % less than in 2019 (1,678 offences).

Finally, it is noted that the narratives of displacement, over-foreignisation and infiltration of one‘s own people, which have traditionally been characteristic of the right-wing extremist faction, have continued to be used as a strong motivator within the scene.

Moreover, in both the virtual and the real world of the right-wing extremist scene in Austria, the topics of anti-Islam, anti-multiculturalism as well as of asylum and refugees will further constitute a central focus of agitation and action.

Left-wing-extremism

The left-wing extremist scene in Austria comprises organisations with Marxist/Leninist and Trotskyite ideologies as well as autonomous anarchist groups. Both the autonomous anarchist groups and the Communist cadre organisations meet with little public response and only have few members. In 2020, the autonomous anarchist groups were the most active ones in the scene.

The internal differences, animosities and rifts among left-wing extremists, which separated the scene into individual factions acting autonomously, were overcome through cooperative platforms formed on certain occasions and for certain periods of time. In particular, anti-fascism and aspects of refugee, migration and asylum policy were subject areas with relevant mobilisation potential. Like in previous years, the protests were not only directed against radical and extremist groups, but also against political parties represented in parliament. In addition to these more traditional fields of action, new areas of agitation and action have at least gained temporary relevance in 2020: climate and environmental issues, the Black Lives Matter movement and the COVID-19 pandemic.

Left-wing extremist activists repeatedly appeared in 2020 at protests against German nationalist fraternities and against a group attributable to the New Right movement. Several events were accompanied by disruptive actions and blockade attempts, which in some cases resulted in violence.

However, it has to be noted that in 2020, the majority of anti-fascist demonstrations organised by groups and advocates of the left-wing extremist spectrum took place without causing any incidents relevant to the state police.

In 2020, a total of 167 criminal acts with proven or suspected left-wing extremist motivation were recorded (2019: 218 criminal acts); one criminal act may comprise several offences separately reported to the authorities. Out of these, 12 criminal acts (7.2 %) were successfully investigated. A total of 257 offences were reported to the authorities in connection with the above-mentioned criminal acts in 2020 (2019: 311 reports), 256 of which were offences defined in the Austrian Penal Code (StGB).

Intelligence services and counter intelligence

Intelligence services and other state and state-related actors engage in the exertion of influence and various forms of procurement in and against Austria. Attempts to exert influence cover all areas of politics, administration and society. The purpose is to create destabilisation, insecurity or polarisation in Austria, the European Union or other Western countries or to promote the interests of foreign countries in other ways.

The aim of information procurement for example is to obtain political and technological secrets or to operate against the diaspora of foreign states or members of the opposition residing in Austria. Diplomatic missions, associations, educational institutions and news agencies also partake in such intelligence-related activities.

Intelligence services are also involved in the procurement of sanctioned goods and foreign currency, as well as weapons, dual-use products, and proliferation-relevant materials. Iran left the nuclear agreement itself after the United States' withdrawal from the agreement and the targeted killing of several key figures and subsequently restarted enriching weapons-grade fissile material. The same applies to the Democratic People's Republic of Korea (DPRK), which already possessed nuclear weapons and – after a period of detente and rapprochement – has recently been advancing its missile programme again. Despite ongoing negotiations, these countries are under great pressure due to impending sanctions. It is therefore to be expected that clandestine procurement attempts by intelligence services will increase again.

Several intelligence services run departments specialised in cyber operations, both in their country of origin and in safe third countries. From there, they launch denial of service attacks such as the attack on the Austrian Federal Ministry for European and International Affairs (BMEIA) at the beginning of 2020, or they distribute ransomware in order to gain foreign currency. The latter was the case with the global attack using the malware WannaCry, which was presumably carried out by a state actor. Furthermore, operational teams located in Europe physically penetrate IT systems on site in order to gain access to classified information.

In addition, such attackers launch online disinformation campaigns, for example by spreading fake news via online platforms or social media.

Intelligence services are also involved in economic espionage. Moreover, there are legal forms of knowledge drain executed by state actors such as the recruitment of highly qualified scientists through scholarships or prizes or the purchase of Austrian key technology companies (aeronautical industry, automobile and conductor manufacturers) by foreign SOEs infiltrated by political cadres. On the one hand, this creates a loss of competitive advantage called forth by the outflow of expertise, and on the other hand, the loss of entrepreneurial control opens up another door for potential interference of foreign states.

Cyber security

The year 2020 was shaped in its entirety by the **impacts of the COVID-19 pandemic**, which also became evident in relation to cyber security in particular. The pandemic

led to a massive increase in targeted phishing and fraud attempts worldwide in which current topics and issues concerning COVID-19 were used as a decoy. Furthermore, an extremely large number of companies and organisations felt compelled to sacrifice the well-established perimeter security of their IT systems virtually overnight for the sake of widespread solutions for staff to work from home. This significantly increased the number of potential targets for cyber attacks and therefore led to a major rise in attacks and attack attempts.

Simultaneously, the number of cyber attacks carried out according to familiar patterns was consistently high or even increasing. This trend was witnessed especially in the context of threats posed by **ransomware and DDoS (Distributed Denial of Service)**. A comparatively new approach attackers follow in this context is to no longer exclusively carry out broad and random attacks, but rather to specifically target and attack potential victims according to, for example, their criticality (e.g. healthcare institutions in connection with COVID-19) or their financial capabilities. The related ransom demands vary accordingly and sometimes reach unprecedented amounts.

Another trend that will require increased attention in the future are cyber attacks that are not directly aimed at one potential victim, but that are rather directed against one of the **organisations upstream in the supply chain** as a first step. In this context, one incident especially worth mentioning was the attack against the company SolarWinds, whose software Orion is used by a large number of authorities and major enterprises around the world. Via the update function of the software provider SolarWinds, the infection of the company network spread to a great number of its customers, who subsequently suffered massive impairments. Maintaining cyber security in one's own supply chain will pose one of the greatest challenges of the future.

Following the **cyber attack on the Austrian Federal Ministry for European and International Affairs (BMEIA)** at the beginning of the year, the national cyber crisis management mechanisms were activated for the first time since the Austrian Law on Network and Information System Security (NISG) had entered into force. After successfully decrypting parts of the malware and recognising the dimensions of this incident, the appropriate crisis management mechanisms for incidents of such kind were initiated together with the Inner Circle of Operational Coordination Structure (IKDOK) and the Cyber Crisis Management Coordination Committee (CKM KA). Under the direction of the Cyber Security Centre, an operational task force consisting of representatives of the Federal Ministry of the Interior (BMI), the Federal Ministry of Defence (BMLV), the Federal Ministry for European and International Affairs (BMEIA) and the Federal Chancellery (BKA), including the Austrian Government Computer Emergency Response Team (GovCERT), was established. Owing to this swift and targeted approach, the attacker was disrupted effectively in his actions. This also allowed for the preparation and successful implementation of the structural clean-up of the system.

4 Abkürzungs-verzeichnis

ACI	Austrian Critical Infrastructure
AdD	Anbieter digitaler Dienste
AEC	Austrian Energy Cert
APT	Advanced Persistent Threats
AQ	Al-Qaida
AQAP	Al-Qaida auf der Arabischen Halbinsel
AQIM	Al-Qaida im Islamischen Maghreb
BKA	Bundeskanzleramt
BLM	Black Lives Matter
BMI	Bundesministerium für Inneres
BMEIA	Bundesministerium für europäische und internationale Angelegenheiten
BMLV	Bundesministerium für Landesverteidigung
BMSGPK	Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz
BNED	Bundesweites Netzwerk Extremismusprävention und Deradikalisierung
BVT	Bundesamt für Verfassungsschutz und Terrorismusbekämpfung
BwD	Betreiber wesentlicher Dienste
CERT	Computer Emergency Response Team
CKM	Cyber-Krisenmanagement
COVID-19	Coronavirus Disease 2019
CSIRT	Computer Security Incident Response Team
CyCLONe	Cyber Crises Liaison Organisation Network
DDoS	Distributed Denial of Service
DO5	Die Österreicher
EGVG	Einführungsgesetz zu den Verwaltungsverfahrensgesetzen
EK	Europäische Kommission
EU	Europäische Union
FPÖ	Freiheitliche Partei Österreichs
FTF	Foreign Terrorist Fighters
GIS	Gebühren Info Service GmbH
GovCERT	Government Computer Emergency Response Team
IaaS	Infrastructure as a Service
IBÖ	Identitäre Bewegung Österreich
IKDOK	Innerer Kreis der operativen Koordinierungsstrukturen
IT	Informationstechnologie
IoT	Internet-of-Things
IKT	Informations- und Kommunikationstechnologie
IS	Islamischer Staat
ISP	Internet Service Provider
LVT	Landesamt für Verfassungsschutz und Terrorismusbekämpfung
NIS	Netz- und Informationssystemsicherheit
NISG	Netz- und Informationssystemsicherheitsgesetz
NISV	NIS-Verordnung

OT	Operational Technology
Opkoord	Operative Koordinierung
ÖSCS	Österreichischen Strategie für Cyber-Sicherheit
ÖVP	Österreichische Volkspartei
PaaS	Platform as a Service
QuaSteV	Qualifizierte Stellen Verordnung
RTR	Rundfunk und Telekom Regulierungs-GmbH
SaaS	Software-as-a-Service
SKKM	Staatliches Krisen- und Katastrophen-Management
StGB	Strafgesetzbuch
TF KBD	Task Force Krisen-Bedarfsdeckung
TTP	Tactics, Techniques and Procedures
WaffG	Waffengesetz
WHO	Weltgesundheitsorganisation
3SV	Sektorspezifische Sicherheitsvorkehrungen