Bundesministerium
Inneres

Bundesamt für Verfassungsschutz
und Terrorismusbekämpfung

Verfassungsschutzbericht 2019

Verfassungsschutzbericht 2019

Wien 2020

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

Vorwort

Liebe Bürgerinnen und Bürger!

Bundesminister
Karl Nehammer, MSc
© BKA / Andy Wenzel

Die Bekämpfung von Terrorismus sowie die Verfolgung rechts- und linksextremistischer Straftaten gehören zu den Aufgaben des Staatsschutzes, aber auch der Bereich der Cyber-Sicherheit, der Schutz kritischer Infrastruktur oder die Spionageabwehr. Nicht vergessen darf man, dass Staatsschutzbehörden auch Sicherheitskonzepte zum Schutz verfassungsmäßiger Einrichtungen erstellen und Präventionsmaßnahmen gegen Radikalisierung formulieren.

Um der Fülle dieser Aufgaben gerecht zu werden, ist es notwendig, das Herangehen immer wieder zu hinterfragen und nach effektiveren Handhaben zu suchen. Deshalb befindet sich der Staatsschutz in Österreich, insbesondere das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung, derzeit in einem Reformprozess – sowohl die organisatorische Ausrichtung als auch die zeitgemäße Aufgabenstellung sollen verbessert werden. Im Klartext bedeutet das, dass eine moderne und effiziente Staatsschutzbehörde geschaffen werden soll, die kriminalpolizeiliche Ermittlungen leisten und nachrichtendienstliche Komponenten abdecken sowie das Vertrauen in der Bevölkerung und den Partnerorganisationen wieder festigen kann.

Zukünftig wird es für alle Mitarbeiterinnen und Mitarbeiter des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung einen verpflichtenden Grundausbildungslehrgang und nachfolgend eine differenzierte Spezialausbildung geben, mit Lernmethoden, die Präsenzschulungen, e-learning-Module und „training on the job“ umfassen. Darüber hinaus soll den Bediensteten eine vertiefende akademische Fachausbildung geboten werden – im Oktober 2021 wird der Fachhochschul-Lehrgang „Staatsschutz“ mit Abschluss „MSc“ starten. Damit soll die Aus- und Fortbildung für die Staatsschutz-Arbeit auf international vergleichbarem Niveau neugestaltet werden.

Ich möchte die bisher geleistete Arbeit der Staatsschutzbehörden keineswegs schmälern. Die Mitarbeiterinnen und Mitarbeiter sind wichtige und verlässliche Partner der Menschen in unserem Land und leisten hervorragende Arbeit. Gemeinsam mit der Polizei und den Sicherheitsbehörden sichern sie unseren Rechtsstaat und sind Garanten für Grund- und Freiheitsrechte in unserem Land.

Denn sicher ist eines: Unsere Demokratie steht derzeit Problemen gegenüber, die in der Gesellschaft diskutiert werden müssen. Das höchste Gut des Menschen, dessen Würde, muss besonders geachtet, das Leben des Einzelnen geschützt werden. Dafür stehen die Mitarbeiterinnen und Mitarbeiter des Staatsschutzes genauso wie alle anderen Polizistinnen und Polizisten in Österreich – ihnen allen gilt mein besonderer Dank für die professionelle Arbeit, die sie leisten.

Liebe Bürgerinnen und Bürger, der vorliegende Verfassungsschutzbericht gibt einen Einblick in die Aufgaben und in die Arbeit der österreichischen Staatsschutzbehörden und informiert über aktuelle und mögliche Entwicklungen in unserem Land, die den Staatsschutz betreffen.

Karl Nehammer
Bundesminister für Inneres

1 Leitbild des BVT

Demokratie ist verletzbar. Das BVT sorgt für ihren Schutz.

Schutz

der Bevölkerung

Sicherheit ist ein elementares Grundbedürfnis der Menschen. Als Teil des staatlichen Sicherheitssystems schützt das BVT die Menschen in Österreich vor weltanschaulich und politisch motivierter Kriminalität und den damit verbundenen Gefahren.

der verfassungsmäßigen Grundordnung

Eine demokratische Gesellschaft bedarf der verfassungsrechtlichen Fundierung und rechtsstaatlichen Absicherung ihrer Werte, Verfahren und Strukturen. Diese sind eine zentrale Voraussetzung für eine funktionierende Demokratie und besonders schützenswert.

der Institutionen und Einrichtungen des Staats- und Gemeinwesens

Eine offene Gesellschaft benötigt funktionierende, verlässliche und robuste Einrichtungen auf rechtsstaatlicher Basis. Sowohl staatliche wie auch gesellschaftliche Organisationen brauchen für den Erhalt ihrer Integrität ein sicheres Umfeld.

vor weltanschaulich und politisch motivierter Kriminalität

Die Bevölkerung, die verfassungsmäßige Grundordnung sowie die Institutionen und Einrichtungen des Staats- und Gemeinwesens können durch weltanschaulich und politisch motivierte Kriminalität unterminiert, verletzt oder gelähmt werden. Das BVT als Teil des staatlichen Sicherheitssystems versteht sich als die zentrale Organisation zum Schutz vor solchen Bedrohungen. Es sorgt dafür, dass das politische und gesellschaftliche Leben in Österreich in einem sicheren Umfeld stattfinden kann.

Schutz durch Wissen und Analyse

Durch kontinuierliche Beobachtung und fundierte Analyse des gefährdungsrelevanten Spektrums gewinnt das BVT präzises und umfassendes Wissen über die aktuelle Lage, Entwicklungen und zukünftige Szenarien. Als wichtiges Frühwarnsystem der Gesellschaft sammelt es gefährdungsrelevante Informationen

im In- und Ausland und untersucht und bewertet diese. Es erstellt auf ihrer Basis Gefährdungsanalysen, Lageeinschätzungen und entwickelt adäquate Handlungsstrategien.

durch Information und Beratung

Das BVT informiert im Rahmen seiner gesetzlichen Aufgaben die Regierung, VerantwortungsträgerInnen, betroffene Menschen und Einrichtungen über aktuelle und potentielle Gefährdungen und trägt zur Entwicklung und Realisierung von Strategien und Maßnahmen zur Gefahrenabwehr bei. Es kooperiert mit allen sicherheitsrelevanten AkteurInnen im In- und Ausland und ist ein kompetenter und verlässlicher Partner in Fragen der inneren Sicherheit.

durch Prävention und Intervention

Durch frühzeitige verhältnismäßige präventive Maßnahmen sowie rechtzeitige Intervention verhindert das BVT das Eskalieren von Bedrohungen. Dabei kommt der bewusstseinsbildenden und vertrauensaufbauenden Kommunikation mit allen Teilen der Bevölkerung eine wichtige Bedeutung zu. Je nach Gefährdungsstufe stehen dem BVT effektive und adäquate Interventionsformen zur Verfügung. Zur Prävention, Intervention und Abwehr von Gefahren nützt das BVT insbesondere das Instrumentarium des Sicherheitspolizeigesetzes und der Strafprozessordnung.

Haltungen

Überparteilichkeit und Objektivität

Das BVT agiert überparteilich und orientiert seine Arbeit am Schutz der verfassungsmäßigen Grundordnung. Seine Aufgaben erfüllt das BVT sachlich, unvoreingenommen und objektiv. Allen Strömungen jenseits des demokratischen Spektrums gilt die gleiche Wachsamkeit.

Angemessenheit und Konsequenz

Klarheit, Weitsicht und Angemessenheit in Bezug auf die Gefährdungslage sind Leitprinzipien der Arbeit des BVT. Kriteriengeleitete Bewertungssysteme ermöglichen eine transparente und nachvollziehbare Einstufung der Gefährdung. Sie bilden die Grundlage für die Gefahreneinschätzung, die Erstellung von Strategien und die Vornahme verhältnismäßiger Interventionen, die vom BVT rechtzeitig und konsequent umgesetzt werden.

Professionalität und Kompetenz

Höchstmögliche Professionalität, beste Ausbildung und Motivation der Mitarbeiterinnen und Mitarbeiter sind ein Garant für vernetztes Denken und effektives

Handeln im BVT. Eine stabile und zugleich flexible Organisationsstruktur ermöglicht, die als nötig erkannten Schritte und Maßnahmen rechtzeitig, konsequent und effizient umzusetzen.

Wertschätzung und Kommunikation

Zielgerichtetes und vertrauensvolles Miteinander erhöht die Effektivität und Qualität der Organisation und ermöglicht zugleich ein gutes Arbeitsklima. Sach- und Teamorientierung sind auf der Grundlage eines professionellen Zugangs und wertschätzenden Umgangs möglich. Im Wissen um den Faktor Mensch ist es wichtig, dass sich die Mitarbeitenden im BVT wohlfühlen und ihr Motivations- und Leistungspotenzial entfalten können.

Transparenz und Kontrolle

Transparenz und Nachvollziehbarkeit sind Grundvoraussetzungen für jede Form von Kontrolle. Ausgestattet mit hoheitlichen Kompetenzen ist dem BVT die Kontrolle der Rechtmäßigkeit seiner Handlungen und Maßnahmen als Ausdruck seiner rechtsstaatlichen und demokratiepolitischen Verantwortung besonders wichtig. Im Rahmen seiner gesetzlichen Informations- und Verschwiegenheitspflichten verfolgt das BVT die Haltung „So viel Offenheit wie möglich und so viel Geheimhaltung wie nötig“.

2 Allgemeines Lagebild

Phänomen Islamistischer Extremismus und Terrorismus

Lagebild

Auch für das Berichtsjahr 2019 stellte der islamistische Extremismus für Österreich, wie auch für andere europäische und außereuropäische Staaten eine anhaltende und erhöhte Bedrohung dar. Die Entwicklungen in diesem Bereich wurden dabei – wie bereits in den vergangenen Jahren – im Wesentlichen unverändert von salafistischen bzw. jihadistischen Akteuren geprägt, denn salafistisch-jihadistische Ideologien verfügen nach wie vor über ein relativ hohes Mobilisierungspotenzial. Politische Konflikte in der Islamischen Welt (insbesondere im Nahen/Mittleren Osten und Nordafrika) sowie die ideologische Aufladung und propagandistische Instrumentalisierung des Kampfes unterschiedlicher islamistischer Akteure gegen die Regime in einigen dieser Staaten (wie zum Beispiel gegen die Herrschaft al-Asads in Syrien) haben diesem Phänomen beziehungsweise den jihadistischen Gruppen/Netzwerken in den vergangenen Jahren einen in seinen Dimensionen, Dynamiken und Auswirkungen nie dagewesenen Mobilisierungsschub verliehen.

Die jihadistische Organisation „Islamischer Staat" (IS) hat durch eine Reihe von militärischen Operationen nicht nur eine relativ große Anzahl an Kämpfern, sondern auch wichtige Führungskader verloren. Nach dem Tod des IS-Anführers und selbsternannten „Kalifen" Abu Bakr al-Baghdadi im Zuge einer US-amerikanischen Militäroperation in Syrien Ende Oktober 2019 waren dessen potenziellen Implikationen für die terroristische Bedrohungslage in Europa Gegenstand sicherheitsbehördlicher Überlegungen.[1]

Nach ihrer territorialen Zerschlagung in Syrien und im Irak war zu beobachten, dass sich die IS-Organisation zunehmend dezentralisierte, um vermutlich weniger von einer zentralen, dominanten Führungsfigur abhängig zu sein und sich in ihren regionalen Ablegern (sog. wilāyāt, „Provinzen") neu konsolidieren zu können. Mit dem Verlust der Territorien erfolgte eine strategische Verschiebung von einer quasistaatlich bürokratisch strukturierten Organisation[2] zu einem nunmehr überwiegend im Verborgenen agierenden

---

1 Ende Oktober 2019 wurde der Tod al-Baghdadis über eine IS-Medienstelle offiziell bestätigt. Einige Tage nach der Mitteilung der Vereinigten Staaten war eine kurze Audio-Botschaft veröffentlicht worden, in der ein IS-Sprecher erklärte, dass das führende IS-Beratungsgremium sich nach der Bestätigung des Todes von al-Baghdadi versammelt und auf einen Nachfolger geeinigt habe. Begleitet wurde diese Verlautbarung von Aufrufen an Muslime weltweit die bay'a auf den neuen Anführer zu leisten, d.h. diesem Treue und Gefolgschaft zu schwören; abschließend wurden Drohungen gegen die USA ausgesprochen und die „Brüder" in den „Provinzen" aufgerufen, Rache zu nehmen.

2 Von dieser suggerierten „Staatlichkeit" ging einige Zeit – insbesondere während der Erfolgsphase des IS-„Kalifats" – eine gewisse, den Idealismus beflügelnde Strahlkraft aus, die für radikalisierte Islamisten eines von mehreren Motiven war, nach Syrien und den Irak auszureisen, um sich den Jihadisten dort anzuschließen.

Netzwerk in Syrien und im Irak. Daneben existieren global verbreitete regionale bzw. lokale IS-Zweigstellen (in den wilāyāt vom Maghreb über die Arabische Halbinsel und den Nord-Kaukasus bis nach Südostasien).

Im Vergleich zur anfänglich erfolgreichen Phase des IS im Zeitraum 2012 bis 2014, in welchem er große territoriale Zugewinne im Irak und in Syrien verbuchen konnte, ist in den letzten Jahren ein signifikanter sukzessiver Rückgang an IS-bezogener Propagandaaktivitäten, was die Produktion bzw. Anzahl der veröffentlichten Botschaften, Videos und Online-Magazine betrifft, zu konstatieren. Dennoch gilt es festzuhalten, dass islamistische Propaganda nach wie vor Verbreitung findet, und lokal wie international können sowohl Anhänger als auch neue Unterstützer mobilisiert bzw. rekrutiert werden. So startete der IS nach dem Fall des „Kalifats" eine Reihe von Propagandakampagnen, um die militärischen Rückschläge bzw. Niederlagen zumindest an der „medialen Front" zu kompensieren und zugleich den eigenen Anhängern und den Gegnern bzw. der übrigen Öffentlichkeit zu signalisieren, dass man als jihadistisches Netzwerk weiterhin weltweit aktiv und handlungsfähig ist.

Die ursprüngliche Avantgarde des globalen Jihads, das islamistische Terrornetzwerk al-Qaida (AQ), scheint bei der jüngeren Generation zwar weniger attraktiv und mit ihrer Propaganda (zumindest gegenwärtig) vom IS gewissermaßen in den Hintergrund gedrängt worden zu sein, jedoch zeichnet AQ sich durch eine organisatorisch-strukturelle Resilienz aus: Das Netzwerk verfügt ungebrochen weltweit über Anhänger beziehungsweise Unterstützer und lokal aktive Zweigstellen, die sich AQ und ihrer Ideologie verpflichtet fühlen.[3]

Die Motive, sich einer extremistischen Gruppe anzuschließen, sind sehr vielfältig. Unterschiedliche Faktoren beeinflussen den Einstieg in den religiösen Fanatismus und wirken bis hin zur extremistischen Gewalt: Lebens- bzw. Sinnkrisen, gefühlte oder tatsächliche Exklusions- und Diskriminierungserlebnisse, deviante Lebenswege oder offene salafistische Missionierung (wie in der Vergangenheit die „Lies!"-Kampagne). Die Typologie von Jihadisten ist dementsprechend heterogen, reicht von „gescheiterten Existenzen", die oftmals arbeitslos bzw. beruflich erfolglos waren, mitunter langjährige (klein)kriminelle „Karrieren" hinter sich haben und desillusioniert in radikal-islamische Kreise abgeglitten sind, bis hin zum religiösen oder politischen Fanatiker.

Bei der Auswahl der Anschlagsziele spielen strategische und praktische Überlegungen eine Rolle. Das potenzielle Zielspektrum islamistischer Terroristen reicht von Objekten

3 Wie z.B. al-Qaida auf der Arabischen Halbinsel (AQAP) und al-Qaida im Islamischen Maghreb (AQIM).

stock.adobe.com

der Kritischen Infrastruktur bis zu sogenannten „weichen Zielen“[4]. Insgesamt steht die symbolische Bedeutung von Anschlagszielen nicht mehr so sehr im Mittelpunkt terroristischer Überlegungen, weil auch mit wenig elaborierten Anschlägen an öffentlichen Plätzen bzw. gegen weiche Ziele entsprechende mediale Resonanz, potenziell große öffentliche Aufmerksamkeit sowie psychologische Auswirkungen in der Bevölkerung und – im Sinne der Terroristen – politische Reaktionen verbunden sind. Zudem zielen die Anschläge in der Regel darauf ab, größtmöglichen Personen- und Sachschaden zu verursachen. In einschlägigen Medien bzw. Foren wird dementsprechend immer wieder auch zu Anschlägen auf stark frequentierten Plätzen aufgerufen.

Der rückläufige Trend in Hinblick auf die Häufigkeit islamistischer Anschläge, der bereits 2018 zu erkennen war, setzte sich im vergangenen Jahr fort: Europaweit – auch in Österreich – ereignete sich 2019 kein größerer islamistisch motivierter Terroranschlag. Dennoch stellen jihadistisch inspirierte Anschlagsplanungen unverändert und in absehbarer Zeit 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 An-

4 Allgemein lassen sich „weiche Ziele“ (soft targets) als relativ leicht zugängliche Ziele mit relativ großen Sicherheitslücken – manchmal auch mit hohem symbolischen Stellenwert – und erhöhtem Personenaufkommen beschreiben (zum Beispiel logistische Knotenpunkte, staatliche Einrichtungen und entsprechende Gebäude, Sportveranstaltungen oder Einkaufszentren).

schläge fortsetzen könnte: Nicht mehr zeitintensive und strapaziöse Ausbildungen oder riskante Reisen zu Terrorcamps im Ausland sind für deren Planung und Umsetzung erforderlich, sondern ressourcenärmere Methoden werden verstärkt in die Überlegungen der Terroristen einbezogen.

Jihad-Reisende

Das Phänomen der sogenannten Jihad-Reisenden (Foreign Terrorist Fighters, FTF) und der aus Syrien und dem Irak zurückkehrenden Jihadisten („Rückkehrer") hat die Sicherheitslage in Österreich und insgesamt in Europa in den vergangenen Jahren stark geprägt. Nach der militärischen Niederlage des IS in Syrien und im Irak sind zwar in Anbetracht der großen Anzahl an Ausreisen in den Jahren davor weniger Jihadisten nach Österreich zurückgekehrt, als erwartet worden war; dennoch stellen diese Personen – durch militärische Ausbildung, gepaart mit Kampferfahrung (Umgang mit Sprengstoffen und Waffen) – ein schwer kalkulierbares Gefährdungspotenzial dar, weil sie empathielos gewalttätig agieren können (Herabsenken der Hemmschwelle) und mitunter Kontakte zu Mitgliedern anderer terroristischer Organisationen oder Zellen unterhalten. Diese Kontakthaltung kann sich aber auch auf ehemalige Kampfgefährten aus anderen Ländern beziehen und somit zu einer weiteren internationalen Vernetzung untereinander führen.

Angesichts der terroristischen Bedrohungslage nahm man in Österreich in den letzten Jahren entsprechende gesetzliche Novellierungen vor und reagierte mit einer umfangreichen Strategie zur Terrorismusbekämpfung:[5] Neben verstärkten repressiven Maßnahmen zur Gefahrenabwehr wird ein starker präventiver und kooperativer, gesamtgesellschaftlicher Ansatz verfolgt. Im Bereich Prävention wurde unter Federführung des BVT ein gesamtstaatlicher Rahmen geschaffen, um auf strategischer Ebene Initiativen und Maßnahmen gegen Extremismus und Terrorismus zu identifizieren.[6] So wurden, um die terroristische Gefährdung zu minimieren, einerseits im Verdacht stehende Personen von der Ausreise aus Österreich in Kriegsgebiete abgehalten und andererseits sämt-

---

5 Aufgrund der besonderen Gefahr für die Sicherheit Österreichs hatten sich das Innen-, Außen- und Justizministerium beim „Gipfel gegen Hass und Hetze" (Oktober 2014) auf ein Anti-Terror-Maßnahmenpaket geeinigt; dieses 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 Im Jahr 2017 wurde das „Bundesweite Netzwerk Extremismusprävention und Deradikalisierung" (BNED) vom BVT gegründet. Eine erste Maßnahme des BNED war die Erstellung einer österreichischen Strategie: Die „Österreichische Strategie Extremismusprävention und Deradikalisierung" bündelt Erfahrungswerte und Umgangspraxen verschiedenster Berufsgruppen, die mit dieser Thematik betraut sind. Im Zentrum stand hierbei wieder der gesamtgesellschaftliche Lösungsansatz.

liche rückkehrende Jihadisten von den Sicherheitsbehörden einvernommen und wegen des Verdachts der Unterstützung bzw. der Mitgliedschaft in einer terroristischen Vereinigung bei der Staatsanwaltschaft angezeigt. Die meisten Verurteilungen nach einem terroristischen Straftatbestand erfolgten hierzulande nach § 278b StGB (Terroristische Vereinigung), gefolgt von § 278d StGB (Terrorismusfinanzierung). Die Maßnahmen zeigten Wirkung: Nach dem „Höhepunkt" der jihadistischen Reisebewegungen 2014 ist bereits seit 2015 ein steter Rückgang an Ausreisen aus Österreich festzustellen und auch die Zahl der Rückkehrer ist in den vergangenen Jahren stark gesunken.

Zahlen zu Foreign Terrorist Fighters (FTF) aus Österreich:
Ende des Jahres 2019 waren dem Bundesamt für Verfassungsschutz und Terrorismusbekämpfung insgesamt 326 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 69 Personen in der Region ums Leben gekommen und 93 Personen wieder nach Österreich zurückgekehrt. Weitere 62 konnten an einer Ausreise gehindert werden und halten sich nach wie vor im Bundesgebiet auf. 102 Jihad-Reisende dürften sich noch im Kriegsgebiet befunden haben.

Inhaftierte terroristische Straftäter und Radikalisierung in Gefängnissen
Infolge der Intensivierung islamistischer Radikalisierung, der Rekrutierung für den sogenannten Jihad sowie des erhöhten Gefährdungspotenzials durch zurückgekehrte Jihadisten und deren Unterstützer waren über die letzten Jahre ebenso wie in Österreich auch in einigen anderen europäischen Staaten eine Reihe von Maßnahmen in der Terrorismusbekämpfung bzw. in der sicherheitsbehördlichen und justiziellen Verfolgung terroristischer Straftäter gesetzt worden.

Einhergehend mit dem behördlichen Verfolgungsdruck war in den betroffenen europäischen Ländern durchwegs eine steigende Anzahl an inhaftierten Terroristen und an radikalisierten Häftlingen zu verzeichnen. In den vergangenen Jahren waren insgesamt nur wenige frühere Inhaftierte aktiv und direkt an Planung und Ausführung beteiligt. Die meisten Gefängnisinsassen sind wegen Unterstützung terroristischer Gruppen beziehungsweise entsprechender Aktivitäten (Gutheißen von Straftaten, Propaganda etc.) verurteilt.

Insbesondere die hauptbetroffenen europäischen Länder sind neben einer steigenden Anzahl von inhaftierten Islamisten, die entweder rechtskräftig verurteilt wurden oder sich in Untersuchungshaft befinden, zudem mit möglichen Auswirkungen der Radikalisie-

rung konfrontiert. Diese Risiken betreffen die Phase während des Gefängnisaufenthalts wie auch die Zeit nach der Haftentlassung. Überdies werden in Haftanstalten oft neue Netzwerke gebildet, die auch nach der Entlassung relevant sind; d.h. die während der Haft geknüpften Kontakte bleiben darüber hinaus aufrecht.

Flüchtlings- und Gefangenenlager in Syrien

Internationale Beobachter und Nichtregierungsorganisationen berichten über humanitär prekäre Verhältnisse in den Flüchtlingslagern in Syrien und in den kurdischen Gefangenenlagern. Die Lager sind überfüllt, medizinische Betreuung, Nahrungsmittelversorgung und hygienische Verhältnisse gelten als desolat. Es ist zu befürchten, dass diese problematischen Verhältnisse eine neuerliche Radikalisierung sowie wachsende Unterstützung für islamistische Gruppen begünstigen bzw. befeuern könnten. Schlechte Behandlung von Gefangenen in den Lagern könnte AQ, IS oder anderen islamistischen Gruppen künftig als Motivation für neue Anschläge dienen. Auch weitere Rekrutierungsbemühungen würden unter solchen Bedingungen auf fruchtbaren Boden fallen. Dies betrifft nicht nur männliche Jihadisten, sondern auch Frauen, die mit Jihadisten liiert waren, und Kinder, die aus diesen Verbindungen stammen.

Frauen und Minderjährige aus dem ehemaligen IS-Gebiet (die meisten von ihnen stammen aus arabischen Ländern) gelten in vielen Fällen nach wie vor als islamistisch ideologisiert bzw. fortgesetzt radikalisiert. Zudem kann nicht ausgeschlossen werden, dass weitere derzeit inhaftierte Personen, die aus europäischen Staaten stammen oder von diesen nach Syrien und in den Irak gereist waren, aus syrischen, irakischen beziehungsweise kurdischen Gefängnissen fliehen. Aus den Gefängnissen geflohene Jihadisten könnten in den Untergrund abtauchen oder sich möglicherweise wieder islamistischen Milizen und Terrororganisationen anschließen. Diese Personen könnten auch versuchen, nach Europa zu reisen und in weiterer Folge terroristisch aktiv werden.

Islamistisch-extremistische Netzwerke auf dem Westbalkan

Als Reaktion auf die sogenannten Jihad-Reisen novellierten einige Staaten auf dem Westbalkan in den letzten Jahren ihre Gesetze im Bereich der Verfolgung terroristischer Straftaten bzw. zur Terrorismusbekämpfung und führten Operationen gegen islamistische Unterstützer- und Rekrutierungsnetzwerke durch. Trotzdem befindet sich nach wie vor eine relativ große Anzahl an islamistischen Extremisten, darunter auch „Jihad-Rückkehrer“, auf freiem Fuß – oft aus Mangel an stichhaltigen Beweisen. Diese Personen stellen ebenso ein Sicherheitsrisiko dar wie jene Islamisten, die derzeit inhaftiert sind; viele von ihnen werden in den kommenden Jahren entlassen, was Strafverfolgungs- und Justizbehörden vor zusätzliche Herausforderungen stellt. Nach der Haftverbüßung könnten ehemalige FTF ihre früheren jihadistischen Netzwerke reaktivieren oder neue Gruppen

bilden und hierdurch ihre Fähigkeiten zur Planung und Umsetzung terroristischer Anschläge steigern.

Hinzu kommen komplexe rechtliche, ethische und praktische Fragen der Rückführung oder Wiederaufnahme von Jihadisten aus den syrischen Lagern (ehemalige FTF in Flüchtlingscamps und in syrischen, irakischen bzw. kurdischen Gefängnissen). Im Zuge der erfolgten Rückführungen aus Lagern in Länder des Westbalkans wurden fast ausschließlich männliche Jihadisten verhaftet und unter Strafverfahren gestellt; Frauen und Minderjährige wurden in der Regel nicht angeklagt und zu ihren Familien/Angehörigen gebracht, Minderjährige sind bis zu einem gewissen Alter strafunmündig. In jenen Fällen, in denen keine Haft verhängt werden kann, sollen die Personen durch eigene Programme resozialisiert werden. Hierbei stellen sich praktische Herausforderungen in erster Linie im Bereich der verfügbaren Ressourcen für Resozialisierungs- bzw. Deradikalisierungsmaßnahmen, etwa von speziell ausgebildetem Personal; denn vor allem für die Betreuung von traumatisierten Minderjährigen bedarf es psychologisch und pädagogisch speziell geschultes Personals, um langfristigen Folgen vorzubeugen, die sich in Zukunft sicherheitsrelevant werden könnten.

Trends und Entwicklungen

Attraktivität und Anziehungskraft islamistischer Ideologien, insbesondere mit salafistisch-jihadistischer Prägung, werden auf nicht absehbare Zeit ungebrochen bleiben. Das religiös-politische Narrativ des „Kalifats“ wird auch nach der militärischen Niederlage der IS-Organisation bzw. der Zerschlagung ihrer quasi-staatlichen Strukturen in Syrien und im Irak fortbestehen. Die dahinterstehenden Ideologeme bleiben organisationsunabhängig bestehen und werden auf die Denk- und Handlungsweisen radikalisierter Islamisten weiterhin einen nicht unerheblichen Einfluss ausüben.

Lokale islamistische Gruppen und Netzwerke (in der sogenannten „Home-grown“-Szene), die sich vor allem aus jungen Muslimen der zweiten und dritten Einwanderergeneration sowie aus zum Islam konvertierten Personen zusammensetzen, werden in Österreich ebenso wie in anderen europäischen Ländern weiterbestehen; diese tragen dazu bei, dass diese Gesellschaften von islamistischer Radikalisierung betroffen sind.

Angesichts der in den vergangenen Jahren rasant angestiegenen Anzahl aufgrund terroristischer Straftaten zu Haftstrafen Verurteilter, stellen sich nachhaltige sicherheits- und – in weiterer Folge – sozialpolitische Herausforderungen in besonderem Maße in der Reintegration vieler Extremisten, wenn diese aus der Haft entlassen werden.

Soziale Medien und einschlägige Internet-Foren spielen, wie schon in vergangenen Verfassungsschutzberichten thematisiert, bei der Radikalisierung eine bedeutende Rolle, da in diesen Online-Netzwerken und -Foren spezielle islamistische beziehungsweise jiha-

distische Inhalte abgerufen werden können. Insbesondere sogenannte „Echo-Kammern“ (Informationsblasen) tragen zu einer weiteren ideologischen Manifestierung und sozialen Abschottung bei. Ein Bedrohungspotenzial geht in diesem Kontext hauptsächlich von radikalisierten Einzelaktivisten und potenziellen Nachahmungstätern aus, die durch die jihadistische Ideologie inspiriert und durch Aufrufe in sozialen Medien motiviert wurden. Zudem finden potenzielle Einzeltäter im Internet zahlreiche Anleitungen zur Herstellung von Sprengmitteln und verschiedenen Giften (z.B. Rizin).

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.

Linksextremismus

Lagebild

Der Phänomenbereich Linksextremismus umfasst in Österreich mehrere staatsschutzrelevante Strömungen. Beobachtungsgegenstand der österreichischen Staatsschutzbehörden sind linksextreme 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 marxistisch/leninistisch/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 2019 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 2019 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 auch im Jahr 2019 lediglich anlassbezogen und temporär in Form von Kooperationsplattformen überwunden. „Antifaschismus“ sowie Aspekte der Flüchtlings-, Migrations- und Asylpolitik waren erneut die Themenbereiche mit den größten Mobilisierungspotenzialen. Dabei wurden analog zu den Vorjahren nicht nur radikale und extremistische Gruppierungen zum Ziel von Protesten, sondern auch im Parlament vertretene Parteien.

stock.adobe.com

Traditionelle antifaschistische Mobilisierungs- und Aktionsanlässe – wie etwa der Wiener Akademikerball (WAB)[7] – wurden von Protestkundgebungen begleitet, an denen auch Gruppierungen und Exponenten der österreichischen linksextremen Szene teilgenommen haben. Im Gegensatz zu früheren Jahren verliefen die Kundgebungen gewaltfrei und ohne staatspolizeilich relevante Vorfälle.[8]

Linksextreme Aktivisten traten im Jahr 2019 wiederholt bei Protestaktionen gegen deutschnationale Burschenschaften und gegen eine der „Neuen Rechten" zuordenbaren Gruppierung in Erscheinung. Bei einigen Veranstaltungen kam es zu Stör- und Blockadeversuchen und in Einzelfällen auch zu Gewalttätigkeiten.

Festzuhalten ist aber, dass die Mehrzahl der im Jahr 2019 stattgefundenen Demonstrationen und Kundgebungen, die von Organisationen/Exponenten des linksextremen Spektrums organisiert wurden oder an denen Szenevertreter teilgenommen haben, ohne staatspolizeilich relevante Vorfälle abgelaufen ist.

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

- Konfrontative Gewalt: meist Gewalt im Zuge von Protestaktionen und Demonstrationen[9]
- Klandestine Gewalt: verborgen vorbereitete und durchgeführte Gewalttaten (oftmals gegen Sachen, Einrichtungen und Objekte)

Im Jahr 2019 wurden sowohl Fälle von konfrontativer als auch von klandestiner Gewaltausübung durch Exponenten des linksextremen Spektrums registriert.

Am 24. Jänner 2019 kam es in Wien im Zuge einer von rund 2.000 Personen – darunter ein rund 50 Personen umfassender „Schwarzer Block" – besuchten Demonstration zu Sachbeschädigungen an Gebäuden von drei Burschenschaften und an einer Polizeiinspektion.

---

7 Beim WAB handelt es sich um die Nachfolgeveranstaltung des letztmalig im Jahr 2012 abgehaltenen Balls des Wiener Korporations-Ringes (WKR-Ball).

8 So wurden etwa bei der Anti-WAB-Demonstration in Wien keine strafrechtsrelevanten Tatbestände registriert. In sicherheitsbehördlicher Hinsicht wurden lediglich einige Identitätsfeststellungen durchgeführt.

9 Es ist evident, dass gewaltbereite Linksextremisten ein Umfeld benötigen, das die Kontrollmöglichkeiten der Sicherheitskräfte erschwert und behindert. Dieses Umfeld bilden Kundgebungsteilnehmer aus den Reihen der Zivilgesellschaft. Sie stellen ein Vielfaches des Mobilisierungspotenzials der Autonomen und bilden jene anonyme Masse, die gewaltbereite Gruppen benötigen, um weitgehend unerkannt agieren zu können. Eine typische Taktik der gewaltbereiten Aktivisten ist das Auftreten in kleinen Bezugsgruppen, die aus der Masse heraustreten, Aktionen und Angriffe setzen und – von der Exekutive nur schwer identifizier- und verfolgbar – wieder in ihr untertauchen.

Durch pyrotechnische Gegenstände geriet eine an einem Burschenschafter-Haus befestigte Fahne in Brand, wodurch die Fassade beschädigt wurde. Weitere Beschädigungen bzw. Verschmutzungen erfolgten durch Beschmierungen und Eierwürfe.

Am 13./14. April 2019 wurde in Kirnberg/Niederösterreich das Soldatendenkmal samt Dollfuß-Gedenkstätte[10] beschädigt und beschmiert. Die mutmaßlichen Täter – ortsfremde Teilnehmer einer in der Region abgehaltenen Veranstaltung – konnten ausgeforscht werden.

Am 7. September 2019 veranstaltete die der „Neuen Rechten" zuordenbare „Identitäre Bewegung Österreich" (IBÖ) in Wien eine Kundgebung zum Thema „Schlacht am Kahlenberg 1683". Gegen diese Kundgebung bzw. gegen deren Veranstalter fand am 6. September 2019 eine als „Antifaschistische Vorabenddemonstration" bezeichnete Aktion von Exponenten des autonomen Szenespektrums statt. Im Zuge der von rund 50 Personen besuchten Demonstration wurde ein Haus, dessen Besitzer in linksextremen Kreisen als „Gönner" rechtsextremer Gruppen eingestuft wird, mit Eiern, Farbbeuteln und Pyrotechnik[11] beworfen. In der Nacht zum 7. September 2019 wurde das Objekt Ziel einer weiteren Aktion. Eine Gruppe von vermummten Personen randalierte vor dem Gebäude, warf Bierflaschen und andere Gegenstände. Zumindest eine Person trat mehrfach gegen die Eingangstür, wodurch diese beschädigt und eine im Hausinneren befindliche Person verletzt wurde. Von einschreitenden Polizeibeamten wurde eine vor dem Haus abgestellte Dose mit Brandbeschleuniger sichergestellt.

Am 7. September 2019 fanden mehrere Protest- und Störaktionen gegen die Kahlenberg-Gedenkkundgebung statt:

- Der linksextremen Szene zuordenbare Aktivisten versuchten mehrfach, die IBÖ-Veranstaltung zu stören. Eine rund 50-köpfige Gruppe, die zum überwiegenden Teil Holzstöcke und andere potenziell waffenfähige Gegenstände mit sich führte, wurde von Polizeikräften mehrmals abgedrängt, sodass es zu keinem direkten Aufeinandertreffen mit den Teilnehmern der Kahlenberg-Gedenkkundgebung gekommen ist. Im Zuge des Einsatzes wurden Polizeikräfte wiederholt mit Knallkörpern und pyrotechnischen Gegenständen beworfen.

---

10 Dr. Engelbert Dollfuß (1892 – 1934) amtierte ab 1932 als Bundeskanzler, schaltete im März 1933 das Parlament aus, verbot 1933 die NSDAP und die Kommunistische Partei, 1934 nach den Februarkämpfen auch die Sozialdemokratische Arbeiterpartei und ließ als einzigen politischen Willensträger die Vaterländische Front zu. Dollfuß wurde bei einem nationalsozialistischen Putschversuch am 25. Juli 1934 im Bundeskanzleramt ermordet.

11 Durch einen pyrotechnischen Gegenstand wurden die Eingangstür und ein Teil der Hausfassade durch Hitzeeinwirkung beschädigt.

- Ein Reisebus, mit dem Teilnehmer der Kundgebung transportiert wurden, wurde durch drei vermummte Personen attackiert und beschädigt. Es ist mit hoher Wahrscheinlichkeit davon auszugehen, dass es sich bei den Tätern um Exponenten der linksextremen Szene gehandelt hat.

Im Jahr 2019 wurden zwei Brandanschläge auf Objekte der Freiheitlichen Partei Österreichs (FPÖ) verübt, die aufgrund der Zielauswahl und der Modi Operandi mit hoher Wahrscheinlichkeit von Exponenten der linksextremen Szene bzw. von Tätern mit linksextremen Tatmotiven begangen worden sein dürften:

- In der Nacht zum 12. August 2019 verübten vier vermummte Personen einen Brandanschlag auf die FPÖ-Zentrale in St. Pölten/Niederösterreich. Mit Steinen wurden Fenster eingeschlagen und in weiterer Folge wurden Molotow-Cocktails gegen das Gebäude geworfen. Der Brandanschlag wurde von Passanten wahrgenommen, die Feuer konnten umgehend gelöscht werden bzw. erloschen von alleine.
- Am 7. September 2019 wurde ein Brandsatz gegen die FPÖ-Bezirkszentrale in Feldbach/Steiermark geworfen, der an der Fassade abprallte und – ohne Schaden anzurichten – am Boden abbrannte.

Internationale Verbindungen

Die österreichische linksextreme Szene verfügt über diverse Auslandskontakte. 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 und die organisatorischen Schwächen der österreichischen Szene zurückzuführen ist.

Kommunikation und Medien

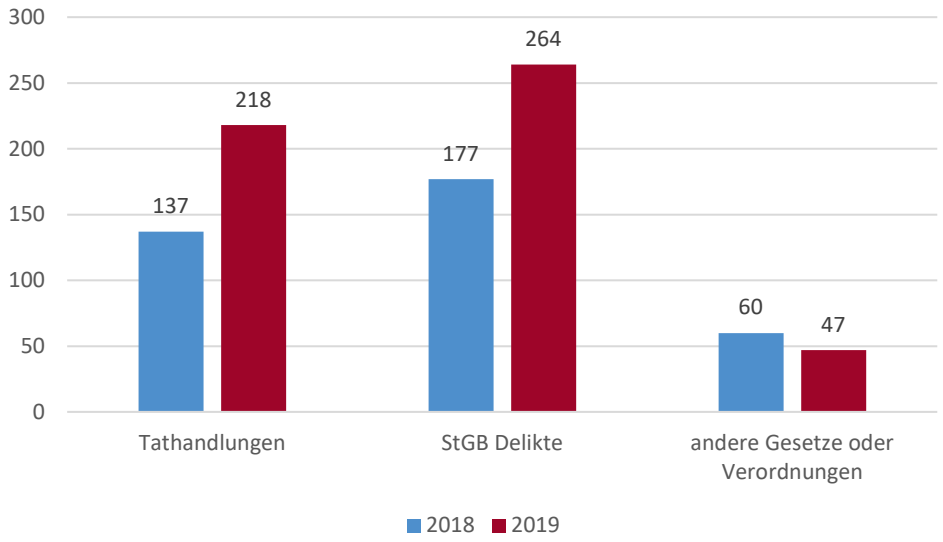
Um ihre Botschaften zu verbreiten, ihre Anliegen zu propagieren und ihre Ziele zu erreichen, nutzen die Exponenten und Gruppierungen der österreichischen linksextremen Szene ein breites Spektrum – von Aufklebern/Flugblättern/Druckwerken über Diskussionsveranstaltungen, Demonstrationen und aktionistischen 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, Blogs und Foren – z.B. WhatsApp und Telegram – 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, eine steigende Tendenz.

2019 sind in Österreich insgesamt 218 Tathandlungen mit erwiesenen oder vermuteten linksextremen Tatmotiven bekannt geworden (2018: 137 Tathandlungen), wobei eine Tathandlung mehrere Delikte mit gesonderten Anzeigen beinhalten kann. 25 Tathandlungen, das sind 11,5 Prozent, konnten aufgeklärt werden (Aufklärungsquote 2018: 18,2 Prozent). Im Zusammenhang mit den angeführten Tathandlungen wurden bundesweit 311 Anzeigen (2018: 237 Anzeigen), davon 264 nach dem Strafgesetzbuch (StGB)[12], erstattet. Im Zuge der Bekämpfung linksextremer Aktivitäten wurden im Berichtsjahr insgesamt 72 Personen angezeigt (2018: 63), davon 29 Frauen (2018: 22) und 3 Jugendliche (2018: 1).



Tathandlungen/Anzeigen – Vergleich 2018/2019

12 Von den 264 Anzeigen nach dem Strafgesetzbuch entfiel die überwiegende Mehrheit auf Sachbeschädigungen (213 Anzeigen nach den §§ 125 und 126 StGB).

Ein Vergleich der Jahre 2018 und 2019 zeigt einen Anstieg sowohl der einschlägigen Tathandlungen (+ 59,1 Prozent) als auch der im Zusammenhang mit diesen Tathandlungen erstatteten Anzeigen (+ 49,1 Prozent). Eine Besonderheit des Jahres 2019 stellten die insbesondere im Zuge des EU- und des Nationalratswahlkampfes gehäuft auftretenden Tathandlungen gegen im Parlament vertretene politische Parteien dar. In Summe wurden im Zusammenhang mit der EU- und der Nationalratswahl österreichweit 113 Tathandlungen[13] mit erwiesenen oder vermuteten linksextremen Tatmotiven bekannt, das sind 51,8 Prozent aller im Jahr 2019 registrierten einschlägigen Tathandlungen .[14]

Der im Jahr 2018 evidente Hotspot-Charakter der Bundesländer Salzburg, Steiermark, Wien und Tirol hat sich im Jahr 2019 fortgesetzt. Darüber hinaus war im Jahr 2019 in Niederösterreich eine merkbare Zunahme sowohl von Tathandlungen als auch von angezeigten Delikten zu verzeichnen:

- Salzburg: 41 Tathandlungen (18,8 Prozent aller linksextrem motivierten Tathandlungen) und 91 Anzeigen (29,2 Prozent aller Anzeigen).
- Steiermark: 47 Tathandlungen (21,5 Prozent) und 50 Anzeigen (16,1 Prozent).
- Wien: 32 Tathandlungen (14,7 Prozent) und 62 Anzeigen (19,9 Prozent).
- Niederösterreich: 32 Tathandlungen (14,7 Prozent) und 38 Anzeigen (12,2 Prozent).
- Tirol: 30 Tathandlungen (13,7 Prozent) und 33 Anzeigen (10,6 Prozent).

13 In 94 Fällen handelte es sich um Sachbeschädigungen – primär in Form von Spray- oder Schmieraktionen gegen Werbe- und Wahlplakate oder von Beschädigungen an Plakatständern.

14 84 Taten richteten sich gegen die Freiheitliche Partei Österreichs (FPÖ), 29 gegen die Österreichische Volkspartei (ÖVP).

Anzeigen	2018	2019
Anzeigen nach dem StGB		
Körperverletzung (§ 83 StGB)	1	2
Schwere Körperverletzung (§ 84 StGB)	4	5
Gefährdung der körperlichen Sicherheit (§ 89 StGB)	0	1
Gefährliche Drohung (§ 107 StGB)	4	4
Üble Nachrede (§ 111 StGB)	1	2
Beleidigung (§ 115 StGB)	0	1
Sachbeschädigung (§ 125 StGB)	110	194
Schwere Sachbeschädigung (§ 126 StGB)	15	19
Diebstahl (§ 127 StGB)	2	12
Diebstahl durch Einbruch oder mit Waffen (§ 129 StGB)	0	1
Brandstiftung (§ 169 StGB)	2	3
Störung der Totenruhe (§ 190 StGB)	0	2
Urkundenunterdrückung (§ 229 StGB)	0	1
Herabwürdigung des Staates und seiner Symbole (§ 248 StGB)	1	1
Widerstand gegen die Staatsgewalt (§ 269 StGB)	5	5
Tätlicher Angriff auf einen Beamten (§ 270 StGB)	1	2
Kriminelle Vereinigung (§ 278 StGB)	0	6
Aufforderung zu mit Strafe bedrohten Handlungen und Gutheißung mit Strafe bedrohter Handlungen (§ 282 StGB)	4	3
Sonstige StGB Delikte	27	0
Anzeigen nach anderen Gesetzen/Verordnungen		
Versammlungsgesetz (VersG)	3	38[15]
Sicherheitspolizeigesetz (SPG)	36	4
Salzburger Landessicherheitsgesetz (S-LSG)	1	5
Sonstige Gesetze/Verordnungen (z.B. Pyrotechnikgesetz, Waffengesetz, Anti-Gesichtsverhüllungsgesetz)	20	0
Summe	237	311

15 Im Zuge eines einzigen Vorfalles – der Versuch der Blockierung einer Demonstration durch Exponenten der autonom-anarchistischen Szene – wurden 35 Anzeigen erstattet.

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.

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).[16]

Der Linksextremismus stellt gegenwärtig keine ernsthafte Gefahr für die Funktions- und Handlungsfähigkeit des Staates bzw. der Verfassung dar. Für die öffentliche Ruhe, Ordnung und Sicherheit sind Teilbereiche des linksextremen Spektrums jedoch – temporär und anlassbezogen – als Risiko zu bewerten.

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

Rechtsextremismus

Lagebild

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. Diese Heterogenität bzw. die Auffassungsunterschiede in Bezug auf die ideologische Ausrichtung verdeutlichen sich innerhalb der Szene oftmals sehr offenkundig. 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.

Gemein sind ihnen das in der gegenwärtigen rechtsextremistischen Szene dominierende Narrative der „Verdrängung", „Überfremdung" und „Unterwanderung des eigenen Volkes" durch von ihnen als fremd wahrgenommene Personen. Verantwortlich, aus Sicht der Rechtsextremisten, an dieser Behauptung sind die „herrschenden Eliten". Parallelen zum dominierenden Agitationsschwerpunkt des „Großen Austausches", wie ihn die Vertreter der Neuen Rechten propagieren, sind deutlich zu erkennen. Kombiniert mit einem Narrativ der „Verdrängung der autochthonen Bevölkerung" wird in der rechtsextremistischen Szene ein Endzeitszenario geschaffen, auf welches es sich vorzubereiten gilt (z.B. durch Kampfsporttrainings).

Rechtsextremistische Gewalt, Aggression und Agitation wird als ein potenzielles Risiko für die Störung der öffentlichen Ruhe, Ordnung und Sicherheit in Österreich bewertet.

Zu den primären Feindbildern rechtsextremistischer Kreise zählen u.a.:

- 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, 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.

Auf internationaler Ebene stellen einschlägige Veranstaltungen, bei denen Musik, Kampfsport und eine rechtsextremistische Ideologie kombiniert werden, eine Möglichkeit zur Vereinigung einer ansonsten heterogenen Szene dar. Diese „Erlebniswelt Rechtsextremismus“ bietet nicht nur eine Treff- und Vernetzungsmöglichkeit einschlägiger Personenkreise, sondern birgt auch die Gefahr eines zusätzlichen Rekrutierungs- und Mobilisierungspotenzials unbekannter Größe.

In Österreich finden solch groß angelegte einschlägige Konzertveranstaltungen wie im Ausland aktuell nicht statt. Da im Bundesgebiet rechtsextremistische Veranstaltungen jeglicher Art in der Öffentlichkeit durch die Sicherheitsbehörden konsequent untersagt

werden, können diese nur konspirativ organisiert und im kleinen, klandestinen Rahmen abgehalten werden. So fand in jüngerer Vergangenheit im Bundesgebiet ein klandestin organisiertes Konzert statt, an dem Personen aus dem In- und Ausland teilnahmen. Im Zusammenhang mit dieser Veranstaltung erfolgten im Berichtsjahr 2019 gerichtlich angeordnete Maßnahmen (unter anderem Hausdurchsuchungen) gegen mehrere Personen. Bei den Hausdurchsuchungen konnte einschlägiges Material sowie Waffen sichergestellt werden.

Die Funktion rechtsextremistischer Musik kann als vielschichtig beschrieben werden. So fördert sie unter anderem das Zusammengehörigkeitsgefühl (netzwerk- und szenebildend) und bietet außerdem die Möglichkeit, sich zum eigenen rechtsextremistischen Gedankengut zu bekennen (identitätsstiftend). Des Weiteren besteht aufgrund der leichten Zugänglichkeit dieser Art von Musik (z. B. über das Internet) ein erhöhtes Potenzial für interessierte Personen, sich rechtsextremistischer Ideologiefragmente anzunehmen und sich zu radikalisieren. Einschlägige Musik kann in diesem Zusammenhang oftmals auch als Einstieg in das Milieu dienen. Darüber hinaus sind Konzertveranstaltungen geeignet, zur Finanzierung der Szene erheblich beizutragen.

Das Internet und im Speziellen die Sozialen Medien spielen bei rechtsextremistischen Gruppierungen und Netzwerken in Österreich eine tragende Rolle. Ihre Funktion ist vielfältig und wird als Kommunikations-, Vernetzungs- und Mobilisierungsinstrument eingesetzt.

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.

Rechtsextremistische Personenkreise, Szenen und Bewegungen in Österreich zielen mit der Schaffung von Feindbildern und einer einhergehenden verhetzenden Rhetorik darauf ab, eine Polarisierung der Gesellschaft herbeizuführen. Dabei werden insbesondere bei komplexen gesellschafts- und sicherheitspolitischen Themen Graubereiche bewusst ausgespart, was zu Schuldzuschreibungen und Generalisierungen führt. Darüber hinaus kann ein dadurch geschaffenes antidemokratisches, anti-pluralistisches sowie nationalistisches Meinungsklima mit dem spaltenden Narrativ - „Wir“ gegen „die Anderen“ – den Nährboden für gefährliche Angriffe auf verfassungsmäßige Einrichtungen und die

stock.adobe.com

Grund- und Freiheitsrechte der Bürger schaffen. [Siehe Fachbeitrag „Rechtsterroristische Anschläge: Ein neuer Tätertyp“]

Des Weiteren zeigte sich im Berichtsjahr 2019, dass die Brisanz des Spannungsfeldes Rechts-/Linksextremismus besondere Sicherheitsrelevanz birgt und im Rahmen der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit eine herausfordernde Aufgabe für die österreichischen Sicherheitsbehörden darstellt. Ein generell nur schwer kontrollierbares Eskalationspotenzial tragen spontane Protestkundgebungen in sich. 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 sind.

Statistik

Das Phänomen Rechtsextremismus zeigte sich den österreichischen Sicherheitsbehörden 2019 in Form von Straftaten sowie als politisch-ideologisch motivierte Aggression und Propagandaaktionismus rechtsextremistischer Gruppierungen und Einzelpersonen.

2019 sind den Sicherheitsbehörden in Österreich insgesamt 954 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 2018 (1.075 Tathandlungen) bedeutet dies einen zahlenmäßigen Rückgang um 11,3 Prozent. 645 Tathandlungen, das sind 67,6 Prozent, konnten aufgeklärt werden. 2018 lag die Aufklärungsquote bei 63 Prozent.

Im Zusammenhang mit den angeführten Tathandlungen wurden 2019 bundesweit 1.678 Delikte zur Anzeige gebracht, das sind um 3,5 Prozent mehr als im Jahr 2018 (1.622 Delikte).

Anzeigen	**2018**	**2019**
Anzeigen nach dem StGB		
Körperverletzung (§ 83 StGB)	18	14
Schwere Körperverletzung (§ 84 StGB)	2	6
Absichtliche schwere Körperverletzung (§ 87 StGB)	0	1
Gefährdung der körperlichen Sicherheit (§ 89 StGB)	0	1
Nötigung (§ 105 StGB)	8	4
Gefährliche Drohung (§ 107 StGB)	29	34
Beharrliche Verfolgung (§ 107a StGB)	1	2
Hausfriedensbruch (§ 109 StGB)	0	1
Beleidigung (§ 115 StGB)	6	4
Berechtigung zur Anklage (§ 115 i.V.m 117 StGB)	9	2
Sachbeschädigung (§ 125 StGB)	229	219
Schwere Sachbeschädigung (§ 126 StGB)	23	19
Diebstahl (§ 127 StGB)	1	8
Diebstahl durch Einbruch oder mit Waffen (§ 129 StGB)	5	8
Raub (§ 142 StGB)	0	1
Betrug (§ 146 StGB)	2	2
Brandstiftung (§ 169 StGB)	3	1
Fahrlässige Herbeiführung einer Feuersbrunst (§ 170 StGB)	0	3
Herabwürdigung religiöser Lehren (§ 188 StGB)	6	1
Pornographische Darstellungen Minderjähriger (§ 207a StGB)	2	50[17]

17 Im Rahmen einer rechtsextremistischen Serientathandlung wurden insgesamt 48 Jugendliche angezeigt, welche in „Whatsapp-Gruppen“ Bilder mit nationalsozialistischen Inhalten sowie pornographische Darstellungen Minderjähriger versandten. Bei zwei weiteren Vorfällen (unabhängig der zuvor genannten Tathandlung) wurden durch zwei unbekannte Täter ebenso Bilder mit NS-Inhalten sowie pornographische Darstellungen Minderjähriger via „Whatsapp-Gruppen“ versandt.

Anzeigen	2018	2019
Sexuelle Belästigung und öffentliche geschlechtliche Handlungen (§ 218 StGB)	1	1
Urkundenunterdrückung (§ 229 StGB)	7	1
Widerstand gegen die Staatsgewalt (§ 269 StGB)	4	4
Verbrecherisches Komplott (§ 277 StGB)	0	3
Aufforderung zu mit Strafe bedrohten Handlungen und Gutheißung mit Strafe bedrohter Handlungen (§ 282 StGB)	25	8
Aufforderung zu terroristischen Straftaten und Gutheißung terroristischer Straftaten (§ 282a StGB)	0	4
Verhetzung (§ 283 StGB)	280	169
Falsche Beweisaussage (§ 288 StGB)	1	1
Verleumdung (§ 297 StGB)	3	2
Andere StGB Delikte	27	0
Anzeigen nach dem Verbotsgesetz	877	1037
Anzeigen nach anderen Gesetzen oder Verordnungen		
Abzeichengesetz 1960 (AbzG)	10	2
EGVG Art III Abs. 1 Z 3 u. 4	5	14
Waffengesetz (§ 50 WaffG)	15	19
Suchtmittelgesetz (SMG)	14	18
Sicherheitspolizeigesetz (SPG)	7	7
Tiroler Landespolizeigesetz (TLPolG)	0	3
Salzburger Landessicherheitsgesetz (S-LSG)	0	2
Notzeichengesetz	0	1
Mediengesetz	0	1
Andere Gesetze	2	0
Summe	**1622**	**1678**

Erläuterungen zur Statistik

In folgenden Deliktskategorien wurde ein Anstieg registriert:

- Anzeigen nach dem Verbotsgesetz: 1.037 Anzeigen (2018: 877)
- EGVG Art III Abs. 1 Z. 3 u. 4: 14 Anzeigen (2018: 5)
- Gefährliche Drohung nach § 107 StGB: 34 Anzeigen (2018: 29)
- § 50 Waffengesetz: 19 Anzeigen (2018: 15)

Zu einem Rückgang kam es in folgenden Deliktskategorien:

- Anzeigen nach dem Abzeichengesetz: 2 Anzeigen (2018: 10)
- Sachbeschädigungsdelikte nach den §§ 125 oder 126 StGB: 238 Anzeigen (2018: 252)
- Verhetzung nach § 283 StGB: 169 Anzeigen (2018: 280)
- Aufforderung zu mit Strafe bedrohten Handlungen und Gutheißung mit Strafe bedrohter Handlungen nach § 282 StGB: 8 Anzeigen (2018: 25)

Österreichweit wurden bei der Bekämpfung rechtsextremistischer Aktivitäten im Jahr 2019 im Rahmen der aufgeklärten Tathandlungen insgesamt 893 Personen durch die Sicherheitsbehörden angezeigt. 65 davon waren Frauen (7,3 Prozent). 2018 wurden 797 Personen (11,7 Prozent davon weiblich) angezeigt. Im Berichtsjahr wurden insgesamt 269 Jugendliche (30,1 Prozent) zur Anzeige gebracht (2018: 104).

Wegen Körperverletzungsdelikten wurden 2019 im Zusammenhang mit 21 einschlägigen Tathandlungen 18 Personen (fünf davon wegen schwerer Körperverletzung, eine wegen absichtlich schwerer Körperverletzung) angezeigt. 2018 waren es im Rahmen von 20 Tathandlungen 16 Personen.

Durch fremdenfeindlich/rassistisch motivierte Tathandlungen wurden im Jahr 2019 sechs (2018: 3), durch islamfeindlich motivierte Tathandlungen keine Person (2018: 1) verletzt. Durch antisemitisch motivierte Tathandlungen kamen im Jahr 2019 keine Personen zu körperlichen Schäden (2018: 4).

Von den insgesamt 954 bekannt gewordenen Tathandlungen waren

- 797 (83,6 %) rechtsextremistisch,
- 89 (9,3 %) fremdenfeindlich/rassistisch,
- 30 (3,1 %) antisemitisch und
- 6 (0,6 %) islamfeindlich

motiviert. Bei 32 Tathandlungen (3,4 Prozent) war eine unspezifische oder sonstige Motivlage hinsichtlich der Tatausführung vorhanden (u.a. Provokationen, Anbieten von NS-Devotionalien auf Flohmärkten ohne Wiederbetätigungsabsicht).

Von den 34 angezeigten Delikten nach § 107 StGB (Gefährliche Drohung) waren 25 rechtsextremistisch, vier fremdenfeindlich/rassistisch und eine antisemitisch motiviert. Bei drei Delikten lag den Tathandlungen eine sonstige oder unspezifische Motivlage zugrunde.

Im Jahr 2019 konnten 18 (2018: 86) fremdenfeindliche/rassistische oder rechtsextremistische Tathandlungen der Asyl- bzw. Flüchtlingsthematik zugeordnet werden. Dies bedeutet einen Rückgang um 79,1 Prozent gegenüber dem Vorjahr. Davon konnten 14 Tathandlungen, das sind 77,8 Prozent, aufgeklärt werden.

Von den 954 Tathandlungen fanden 326 (34,2 Prozent) im Internet statt. 2018 lag der Anteil der Internetdelikte bei 36,4 Prozent (391 Tathandlungen).

Bei der Internet-Meldestelle „NS-Wiederbetätigung“ sind im Jahr 2019 insgesamt 3.081 Hinweise davon 964 relevante[18] Sachverhalte eingegangen (2018: 3.176 Eingänge – 1.440 relevant).

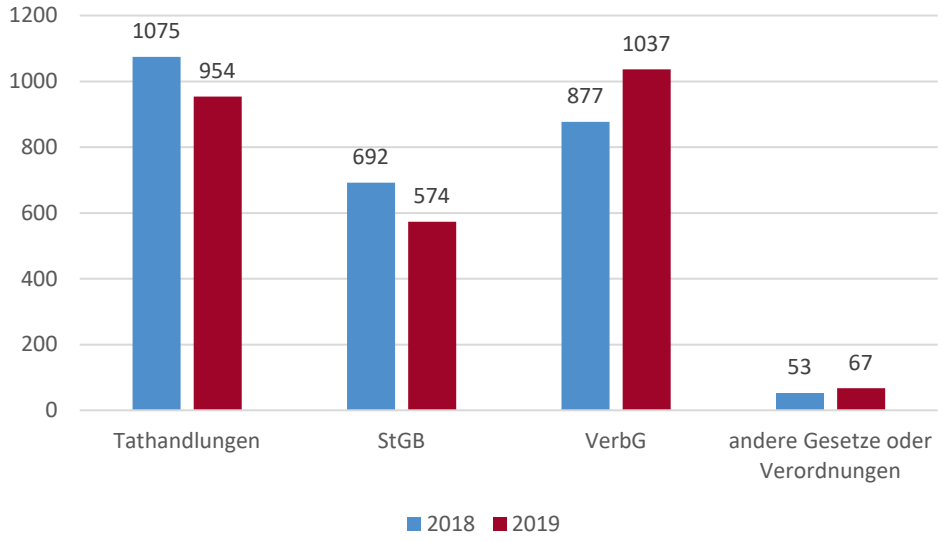


Abbildung: Tathandlungen/ Anzeigen – Vergleich 2018/2019

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

Trends und Entwicklungen

Im Phänomenbereich Rechtsextremismus zeigen die jüngsten Entwicklungen, dass eine Modernisierung, Professionalisierung und Internationalisierung der rechtsextremistischen Szene stattgefunden hat. Einschlägige Veranstaltungen mit Festivalcharakter, grenzüberschreitende Veranstaltungsbesuche rechtsextremistischer Akteure oder der internationale Austausch neurechter Bewegungen veranschaulichen dies deutlich.

Groß angelegte und professionell ausgetragene Veranstaltungen im Ausland bieten gerade durch die Kombination von Musik, Kampfsport und Politik die Möglichkeit, dass sich rechtsextremistische Szeneangehörige aus verschiedenen Ländern treffen, vernetzen und das Gemeinschaftsgefühl unter ideologisch Gleichgesinnten öffentlich ausleben können. Durch diese „Erlebniswelt Rechtsextremismus", in der die Ideologie vorerst oft nur eine zweitrangige Rolle spielt, besteht auch die Möglichkeit zur Rekrutierung und Mobilisierung von Sympathisanten. Rechtsextremistische Großveranstaltungen finden in Österreich aktuell nicht statt. Die Beteiligung von österreichischen Szeneproponenten an einschlägigen Veranstaltungen im Ausland ist jedoch feststellbar.

Darüber hinaus zeichnen sich innerhalb der rechtsextremistischen Szene in Österreich Veränderungen auf personeller, als auch auf organisatorischer Ebene ab. War es unter anderem durch das Ableben von Führungspersönlichkeiten des rechtsextremistischen Milieus sowie justizieller Maßnahmen zu einem Vakuum gekommen, organisierten sich im Berichtjahr 2019 alte Strukturen und Netzwerke rund um langjährige Führungskader des „klassischen" Neonazismus in Österreich neu. In der jüngeren Vergangenheit wurden unter anderem Szeneveranstaltungen im Ausland von Akteuren des heimischen neonazistischen Spektrums besucht.

Im Gegensatz dazu befinden sich neurechte Bewegungen in Österreich aktuell am Scheideweg. In den letzten Jahren war es ihnen möglich, das zuvor angeführte Vakuum teilweise für ihre Zwecke öffentlichkeitswirksam zu nutzen. So sorgten sie vor allem mit ihren medial inszenierten Kampagnentätigen und deren Darstellung auf sämtlichen zur Verfügung stehenden sozialen Netzwerken für eine erhöhte Aufmerksamkeit und Polarisierung im öffentlichen Raum. Aktuell ist jedoch festzustellen, dass es zu einer Verlagerung der strategischen und operativen Ausrichtung neurechter Bewegungen im Bundesgebiet gekommen ist. Mehrere Faktoren dürften diese Entwicklung bedingt haben. So zeigte sich einerseits, dass aufgrund internationaler Ereignisse, welche auf die Leitkampagne „Der große Austausch" der Neuen Rechten Bezug nahmen, ein Wandel der öffentlichen Wahrnehmung dieser Gruppierungen stattgefunden hat. Andererseits dürften die Ermittlungen und Maßnahmen der österreichischen Behörden in den letzten Jahren zu Veränderungen in ihren grundlegenden Strukturen geführt haben.

Als ein einigendes Element in der rechtsextremistischen Szene können Aktionen und Agitationen gegen die „Verdrängung der autochthonen Bevölkerung" bewertet werden.

Abschließend wird festgehalten, dass die Themen „Anti-Islam“, „Anti-Multikulturalismus“ sowie die Asyl- und Flüchtlingsthematik weiterhin dazu geeignet sind, einen zentralen Agitations- und Aktionsschwerpunkt der heimischen rechtsextremistischen Szene in der virtuellen wie auch in der realen Welt darzustellen.

Nachrichtendienste und Spionageabwehr

Lagebild

Österreich ist nach wie vor eines der zentralen Zielgebiete für ausländische Nachrichtendienste und fungiert zugleich als internationale nachrichtendienstliche Drehscheibe. Als eine der führenden Industrienationen und Standort zahlreicher Unternehmen der Spitzentechnologie ist Österreich ein bevorzugtes Operationsgebiet für entsprechende nachrichtendienstliche Aktivitäten ausländischer Staaten. Neben seiner Mitgliedschaft in der Europäischen Union und dem Sitz einer Reihe internationaler Organisationen sind Österreichs wissenschaftliche und wirtschaftliche Stärke bestimmende Faktoren. Des Weiteren spielen Österreichs zentrale geographische Lage und die ausgezeichnete Infrastruktur für Handel und Transport eine besondere Rolle für Anbahnungsgeschäfte jeglicher Beschaffungsvorgänge.

Österreich ist aber auch selbst ein Ziel nachrichtendienstlicher Beeinflussung und Ausspähung. Als größte Bedrohung im Rahmen nachrichtendienstlicher Aktivitäten im Land, stellen sich für Österreich neben diversen Anwerbungsversuchen, Bestrebungen der Einflussnahme zur Manipulation der westlichen Gesellschaft sowie der Schwächung und Destabilisierung der politischen Situation des Ziellandes durch ausländische Nachrichtendienste dar. 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.

Im Jahre 2019 konnten vom BVT in den verschiedensten gesellschaftlichen Bereichen Anwerbungsversuche durch ausländische Nachrichtendienste festgestellt werden. Neben dem Versuch, mit Hilfe von menschlichen Quellen an vertrauliche bzw. geheime Informationen zu gelangen („klassische“ Spionage), haben nachrichtendienstliche Aktivitäten zum Zwecke der Einflussnahme auf staatliche Entscheidungs- und Machtstrukturen an Relevanz gewonnen. Ebenso wird bei der Informationsbeschaffung durch ausländische Nachrichtendienste vermehrt auf die Diaspora in Österreich bzw. deren hier etablierte Organisationen zurückgegriffen. Im internationalen Vergleich ist in Österreich für Spionageaktivitäten jedoch ein relativ geringes Strafmaß zu erwarten. Wer „zum Nach-

teil der Republik Österreich einen geheimen Nachrichtendienst einrichtet oder betreibt oder einen solchen Nachrichtendienst wie immer unterstützt", ist laut Strafgesetzbuch mit einer Freiheitsstrafe bis zu drei Jahren zu bestrafen.

Die politischen Zielsetzungen der jeweiligen ausländischen Regierungen legen die Kernpunkte der Aufklärungsaktivitäten ihrer Nachrichtendienste fest. Je nach den politischen Vorgaben können die nachrichtendienstlichen Aktivitäten politischen, wirtschaftlichen, (technisch-)wissenschaftlichen oder militärischen Interessen dienen. 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 in anderen Staaten zu beauftragen. Für eine politische Aufklärung von Interesse sind z.B. die österreichische Haltung zu Fragen der Außen-, Sicherheits-, Finanz- und Energiepolitik sowie auch die Rolle Österreichs in internationalen Organisationen. Ansatzpunkte für derartige Aufklärungsmaßnahmen sind vor allem politische Entscheidungsträger, Denkfabriken, Nichtregierungsorganisationen sowie Diasporavereine.

Auch Österreichs Landesverteidigung ist Ziel ausländischer Spionage. Das zeigte beispielsweise der Ende 2018 bekannt gewordene Fall jenes ehemaligen Bundesheeroffiziers, der von einem militärischen Auslandsnachrichtendienst angeworben worden war und mit diesem etwa 25 Jahre lang kooperierte. Durch seine Position hatte der Soldat Zugang zu militärischen Geheimnissen des österreichischen Bundesheeres sowie relevante Informationen über Partnerstaaten bzw. -organisationen. Diese Informationsbeschaffung wurde dem ehemaligen Oberst von seinem ausländischen Auftraggeber finanziell abgegolten. Der durch diese Spionage entstandene Schaden lässt sich wirtschaftlich nicht

stock.adobe.com

bemessen, jedoch hätten die erlangten Informationen im Falle eines militärischen Konflikts der Landesverteidigung Österreichs mit hoher Wahrscheinlichkeit zum Nachteil gereicht.

Zu einem begehrten Ausspähungsziel ausländischer Nachrichtendienste in Österreich gehören auch systemoppositionelle Gruppierungen. Entsprechende nachrichtendienstliche Aktionen ausländischer Dienste in Österreich sollen nachhaltig zur Kontrolle konfessioneller und nationaler Minderheiten beitragen. Die Beobachtung und Kontrolle von regimekritischen Oppositionsbewegungen in Österreich stellen somit einen wichtigen Schwerpunkt fremder Dienste dar.

Die Zahl diplomatischer Vertretungen und hier stationierter Nachrichtendienstoffiziere hat sich in den letzten Jahren kaum verändert und bleibt unvermindert hoch. Auf diese Weise werden zum einen gute bilaterale Beziehungen gefördert und zum anderen auch Aufklärung unter Zuhilfenahme bewährter Spionagemethoden für andere Staaten betrieben.

Eine große Anzahl von ausländischen Nachrichtendienstoffizieren ist in Österreich nach wie vor unter der Tarnung von sogenannten Legalresidenturen wie Botschaften, Konsulaten und internationalen Organisationen tätig. Hinzu kommt eine ebenfalls konstant bleibende Zahl halboffizieller Einrichtungen – darunter sind unter anderem Vertretungen von Fluggesellschaften, Presseagenturen, Vereinen, Kulturzentren, aber auch Firmenniederlassungen zu verstehen –, 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 im Ausland ermöglichen. Durch die zunehmende Digitalisierung hat zugleich auch die technische Informationsbeschaffung konstant an Bedeutung gewonnen. Rapide Entwicklungen der Informations- und Kommunikationstechnologie sowie eine intensive Tarnung erschweren die Verfolgung von Cyberangriffen und machen staatliche Spionageaktivitäten im Internet zu einem herkömmlichen Instrumentarium vieler Nachrichtendienste. Auch in Österreich konnten derartige, zum Teil gezielt gegen öffentliche Institutionen gerichtete Angriffe festgestellt werden.

Die Verhinderung und Aufklärung illegaler nachrichtendienstlicher Aktivitäten in Österreich gehört zu den Kernaufgaben des BVT. Aus diesem Grund wurden im Jahre 2019 eine Reihe von Sensibilisierungsmaßnahmen durchgeführt und eine Vielzahl an Präventionsveranstaltungen abgehalten. Bei Behörden und sonstigen staatlichen Einrichtungen sowie Wirtschaftstreibenden und universitären Institutionen soll so erhöhtes Bewusstsein geschaffen werden, um Anwerbungsversuchen präventiv entgegenzuwirken. Ebenso stellt die Aufklärung über Spionagebedrohungen auch auf internationaler Ebene eine essentielle Aufgabe zur Früherkennung illegaler nachrichtendienstlicher Tätigkeiten dar.

Trends und Entwicklungen

Forschungseinrichtungen, Hochschulen, „Hidden Champions“[19] und innovative mittelständische Unternehmen tragen wesentlich zur heimischen Wirtschaft und zu den Rahmenbedingungen des Wirtchaftsstandortes Österreich bei. Konkurrenzfähige österreichische Unternehmen werden Ziele von Wirtschaftsspionage. Ein gemeinsames Vorgehen von BVT und Wirtschaft, Wirtschaftsverbänden und universitären Einrichtungen, ist für die erfolgreiche Bekämpfung von Wirtschafts- und Industriespionage somit unerlässlich.

Einen wirksamen Schutz und zugleich auch das größte Risiko für ein Unternehmen stellt der Faktor „Mensch“ dar. So können Geschäfts- und Betriebsgeheimnisse (sogenannte Wirtschaftsgeheimnisse) ausnahmslos in Synergie mit Mitarbeitern und Technik gewahrt werden.

Der Fokus der Vortragstätigkeiten des BVT lag auf einzelnen heimischen Unternehmen sowie auf Branchenveranstaltungen. Dadurch konnte auf spezielle Spionagemethoden eingegangen sowie geeignete Schutzmaßnahmen gegen ungewollten Informationsabfluss aufgezeigt und Diskussionen mit Veranstaltungsteilnehmern geführt werden.

Der Wirtschaftsstandort Österreich steht für Produkte hoher Qualität sowie für neuartige Lösungen.

Auf divergierende Faktoren wie Standort, Branche, Warensortiment oder Internationalisierungsgrad ist bei der Formulierung von geeigneten Schutzmaßnahmen Bedacht zu nehmen. Deshalb müssen für jedes Unternehmen entsprechende Sicherheitskonzepte auch individuell erarbeitet werden.

Durch langjährige Kooperationen von BVT und den für Wirtschaftsschutz zuständigen Behörden anderer europäischer Staaten, wird eine Analyse aktueller Vorgehensweisen von Akteuren der Wirtschafts- und Industriespionage ermöglicht. Die daraus gewonnenen Erkenntnisse werden infolge vom BVT in persönlichen Gesprächen sowie im Rahmen von Vorträgen an Bedarfsträger vermittelt. Dabei nehmen „Best-Practice“-Beispiele österreichischer sowie internationaler Unternehmen einen hohen Stellenwert ein.

Der Schutz von Geschäftsgeheimnissen wurde auf europäischer Ebene im Rahmen einer Richtlinie[20] sichergestellt. Diese verfolgt das Ziel, Unternehmen europaweit ein

---

19 Unter dem Begriff „Hidden Champions“ (heimliche Gewinner) werden in Nischen-Marktsegmenten zu Europa- oder Weltmarktführern etablierte, mittelständische Unternehmen subsumiert.

20 Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäfts-

möglichst einheitliches Schutzniveau vor Geheimnisverrat und Wirtschaftsspionage zu gewährleisten. Mit der EU-Richtlinie soll eine effektivere Abschreckung gegen und die Bekämpfung von Industriespionage und Geheimnisverrat erreicht werden. Der effektive Schutz von Geschäftsgeheimnissen liegt jedoch nicht nur im Interesse der Unternehmen, sondern auch im Interesse des Wirtschaftsstandortes Österreich. Somit liegt der Verabschiedung der Richtlinie auch ein wirtschaftspolitischer Gedanke zu Grunde, nämlich Europa und schlussendlich auch Österreich als Wirtschaftsstandort zu stärken. Unternehmen sollten Anreize bekommen, grenzüberschreitend zu kooperieren, was letztlich zu einer Ankurbelung der Innovationskraft europäischer Unternehmen führen sollte.

Desinformationskampagnen, insbesondere die Verbreitung von Fake News durch fremde Nachrichtendienste zur Einflussnahme auf andere Länder, gewinnen international zusehends an Bedeutung. Ziele solcher Unternehmungen können dabei eine gesellschaftliche Polarisierung und Spaltung, negative Beeinflussung demokratischer Strukturen und Prozesse oder das Schüren von Unsicherheiten und Misstrauen in der Bevölkerung, darstellen. Insbesondere im Zusammenhang mit anstehenden Wahlen oder Referenden können sich solche Versuche der Einflussnahme intensivieren.

Cyber-Sicherheit

Lagebild

In gesamteuropäischer Perspektive haben Cyber-Angriffe 2019 zugenommen. Auch die österreichische Kriminalstatistik sieht bei Cybercrime-Delikten eine Verdoppelung der Anzeigen im Vergleich zum Vorjahr. Die Zunahme von Cyber-Angriffen betrifft auch Betreiber kritischer Infrastrukturen und verfassungsmäßiger Einrichtungen. Insbesondere ist dabei von einer hohen Dunkelziffer von unerkannten oder nicht gemeldeten Vorfällen auszugehen.

Im Jahresverlauf 2019 kam es insbesondere zu Erpressungsversuchen mittels Verschlüsselungs-Software (Ransomware). Hier werden Zielsysteme mittels Datenverschlüsselung blockiert und für eine neuerliche Freischaltung das Opfer zur Zahlung einer Lösegeldsumme (in Kryptowährungen wie z.B Bitcoin) aufgefordert. Angriffe erfolgten meist in Form von präparierten Word- und PDF-Dokumenten in den Anhängen von E-Mails, die als Zustellbenachrichtigung oder Rechnung getarnt waren. Sie zielten vorrangig auf Betreiber kleiner und mittlerer Unternehmen der kritischen Infrastruktur und auf verfassungsmäßige Einrichtungen (Behörden) ab und verursachten teilweise erheblichen

geheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung (Text von Bedeutung für den EWR).

Schaden. Dabei lässt sich ein Trend weg von einfacheren Zielen, wie etwa privaten Internetnutzern, hin zu zahlungskräftigeren Firmen und Organisationen ausmachen. Die Angriffe zeigen eine zunehmende technische Präzision, Täter nehmen neuerdings vermehrt einzelne, besonders finanzstarke Ziele ins Visier. Einem internationalen Trend folgend, und vielleicht durch eine spezifische Verwundbarkeit (Auslastung, veraltete Systeme) bedingt, nehmen insbesondere Angriffe auf Institutionen des Gesundheitswesens (Spitäler) zu.

Erpressungen mittels spezieller Schadsoftware (Ransomware) werden vor allem über Phishing-Mails eingeleitet: Diese enthalten Links, die User auf falsche Internetseiten führen und dort die Infiltration mit der Schadsoftware auslösen können. In anderen Fällen enthalten Phishing-Mails selber die mit der Schadsoftware infizierten E-Mail-Anhänge. Es sind aber auch Ransomware-Angriffe ohne vorheriges Phishing vorgekommen, wie man am Beispiel von WannaCry im Mai 2017 sehen konnte: Damals hatte eine im Betriebssystem Windows vorhandene Schwachstelle (Exploit) mit dem Namen EternalBlue ausgereicht, dass sich der Wurm verbreitete. Ebenfalls im Berichtsjahr 2019 stieg die Zahl solcher Fälle, in denen sensible Zugangsdaten, wie Benutzernamen und Kennwörter durch Phishing speziell im Mobilfunkbereich (Smartphones) widerrechtlich entwendet wurden. Während herkömmliche E-Mail-Infrastrukturen eingehende Phishing-Mails leichter erkennen und damit ein Eindringen von Angreifern in Zielnetzwerke erschwert wird, bieten E-Mail-Dienste auf Smartphones einen geringeren Schutz und die zusätzlich auf dem System installierten sozialen Netzwerke, Messenger-Apps und SMS/MMS bilden weitere Einfallstore.

Es kam zu Fällen, in denen ein Ransomware-Angriff mit einer sorgfältigen Auswahl des Opfers vorbereitet worden war und wo die Einschleusung von Schadcode in Zielsysteme mittels „maßgeschneidertem“ Spear-Phishing versucht wurde. Die Höhe der anschließenden Geldforderung richtete sich nach der wirtschaftlichen Potenz der jeweiligen Opfer, deren Hintergrund zuvor von Täterseite entsprechend ausgeforscht worden war. Insgesamt hat die Gefahr der missbräuchlichen Verwendung sensibler Unternehmensinformationen für Angriffe mit Social-Engineering-Techniken (dazu zählt auch Spear-Phishing) durch die bestehenden Offenlegungspflichten für Unternehmen zugenommen, auch durch deren bisweilen überschießende Informationspolitik oder durch Indiskretionen von Mitarbeitern in sozialen Medien.

Insbesondere kleine und mittlere Unternehmen (KMU) waren durch die Schadsoftware Emotet bedroht. Mit dieser können Angreifer auf Firmennetzwerke zugreifen, sich dort unerkannt über zahlreiche Endgeräte ausbreiten und nach einer taktischen Wartefrist von einigen Tagen bis hin zu Wochen einen Verschlüsselungsprozess starten, der ganze Firmennetzwerke arbeitsunfähig machen kann. In der zweiten Jahreshälfte 2019 kam es zu einer solchen Welle von Fällen mit Emotet-Malware-Spam, die je nach Anlass eine Ransomware (Ryuk, GandCrab/REvil/Sodinokibi), einen Banking-Trojaner (Trickbot)

oder aber Wiperware (löscht den Inhalt auf angegriffenen Systemen) auf Zielsystemen platzierte. Auch das Nachladen von Software zum illegitimen Mining von Kryptowährung konnte in diesem Zusammenhang beobachtet werden.

Der Trojaner **Emotet** „nistet" sich in fremde E-Mail-Konten ein und „lernt" deren aktive Korrespondenz zu übernehmen. So kann er sich mit eigenen, maßgeschneiderten E-Mails am tatsächlichen E-Mail-Verkehr „beteiligen", ohne dass der Absender dies bemerkt oder der Empfänger die Fälschung erkennt. Solche vertrauenerweckenden E-Mails enthalten dann falsche Links, die das ahnungslose Opfer direkt auf schädliche Websites führen und dort entweder mit Trojanern infizieren oder aber – kaum besser – zur Preisgabe sensibler Daten (Benutzername, Passwort) verleiten.

Die Blockierungen ganzer Systeme durch Distributed Denial of Service (DDoS)-Angriffe kamen im Berichtsjahr 2019 teilweise ohne Bekennerschreiben oder finanzielle Forderungen an die Opfer aus, weshalb keine konkreten Informationen zu Motiven oder Hintergründen auf Täterseite erhoben werden konnten. Betroffen waren von solchen Angriffen unter anderem Teile der ÖBB Online-Verkaufs-Infrastruktur, die Website der Stadt Wien sowie das Wahlkartenamt der Gemeinde Wien vor den Wahlen zum EU-Parlament im Mai 2019. Rechtzeitige Gegenmaßnahmen auf Zielseite trugen entscheidend zur Eindämmung von Angriffen bei, sodass Totalausfälle wichtiger Dienste verhindert werden konnten. Es kam aber auch zu Erpressungsversuchen mittels DDoS-Angriffen, deren Urheber sich in Bekennernamen mit Namen großer krimineller Hackergruppen (wie „Fancy Bear", „Phantom Squad", oder „Cozy Bear") schmückten, bei denen es sich aber eher um Trittbrettfahrer gehandelt haben dürfte. Fristen zur Zahlung von Lösegeld wurden von den Opfern häufig ignoriert, ohne dass es zu weiteren Folgen kam.

Die Entscheidung einiger Produkthersteller, den Support mit Sicherheitsupdates bei älteren Anwendungen (Apps) und Betriebssoftware einzustellen, stellt ein generelles Sicherheitsproblem für die Cyber-Landschaft in Österreich dar. Da hiervon auch der Support für Windows 7, Windows Server 2008 und Server 2008 R2 betroffen ist, bekamen mit Januar 2020 nur noch Kunden des kostenpflichtigen Support-Programms Extended Security Update (ESU) entsprechende Sicherheits-Patches. Veraltete Systeme stellen jedoch gefährliche Einfallstore dar und können Angreifern Zugang zu weiteren Geräten und Netzwerken eröffnen. Bei Windows 7 handelt es sich um ein in Österreich immer noch sehr verbreitetes Betriebssystem, und es ist mit einer großen Dunkelziffer gerade auch bei solchen Geräten zu rechnen, die in sicherheitsempfindlichen Sektoren wie dem Spitals- und Gesundheitswesen zum Einsatz kommen.

Ein anderer Aspekt, der mit der Entwicklung neuer Versionen von Apps und Betriebssoftware einhergeht, sind Sicherheitslücken (Software-Schwachstellen), die in älteren

Versionen noch nicht enthalten gewesen waren und die oft genug erst mit deutlicher zeitlicher Verzögerung geschlossen werden können. Von den im Berichtszeitraum gefundenen und als kritisch eingestuften Sicherheitslücken sind insbesondere BlueKeep und Foreshadow zu erwähnen. Weiters wurde im Berichtszeitraum 2019 eine Schwäche bei der Prüfung elektronischer PDF-Signaturen festgestellt. Mittels dieser können Angreifer unberechtigte Änderungen am Inhalt von PDF-Dateien vornehmen, ohne die PDF-Signatur zu verletzen. Durch solche Fälschungsanfälligkeit aber ist die Authentizität und Integrität von Dokumenten nicht mehr gegeben. Jegliches elektronisches Aktensystem wäre damit ad absurdum geführt. Potenziell betroffene Stellen wurde entsprechend in Kenntnis gesetzt.

BlueKeep ist eine im Remote-Desktop-Protocol-Dienst (RDP) von Microsoft-Windows enthaltene Sicherheitslücke, die einen Fernzugriff auf Computer mit Windows-Betriebssystemen ermöglicht. Kurz nach Bekanntwerden der Schwachstelle lag die Zahl anfälliger Computer in Österreich im vierstelligen Bereich. Zeitnahe Informationsmaßnahmen halfen bei der effektiven Eindämmung des bestehenden Risikos.

Foreshadow ist eine Sicherheitslücke, die virtualisierte Umgebungen (meist Cloud-Dienste) betrifft und die bei Hyperthreading das unberechtigte Ausführen von Codes ermöglicht. Mittels der bei Intel-Prozessoren serienmäßig implementierten spekulativen Codeausführung werden Speicheradressen in den Cache des Prozessors geladen, auf die der jeweilige Prozess eigentlich keinen Zugriff haben sollte. Neben der im Jahr 2018 bekannt gewordenen Lücke Meltdown/Spectre handelt es sich bei Foreshadow um eine weitere innerhalb der Intel-Prozessoren-Architektur vorhandene Schwachstelle.

Eine **PDF-Signatur** ermöglicht die rechtssichere elektronische Unterschrift von Formularen im PDF-Format (etwa mittels sogenannter Handysignatur).

Eine grundsätzliche Bedrohung für die Sicherheit der öffentlichen Verwaltung und von Unternehmen liegt in den Möglichkeiten der Cyberspionage durch Einsatz sogenannter Advanced Persistent Threats (APT). Diese dienen der langfristig angelegten und aufwändig vorausgeplanten Beschaffung von Informationen aus Wirtschaft und Industrie, oder aber der Ausspähung politischer Gegner. Dabei dringen die APTs tief in Computernetzwerke ihrer Ziele ein und sind selbst nur schwer zu entdecken, weshalb immer mit einer hohen Dunkelziffer von letztlich nicht erkannten Fällen gerechnet werden muss. Darüber hinaus bieten sich dem Angreifer mit APTs auch Möglichkeiten, Computernetzwerke in Produktions- und Lieferketten zu sabotieren, was bis zur vollständigen Zerstörung – etwa durch Datenlöschung, Datenmanipulation oder damit verbundenem physischen Schaden – gehen kann. Eine besondere Herausforderung aus einer Cyber-

Sicherheits-Perspektive stellt auch der zunehmende Trend dar, solche Dienste, die bislang im Gerät selbst angesiedelt waren, in sogenannte Clouds auszulagern. Die zunehmende Inanspruchnahme von Cloud-Services wird langfristig auch das Interesse von Cyber-Kriminellen wecken, weshalb die Etablierung von Sicherheitsmaßnahmen in diesem Bereich besonders vordringlich ist.

Im Frühjahr 2019 wurde bekannt, dass die EU-Delegation in Moskau Ziel eines als APT einzuschätzenden Angriffs geworden war (nachdem es bereits im April 2016 zu unberechtigten Zugriffen auf das EU-eigene Netzwerk gekommen war). Ebenfalls zu Jahresbeginn 2019 konnte ein Angriff auf das COREU/CORTESY-Netzwerk der EU unterbunden werden. Dieses von EU-Mitgliedstaaten genutzte Netzwerk dient dem Austausch von Dokumenten im Zusammenhang mit der „Gemeinsamen Außen- und Sicherheitspolitik" (GASP). Im Zeitraum Juli bis August 2019 kam es auch zu unberechtigten Zugriffen auf die Netzwerkinfrastruktur von zwei österreichischen Parteien und einem Ministerium mit partiellem Datenabfluss. Mit Jahresende 2019 kam es zu einem gezielten Angriff auf das Bundesministerium für europäische und internationale Angelegenheiten mit dem Zweck der Informationsbeschaffung, die sich bis in das Jahr 2020 hinein fortsetzte. Durch umgehend eingeleitete Gegenmaßnahmen konnte ein größeres Schadensausmaß verhindert und unter Beteiligung von BMI, BKA, BMEIA und BMLV die IT-Systeme mit 10. Februar 2020 bereinigt und der Angriff erfolgreich abgewehrt werden.

Die weltweite Einführung des neuen Mobilfunkstandards 5G wird dazu beitragen, dass Datenströme durch dezentrale Datenverarbeitung ressourcenschonender fließen und Ausbaumöglichkeiten für das Internet of Things (IoT) entstehen. Auch die Sicherheit dieser „Fünften Generation" des Mobilfunknetzes stand während des Jahres 2019 im Fokus der Aufmerksamkeit von Cyber-Sicherheitsbehörden. Die EU führte dazu eine koordinierte Risikoanalyse bezüglich der Lage in einzelnen Mitgliedstaaten durch und veröffentlichte entsprechende Ergebnisse im Oktober 2019. Demnach werden die EU-Mitgliedstaaten den folgenden möglichen Szenarien eine erhöhte Aufmerksamkeit schenken: ein lokaler oder überregionaler Zusammenbruch von 5G-Netzen; die Ausspähung von Daten und Datenverkehr; mögliche Modifikationen oder Umleitungen von Daten und Datenverkehr; die Zerstörung oder Veränderung von digitalen Infrastruktur- und Informationssystemen.

Eigentliches „Sorgenkind" aber bleibt immer noch das Passwort. Zu Jahresbeginn 2019 kam es zu einem gravierenden Leak von Login-Daten (Credentials), von dem auch österreichische Internet-User betroffen waren. Die später als „Collection #1–5" bezeichnete Veröffentlichung geschah in fünf aufeinander folgenden Tranchen mit einem Gesamtumfang von mehr als 1,3 Milliarden Zugangsdaten aus unterschiedlichen Quellen. Dies Datenleak stand in einer Reihe mit zahlreichen ähnlichen im genannten Berichtszeitraum, stellte aufgrund seiner besonderen Größe aber einen vorläufigen Höhepunkt dar. Durch rechtzeitige Information konnte zumindest bei betroffenen staatlichen Stellen nach derzeitigem Kenntnisstand größerer Schaden abgewendet werden.

stock.adobe.com

Ein Schlüssel zu mehr IT-Sicherheit in diesem Kontext ist die konsequente Einführung der sogenannten Multi-Faktor-Authentisierung (MFA) in allen Bereichen. Ein Faktor ist hier beispielsweise die Nutzung biometrischer Charakteristika, unter anderem Fingerabdrücke, Iris-Erkennung, Gesichtserkennung, die menschliche Stimme oder das Gangmuster. Ein weiterer Faktor, welchen Unternehmen im Berichtsjahr 2019 zunehmend umsetzten, sind One-Time Authorization Codes (OATC). Letztere sieht vor, dass Nutzer für jede Session einen zusätzlichen einmalig verwendbaren Zugangscode bekommen.

Zu staatsschutzrelevanten Herausforderungen zählt auch zunehmend die Sorge, dass mittels Cyber-Angriffen politische Wahlen manipuliert werden könnten. In einem solchen Fall wäre nicht nur ein hohes gesellschaftliches Schutzgut verletzt, sondern könnte auch das Vertrauen in den demokratischen Prozess an sich untergraben werden. Deshalb hat das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung auch im Berichtsjahr 2019 den Ablauf mehrerer politischer Wahlen auf Bezirks-, Landes-, Bundes- und Europaebene (darunter eine Nationalratswahl und eine Europawahl) begleitet. Dabei wurde festgestellt, dass sich entsprechende Systeme auf einem aktuellen technologischen Stand befinden und keine signifikanten Sicherheitsmängel erkennbar waren. Insbesondere im Hinblick auf die Europawahl war auch ein neues, noch umfassenderes Prüfkonzept erstellt worden, dessen Anwendung die Gefahr künftiger Cyber-Angriffe in diesem Bereich weiter minimieren wird.

Ein 2019 in der Öffentlichkeit besonders diskutiertes Thema waren die Fortschritte im Bereich der künstlichen Intelligenz (KI). Aus einer Cyber-Sicherheitsperspektive ist damit zu rechnen, dass insbesondere die hochgradig wirkungsvollen Angriffsarten, wie Phishing, zukünftig das maschinelle Lernen zu ihrem Vorteil nutzen werden. Mit Mitteln der künstlichen Intelligenz kann die Wirksamkeit von Angriffen automatisiert werden und es können bestehende Methoden optimiert und neue Methoden zielgerichtet gesucht werden. Insbesondere aber für den weiteren gesellschaftlichen Bereich sind Auswirkungen von erheblicher Tragweite zu erwarten, die auch aus einer Staatsschutzperspektive heraus in gleich mehrfacher Weise relevant sind (siehe dazu den Fachbeitrag „Künstliche Intelligenz und nationale Sicherheit“).

Trends und Entwicklungen

Aktuell zeichnet sich ein deutlicher Anstieg der Zahl von Angriffen auf computerbasierte Systeme in staatlichen Institutionen, Unternehmen aus dem Wirtschaftssektor und privaten Haushalten in Österreich ab. Solche Angriffe können ideologisch oder finanziell motiviert sein und einen staatlichen oder nicht staatlichen Hintergrund haben. Dabei kommt es häufig zum Einsatz von Schadsoftware (Trojaner), mit der Daten ausgespäht (Spionage) oder verändert (Desinformation) werden oder ganze Computersysteme unbrauchbar gemacht werden können. Letzteres kann als politische Subversion (Hacktivismus) oder Vandalismus in Erscheinung treten oder sogar Formen des Terrorismus (etwa durch mit Cyberangriffen erzielte Sabotage) annehmen. Sehr häufig kommt es auch zu Fällen von Erpressung, wenn Systeme durch elektronische Angriffe blockiert und erst gegen hohe Lösegeldzahlungen wieder (oder auch nicht) freigeschaltet werden (sogenannte Ransomware-Angriffe). Andere Angriffsarten sind Cyber-Betrug, etwa durch gefälschte Internetseiten (Defacement), sowie die illegitime Veröffentlichung von Persönlichkeitsdaten, Zugangsdaten und Passwörtern im Internet (Leak). Besonders brisant erscheint die zunehmende Abhängigkeit und Angreifbarkeit auch physischer Alltagsgegenstände von elektronischen Netzwerken im Rahmen des Internet of Things (IoT), mit der es zu ungewollten Ausspähungen in allen Bereichen des Lebens bis hin zum vollständigen Ausfall zentraler technischer Dienstleistungen durch gezielte Sabotage (Blackout) kommen kann.

Mit zunehmender Abhängigkeit vom Internet wird die Cybersicherheit zu einer sicherheitspolitischen Aufgabe von gesamtgesellschaftlicher Größe. Die Handlungsfähigkeit verfassungsmäßiger Einrichtungen und der öffentlichen Verwaltung und die Bereitstellung lebenswichtiger Dienste (Energie, Verkehr, Bankwesen, Finanzmärkte, Gesundheitswesen, Trinkwasserversorgung, Digitales) durch eine kritische Infrastruktur ist ein tragender Grundpfeiler für gesellschaftliche Stabilität und die öffentliche Sicherheit. Wenn diese beeinträchtigt ist, und darüber hinaus noch gesteigerte Möglichkeiten für Spionage, Sabotage oder Desinformation durch fremdstaatliche Akteure bestehen, liegt eine erhebliche staatsschutzrelevante Bedrohungslage vor. Cybersicherheit ist daher auf ein

hohes gemeinsames Sicherheitsniveau von Netzwerken und Informationssystemen in Österreich angewiesen. Dazu trägt schon im Vorfeld, insbesondere aber bei tatsächlichen Vorfällen, die eingespielte Zusammenarbeit der dafür zuständigen Behörden in den einzelnen Ressorts (Bundesministerien für Inneres, Äußeres und Landesverteidigung sowie Bundeskanzleramt) in entscheidender Weise bei. Das Cyber Security Center (CSC) im BVT koordiniert zu diesem Zweck den „Inneren Kreis der operativen Koordinierungsstrukturen" (IKDOK) und ist auch operative Behörde im Rahmen des Netz- und Informationssystemsicherheitsgesetzes. Weitere Aufgaben des CSC liegen in der Präventionsarbeit und Beratung sowie der Ausgabe von Frühwarnungen zu aktuellen Gefährdungslagen und Bedrohungen im Cyberraum an Unternehmen kritischer Infrastrukturen und verfassungsmäßiger Einrichtungen. Damit setzt das CSC zentrale Vorgaben des mit Anfang 2019 in Kraft getretenen Netz- und Informationssystemsicherheitsgesetzes (NISG) um.

Mit dem NISG wurde die Schaffung eines hohen gemeinsamen Sicherheitsniveaus zur erfolgreichen Abwehr von Angriffen im Cyber-Raum auf eine rechtliche Grundlage gestellt. Diese sieht eine Übernahme strategischer Aufgaben durch das Bundeskanzleramt vor und belässt die operative Umsetzung entsprechender Regelungen in der Verantwortung des Bundesministeriums für Inneres.

Im August 2016 verabschiedete die Europäische Union eine Richtlinie zur Netz- und Informationssicherheit (NIS) mit dem Ziel der Schaffung eines gemeinsamen hohen Sicherheitsniveaus im europäischen Cyberraum. Sie sieht eine verbesserte Reaktionsfähigkeit der EU-Mitgliedsstaaten auf Cyberangriffe durch den Ausbau von Cybersicherheits-Kapazitäten, eine verstärkte Zusammenarbeit auf EU-Ebene sowie Maßnahmen für die Risikominderung und Vorfallsbearbeitung vor. Die EU-Mitgliedsstaaten begannen mit Mai 2018 mit der Umsetzung in nationale Gesetze. Österreich hat ein eigenes **Netz- und Informationsgesetz (NISG)** mit Jahresbeginn 2019 verabschiedet, das die Einrichtung von NIS-Behörden und zentralen Anlaufstellen, das Vorgeben von Sicherheitsmaßnahmen, das Vereinbaren von Meldepflichten und die Identifizierung und Verständigung von Betreibern kritischer Infrastruktur und wesentlicher Dienste regelt.

Dabei hat sich in der Vergangenheit gezeigt, dass eine erfolgreiche Bewältigung von Cyber-Angriffen nur im Rahmen einer umfassenden, vertrauensvollen Zusammenarbeit aller beteiligten Akteure auf staatlicher und nichtstaatlicher Ebene gelingen kann.

Während die Kooperation staatlicher Stellen bereits seit mehreren Jahren etabliert ist und auch die Kommunikation der staatlichen Seite mit betroffenen Unternehmen auf einer soliden Basis steht, stellt die Identifizierung des nationalen Computernotfallteams (CERT.at) und die geschaffene Möglichkeit zur Implementierung sektorenspezifischer

Computernotfallteams einen weiteren Meilenstein in der Zusammenarbeit dar. Privatrechtlich organisierte Teams von Spezialisten werden zur Informationsdrehscheibe für ihren jeweiligen Sektor und bilden das Bindeglied zwischen betroffenen Unternehmen und staatlichen Behörden. Österreich hatte mit dem Austrian Energy CERT (AEC) bereits zuvor ein auf den Bereich der nationalen Elektrizitäts- und Energieversorgung spezialisiertes Computernotfallteam eingerichtet und konnte im Berichtsjahr 2019 die Vorarbeiten für ein Finanzdienstleister Computernotfallteam (FinCERT) weiter vorantreiben.

CERT.at (Computer Emergency Response Team) ist der Ansprechpartner für IT-Sicherheit im nationalen Umfeld. Es vernetzt CSIRTs (Computer Security Incident Response Teams) aus den Bereichen kritischer Infrastruktur und Informations- und Kommunikationstechnik und gibt Warnungen oder Hinweise für kleine und mittlere Unternehmen heraus.

Ein **sektorenspezifisches Computernotfallteam** ist ein zumeist privatrechtlich organisiertes Team von Spezialisten, das ein wichtiges Element bei der Erhöhung der Resilienz eines Sektors gegenüber Bedrohungen aus dem Cyber-Bereich darstellt. Die Implementierung solcher Computer-Notfallteams liegt in der Verantwortung der einzelnen Unternehmen des betreffenden Sektors. Von staatlicher Seite sind dabei mit der Verabschiedung des Netz- und Informationssystemsicherheitsgesetzes (NISG) die nötigen rechtlichen Rahmenbedingungen gegeben. Diese fungieren als Ansprechpartner für die angeschlossenen Unternehmen auf der einen Seite, wie auch für die Organe der staatlichen Institutionen auf der anderen Seite und bilden somit eine wichtige Drehscheibe für den schnellen Austausch sicherheitsrelevanter Informationen.

Ein weiterer Schritt zur Resilienz gegen Cyber-Angriffe ist die Bewusstmachung in Firmen und verfassungsmäßigen Einrichtungen gegenüber Gefahren aus dem Cyber-Raum (Cyberwareness), um mögliche Angriffe frühzeitig zu erkennen und Schaden effektiv abwehren zu können. Entsprechende Schulungen durch das BVT wurden von Unternehmen der kritischen Infrastruktur und Behörden auch 2019 nachgefragt und zeigen den besonderen Bedarf auch in diesem Bereich. Schließlich wurden im Jahresverlauf 2019 zur Erprobung festgelegter Prozesse, zur Überprüfung gesetzter Maßnahmen sowie zur Festigung innerstaatlicher und internationaler Zusammenarbeit im Cyber-Bereich unterschiedliche Cyber-Übungen durchgeführt. Dazu gehörte ein von der Finanzmarktaufsicht (FMA) gemeinsam mit dem Kuratorium Sicheres Österreich (KSÖ) und der Österreichischen Nationalbank veranstaltetes Planspiel „Cyber Coin 2019“, ein Vernetzungstreffen europäischer NIS-Behörden „Blue OLEX 2019“ in Paris, sowie ein Workshop zu Methoden und Konzepten der Informationsverteilung und Lagebildgenerierung speziell im Bereich des Cyber-Krisenmanagements (CKM). Hier konnte das

Bundesamt für Verfassungsschutz und Terrorismusbekämpfung ein breites Feld von Einsatzbereichen trainieren. Dort gemachte Erfahrungen sind entscheidend für den weiteren Prozess bei der dringend notwendigen Schaffung einer gesamtstaatlichen Resilienz im Bereich der Cybersicherheit.

3
Fachbeiträge

Extremismusprävention und Deradikalisierung als gesamtgesellschaftlicher Auftrag

Aufgrund der europaweiten Bedrohung von Radikalisierung und Rekrutierung entlang des politisch, religiös oder weltanschaulich motivierten Extremismus, stehen die österreichischen Sicherheitsbehörden vor immer komplexeren Aufgaben zur Wahrung der inneren Sicherheit. Ihre strategische und operative Arbeit ist nicht nur vor dem Hintergrund einer gesellschaftlichen Polarisierung, sondern auch der Digitalisierung zunehmend gefordert. Moderne technologische Innovationen bieten Möglichkeiten einer transnationalen Vernetzung, die eine Rekrutierung und Verbreitung von extremistischer Propaganda erleichtert. Auf diese Weise verlagern sich extremistische Aktivitäten und Radikalisierungsprozesse allmählich auf soziale Netzwerke und das Internet, was eine effektive Gefahrenabwehr weiter erschwert.

Radikalisierung wird als individueller Prozess verstanden und folgt keinem allgemeingültigen Muster, weshalb die Beweggründe stets individuell zu betrachten und präventiv auf sie einzuwirken sind. Daher gilt es, auf bereits bestehende bundesweite Maßnahmen in der Extremismusprävention und Deradikalisierung aufzubauen und neue zu etablieren, um den staatsschutzrelevanten Aufgaben in Österreich gerecht zu werden.

Bei der Vorbeugung und Bekämpfung aller Erscheinungsformen des gewaltbereiten Extremismus nehmen die österreichischen Sicherheitsbehörden einen zentralen Stellenwert ein. Zur Erfüllung dieses Auftrags setzen sie nicht nur auf repressive, sondern nun vermehrt auf präventive Maßnahmen. Hierfür bedarf es jedoch einer Kooperation mit bundesweiten Akteuren und Einrichtungen, denen in diesem Bereich eine bedeutsame Schlüsselrolle zukommt. Gesamtgesellschaftliche Herausforderungen – wie zunehmende Radikalisierungs- und Rekrutierungstendenzen – erfordern einen gesamtgesellschaftlichen Lösungsansatz, zu dem sich das BVT in der Präventions- und Deradikalisierungsarbeit bekennt. Aus sicherheitsbehördlicher Perspektive liegt die Bestrebung dieses Ansatzes in der Verhinderung von relevanten Straftaten sowie der Radikalisierungsprävention, die in Österreich im primären, sekundären und tertiären Bereich zu verwirklichen ist. Mit diesem Ansatzsoll einem schrittweisen Abdriften in gewaltbereite extremistische Milieus vorbeugt werden, die ein Gefährdungspotenzial für den gesellschaftlichen Zusammenhalt und die öffentliche Sicherheit darstellen. Vor diesem Hintergrund ist die Erkenntnis, dass auch Deradikalisierungsarbeit nicht als primäre Aufgabe von Sicherheitsbehörden zu betrachten ist, da für die Bewältigung von Radikalisierung und Extremismus nur gesamtgesellschaftlich vorgegangen werden kann.

Um die Resilienz gegen extremistische Narrative und Ideologien in der Gesellschaft zu stärken, soll das BVT daher nicht nur den Erwartungen an seine Schutzfunktion bei strafrechtsrelevanten Tatbeständen entsprechen. Vielmehr liegt der Fokus nun auf präventiven Maßnahmen unter der Prämisse dieses Lösungsansatzes. Infolgedessen haben

die Sicherheitsbehörden in den letzten Jahren maßgeblich an ihnen beigetragen, um ideologisch und/oder religiös motivierter Kriminalität entgegenzuwirken.

Präventions- und Deradikalisierungsmaßnahmen der Sicherheitsbehörden

Geleitet von dieser Prämisse, lag der Schwerpunkt im Jahr 2019 vor allem in einer umfassenden Wissensvermittlung und Stärkung der gesamtstaatlichen Vernetzung. Im Bundesministerium für Inneres wurden unter anderem regelmäßige Sensibilisierungsveranstaltungen zum Thema Radikalisierung und Extremismus abgehalten. Darüber hinaus konnte eine strategische Neuausrichtung des im Jahre 2017 auf Initiative des BVT gegründeten „Bundesweiten Netzwerks Extremismusprävention und Deradikalisierung" (BNED) erreicht werden. Mit der ganzheitlichen Vernetzungsarbeit wird unter der Koordination des BVT eine zielgerichtete Umsetzung von bundesweiten Präventions- und Deradikalisierungsmaßnahmen gewährleistet.

Neben der erfolgreichen Fertigstellung der „Österreichischen Strategie Extremismusprävention und Deradikalisierung" wurde ein Deradikalisierungsprogramm konzipiert. Ziel dabei ist das Aufzeigen von Alternativen zu extremistischen Ideologien durch individuelle Betreuungsmaßnahmen sowie der Verhinderung einer weiteren Radikalisierung und Begehung von ideologisch oder religiös motivierten Straftaten. Nach einer externen Evaluierung seiner Pilotphase und den daraus resultierenden Handlungsempfehlungen, wurde das Konzept des Programmes überarbeitet. Ausstiegsbegleitung soll in Österreich künftig auf alle Extremismusformen anwendbar sein und von zivilgesellschaftlichen Akteuren mit Erfahrungen in der praktischen Fallarbeit umgesetzt werden. Die koordinierte Deradikalisierungsarbeit wird für ausstiegswillige Personen etabliert, um ihnen nicht nur einen erfolgreichen Ausstieg aus bzw. eine Distanzierung von extremistischen Milieus und Ideologien, sondern auch eine Rehabilitierung und Reintegration in die Gesellschaft zu ermöglichen.

Eine weitere Errungenschaft für den Bereich Extremismusprävention und Deradikalisierung ist die gesetzliche Verankerung von sicherheitspolizeilichen Fallkonferenzen, die ab 1. Januar 2020 durchgeführt werden können. Mit der Einführung dieses Rechtsinstruments ist es fortan möglich, durch Informationsaustausch zwischen zuständigen Behörden und Institutionen koordinierte Maßnahmen zur Verhinderung von Straftaten zu setzen. Auf Basis einer Gefährdungseinschätzung und Sicherheitsplanung, können unter der Leitung der Sicherheitsbehörde besondere Schutzmaßnahmen auch für Hochrisikofälle des gewaltbereiten Extremismus erarbeitet und zum Schutz der Allgemeinheit umgesetzt werden. Dies soll in enger Zusammenarbeit mit jenen Behörden und Einrichtungen geschehen, die mit dem Vollzug öffentlicher Aufgaben – insbesondere zum Schutz vor bzw. der Vorbeugung von Gewalt sowie der Betreuung von Menschen – betraut sind. Sicherheitspolizeiliche Fallkonferenzen werden bei Bedarf im österreichischen Deradi-

stock.adobe.com

kalisierungsprogramm eingesetzt, um Fällen des gewaltbereiten Extremismus individuell zugeschnittene Maßnahmen und lösungsorientierte Perspektiven zu bieten.

Ein Beispiel für eine sicherheitspolizeiliche Fallkonferenz:
Eine Person radikalisiert sich zunehmend in eine extremistische Ideologie. Aufmerksam geworden durch die Veränderung wendet sich ein Familienmitglied an eine Organisation außerhalb der Sicherheitsbehörde. Diese Organisation wendet sich an die Sicherheitsbehörde, um die Einberufung einer Fallkonferenz anzuregen. Nach Prüfung des Falles kann durch die Sicherheitsbehörde eine Fallkonferenz einberufen werden, wenn die gesetzlichen Voraussetzungen gemäß § 22 Abs. 2 SPG erfüllt sind. Im Einzelfall werden erforderliche Maßnahmen mit Behörden und jenen Einrichtungen, die mit dem Schutz vor und der Vorbeugung von Gewalt sowie der Betreuung dieser Person betraut sind oder herangezogen werden können, erarbeitet und koordiniert.

Durch die Gesetzeskonformität und rechtsstaatliche Legitimierung werden in Österreich nicht nur die gesamtgesellschaftliche Kooperation, sondern auch der institutionsübergreifende Informationsaustausch auf eine europaweit einzigartige Ebene gehoben. Sie wird es ermöglichen, die bundesweite Radikalisierungsprävention und Deradikalisierungsarbeit noch effizienter, wirkungsvoller und nachhaltiger umzusetzen.

Da Radikalisierung entlang des gewaltbereiten Extremismus einen gesamtgesellschaftlichen Diskurs erfordert, haben es sich die Sicherheitsbehörden zum Ziel gesetzt, verstärkt an nationalen und internationalen Projekten im Bereich Extremismusprävention und Deradikalisierung mitzuwirken. Auf diese Weise soll dem gesamtstaatlichen Auftrag auch in der Sicherheitsforschung Folge geleistet werden. Trotz beachtlicher Fortschritte in der europaweiten Präventions- und Deradikalisierungsarbeit bedarf es mehr denn je der Entwicklung von Ausstiegsprogrammen, um dem gewaltbereiten Extremismus effektiv entgegenzuwirken. Unter der Koordination des BVT wurde im Rahmen eines EU-Projektes daher neben Österreich in vier weiteren Partnerländern (Deutschland, Frankreich, Italien und die Slowakei) ein Handbuch für Ausstiegsarbeit entwickelt. Die Methoden im Handbuch bauen auf praktische Kenntnisse von internationalen Experten der Zivilgesellschaft sowie auf die Pilotphase des österreichischen Deradikalisierungsprogrammes auf. Mit der Implementierung nationaler und zivilgesellschaftlich basierter Ausstiegsbegleitung im Projekt, wird eine Professionalisierung und Erarbeitung neuer Qualitätsstandards in der europaweiten Deradikalisierungsarbeit angestrebt. Nach dem Vorbildmodell des BNED werden durch den Aufbau von lokalen Netzwerken in den Partnerländern darüber hinaus die Rahmenbedingungen geschaffen, um koordinierte Präventions- und Deradikalisierungsmaßnahmen fortlaufend zu etablieren und zu erweitern. Österreich gilt aufgrund der kontinuierlich ausgebauten Expertise und Reflexion europaweiter Erfahrungen daher sowohl mit den bundesweiten Netzwerkstrukturen, als auch den neu etablierten Innovationen im Deradikalisierungsprogramm, als ein europäischer Vorreiter für internationale Standards.

Infolge einer nationalen Kooperation zwischen Behörden, Zivilgesellschaft und Wissenschaft, wurden außerdem Sensibilisierungsmaßnahmen für die Primär- und Sekundärprävention (bei Primärprävention sollen Zielgruppen auf die Gefahren von Radikalisierung generell sensibilisiert werden, während bei Sekundärprävention Personen adressiert werden die gefährdet sind sich zu radikalisieren, und im Umfeld von Personen stehen, die bereits erste Anzeichen für eine individuelle Entwicklung hin zu einer Radikalisierung zeigen) erarbeitet. Der Fokus lag hierbei auf einer Bewusstseinsbildung über die Wirkung von extremistischen Narrativen und ideologischen Deutungsangeboten. Unter Beteiligung der Sicherheitsbehörden wird schließlich die erste österreichische Plattform für Extremismusprävention geschaffen, die Gegennarrative und alternative Narrative zu Extremismus beinhaltet. Neben gebündelten Ressourcen zum Thema (De-)Radikalisierung und Extremismus werden pädagogisch aufbereitete Materialien erarbeitet, um künftig in der pädagogischen Praxis des Bildungs- und Jugendbereichs effektivere Präventionsarbeit leisten zu können. Mit der Unterstützung dieser bewusstseinsschaffenden Maßnahme sollen das kritische Denken und die Resilienz in der Österreichischen Bevölkerung gegenüber extremistischen Weltanschauungen und Propaganda gestärkt werden.

Ausgehend von diesen Maßnahmen ist es für die Sicherheitsbehörden nun von größter Relevanz, das Deradikalisierungsprogramm und die sicherheitspolizeilichen Fallkonferenzen

im Jahr 2020 umzusetzen. Das primäre Ziel ist die Überführung des Programmes in den Regelbetrieb, während es evaluativ begleitet und durchgehend einer Qualitätskontrolle unterzogen wird. Mit seiner Verankerung im internationalen Projekt, wird es einen wertvollen Beitrag in der europaweiten Präventions- und Deradikalisierungsarbeit leisten. Aufgrund der letzten terroristischen Attentate im deutschsprachigen Raum, wird darüber hinaus im strategisch neu ausgerichteten BNED ein Fokus auf die Querschnittsmaterie Antisemitismus gelegt. Gruppenbezogener Menschenfeindlichkeit mit identifizierten Abwertungsideologien soll auf diese Weise noch wirkungsvoller begegnet werden. Wie im Regierungsprogramm 2020 – 2024 bereits festgehalten, werden die Sicherheitsbehörden zur Bewältigung von Radikalisierung und Extremismus auch künftig auf präventive Maßnahmen setzen und neue vorantreiben. Angesichts der bisherigen Erfolge stellt die gesamtgesellschaftliche Kooperation auf sämtlichen Ebenen hierbei ein essentielles Kriterium dar.

Das Linksextreme Aktionsfeld Antifaschismus

Vorbemerkung

Politisches Engagement im Bereich Antifaschismus – verstanden als Ablehnung oder Bekämpfung von Rechtsextremismus/Faschismus/(Neo-)Nazismus – hat per se nichts mit Linksextremismus zu tun.

Antifaschismus ist in der österreichischen Verfassung als staatspolitischer Grundsatz festgelegt. Bereits im Verfassungs-Überleitungsgesetz 1945, mit dem nach dem Zweiten Weltkrieg und der Befreiung Österreichs vom nationalsozialistischen Regime die heute geltende österreichische Verfassungsordnung in Kraft gesetzt wurde, wird klar gegen Faschismus, Nationalsozialismus und Nazismus Position bezogen. In weiterer Folge wurden Verfassungsbestimmungen beschlossen, die Österreich zu einem dezidiert antifaschistischen Staat machen:

- Das in Verfassungsrang stehende Verbotsgesetz 1947 untersagt jedem, sich „für die NSDAP oder ihre Ziele irgendwie zu betätigen".
- Der Staatsvertrag von Wien 1955 verlangt in Artikel 9 – der in Verfassungsrang steht – die „Auflösung der NSDAP und der ihr angegliederten und von ihr kontrollierten Organisationen einschließlich der politischen, militärischen und paramilitärischen". Weiters verpflichtet sich Österreich, „alle Organisationen faschistischen Charakters aufzulösen (…), und zwar sowohl politische, militärische und paramilitärische, als auch alle anderen Organisationen, welche einer irgendeiner der Vereinten Nationen feindliche Tätigkeit entfalten oder welche die Bevölkerung ihrer demokratischen Rechte zu berauben bestrebt sind".

stock.adobe.com

Aktionsfeld Antifaschismus

Die unter dem Überbegriff Linksextremismus zu subsummierenden Gruppen, Organisationen, Vereine, Bewegungen, Netzwerke, Personenverbindungen und subkulturellen Strukturen bilden weder in Ideologie noch in der Praxis ein homogenes Phänomen.

Linksextremisten sind in verschiedenen gesellschaftlichen und politischen Themenfeldern aktiv, wobei ihr Interesse an der tatsächlichen Behebung von Missständen und der Lösung von Problemen meist sekundär ist. Das Handeln linksextremer Gruppen/Organisationen orientiert sich primär an ihrem grundsätzlichen Ziel – der Abschaffung bzw. Beseitigung der gegebenen Staats-, Gesellschafts- und Wirtschaftsordnung. Die parlamentarische Demokratie soll zerstört und durch ein kommunistisches oder ein „herrschaftsfreies", anarchistisches System abgelöst werden. Um dieses Ziel zu erreichen, wird der Einsatz von Gewalt – verstanden als „revolutionäre Gewalt" gegen die „Herrschenden" – grundsätzlich als legitimes Mittel angesehen.

Bei ihren einschlägigen Aktivitäten kristallisieren sich einige Handlungsfelder heraus, die de facto von allen in Österreich aktiven linksextremen Spektren thematisiert werden und folglich szeneübergreifende Relevanz besitzen. Ein im gesamten Phänomenbereich Linksextremismus höchste Priorität genießendes Handlungsfeld stellt der Themen-, Agitations- und Aktionskomplex „Antifaschismus" dar.[21]

„Antifaschismus" ist in der linksextremistischen Diktion mehr als der bloße Kampf gegen den Rechtsextremismus. Aus linksextremer Sicht hat der „Faschismus" seine Wurzeln im „Kapitalismus". Folglich gilt der Kampf von Linksextremisten gegen Rechtsextremismus nur dann als zielführend, wenn er die vermeintlichen gesellschaftlichen Voraussetzungen inkludiert und angreift. Dieser Logik folgend ist „Antifaschismus" nach linksextremem Verständnis immer auch „Kampf gegen das kapitalistische System".[22]

---

21 Neben „Antifaschismus" sind als weitere relevante Aktionsfelder insbesondere „Antikapitalismus", „Antiimperialismus", „Antirepression" und „Antiglobalisierung" zu nennen.

22 Die ideologische Grundlage des Linksextremismus ist die Ablehnung des „kapitalistischen Systems als Ganzes". Die Bedeutung und Rolle des „Kapitalismus" geht in der linksextremen Ideologie weit über die einer Wirtschaftsform hinaus: Ihm wird eine konstituierende und

Linksextremistischer „Antifaschismus“ wendet sich zwar gegen tatsächlichen und auch gegen angeblichen Faschismus bzw. Rechtsextremismus, damit ist aber zwangsläufig keine Bejahung der Demokratie verbunden. Linksextremistischer „Antifaschismus“ beschränkt sich nicht auf die Ablehnung des Faschismus oder Rechtsextremismus wie im demokratischen Sinne. Linksextremisten beziehen darüber hinaus das kapitalistische Wirtschaftssystem und damit auch die bürgerliche Staatsform mit in ihr Faschismusbild ein. Die linksextreme Konzeption von „Antifaschismus“ impliziert folglich auch die Forderung nach einer Überwindung der bestehenden Gesellschafts- und Staatsordnung, da diese zumindest für „faschistische“ Tendenzen mitverantwortlich ist. Diese in der linksextremen Szene allgemein gängige Grundhaltung findet ihren Ausdruck in der zweifachen Frontstellung des Handlungsfeldes „Antifaschismus“: sowohl gegen angebliche und tatsächliche Rechtsextremisten, als auch gegen Einrichtungen und Personen des politischen und wirtschaftlichen Systems.

Während der „Antifaschismus“ von Angehörigen des marxistisch-leninistischen Bereichs des linksextremen Spektrums meist in gewaltfreier Form artikuliert und manifestiert wird, ist der „Antifaschismus“ der Autonomen grundsätzlich als gewaltbereit einzustufen. Für Autonome gehört die Bereitschaft zur Gewaltanwendung zu den grundlegenden Merkmalen des eigenen politischen Selbstverständnisses, die Ablehnung des staatlichen Gewaltmonopols wird derart unmissverständlich deutlich gemacht.

Die grundsätzliche Gewaltbereitschaft des autonomen Spektrums eröffnet ein problematisches Spannungsfeld bei der zivilgesellschaftlich legitimen und aus demokratiepolitischer Sicht notwendigen Bekämpfung des Rechtsextremismus. Es ist evident, dass zivilgesellschaftliche Organisationen und Gruppierungen bzw. von zivilgesellschaftlichen Strukturen organisierte Demonstrationen und Veranstaltungen von gewaltbereiten bzw. gewalttätigen Linksextremisten als Deckung für militante Aktionen genutzt bzw. missbraucht werden.

Die in der Vergangenheit bei Zivilgesellschaft, Politik und Medien wiederholt feststellbare fehlende beziehungsweise nur teilweise Distanzierung von gewaltaffinen Linksextremisten stellt ein Problem dar, da dadurch Linksextremisten bzw. linksextrem motiviertem Agieren eine Legitimität verliehen wird, die kritisch zu hinterfragen oder aus Sicht des Staatsschutzes nicht begründbar ist. Grundsätzlich ist im Kontext „Antifaschismus“ die Frage virulent, ob Demokraten mit Linksextremen gegen Rechtsextreme demonstrieren wollen oder nicht. Fakt ist, dass diejenigen Gruppen und Vertreter der Zivilgesellschaft,

perpetuierende Rolle bei der Etablierung und Bewahrung der „bürgerlichen Herrschaftsverhältnisse“ durch „Repression“ nach innen und „Aggression“ nach außen beigemessen. Somit ist in der Weltsicht von Linksextremisten der „Kapitalismus“ de facto für alle gesellschaftlichen und politischen Missstände – von sozialer Ungerechtigkeit über Rassismus und Rechtsextremismus bis hin zur Umweltzerstörung und zu Kriegen – verantwortlich.

die sich dafür entscheiden, gemeinsam mit Linksextremen gegen Rechtsextreme zu demonstrieren, die gesellschaftliche Akzeptanz der Linksextremen erhöhen.

Festzuhalten ist, dass **Antifaschismus** – verstanden als Ablehnung oder Bekämpfung von Rechtsextremismus/Faschismus/(Neo-)Nazismus – per se nichts mit Linksextremismus zu tun hat. In der linksextremen Szene wird unter „Antifaschismus" aber ein breiteres Handlungsfeld verstanden. Im Sinne der klassischen marxistisch-leninistischen Faschismus-Theorie wird unter „Faschismus" eine Ausprägung bzw. Form des Kapitalismus verstanden, die direkt oder indirekt für das Entstehen entsprechender Bewegungen, Parteien und Regime verantwortlich ist. Folglich bedingt in der linksextremen Sichtweise eine erfolgreiche Bekämpfung des Faschismus eine Überwindung bzw. Abschaffung des Kapitalismus, und damit verbunden wird als Notwendigkeit auch eine Auflösung aller „bürgerlichen" politischen Ordnungsvorstellungen postuliert, gelten diese doch in der linksextremen Weltsicht zumindest als Bedingungsfaktoren für Faschismus und Rechtsextremismus. Folgerichtig agitiert und agiert ein solcher „Antifaschismus" auch gegen die Normen und Regeln eines demokratischen Verfassungsstaates.

Die theoretischen Folgen der linksextremen Faschismusdefinition und die in der Praxis gelebten Formen des „Antifaschismus" machen die Beteiligung von Linksextremisten an Demonstrationen gegen rechtsextreme, neonazistische, rassistische Veranstaltungen, Kundgebungen etc. problematisch. Die aus demokratiepolitischer Sicht nicht nur legitimen, sondern auch notwendigen öffentlichen Proteste gegen rechtsextreme Umtriebe und die dezidierte Ablehnung von rechtsextremem Gedankengut, werden von Linksextremisten oftmals instrumentalisiert und missbraucht. Gewaltbereite Exponenten der linksextremen Szene – in der Regel vor allem Vertreter des autonomen Spektrums – begehen bei an sich friedlichen Protesten und Demonstrationen Gewalttaten und diskreditieren auf diese Weise Ziele und Anliegen des zivilgesellschaftlichen Antifaschismus.

Rechtsterroristische Anschläge: Ein neuer Tätertyp

Nach den Anschlägen von Anders Behring Breivik in Norwegen im Juli 2011, bildeten sich in Europa zahlreiche Personenkreise, Netzwerke und Gruppierungen, die unter anderen der Neuen Rechten zuzuordnen sind (wie z.B. die Identitäre Bewegung Österreich). Wie Breivik, inszenieren sich diese als Vertreter der „letzten Generation", „die noch etwas ändern kann". Der Attentäter auf der Insel Utøya rechtfertigte seine Tat in einem sogenannten Manifest u.a. mit der „Notwendigkeit, dass keine Zeit im Kampf gegen die

Islamisierung“ und für das „weiße Europa“ zu verlieren sei. Die verschwörungstheoretische Formel des sogenannten „großen Austauschs“ ist eine der wirkungsmächtigsten Erzählungen neurechter Akteure, um vor einem vermeintlichen „Bevölkerungsaustausch“ (bspw. Christen gegen Muslime) zu warnen. Bekanntheit erlangte diese Phrase durch die Publikation „Le Grand Remplacement“ (2011) des französischen Autors Renaud Camus.

Von Akteuren und Vertretern der Neuen Rechten wird zumeist kein offener Rassismus mehr vertreten, allerdings ersetzen sie ihr rassistisches, nationalistisch-völkisches Weltbild formal gesehen durch den sogenannten „Ethnopluralismus“, der auf dem Konzept von in sich geschlossenen „homogenen“ Kulturen und Gesellschaften basiert. Darüber hinaus werden Parolen wie „Ausländer raus“ durch Angstkonstruktionen wie „Entwurzelung“, „Überfremdung“ oder „Islamisierung Europas“ ersetzt. In den öffentlichen und politischen Meinungsbildungsprozess werden diese Diskurse strategisch eingeschleust und im Internet (über einschlägige Foren hinaus) massenhaft verbreitet. Mit dem überhöhten Bezug auf „Nation“ wird seitens der Agitatoren der Neuen Rechten gegen jegliche Form der auf Pluralismus und Menschenrechten beruhenden Gesellschaftsordnung argumentiert und mobilisiert. Dieser Diskurs bietet einen ideologischen Nährboden für radikales bis rechtsextremes Gedankengut bzw. suggeriert eine sogenannte Handlungsnotwendigkeit, um die „Einheit des wahren Volkes“ nicht zu gefährden. Wie in den vergangenen Jahren bereits auf erschreckende Weise ersichtlich wurde, entlädt sich die derart aggressiv konstruierte „Gefahr vom Zerfall der eigenen Kultur und Nation“ in Form von rechtsextremen Agitationen und Gewalttaten gegen Juden und Muslime und deren Einrichtungen, Personen, die einem Fremdheitsstereotyp entsprechen sowie Repräsentanten der staatlichen Ordnung.

Rechtsextremisten im Schutz des Netzes und der „alternativen Wirklichkeiten“

Ohne großen Aufwand und mit beachtlicher Wirkung dienen die sozialen Medien als wichtigste Rekrutierungs- und Kommunikationsinstrumente auch für rechtsextreme Gruppierungen, Bewegungen und Netzwerke, um antisemitische und rassistische Verschwörungstheorien oder Szenarien einer vermeintlichen „Islamisierung Europas“ zu verbreiten.

„Anti-Asyl“, „Anti-Multikulturalismus“ und „Anti-Islam“ bilden die zentralen Agitations- und Aktionsschwerpunkte von rechtsradikalen und rechtsextremen Personenkreisen, Szenen und Bewegungen in weiten Teilen Europas und in Österreich. Nicht nur in einschlägigen Foren und Blogs dominieren Kampagnen und Themen, die Hasskriminalität und Ressentiments gegen Migranten und Flüchtlinge sowie gegen Muslime schüren.

Darüber hinaus wird von Teilen des rechtsextremen Spektrums der Verschwörungsmythos in Bezug auf eine vermeintliche „Unterwanderung“ durch den Islam in Europa, als eine von „Juden (als „Strippenzieher“) gesteuerte Maßnahme zur Vernichtung der weißen Rasse“ propagiert. Selbst in nicht extremistischen Online-Plattformen ist dies unschwer als antisemitische Äußerung zu verstehen und trägt zur kollektiven Abwertung von Gruppen und Minderheiten bei, die von rechtsextremen Kreisen als „Feinde des Volkes“ eingestuft werden.

Seit den Account-Sperrungen auf Plattformen wie Facebook und YouTube werden alternative Internet-Foren wie Imageboards (z.B. 4chan oder 8chan) und Messaging-Dienste wie Telegram für rechtsextreme Akteure und Gruppierungen immer attraktiver. Diese Plattformen dienen nicht nur der Internationalisierung und Rekrutierung neuer Sympathisanten und Mitglieder, der Verherrlichung von Rechtsterroristen und ihrer Attentate (bspw. wird der Attentäter von Christchurch als „Heiliger Brenton“ – der bereits auch Nachahmer inspirieren konnte – „verehrt“), sondern werden auch gezielt für koordinierte Desinformationskampagnen genützt. Neben diesen sozialen Netzwerken existiert in der realen wie in der virtuellen Welt eine „Medienlandschaft“, die sich im Gegensatz zu den sogenannten „linken Mainstream-Medien“ gerne als „alternative Medien“ inszenieren und ideologisch spezifizierte Fake News oder wirklichkeitsverzerrende Informationen verbreiten. Das Ziel ist, die Reichweite von rechtsextremen, fremdenfeindlich/rassistischen, islamfeindlichen und antisemitischen Inhalten zu vergrößern sowie eine größtmögliche Emotionalisierung von öffentlich geführten Debatten zu erzielen.

Nutzer dieser „alternativen“ Informations- und Kommunikationskanäle sehen sich selbst oft als Opfer „globaler Eliten“, der „Gesinnungsjustiz“ oder auch der sogenannten „Lügenpresse“. Die Inhalte derartiger Websites suggerieren einen dringenden Handlungsbedarf, um die vermeintlich gefährdete (eigens definierte sowie aufgewertete) „Gruppe“ zu schützen. Die Rechtsterroristen von Pittsburgh[23], Christchurch, Poway[24], El Paso[25] und Halle, nutzten das Internet und bewaffneten sich in der realen Welt, um

23 Im Oktober 2018 stürmte Robert Bowers schwer bewaffnet die „Tree-of-Life-Synagoge“ in Pittsburgh im US-Bundesstaat Pennsylvania, und tötete dabei mehr als zehn Menschen. Das Attentat begründete er u.a. damit, dass „Juden den Tod verdient hätten“, da „jüdische Organisationen“ (Anm. Flüchtlingshilfsorganisationen) „Eindringlinge“, die unsere Leute töten, unterstützen“.

24 Zum Abschluss des jüdischen Pessach-Festes im April 2019 stürmte John Earnest die Chabad-Synagoge im kalifornischen Poway, und schoss auf die Besucher des Gottesdienstes. In seinem Manifest beschrieb er, dass Juden „nichts als die Hölle“ verdient hätten und er werde „sie dorthin schicken“.

25 Patrick Crusius rechtfertigte sein Massaker mit zahlreichen Toten und Verletzten im August 2019 in einer Walmart-Filiale im texanischen El Paso, mit dem vermeintlichen „Bevölkerungsaustausch“ durch eine „hispanische Invasion“ in Amerika.

stock.adobe.com

einen selbst erklärten postmodernen „Kreuzzug“ zu führen („Christentum gegen Islam“, „Weiß gegen Schwarz“ etc.).

Der „einsame Wolf“ im neurechten Schafspelz

Die „einsamen Wölfe“, als auch Rechtsterroristen oftmals bezeichnet werden, sind Anhänger von Verschwörungstheorien und weisen nicht nur ideologische Parallelen auf, sondern sie begreifen sich zumindest in Teilen auch als Fortsetzung und beziehen sich in ihrem Tun und Handeln aufeinander. Der Attentäter von Pittsburgh, Robert Bowers, hat den „Schlachtruf“ aus 14 Wörtern ebenso zitiert wie Brenton Tarrant, der Attentäter von Christchurch, der auf sein Gewehr die Chiffre „14“ aufmalte: „We must secure the existence of our people and a future for white children“ („Wir müssen die Existenz unseres Volkes und eine Zukunft für weiße Kinder sichern“). Dem amerikanischen Rechtsterroristen David Lane wird dieser zugeordnet und findet als sein „Vermächtnis“ in der rechtsextremen Szene maßgebliche Vorbildwirkung.

Stephan Balliet versuchte im Oktober 2019 am jüdischen Versöhnungstag Jom Kippur mit selbstgebauten Waffen gewaltsam in eine Synagoge in Halle einzudringen. Als Ziel gab er die Tötung von „so vielen Anti-Weißen wie möglich, vorzugsweise Juden“ an. Zudem wollte er den Beweis erbringen, dass improvisierte Waffen schlagkräftig sind. Wie der Attentäter von Christchurch, ging er mit taktischer Schutzkleidung in einem

mit Sprengsätzen und Waffen beladenen Auto auf einen selbst ausgerufenen Kreuzzug, streamte mittels Helmkamera die Tat live auf einem Videoportal und veröffentlichte zur Tatbegründung ein in englischer Sprache verfasstes Manifest. Nutzer von sogenannten Imageboard-Websites „bewerteten" den Angriff in Halle, ob dieser den Tathandlungen wie sie in Pittsburgh, Christchurch, Poway und El Paso stattfanden, „gerecht" geworden sei: (…) „Was für eine Enttäuschung", „Er war einer von uns" (…). All diese rechtsextremen Attentäter waren Teil dieser Subkultur im Internet.

Neben dem Rechtsterroristen von Halle, nahmen auch die Attentäter von Poway und El Paso Bezug auf Brenton Tarrant, der im März 2019 mehr als 50 Menschen in zwei Moscheen im neuseeländischen Christchurch erschoss. Nicht nur der Inhalt, bereits der Titel seines online gestellten Manifests „The Great Replacement" weist auf konzeptuelle Überschneidungen mit der von neurechten Bewegungen propagierten verschwörungstheoretischen Formel und der gleichnamigen Kampagne hin. „Der große Austausch" ist eine seit 2015 beworbene Großkampagne der Identitären Bewegung Österreich (IBÖ) und wurde von exponierten Akteuren in sozialen Netzwerken mit „(…) what we call the great replacement" ins Englische übersetzt.

Der Attentäter von Christchurch unternahm in den vergangenen Jahren zahlreiche Reisen nach Europa und Asien und befasste sich vor Ort u.a. mit Feldherren und Fürsten, die er als „Retter des Abendlandes" sah. In Österreich hielt sich Tarrant im November und Dezember 2018 auf. Vor seinem Aufenthalt in Österreich erfolgte bereits im Jänner 2018 eine Spende von 1.500 € an einen exponierten Vertreter der IBÖ. In dem von Brenton Tarrant veröffentlichten Manifest erklärte er zwar, dass er „keiner bestimmten Organisation angehöre", die Attacken in Christchurch allerdings „in den vergangenen drei Monaten" (Anmerkung: vor dem Tatzeitpunkt) geplant zu haben – Österreich wurde auch als eines der Länder benannt, aus denen der „erhoffte Aufstand" seinen Ausgang nehmen könnte. Darüber hinaus wurden die von ihm genutzten Waffen zur Tatbegehung mit historischen Ereignissen und Namen beschriftet, die auch eine Verbindung zu Österreich aufweisen. Beispielsweise: „1683", „Vienna" sowie „Ernst Rüdiger von Starhemberg" („Verteidiger Wiens" während der zweiten „Türkenbelagerung" im Jahr 1683). Diese Termini erfreuen sich insbesondere bei der Identitären Bewegung großer Beliebtheit und dienen beispielsweise bei (Protest-)Aktionen als „legitime" Anknüpfungspunkte, um für „Remigration" und „De-Islamisierung" zu mobilisieren. Anders Behring Breivik wird im Manifest als „Inspiration" für den Anschlag genannt, und wie auch dieser zieht Tarrant die Legitimation für seine Tathandlung aus der von Neurechten lancierten Rhetorik, dass „der Untergang der „Weißen" unmittelbar bevor stehe" und dass es folglich an der Zeit sei, zu handeln.

Die Propaganda der Tat als Modus Operandi für Rechtsextremisten

Die Attentäter waren und sind offenbar von rechtsextremen Ideologien inspiriert und motiviert. Die Auswahl symbolträchtiger Ziele und Opfer, die Absicht eine möglichst

hohe Anzahl an „Feinden“ zu töten, Manifeste und Erklärungen, die mittels Echtzeitübertragung im Internet veröffentlicht werden, die ausgeprägte Waffenaffinität sowie Anleihen aus der Gaming-Szene, lassen die Rechtsterroristen zu einem Teil eines transnational agierenden Netzwerkes werden. Sie sind nicht mehr an starre, streng hierarchische und feste Organisationsstrukturen gebunden, sondern vernetzen sich mit einer zunehmend heterogenen Szene im digitalen Universum. Auch ohne aktive Aufrufe zur Gewaltanwendung, können neurechte Narrative wie der „Bevölkerungsaustausch“ als handlungsleitend interpretiert werden und folglich zu terroristischen Anschlägen führen. Ein neuer Tätertyp, der Nachahmer ist und zugleich weitere Gleichgesinnte zu öffentlichkeitswirksamen Attentaten anregen möchte, stellt eine herausragende Gefahr für rechtsextreme Feindbilder und ihre Einrichtungen dar. Auch wenn Rechtsterrorismus als globales Phänomen erkannt wird, stellt die ideologisch konstruierte Gefahr vom „Volkstod“ sowie die zunehmende Nutzung des Internets (Radikalisierung und Rekrutierung), Sicherheitsbehörden vor neue Herausforderungen, denen mit aller Aufmerksamkeit, Beobachtung und Schärfe entgegen zu treten ist.

Proteste und Unruhen in der Gesellschaft als demokratiepolitische Herausforderung

Demonstrationen, Versammlungen, Protestkundgebungen und freie Meinungsäußerungen sind eine der wichtigsten und unverzichtbaren Tragsäulen moderner Demokratien.[26] Jedoch stellen anhaltende Protestwellen und Unruhen auch eine besondere Herausforderung für Demokratien dar. Dies gilt insbesondere, wenn es im Rahmen von Protestereignissen zu Gewaltausschreitungen oder zur Teilnahme von radikalisierten und gewaltbereiten Splittergruppen kommt.

Das Jahr 2019 war nahezu weltweit von massiven Unruhen, Massenprotesten und gewaltsamen Ausschreitungen geprägt. Ob in Hongkong, im Nahen Osten, Lateinamerika oder in Europa; überall waren Millionen Menschen auf den Straßen. Dabei ist auffallend, dass die Protestthemen je nach Region und wirtschaftlicher, sozialer und politischer Entwicklung zwar höchst unterschiedlich waren, jedoch die Formensprache des öffentlichen Straßenprotests gegenwärtig eine Renaissance erlebt. Dafür gibt es zahlreiche Gründe.

Es kann erkannt werden, dass das Internet allein kein „Straßenersatz“ für gesellschaftliche Konflikte ist. Als Netzwerke für laufende Informationsversorgung zu Themen, die empören und mobilisieren sollen, leisten digitale Kommunikationsmedien zweifelsohne

26 Das Grundrecht der Versammlungsfreiheit ist in Österreich verfassungs- und europarechtlich geschützt. Die Rahmenbedingungen für die Versammlungsfreiheit regelt das Versammlungsgesetz 1953.

einen zentralen Beitrag für spontane Zusammenschlüsse und Protestappelle. Die Geschichte zeigt uns, dass der Protest öffentlichen Raum sucht, um sich Gehör zu verschaffen. Durch großflächige Aufrufe an eine zunächst anonyme Masse im Internet, stellt sich für Initiatoren die wichtige Frage, ob dabei nicht auch gewaltbereite Aktivisten oder Gruppierungen aus einem extremistischen Spektrum angesprochen und mobilisiert werden. Ob gewaltbereit oder moderat gibt hinsichtlich der weiteren Mobilisierung auch darüber Auskunft, inwieweit eine Bewegung erfolgreich oder erfolglos ist. Die oben beschriebene Renaissance der Protestbewegungen steht somit global in einem engen Zusammenhang mit der Ausbreitung von Teilöffentlichkeiten im Internet und der bildreichen Aufmerksamkeitserzeugung durch Protestereignisse sowie die Themenaufbereitung in der Öffentlichkeit selbst.

Protestbewegungen leisten gesellschaftliche Beiträge, die in ihrer appellativen und alarmierenden Inszenierungsform der Aufmerksamkeitserzeugung dienen. Ihre Funktion ist es, Konflikte und Kritik öffentlich sichtbar zu machen, indem sie a) eine geeignete thematische Form (das, wogegen sich der Protest richtet) finden und b) so viele wie möglich zum Mitmachen animieren möchten. Wenngleich der Protest auf der Straße als eine der traditionellsten Formen dieser öffentlich sichtbaren Widersprüche beschrieben werden kann, sind die Protestformen um einiges vielfältiger geworden. Dazu zählen Medienaktivismus, Desinformationskampagnen, Spontankundgebungen, Straßentheater, Störaktion, Flashmobs, Angriffe auf Einrichtungen und Unternehmen Kritischer Infrastruktur genauso, wie sämtliche Formen des zivilen Ungehorsams.

Das Internet als Bildmedium und der Kampf um Aufmerksamkeit

Der Kampf um Aufmerksamkeit für Themen der Protestierenden verfolgt vielseitige Strategien, in denen (vermehrt auch bewegte) Bilder eine besondere Rolle spielen. Auch wenn die klassischen Protestformen in ihrer Variation relativ konstant geblieben sind, ist eine Professionalisierung in der Aufmerksamkeitserzeugung durch dauerhafte selbstgestaltete Medienbegleitung evident. Was früher noch das schlichte Plakat und der Flyer war, wurde durch gezielte Kampagnenarbeit in den sozialen Medien oder via Newsletter ersetzt. Die Idee der sogenannten Internet- bzw. Smartphone-Generation ist der Aufruf: „From tweet to street!“. Dabei spielen Bilder eine immer wichtigere Rolle. Kameras sind die ständigen Begleiter und können relativ kostengünstig und ohne aufwändige Ressourcen Aufnahmen von Protestevents live via Smartphones übertragen. Dies erreicht potenziell auch etwaige Sympathisanten, die an den Protesten selbst gar nicht teilnehmen. Zudem greifen auch Massenmedien im Rahmen ihrer Berichterstattung gerne auf Bilder von Protestierenden zurück, da Unruhen und Konflikte in der Gesellschaft einen beliebten Nachrichtenwert darstellen und die Aufmerksamkeit durch beeindruckende Bilder und Videos von Massen auf den Straßen gesichert ist. Diese Bilder

können motivieren, in Folge weiter mobilisieren oder durch Gewaltausschreitungen auch skandalisieren. Dadurch hat sich der Protest der Gegenwart, Massendemonstrationen und Unruhen veralltäglicht.[27] Es ist abzusehen, dass sich dieser Entwicklungstrend auch in den kommenden Jahren fortschreiben und intensivieren wird.

Unterschiedliche Protestbewegungen weltweit im Aufwind

Die Protestereignisse der Demokratiebewegung in Hongkong, die Gelbwestenbewegung (gilets jaunes) in Frankreich und auch die in Österreich stattgefundenen Klimastreiks haben in der jüngeren Vergangenheit für weltweites Aufsehen gesorgt. Die Auslöser für diese Protestwellen waren höchst unterschiedlich, jedoch ist ihre Langatmigkeit und Zähigkeit im Vergleich zu anderen Protestbewegungen signifikant. Dies sticht insofern hervor, weil beispielsweise bei den Gelbwestenprotesten in Frankreich gewaltsame Erscheinungsformen wie Straßensperren, Blockadeaktionen, Sachbeschädigungen und Konfrontationen mit Polizeikräften schon am Beginn standen und die Zahl der Teilnehmenden trotzdem anstieg und in einer ersten Welle weitere Teilnehmer nicht abschreckte. In Österreich kam es zwar vereinzelt zu Aufrufen bei diversen Protestveranstaltungen auch gelbe Westen zu tragen, jedoch blieb eine derartige Entwicklung wie in Frankreich aus.

Auch in Hongkong startete eine breite Protestbewegung gegen ein Gesetz, das die Auslieferung von Häftlingen von der Sonderverwaltungszone an die Volksrepublik China ermöglichen sollte. In der Mitte des Jahres 2019 erreichten die Protestunruhen in Hongkong einen gewaltsamen Höhepunkt. Dieser führte zu Verhaftungen von tausenden Personen und es kam zudem auch zu Verletzten und einigen Toten (darunter auch ein Passant). Von den Aktivisten der Demokratiebewegung in Hongkong wurde das brutale Vorgehen der Polizei scharf kritisiert und animierte in Folge den Widerstand der Oppositionsbewegung noch mehr.

Eine weitere internationale Protestbewegung erreichte mit ihren sogenannten „Klimastreiks“ im Jahr 2019 einen fulminanten Aufschwung. Diese Umweltbewegung setzte, neben der großen Teilnehmerzahl, auch eine enorme Bandbreite an Protestvariationen frei. Diese umfassten „Schulstreiks“ und Demonstrationen am internationalen Klimaprotesttag („Black Friday“), die auch in Österreich zu einer Teilnahme von tausenden Demonstranten führte. Am sogenannten „Earth Strike“ nahmen Ende September 2019 weltweit Millionen Menschen teil. Auch in Österreich konnten Zehntausende in sämtlichen Hauptstädten mobilisiert werden. Historisch betrachtet, scheinen Themen welche

27 Vgl. Rucht, Dieter (2007): Vom Elend der „Latschendemos“, in: Geiselberger,Heinrich (Hrsg.) Und Jetzt?, Suhrkamp, Frankfurt am Main, S. 183-202, S. 198.

stock.adobe.com

die Umwelt(-politik) betreffen besonders in Österreich geeignet zu sein um eine große Mobilisierung zu erzielen.[28]

Obwohl die Themen der hier genannten Protestbewegungen der jüngeren Vergangenheit nicht unterschiedlicher sein könnten, haben sie durch ihre Ritualisierung (tägliches oder wöchentliches Auftreten), aber auch durch ihre mediale Begleitung mittels Social-Media-Plattformen und Informationsvernetzung partielle Gemeinsamkeiten. Zudem kann eine gemeinsame und geschlossene ideologische Herkunft der Protestierenden bei den beschriebenen Protestfällen nicht zweifelsfrei erkannt werden. Auch hinsichtlich der Teilnehmerstrukturen ist erkennbar, dass die Proteste der Gegenwart nicht nur junge Menschen aus beispielsweise dem studentischen Milieu erreicht, sondern auch sehr unterschiedliche soziale und berufliche Gruppen aus der Mitte der Gesellschaft zunehmend mobilisieren und ansprechen kann. Neben diesen prominenten Protestereignissen haben sich 2019 auch in anderen Regionen der Welt Unruhen entzündet. In Algerien und Irak richtete sich der Unmut der Bevölkerung gegen Korruption und Arbeitslosigkeit. In Ecuador und Iran radikalisierten sich die Aufstände gegen Benzinpreiserhöhungen, was im Iran sogar dazu führte, dass die Sicherheitskräfte die Proteste gewaltsam (dabei kam es zu Verletzten und Toten) brutal niederschlugen und sogar der Zugang zum Internet vom Regime nahezu vollständig gesperrt wurde. Auch im Sudan war die Initialzündung für Aufstände die Verdreifachung der Brotpreise, was zu einem landesweiten Aufstand gegen das Regime führte, nachdem die Polizei auf Protestierende geschossen hatte und es dabei zu Toten und Verletzten gekommen war. Diese Unruhen und Aufstände führten zu massiven politischen Umwälzungen im Sudan und zum Sturz des Präsidenten. Ob steigende Brot- und Treibstoffpreise, oder Steuern auf Gespräche bei Messenger-Diensten (wie im Libanon); daran zeigt sich deutlich, dass soziale und Fragen der ökonomischen Verteilung das Protestaufkommen auch in undemokratischen

28 Beispielsweise sei hier an die Besetzung der Hainburger Au (1984) und 1977/1978 an die Proteste gegen das Atomkraftwerk in Zwentendorf erinnert.

Regionen zunehmend dominieren und auch in höchst repressiven politischen Systemen zum Mittel des Protests gegriffen wird.

Entwicklungstrends und Herausforderungen für die Sicherheit

Es kann festgestellt werden, dass das Austragen gesellschaftlicher Konflikte in Form von Protestgewalt und Polarisierung im öffentlichen Raum weltweit zunimmt. Dieser Umstand ist auch den extremistischen Rändern in der Gesellschaft bekannt. Diese greifen oft Stimmungen auf und manipulieren und instrumentalisieren diese bei Protesten für ihre extremistischen Ansichten oder Machteroberungsfantasien. Derart extremistische Gruppierungen und Bewegungen zeichnen sich durch die vollkommene oder überwiegende Ablehnung der für einen demokratischen Rechtsstaat erforderlichen Prinzipien aus. Ein weiteres Merkmal dieser Gruppen, Netzwerke, Bewegungen und Szenen ist die positive Beantwortung der Gewaltfrage. Zur Durchsetzung der eigenen politischen Ideen wird Gewaltanwendung befürwortet, gerechtfertigt, geduldet, praktiziert oder dazu provoziert.

In den letzten Jahren ist auch in Österreich tendenziell ein Anstieg der Gewaltbereitschaft bei Konfrontationen beispielsweise zwischen links- und rechtsextremistischen Gruppierungen zu verzeichnen. Dabei ist das öffentliche Zusammentreffen der ideologischen Gegenspieler meist durch Provokationen und Aggressivität geprägt. Evident ist, dass es sich bei den Anlassfällen für links-/rechtsextreme Konfrontationsgewalt mehrheitlich um Ereignisse, Veranstaltungen, Kundgebungen etc. handelt, die unter dem Überbegriff „Antifaschismus“ zu subsumieren sind.

Träger der gewalttätigen linksextremen Proteste sind vor allem autonome Gruppierungen. Ihre Aktivitäten werden wesentlich durch die Größe der jeweiligen Protestveranstaltung bestimmt und ihre (gewalttätigen) Aktionen setzen sie aus dem Schutz der Masse heraus. Sowohl der Links- als auch der Rechtsextremismus stellen jeweils für sich eine staatsschutzrelevante Gefährdungssituation dar. Zudem ist zunehmend zu beobachten, dass sich auch importierte Konflikte aus anderen Ländern auch auf den Straßen Österreichs entladen und zu gewaltsamen Ausschreitungen führen. Die genaue Beobachtung der einschlägigen Szenen in Österreich und deren Entwicklungen zählen zu den wesentlichen Aufgabenstellungen der Sicherheitsbehörden.

Die in Form von Protestgewalt, Polarisierungen und Radikalisierung im öffentlichen Raum evidenten Konfrontationspotenziale zwischen antagonistischen Extremismen, bergen eine besondere Sicherheitsrelevanz und stellen im Rahmen der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit eine herausfordernde Aufgabe insbesondere für Einsatzkräfte dar. Dabei ist die Gefahr nicht zu unterschätzen, dass sich die Gewalt nicht nur gegen den ideologischen Gegner richtet, sondern in ihrer Dynamik auch Drittziele (Exekutive, Privatpersonen, öffentliches und privates Eigentum) betroffen sein können. Rechts- und Linksextremismus entwickelt sich auch in Österreich permanent weiter.

Neben szeneinternen personen- und organisationsbezogenen Prozessen nehmen auch gesellschaftliche, ökologische, wirtschaftliche, und politische Konflikte Einfluss auf ihre Entwicklung und damit auch auf das Konfliktfeld Links-/Rechtsextremismus. Kontinuierliche Beobachtung, Analyse, Verarbeitung von Hinweisen aus der Bevölkerung und den jeweils aktuellen szenespezifischen Entwicklungstendenzen angepasste präventive und repressive Maßnahmen sind erforderlich, um sämtlichen Konfliktfelder weiterhin mit Erfolg begegnen zu können und gewaltsame Ausschreitungen bei Protesten nachhaltig entgegenwirken zu können.

Künstliche Intelligenz als disruptive Technologie

Welche Schuld trägt künstliche Intelligenz?

Zibetkatzen sind bodenbewohnende, recht großen Schleichkatzen, die meistens auf dem grauen und gelben Fell ein Streifen- oder Fleckenmuster tragen. Die Gattung kam zu kurzzeitiger Berühmtheit, als man sie der Übertragung des SARS-Virus auf den Menschen verdächtigte. Dies Missverständnis ging jedoch auf einen Übersetzungsfehler zurück; gemeint war nämlich der Larvenroller (eine weitere Art von Schleichkatze). Aber auch der Larvenroller könnte das SARS-Virus nur von anderen, noch unbekannten Tieren empfangen haben – und damit selber eigentlich unschuldig sein.

An solche Verleumdungen hat man sich im Bereich der künstlichen Intelligenz (KI) schon gewöhnt, wird man doch für alles verantwortlich gemacht, was es an positiven und negativen Vorstellungen von einer automatisierten Zukunft gibt. Zwar geht mit KI ein alter Traum in Erfüllung, dass der Mensch die Maschine für sich arbeiten lässt. Den Roboter nur zu erwähnen, löst aber auch schon Ängste aus. Zu diesem Thema hat fast jeder eine Meinung (aber nicht jeder hat den Überblick, worum es dabei wirklich geht).

Die Welt steht heute an einer Schwelle, wo tatsächlich ein großer Teil von menschlicher Arbeitsleistung an Maschinen abgegeben werden kann. Tatsächlich erzielt KI in manchen Bereichen sogar bessere Ergebnisse, als es Menschen leisten könnten. KI kommt heute schon im Gesundheitswesen, Militär, Rechtswesen und Marketing zum Einsatz; sie ist aus Unterhaltungsindustrie und Computerspielen nicht mehr wegzudenken und sitzt in Alltagsgeräten wie TV, Handy, Auto und Staubsauger bis hin zur elektrischen Zahnbürste. Auf der Hand liegt, dass industrielle Hersteller die bestehenden Erwartungen in solche „Zukunftstechnologie“ ihrerseits noch anfeuern. Dabei wird auch die eine oder andere Übertreibung als geschäftsfördernd in Kauf genommen. So ist es für den Beobachter nicht immer ganz einfach, den Mythos von der Realität zu unterscheiden.

Das Zukunftsszenario der intelligenten Mensch-Maschine würde man in der Wissenschaft eher mit dem Begriff der starken Intelligenz fassen. So etwas gibt es aber noch nicht,

und sollte das jemals der Fall sein, ist der Weg dahin jedenfalls noch weit. Es ist deshalb besser, ausufernde Erwartungen an die KI einzubremsen und die Diskussion wieder auf eine konstruktive, sachliche Ebene zurückzuholen.

Künstliche Intelligenz und maschinelles Lernen

Man bezeichnet mit künstlicher Intelligenz maschinelle (Computer-)Systeme, die ihre Umwelt ohne fremde Hilfe wahrnehmen, daraus ihre Schlüsse ziehen und in Antwort darauf eigene Handlungen setzen können, die vorher noch nicht entsprechend geplant gewesen waren.

Solche Definition kann nach derzeitigem Stand der Dinge nicht viel mehr als ein Annäherungswert sein. Denn den Roboter, der mit dem Menschen auf Augenhöhe lebt, gibt es noch nicht. Vielmehr beschränkt sich das technisch Machbare in den meisten Fällen auf das, was man schwache Intelligenz nennt und das als **„maschinelles Lernen“** eine weitaus präzisere Bezeichnung erfahren würde. Dieser Begriff bietet den Vorteil, weniger die Fantasie zu stimulieren und dadurch in nützlicher Weise zur Versachlichung der Debatte beizutragen. Beim maschinellen Lernen (ML) handelt es sich nämlich streng genommen nur um einen Teilbereich des an sich viel umfassenderen Phänomens der künstlichen Intelligenz. Fast alles, was bislang als KI verkauft wird, besteht in Wahrheit aus ML. Dabei geht es darum, Computer in die Lage zu versetzen, Dinge unabhängig von menschlicher Hilfe zu lernen. Aber wie soll das funktionieren?

Eine Maschine kann so programmiert werden, dass sie eine gegebene Situation wiedererkennt. Um alle möglichen Abweichungen von der Standardsituation mit dabeizuhaben, muss man auch diese mitprogrammieren. Ein prägnantes Beispiel wäre ein Programm, das einen bestimmten Gegenstand automatisch erkennen soll. Man gibt als Parameter alle jene Eigenschaften ein, die auf unterschiedlichste Versionen desselben Gegenstands zutreffen können. Es liegt auf der Hand, dass bei anspruchsvoller Ausgangsfragestellung (man erwartet sich von KI mehr als nur einzelne Gegenstände richtig zu erkennen) die Komplexität der möglichen Varietäten zunehmen wird. Man programmiert also gewissermaßen „hinterher“, und irgendwann ist der Zeitpunkt erreicht, an dem das Ergebnis den Aufwand nicht mehr lohnt.

Besser die Maschine lernt selbständig. Dann füllt man sie mit einer größtmöglichen Zahl an Bildern des gewünschten Gegenstands, und das System vermag es, die komplexen Einzeldaten auf einer höheren abstrakten Ebene derart zu verbinden, dass die Erkenntnisfähigkeit potenziert wird. Solche selbstlernenden Datensets auch mithilfe des „tiefen Lernens“ (**Deep Learning**) dann wieder mit weiteren Datensets zu verknüpfen, schafft größere kognitive Systeme, die sich der komplexen Wirklichkeit tatsächlich in gewisser Weise annähern. Sie können dann Aufgaben übernehmen, mit denen Erwartungen an „künstliche Intelligenz“ zumindest in Ansätzen erfüllt werden. Vor allem erledigen sie

bestimmte Dinge sorgfältiger und komplexer, als es dem Menschen jemals möglich wäre. Solche selbstdenkenden Systeme werden nie die Schwelle überschreiten und gegen den Menschen „rebellieren“ können, aber sie vermögen die unerreichte kognitive Flexibilität des Menschen durch ihre ganz eigenen Fähigkeiten sinnvoll zu ergänzen.

Problematisch wird es dann, wenn die Maschine eines Tages wirklich autonom denkt, dabei aber den Weg ihrer Entscheidungsfindung nicht mehr transparent macht. Denn Maschinen sind blind für ihre Umgebung und taub für Zwischentöne. Auch das stärkste lernfähige System verfügt nicht in hinreichender Weise über Empathie und gesunden Menschenverstand, um dynamische Alltagssituationen in einer dem Menschen angemessenen Weise wirklich zu bewältigen. Ein solches System würde dann besser als der Mensch, aber nicht mehr im Sinne des Menschen denken. Es „weiß“ nur das, was ihm zuvor einprogrammiert worden ist. Ist diese Datengrundlage aber ungenügend, kommt es zwangsläufig („lernend“) zu verkürzten Schlussfolgerungen und einer verzerrten Sicht der Wirklichkeit. Oder schlimmer noch: Es schafft, durch maschinelle Überlegenheit legitimiert, erst eine dem Menschen abträgliche neue „Wirklichkeit“.

Künstliche Intelligenz und Cyber-Sicherheit

Das Jahr 2019 sah eine starke Zunahme kritischer Angriffe und Datenlecks in einer bislang so nicht gekannten Größenordnung. Infolge dieser Entwicklung wurde für das Jahr 2020 ein möglicher Gesamtschaden in einer Größenordnung von weltweit 5 Billionen US-Dollar vorausgesagt. Mit der Zunahme der Angriffe steigen wiederum die Anforderungen an oft unterbesetzte IT-Sicherheitsteams in Behörden, Unternehmen und kritischen Infrastrukturen auch in Österreich. Im Gegenzug wird aber ein allgemeiner Mangel an wirklichen Cyber-Sicherheitsexperten konstatiert. So sucht man händeringend nach Möglichkeiten, dieses Dilemma mithilfe technischer Innovation zu überwinden.

Hier kommt künstliche Intelligenz ins Spiel. Einer der derzeit vielversprechendsten Ansätze ist die Verwendung im Bereich der Erkennung von **Schadsoftware**. Hier scheitern

stock.adobe.com

konventionelle Netzsicherheits-Systeme oft an der immensen Zahl von Malware, die täglich auf das System einströmen und mit konventioneller menschlicher Steuerung nicht mehr zu bewältigen sind. Maschinenlernende Systeme können hier eine Entlastung schaffen und, sobald entsprechend trainiert, mit ihrer überlegenen rechnerischen Kapazität selbst kleinste Verhaltensmerkmale von Angriffen aufspüren, wie es ein menschlicher Cyber-Sicherheitsexperte so niemals könnte.

Zusätzliche Einsatzmöglichkeiten bietet die automatisierte Erkennung von **Phishing**-Mails. Letztere sind deshalb gefährlich, weil sie legitimen E-Mails täuschend ähnlich sehen und den Empfänger dazu verleiten, ein angehängtes Dokument, das mit bösem Schadcode belastet ist, unbedacht zu öffnen, oder eigene sensible Daten (Passwörter!) in eine vermeintlich seriöse Eingabemaske zu füttern. Intelligente Systeme sind in der Lage, mithilfe von Algorithmen solche Kampagnen immerhin zu erkennen und dann wie herkömmliche E-Mail-Spam-Filter zu blockieren.

Datenlecks wiederum können zur Preisgabe äußerst sensibler persönlicher Informationen im Internet führen. Diese lassen sich anschließend maschinell mit anderen öffentlich einsehbaren Informationen zur selben Person abgleichen. Wenn sie dann auf kriminellen Plattformen und zu hohen Preisen (zum Beispiel im Darknet) gehandelt werden, kann dies zur erheblichen Gefahr für die Sicherheit und das Vermögen der betroffenen Opfer werden, etwa durch persönliche Erpressung, das hochgradig effektive **Spear-Phishing** oder auch „nur“ den missbräuchlichen Zugriff auf Bankkonten und Kreditkarten. Häufig sind solche Datendiebstähle selbst das Ergebnis erfolgreicher Phishing-Kampagnen, aber auch ganze Datenbanken großer Online-Dienstleister können gehackt und ihr sensibler Inhalt anschließend ungefragt veröffentlicht werden. Mittels spezieller selbstlernender **Webcrawler** lassen sich solche Plattformen oder die auf ihnen geteilten sensiblen Daten gezielt aufspüren und ihr weiterer Missbrauch unterbinden. Das funktioniert auch in solchen Bereichen des Internet (Deepweb, Darknet), die nicht von gängigen Suchmaschinen wie Google etc. ohne weiteres erschlossen werden können: Suchprogramme können sich intelligent als menschliche Akteure „tarnen“ und unerkannt in geschlossene (kriminelle) Gruppen eindringen, indem sie herkömmliche Schutzvorrichtungen unterlaufen (etwa die Captcha genannten automatischen Tests, mit denen Menschen von Spambots unterschieden werden sollen – „auf welchen der neun Bilder ist ein Auto zu sehen?“).

Weitere Möglichkeiten liegen in der Schaffung einer umgebungsintelligenten Verhaltensanalyse: Hier gelingt die Verbindung von **Big Data** und maschinellem Lernen, wenn ein lernfähiges System mit Daten zum User-Verhalten bestückt wird, das seinerseits dann selbständig komplexe Grundmuster entwickelt, vor deren Hintergrund dann kleinste Abweichungen (etwa durch ungewöhnliches Verhalten seitens böswilliger Angreifer) erkannt und ausgefiltert werden können. Auf solcher Grundlage werden herkömmliche Dichotomien („guter/schlechter“ Datenverkehr, „saubere/befallene“ Datensysteme etc.) überwunden und die Netzsicherheit an die viel subtileren Ereignisse in der Praxis an-

passt. Bei der aktiven Suche nach Angreifern wiederum hilft der sogenannte Honigtopf, wo ein vermeintlich menschlicher Akteur (in Wahrheit ein mit KI entwickeltes komplexes Personenprofil) im Internet Kontakte anzieht und unter diesen, mittels eigenem ML, legitime von bösartigen Akteuren trennen kann. Letztere werden dann für alle User gleich (etwa in einer Firma oder Behörde) vom gesamten System blockiert.

Die Risiken und Nebenwirkungen

Allein die hier aufgezählten Beispiele machen deutlich, wie entscheidend maschinelles Lernen (ML) zur Netzwerksicherheit beitragen kann und welches Potenzial in künstlicher Intelligenz (KI) liegt. Davon können Behörden, Unternehmen und Privatnutzer des Internet auch in Österreich in gleicher Weise profitieren. Allerdings hätte gegen zukünftige „KI-Hacker" auch das sicherste KI-unterstützte System in Wahrheit keine Chance. Damit wird das Ganze zum Katz-und-Maus-Spiel ohne erkennbaren Mehrwert für die Sicherheit.

Bedenklich stimmt in diesem Zusammenhang auch, dass mit neuronalen Netzen und Sprachsynthese schon heute die Mimik in Gesichtern und der authentische Klang von Stimmen gefälscht werden können: Erschreckend echte Kopien von realen Personen (Staatsoberhäupter, Firmenchefs) können Falschmeldungen verkünden und Fehlentscheidungen provozieren. Damit droht eine Welt, in der man nichts und niemandem mehr Glauben schenken könnte. Beunruhigend ist auch die Aussicht, dass bösartige Hacker die eigene Schadsoftware auf eine Weise mit KI optimieren könnten, dass sie von schon bestehenden Skripten „lernt" und damit zu noch gefährlicheren Angriffsformen „mutiert". Damit könnte sich dann jedes Cyber-Sicherheitssystem, auch ein zukünftiges KI-gesteuertes, überwinden lassen. Aus einer Sicherheitsperspektive gesehen, wäre man damit aber auf den Nullpunkt zurückgeworfen. Man hätte nichts gewonnen und würde der Gegenseite vielmehr wieder nur „hinterher" programmieren. Intelligente Malware wäre das Ende einer jeden Vorstellung von Cyber-Sicherheit.

An dieser Stelle kommt dann auch in besonders drastischer Weise zum Tragen, wie angreifbar KI-Systeme in Wirklichkeit sind. Denn mit bösartiger Datenmanipulation könnte sich das Lernverhalten unbemerkt auch in eine falsche Richtung lenken lassen und eine Maschine so nicht „erzogen", sondern in Wahrheit „verzogen" wird, dass sie sich zuletzt gar nicht mehr im beabsichtigten Sinn steuern lässt. Auch könnten mutwillige falsche Fährten gelegt werden, mit der Absicht ein System bewusst zu Fehlentscheidungen zu verleiten. Aber allein auch die bösartige Ausnutzung von Schwachstellen, wie sie in jedem autonomen KI-System vorkommen können, hätte Folgen, die um ein Vielfaches drastischer wären, als es bisherige Angriffe auf herkömmliche Software sind.

Ein weiterer möglicher „Geburtsfehler" von KI liegt darin, dass KI-Systeme umso lern- und anpassungsfähiger bleiben müssen, je komplexer die reale Welt wird. Dazu braucht es noch mehr Daten als bisher, die zwar in entsprechend großer Zahl verfügbar sind, die

aber in ihrer nötigen Datenqualität noch sorgfältiger als bisher geprüft werden müssten. Angesichts der Tatsache, dass eine fehlerhafte Datengrundlage (durch ungenaue Erhebung oder aktive Datenmanipulation) gerade bei autonomen Systemen verhängnisvolle Auswirkungen mit sich bringen würde, könnte der Bedarf an „richtigen" Daten und Datenhygiene Entwickler zukünftig vor noch größere Herausforderungen stellen.

Zu den technischen Aspekten kommen die gesellschaftlichen Herausforderungen: Es ist ein offenes Geheimnis, dass in manchen Bereichen von Produktion und Dienstleistung KI effizienter als der Mensch arbeiten könnte. Dadurch drohen ganze Berufsfelder zu verschwinden, darunter „Klassiker" kindlicher Berufsplanung, wie Buslenker oder Baukranführer, sowie ganz allgemein qualifizierte Tätigkeiten der maschinellen Produktion, medizinischen Diagnostik, Rechtspflege, Schul- und Unterrichtswesen oder der Verwaltung. Auch kommen regelmäßig Bedenken, dass KI-Systeme helfen könnten, den vielzitierten „Überwachungsstaat" zu realisieren, und in der Tat hat es im Hinblick auf videoanalytische und andere Überwachungssysteme schon Möglichkeiten einer missbräuchlichen Verwendung im Sinne einer Einschränkung von Freiheits- und Persönlichkeitsrechten gegeben.

KI ist aber auch ein Geschäftsmodell. Fachliteratur und Medienberichte springen schnell auf und lesen sich nicht selten wie Werbeprospekte für KI-Produkte. Damit aber verstärken sie ein latentes gesellschaftliches Unsicherheitsgefühl, das privaten Herstellern von Sicherheitsprodukten nicht zuletzt auch Aufträge aus öffentlichen Mitteln sichert: Wenn der „Feind" nicht schläft, muss auch die gute Seite in KI investieren. So dürfte für die kommenden Jahre mit massiven Investitionen in diesen unumgänglich gewordenen Bereich gerechnet werden, und Experten prognostizieren bis zum Jahr 2025 weltweite Ausgaben von mehr als 30 Mrd. US-Dollar allein für KI-basierte Cyber-Sicherheitssysteme und ihre Dienste. Vielleicht hätte die mit zunehmenden Mitbewerbern um diesen großen Kuchen immer mehr geforderte „Marktfähigkeit" zumindest den nützlichen Nebeneffekt, dass KI-Produkte langfristig anwendungsfreundlicher und auch für Menschen ohne größere technische Kenntnisse verstehbar werden.

Die Entwicklung von KI-Systemen schreitet noch schneller voran, als ursprünglich von Experten erwartet worden war. Sie lässt sich nicht ignorieren, und bringt in Wahrheit deutlich Vorteile mit sich. Diese aber würden vor allem solchen gesellschaftlichen Gruppen zugutekommen, die sich schon jetzt mit höherer Bildung und wirtschaftlicher Prosperität positionieren können. Deshalb ist auch in Österreich mit gesellschaftlicher Divergenz in diesem Bereich und ganz konkret mit „Verlierern" der Entwicklung und möglichen disruptiven Auswirkungen auf das friedliche Zusammenleben zu rechnen. „Das Buch ist immer so schlau wie seine Leser", weshalb KI zum Werkzeug derjenigen wird, die es zu nutzen wissen. Somit liegt es in der Hand des Menschen und wäre es nicht der Technik anzulasten, dass KI ihren Nutzen entfaltet (wir erinnern an die Zibetkatzen vom Anfang).

Die Europäische Union greift den Punkt der nötigen gesellschaftlichen Achtsamkeit auf und hat für 2020 ein „Weißbuch zu künstlicher Intelligenz“ geplant. Dieses wird die Themen Cyber-Sicherheit, Schutz kritischer Infrastruktur, Auswirkungen auf den Datenschutzbereich und die Grundrechte behandeln. Besondere Bedeutung kommt dabei der Ausstattung von Strafverfolgungsbehörden mit geeigneten Instrumenten zum Schutz vor Terror, terroristischer Propaganda im Internet, Identifizierung gefährlicher Stoffe und Gegenstände, Aufdeckung verdächtiger Transaktionen, biometrischer Fernidentifikation sowie der Analyse großer Datenmengen zu.

Schutz kritischer Infrastruktur – Schützenswertes Krankenhaus

Vor dem Hintergrund einer anhaltenden Bedrohung durch terroristische Anschläge, einer steigenden Computerkriminalität sowie einer wachsenden Abhängigkeit von Staat, Wirtschaft und Gesellschaft von funktionierenden Infrastrukturen, gewinnt besonders der Schutz kritischer Infrastruktur (SKI) immer mehr an Bedeutung. Österreich als hochentwickeltes Wirtschaftsland, ist substanziell vom kontinuierlichen Funktionieren seiner kritischen Infrastruktur abhängig.

Die Versorgung mit wesentlichen Dienstleistungen und Gütern ist größtmöglich sicherzustellen, denn temporäre Störungen oder längerfristige Ausfälle hätten rasche und unmittelbare Auswirkungen auf die Wirtschaft und die Bevölkerung. Diese Aufgabe kann nur in einer engen und vertrauensvollen Zusammenarbeit zwischen den staatlichen Stellen und den Betreibern kritischer Infrastrukturerfolgreich erfüllt werden.

Die Gesundheitsversorgung ist dabei ein wesentlicher Eckpfeiler – dementsprechend zählen neben Pharmazieherstellern, Pharmaziegroßhändlern und Rettungsorganisationen insbesondere Krankenhäuser zur kritischen Infrastruktur, für deren vorbeugenden Schutz die Sicherheitsbehörden gem. § 22 Sicherheitspolizeigesetz (SPG) zuständig sind.

Für die operative Umsetzung von Schutzmaßnahmen ist für das Bundesministerium für Inneres das BVT gemeinsam mit den LVT der Landespolizeidirektionen zuständig.

2018 wurde die Workshop-Reihe „Schützenswertes Krankenhaus“ gestartet, die 2019 auch für den österreichischen Sicherheitspreis unter den Top 3 nominiert war. Für die Workshops wurden mehrere Szenarien als relevant identifiziert und als Grundlage herangezogen:

Cyber-Sicherheit im Krankenhaus

Krankenhäuser sind eine der tragenden Säulen des Gesundheitswesens in unserem Land. Die Mitarbeiterinnen und Mitarbeiter in Krankenhäusern erbringen täglich für die Gesellschaft wesentliche Hilfeleistungen in medizinischen und pflegerischen Aufgabenbereichen. Diese Tätigkeiten unterliegen einer Reihe von Abhängigkeiten. So ist das Krankenhaus als kritische Infrastruktur selbst auf andere Einrichtungen der kritischen Infrastruktur, wie beispielsweise die Energie- und Wasserversorgung, angewiesen. Gleichzeitig besteht jedoch auch eine permanent wachsende Abhängigkeit von der IKT-Infrastruktur und den damit verbundenen Dienstleistungen.

Vor diesem Hintergrund muss beachtet werden, dass seit mehreren Jahren das Gesundheitswesen im allgemeinen sowie Krankenhäuser im speziellen immer stärker in den Fokus der internationalen Cyber-Kriminalität rücken. Eine Studie eines renommierten internationalen Cyber-Sicherheitsunternehmens hat aufgezeigt, dass im Jahr 2018 das Gesundheitswesen derjenige Sektor kritischer Infrastruktur war, der weltweit am häufigsten mit Cyber-Angriffen aller Art konfrontiert war.

Als Beispiel für diese Entwicklungen können Ransomware-Angriffe angeführt werden. Während diese Angriffsart in den vergangenen Jahren durch ungezielte, breit gestreute Kampagnen aufgefallen war, zeigt sich mittlerweile eine starke Tendenz zu spezialisierten Ransomware-Angriffen („targeted ransomware“). Die Angreifer versuchen nicht mehr, ihre Einkünfte durch möglichst viele, dafür geringe Lösegeldforderungen zu maximieren,

stock.adobe.com

sondern attackieren gezielt wenige große Opfer mit entsprechend hohem Schadenspotenzial und ungleich höheren finanziellen Möglichkeiten. Im Fokus der Angreifer stehen dabei immer häufiger auch medizinische Einrichtungen wie Krankenhäuser.

Vor allem auf diesen Überlegungen basiert die Initiative des BVT, im Rahmen des Projekts „Schützenswertes Krankenhaus", der Cyber-Sicherheit und der Resilienz von Krankenhäusern in Österreich maßgeblichen Raum bei den entsprechenden Workshops zu geben. So sind vor allem PatientInnendaten ein besonders wertvolles Gut im Gesundheitswesen, weshalb ihr Schutz höchste Priorität erfordert. Gleichzeitig darf nicht vergessen werden, dass Mitarbeiterinnen und Mitarbeiter in Krankenhäusern nicht nur beruflich, sondern auch privat von Cyber-Angriffen gefährdet sind. Ein umfassender Ansatz war daher das Gebot der Stunde.

Bei Cyber-Angriffen auf Gesundheitseinrichtungen sind auf Basis aktueller Untersuchungen mittlerweile alle drei sogenannten Schutzziele der Informationssicherheit betroffen.

- Unter Vertraulichkeit von Daten versteht man, dass gespeicherte Daten nur von demjenigen Personenkreis eingesehen werden darf, der dazu explizit berechtigt ist. Diebstahl und Handel mit diesen Gesundheits- und PatientInnendaten entwickeln sich immer mehr zu einem lukrativen Verbrechenszweig.
- Die Integrität von Daten bedeutet, dass sichergestellt sein muss, dass Daten niemals unbemerkt verändert bzw. manipuliert werden können. Mitarbeiterinnen und Mitarbeiter in Krankenhäusern müssen sich darauf verlassen können, dass die gespeicherten PatientInnendaten korrekt sind. So stellt die unbemerkte Manipulation dieser Daten ein großes Potenzial für Sabotage- oder Erpressungsaktivitäten gegenüber Krankenhäusern dar.
- Die Verfügbarkeit von Daten oder Geräten bedeutet, dass dem Krankenhauspersonal die Gesundheitsdaten, aber auch wichtige, IKT-gestützte medizinische Geräte uneingeschränkt zur Verfügung stehen müssen. Auch hier besteht erhebliches Potenzial für Sabotage- oder Erpressungsaktivitäten.

Ein wesentlicher Schwerpunkt der Cybersicherheits-Workshops mit dem medizinischen und pflegerischen Personal war es, innerbetriebliche Abhängigkeiten von der IKT-Infrastruktur herauszuarbeiten. Dabei stellte sich heraus, dass im modernen Krankenhausbetrieb nahezu alle medizinischen Prozesse mittelbar oder unmittelbar von einer funktionierenden IKT-Umgebung abhängig sind. Gleich, ob es sich um intensivmedizinische Geräte, um die Datenhaltung, um die bildgebende- oder Labordiagnostik oder die Klima- und Haustechnik handelt, überall sind entsprechende Anhängigkeiten gegeben, die beachtet werden müssen. Dabei ist entscheidend, dass die Krankenhäuser die betriebskritischen Prozesse identifizieren und für diese Notfallkonzepte für IKT-Ausfallszenarien – auch längerer Dauer – entwickeln und regelmäßig beüben. Entscheidend

dabei ist auch eine Bewertung, inwieweit die Anwendung von alternativen Prozessen die Gesamtleistungsfähigkeit negativ beeinflusst.

Das häufigste initiale Angriffsziel eines Cyber-Angriffs sind nicht technische Einrichtungen, sondern die Mitarbeiterinnen und Mitarbeiter des Krankenhauses. Aus diesem Grund wurde ein weiterer, zentraler Schwerpunkt auf das Erfordernis gerichtet, dass parallel zum Einsatz technikbasierter Cyber-Sicherheit, der Bewusstseinsbildung der Mitarbeiterinnen und Mitarbeiter („Cyber-Awareness") größtmöglicher Stellenwert beizumessen ist. Diesbezügliche Maßnahmen verfolgen den Ansatz, dass entsprechend vorbereitete und geschulte Mitarbeiterinnen und Mitarbeiter durch das Bewusstsein in Bezug auf mögliche Bedrohungen sowie dementsprechende Aufmerksamkeit und durch richtige Reaktion, potenzielle Cyber-Angriffe erkennen und bereits verhindern können, bevor ein Schaden entsteht. Wesentliche Elemente aus diesem Bereich umfassen beispielsweise die Wahl geeigneter Kennwörter, das Erkennen „bösartiger" E-Mails oder den richtigen Umgang mit externen Datenträgern.

Abschließend wurde auch ein Appell an das Management der jeweiligen Gesundheitseinrichtungen gerichtet. Cyber-Sicherheit erfordert ein unbedingtes Bekenntnis der Führungsebene. Cyber-Sicherheit kann nicht verordnet werden („fire and forget"), sondern muss fest in der Organisationskultur verankert und tagtäglich von allen Beteiligten gelebt werden.

Objektschutz von Krankenhäusern

Krankenhäuser sind Orte, an denen wiederholt strafbare Handlungen begangen werden, wie beispielsweise Diebstahl, Vandalismus, Bombendrohungen, gewalttätige Handlungen gegen medizinisches Personal, PatientInnen oder BesucherInnen. Im Krankenhausbereich zielt der Objektschutz auf die Abwehr oder Verhinderung der Zerstörung, einer Beschädigung bzw. einer Beeinträchtigung der Funktionalität von sensiblen Einrichtungen ab. Die Sicherheitsmaßnahmen wie z. B. bauliche und sicherheitstechnische Vorkehrungen sind regelmäßig zu evaluieren.

Das Thema Sicherheit in Krankenhäusern umfasst nicht nur Personen, sondern auch Technik, Gebäude, Liegenschaften und Medizinprodukte. Ein umfassendes Sicherheitsmanagement/Risikomanagement kann ein systematisches Erkennen, Analysieren, Bewerten, Überwachen und Kontrollieren sicherstellen. Empfohlen werden technische, personelle und organisatorische Maßnahmen wie z. B. ein adäquater Perimeterschutz, der bestimmten baulichen Voraussetzungen entsprechen, mittels Videoüberwachung ergänzt werden, die äußere Umschließung des KH-Geländes vor unbefugtem Betreten schützen und den Personen- und Fahrzeugverkehr über kontrollierte Zugangs- bzw. Zufahrtsstellen leiten sollte.

Auch die Schließsysteme sollten dem aktuellen Stand der Technik entsprechen. Das Schließen der Türen (kein „Raucherkeil“) oder das Ansprechen von unbekannten Personen in kritischen Bereichen einer Klinik, fordert eine regelmäßige Sensibilisierung der Mitarbeitenden ein. Regelmäßige Deeskalations- und Verhaltenstrainings im Umgang mit aggressiven Personen sollten für das Personal durchgeführt werden, ebenso sollten aus datenschutzrechtlichen Gründen Film- und Fotografierverbote bestehen, Telefonie und Waffenverbote deutlich aufgezeigt sowie Besuchszeiten auch aus Sicht der Sicherheit nicht allzu moderat gehandhabt werden. Piktogramme erweisen sich in vielen Fällen als nützliche Hilfsmittel, um solche Verbote bekanntzumachen und die Hausordnung durchzusetzen.

Ab einer gewissen Krankenhausgröße (z. B. 500 Betten) wäre eine Ausstattung mit einer Sicherheitszentrale, mit ausgebildetem Sicherheitspersonal, Videoübertragungen und Alarmierungen inklusive Notfallbutton empfehlenswert, damit Vorfälle gebündelt an einer Stelle erfasst, ausgewertet und mit Maßnahmensetzungen durch die Mitarbeitenden behandelt werden können.

Medizinischer Krisen- und Katastrophenschutz

Das Risiko besteht hierbei in einem Massenanfall an Patientinnen und Patienten nach einem Großschadensereignis oder im Falle einer Massenerkrankung. Der Blick richtet sich dabei von der alltäglichen Arbeit in einem Krankenhaus auf die besonderen Herausforderungen, die bei Großschadensereignissen wie Naturkatastrophen oder Terroranschlägen auf Krankenhausbetriebe zukommen können.

Die Folgen derartiger Ausnahmesituationen können vielfältig sein und sich z. B. dahingehend zeigen, dass Mitarbeitende ausfallen und somit keine adäquate PatientInnenbetreuung mehr möglich ist. Auch Verletzte, die aus eigenem in die Notaufnahme eines Krankenhauses kommen oder ein zu erwartender Ansturm von Angehörigen, sind mögliche Szenarien.

Darüber hinaus können andersgeartete Verletzungsmuster auftreten, deren Behandlungen bereits im Vorfeld gezielte Schulungen einfordern. Das wesentliche Element aller Szenarien ist die Herausforderung der Weiterversorgung der PatientInnen. Daher wäre eine ausreichende Krisenbevorratung mit Medikamenten, medizinischem Equipment wie z. B. Schutzausrüstungen, Sterilgut, Lebensmitteln, Wäsche, Diesel für die Notstromaggregate etc. anzuraten.

Sonstige Risiken

Neben den zuvor genannten Risiken wurden auch der Ausfall der Energie- oder Wasserversorgung, der Eintritt sicherheitspolizeilicher Lagen sowie die Abhängigkeiten von

anderen Bereichen der Daseinsvorsorge, insbesondere erforderliche Zulieferketten und deren Resilienz, untersucht und Maßnahmen abgeleitet.

Auf diesen Szenarien basierend, verfolgen die Workshops das Ziel der Sensibilisierung der Mitarbeiterinnen und Mitarbeiter in Krankenhäusern sowie die Entwicklung von Mindestsicherheitsstandards in den Bereichen Cyber-Sicherheit, Objektschutz und medizinischer Krisen- und Katastrophenschutz, unter Berücksichtigung des vorbeugenden Schutzes, der Abwehr und der Widerstandsfähigkeit.

Im Jahr 2019 wurden durch das BVT insgesamt 29 Begehungen in Krankenhäusern sowie zehn Workshops zu den genannten Themen organisiert und abgehalten. Weitere Workshops sollen in den Jahren 2020 und 2021 stattfinden.

4 General Situation Report

Islamist extremism and terrorism

As in previous years, Islamist extremism posed a continuing and increased threat for Austria as well as for other European and non-European countries in 2019. The representatives of the Salafist and Jihadist environments, whose mobilisation potential is still relatively high, continue to be the central actors in this field.

The number of attacks continues to decrease — a trend that has been evident across Europe since 2018. Nevertheless, attacks based on Jihadist motives continue to pose one of the greatest challenges for Europe and Austria in terms of security.

The Islamic State (IS) not only lost a large number of fighters and leading cadres, but also almost all of the territories they controlled in Syria and Iraq. The IS is primarily a network operating in secret, with various regional branches around the world. Al-Qaeda (AQ), the origin of global Jihad, also still has members and active branches worldwide.

In the last years, the phenomenon of Jihad travellers (Foreign Terrorist Fighters, FTF) has had a major influence on the security situation in Austria and across Europe. Due to their military training combined with the experience they gained in combat, they pose a threat potential that is difficult to predict. The number of departures from Austria has continuously decreased since 2015 and the number of returnees has gone down considerably. Islamist ideologies will keep their appeal and attractiveness and will continue to do so in future. The religious and political narrative of a "caliphate" will continue to exist even after the military defeat of the IS. The underlying ideologies will persist regardless of the governing organisations and will continue to exert considerable influence on the way radicalised Islamists think and act.

The trend of using rather simple means to carry out attacks will most likely continue. In the homegrown scene, local Islamist groups and networks will persist, both in Austria and in other European countries. Social media and relevant online forums will continue to play a vital role in radicalisation, as special Islamist content can be accessed in these online communities and forums. In this context, the threat potential emanates from radicalised single perpetrators and potential copycat perpetrators. Most likely, Islamist attacks carried out by radicalised single perpetrators or small groups acting autonomously will continue to present a high risk in Austria and Europe.

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 autono-

mous-anarchist groups and the Communist cadre organisations meet with little public response and only have few members.

In 2019, the autonomous-anarchist groups were the most active ones in the scene. Their activities, rallies and protests – mainly actions that can be subsumed under the general term of "anti-fascism" – occasionally also resulted in violence.

Due to their restricted range of influence and their limited means, and despite evident animosities and considerable ideological differences, left-wing extremist activists from different groups are prepared to cooperate on certain occasions and on a temporary basis. Events such as the Vienna Academics' Ball (Wiener Akademikerball, WAB) are traditionally used for anti-fascist mobilisation and actions. In 2019, these events were again accompanied by protest rallies, in which groups and advocates of the left-wing extremist scene participated. Left-wing extremist activists were also noticed around some events of German nationalist fencing fraternities, holding protests against a grouping of the "New Right", against hostility towards asylum seekers and xenophobia. Several demonstrations were accompanied by disruptive actions and blockade attempts. In individual cases, the events resulted in violence.

However, it has to be noted that in 2019, the majority of anti-fascist demonstrations, which were organised by groups/advocates of the left-wing extremist spectrum and were attended by representatives of this scene, took place without causing any incidents relevant to the state police.

In 2019, a total of 218 criminal acts with proven or suspected left-wing extremist motivation were recorded (2018: 137 criminal acts). One of these criminal acts may comprise several offences, which are separately reported to the authorities. Out of those, 25 criminal acts (11.5 percent) were successfully investigated. A total of 311 complaints were filed in connection with the criminal offences mentioned above (2018: 237 reports), 264 of them under the Austrian Penal Code (StGB).

Right-wing-extremism

The right-wing extremist scene in Austria has a heterogeneous structure. Both regarding its ideology and its external appearance it becomes evident 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. The heterogeneous structure and the differences in the ideological orientation are often quite obvious within the scene. 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.

They all share common narratives which dominate the current right-wing extremist scene, such as “displacement”, “over-foreignisation” and “infiltration of the own people” by individuals they perceive as foreign. From the right-wing extremists’ point of view, the ruling elites are the ones to be held responsible for these things. There are clearly visible parallels to the dominant focus of agitation of the „Great Replacement“, as propagated by the New Right. Alongside with the formulation of a narrative thematising the “displacement of the autochthonous population”, the right-wing extremist scene creates a doomsday scenario one has to prepare for (e.g. by practicing martial arts). Right-wing extremist violence, aggression and agitation entail a potential risk of disturbing public peace, order and security in Austria.

In 2019, the Austrian security authorities registered a total of 954 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 2018 (1,075 offences), the number decreased by 11.3 percent. Out of these, 645 criminal acts (67.6 percent) were successfully investigated. In 2018, the rate of successfully solved cases amounted to 63 percent. In connection with the criminal offences mentioned, 1,678 offences were reported in Austria in 2019, which is 3.5 percent more than in 2018 (1,622 offences).

In conclusion, it is noted that the topics of “anti-Islam”, “anti-multiculturalism” as well as asylum and refugees continue to be a central focus of agitation and action, in both the virtual and the real world of the right-wing extremist scene in Austria.

Intelligence services and counter intelligence

Intelligence actors operate both in Austria and against Austrian interests. Among other things, this attractiveness is due to the fact that Austria is an important business location, that it is a member of the European Union and that many international organisations are based in Vienna. Intelligence activities can mainly be divided into the categories of influence and information procurement.

All areas of politics and society can be targets of influence. 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.

For example, information procurement aims at obtaining political and technological secrets, or is directed against the diaspora of foreign states or members of the opposition residing in Austria.

Diplomatic representations in Austria play an essential role when it comes to implementing these activities. They serve as a place intelligence agents can operate from in disguise and with diplomatic immunity. In addition, there are other state-affiliated organisations, such as airlines, news agencies or cultural associations, which serve as covers for these persons.

In the age of digitalisation, intelligence actors have increasingly started to exert influence and to procure information through cyber-attacks against sensitive and critical devices, through cyber espionage and by conducting misinformation campaigns, such as the spreading of fake news via online platforms or social media.

Cyber security

In 2019, a continued increase in cyber crime cases and cyber attacks against providers of critical infrastructures and on constitutional institutions was witnessed in Austria as well as in the pan-European context. There were cases of spying (espionage), alteration of data (disinformation) and temporary blocking of entire computer systems (sabotage), however, it is assumed that there is a much higher additional number of undetected or unreported cases.

The focus was on attempted extortion through blocking systems using encryption software (ransomware) and subsequent ransom demands. Placement of malware via phishing e-mails containing the Trojan EMOTET became a growing challenge, in particular for small and medium-sized companies in Austria. Distributed Denial of Service (DDoS) attacks impaired the operability of entire systems, such as parts of the online sales infrastructure of the Austrian Federal Railways (ÖBB), the website of the City of Vienna as well as the local electoral office responsible for voting cards of the City of Vienna in the run-up to the elections to the European Parliament in May 2019.

A further threat lies in cyber espionage directed against institutions of public administration and companies via Advanced Persistent Threats (APT). The EU delegation in Moscow was the target of such an attack. Furthermore, in the beginning of 2019, an attack against the common COREU/CORTESY network of the EU had to be stopped. In the summer of 2019, unauthorised access to the network infrastructures of two Austrian parties and one ministry, including partial data leakage, was detected. By the end of 2019, an attack targeting the Federal Ministry for European and International Affairs (BMEIA) was fended off in a joint initiative of the Ministry of the Interior (BMI), the

Austrian Federal Chancellery (BKA), the Federal Ministry for European and International Affairs (BMEIA) and the Federal Ministry of Defence (BMLV). The affected IT systems were cleansed by 10 February 2020.

Beyond that, there were cases of cyber fraud e.g. by the use of fake websites (defacement), as well as the illicit publication of sensitive personal data, access data and passwords on the internet (leak). Among the particularly sensitive issues are increasing possibilities of espionage and sabotage of daily routine activities via technical devices using the Internet of Things (IoT). In addition, the security of the "fifth generation" of mobile networks (5G) was in the focus of attention of cyber security authorities in 2019. For this reason, the European Union published a coordinated risk analysis on the situation in the individual member States in October 2019.

However, in the field of cyber security, the password has remained the most important cause for concern. Establishing an additional multi-factor authentication (MFA) would be the best support in this context. Security flaws such as BLUEKEEP or FORESHADOW, which exist in commonly used operating systems and are not always closed, can be gateways for attacks. The growing trend of outsourcing formerly device-based services to cloud services is presumably attractive for cyber criminals. For this reason, it is of highest priority to establish specific security measures in this field.

In order to defend Austrian critical infrastructures (energy, transport, banking and finance, healthcare, drinking water supply, digital infrastructures) against attacks, cyber security relies on a high common security level of networks and information systems on a national level. In the last years, a corresponding directive issued by the European Union was implemented step-by-step. With the Austrian Law on Network and Information System Security (NISG), which became effective in the beginning of 2019, this directive gained a legal basis.

5 Abkürzungs-verzeichnis

AbzG	Abzeichengesetz
AEC	Austrian Energy Cert
ATP	Advanced Persistent Threats
AQAP	Al-Qaida auf der Arabischen Halbinsel
AQIM	Al-Qaida im Islamischen Maghreb
BMLV	Bundesministerium für Landesverteidigung
BNED	Bundesweites Netzwerk Extremismusprävention und Deradikalisierung
BVT	Bundesamt für Verfassungsschutz und Terrorismusbekämpfung
CERT	Computer Emergency Response Team
CKM	Cyber-Krisenmanagement
CSIRT	Computer Security Incident Response Team
CSC	Cyber Security Center
DDoS	Distributed Denial of Service
EGVG	Einführungsgesetz zu den Verwaltungsverfahrensgesetzen
ESU	Extended Security Update
EU	Europäische Union
FinCERT	Finanzdienstleister Computerteam
FMA	Finanzmarktaufsicht
FTF	Foreign Terrorist Fighters
GASP	Gemeinsame Außen- und Sicherheitspolitik
IKDOK	Innerer Kreis der operativen Koordinierungsstrukturen
IoT	Internet-of-Things
IS	Islamischer Staat
KI	Künstliche Intelligenz
KMU	Kleine und mittlere Unternehmen
KSÖ	Kuratorium Sicheres Österreich
ML	Maschinelles Lernen
NIS	Netz- und Informationssystemsicherheit
NISG	Netz- und Informationssystemsicherheitsgesetz
NSDAP	Nationalsozialistische Deutsche Arbeiterpartei
OATC	One-Time Authorization Codes
RPD	Remote-Desktop-Protocol
SKI	Schutz kritischer Infrastruktur
S-LSG	Salzburger Landessicherheitsgesetz
SMG	Suchtmittelgesetz
SPG	Sicherheitspolizeigesetz
StGB	Strafgesetzbuch
TLPolG	Tiroler Landespolizeigesetz
VerbG	Verbotsgesetz
VersG	Versammlungsgesetz
WAB	Wiener Akademiker Ball
WaffG	Waffengesetz
WKR	Wiener Korporations-Ring