Spionageabwehr / Proliferation / Elektronische Angriffe

7. Spionageabwehr / Proliferation / Cyberabwehr

7.1 Spionageaufkommen in Niedersachsen

Als Teil der jeweiligen Sicherheitsarchitektur verfügen zahlreiche Staaten über Nachrichtendienste, die Informationen auch mit nachrichtendienstlichen Mitteln sammeln und auswerten. Insbesondere totalitäre Staaten verfügen über Geheimdienste, die auch aktiv Maßnahmen ergreifen, z. B. politisch Einfluss nehmen, Sabotage betreiben oder Attentate verüben. Bei manchen Geheimdiensten kommen auch paramilitärische Abteilungen zur Durchführung von geheimen Kommandounternehmungen zum Einsatz. Heute wird die klassische Spionage als Phänomen aus vergangenen Zeiten betrachtet, aber auch in unserer „digitalen" Zeit mit weltweiter Datenvernetzung und schnell voranschreitenden technischen Entwicklungen werben ausländische Nachrichtendienste menschliche Quellen an.

In der Bundesrepublik Deutschland sind der Auslandsnachrichtendienst (BND), der Inlandsnachrichtendienst (Verfassungsschutz) sowie der militärische Nachrichtendienst (BAMAD) mit der Informationsbeschaffung betraut.

Nachrichtendienste unterliegen in Rechtsstaaten einer Fach- und Rechtsaufsicht durch die vorgesetzten Dienststellen, weil Nachrichtendienste, wie alle staatliche Gewalt, an Recht und Gesetz gebunden sind. Infolge ihrer verdeckten Arbeitsweise und des häufig regen Interesses von Regierungsstellen an der Informationsgewinnung wird eine Aufsicht durch Exekutivbehörden selbst oftmals nicht als hinreichend erachtet. Die Kontrolle wird daher durch parlamentarische Gremien ergänzt. Diese kann dann durch Debatten, Aktuelle Stunden oder durch parlamentarische Anfragen in und aus den jeweiligen Parlamenten erfolgen.[202]
Das Sachgebiet Spionageabwehr im Niedersächsischen Verfassungsschutz hat den gesetzlichen Auftrag, alle Informationen über sicherheitsgefährdende oder geheimdienstliche Aktivitäten zu erheben

202 Siehe dazu auch Kapitel 1.6.

und Spionage sowie Proliferation[203] zu verhindern. Da Niedersachsen als erfolgreicher Wirtschaftsstandort potenzielles Ziel von Spionageaktivitäten fremder Geheim- oder Nachrichtendienste[204] ist, gilt es, ihn vor derartigen Aktivitäten zu bewahren. Zudem geht es darum, den Schutz der in Niedersachsen lebenden Bürgerinnen und Bürger zu gewährleisten. Die im Folgenden aufgeführten Beispiele sollen zu einer Sensibilisierung der Bürgerinnen und Bürger, aber auch der niedersächsischen Wirtschaft beitragen.

Hauptakteure der klassischen Spionageaktivitäten in der Bundesrepublik Deutschland sind nach wie vor die Russische Föderation, die Volksrepublik China, der Iran, aber in Teilen auch die Türkei. Die Schwerpunkte dieser Länder orientieren sich an den politischen Vorgaben und wirtschaftlichen Prioritäten.

Aufgrund desolater Sicherheitslagen in ihren Heimatländern und damit verbundener existenzieller Bedrohungen, sucht eine große Zahl von Menschen Zuflucht und Schutz in Europa. Insbesondere Deutschland ist Ziel von Flüchtlingsbewegungen, die ihren Ursprung vor allem in Afghanistan, im Irak, in Syrien sowie in der Ukraine, aber auch in den Ländern Zentral- und Westafrikas haben. Mit der sich vergrößernden Exilgemeinde ist die Ausforschung oppositioneller Aktivitäten zur wichtigen Zielvorgabe für fremde Dienste in Deutschland geworden.
Fremde Geheim- oder Nachrichtendienste sind in unterschiedlicher Personalstärke u. a. an den jeweiligen amtlichen Vertretungen (z. B. Botschaften, Generalkonsulate = Legalresidenturen) in Deutschland präsent und unterhalten dort Stützpunkte. Geheim- und Nachrichtendienstmitarbeitende können dort, als Diplomatinnen und Diplomaten getarnt, tätig werden und Informationen beschaffen, oder sie leisten Unterstützung bei geheimdienstlichen Operationen ihrer Zentralen.
Eine Vielzahl von Informationen, die für fremde Geheim- oder Nachrichtendienste interessant erscheinen und früher nur mit klassischen

203 Proliferation ist die Weiterverbreitung von ABC-Waffen und Trägersystemen; siehe auch Kapitel 7.2.

204 Im Gegensatz zu Geheimdiensten unterliegen Nachrichtendienste einer rechtsstaatlichen Kontrolle und haben keine polizeilichen Befugnisse. Die deutschen Verfassungsschutzbehörden sind demnach Nachrichtendienste. Siehe dazu auch Kapitel 1.7.

Spionagetätigkeiten zu erheben waren, sind heutzutage mit relativ geringem technischen Aufwand und fast ohne Risiko auf virtuellem Wege zu erlangen. Zum Teil ist aufgrund bestimmter Parameter (z. B. welcher Angriffsweg und welche Infrastruktur genutzt werden), auch von einer geheim- oder nachrichtendienstlichen bzw. staatlichen Beteiligung auszugehen.

Vor dem Hintergrund insbesondere des russischen Angriffskrieges gegen die Ukraine erlebt die klassische Spionage gewissermaßen eine „Renaissance" nach dem Ende des „Kalten Krieges". Im Umkehrschluss bedeutet dies insoweit jedoch nicht, dass die klassischen Spionageaktivitäten ausgedient haben. Entsprechende Verdachtsfälle sind im Fachbereich Spionageabwehr im Niedersächsischen Verfassungsschutz auch im Jahr 2023 bekannt geworden.

Nachfolgend werden exemplarisch einige Bearbeitungsschwerpunkte der niedersächsischen Spionageabwehr im Berichtszeitraum dargestellt.

Logo des SWR

Russland

Der russische Auslandsnachrichtendienst nennt sich Sluschba wneschnei raswedki (SWR, auch SVR, Dienst der Außenaufklärung der Russischen Föderation). Seine Aufgabe ist es, Informationen in den Bereichen Politik, Technologie, Wirtschaft und Wissenschaft zu beschaffen, um sie sowohl für die Politik als auch die Wirtschaft in Russland nutzbar zu machen.

Einflussnahme und Desinformation

Über seine Spionageaktivitäten hinaus ist Russland bestrebt, Einfluss auf die öffentliche Meinungsbildung und den politischen Diskurs in Deutschland auszuüben. Die Einflussnahme erfolgt sowohl durch staatliche Stellen wie auch durch Einzelpersonen über soziale Netzwerke, Institute, Organisationen und russische Staatsmedien. Oft wird versucht, die wahren Urheber durch Fake-Profile und Social Bots zu verschleiern.

Jede Zielgruppe wird gezielt angesprochen. Dafür werden ganz unterschiedliche Instrumente und Kanäle benutzt. Die Verbreitung russlandfreundlicher Narrative findet über die offiziellen Kanäle statt, dazu gehören z. B. auch Verlautbarungen des Präsidenten selbst oder des Außenministeriums, über die Staatsmedien, die staatsnahen Informationsportale sowie über soziale Medien. Über diese Kanäle verfolgt Russland das Ziel, Ängste und Sorgen z. B. vor Lebensmittel- und Energieknappheit der deutschen Bevölkerung zu schüren und anzuheizen.

Diese Aktivitäten zielen u. a. darauf ab, das Vertrauen der Bevölkerung in die Stabilität und Handlungsfähigkeit der demokratischen Institutionen und Mechanismen zu untergraben, die westliche Wertegemeinschaft zu diskreditieren und Bündnisse wie EU sowie NATO zu schwächen.

Die öffentliche Meinung soll im Sinne Russlands beeinflusst und die eigene Machtposition gestärkt werden. Dafür werden auch aktuelle politische und gesellschaftliche Ereignisse sowie Entwicklungen aufgegriffen. So berichten russische Staatsmedien immer wieder einseitig über Demonstrationsgeschehen auch in Deutschland. Insbesondere bei der Berichterstattung über Demonstrationen gegen den Ukraine-Krieg versucht Russland über die Verbreitung von Narrativen sein Handeln gegenüber seiner eigenen Bevölkerung und der russischsprachigen Diaspora im Ausland zu rechtfertigen, aber auch, um in der deutschen Bevölkerung Zweifel an der Regierungsfähigkeit der Bundesregierung zu schüren. Auf diese Weise kann mittelbar auf die Meinungsbildung und möglicherweise auf das Wahlverhalten der Bevölkerung in Deutschland Einfluss genommen werden. Nicht Kreml-genehme Berichterstattung wird in Russland unter Strafe gestellt.

Vor dem Hintergrund des russischen Angriffskrieges gegen die Ukraine wurden im Verfassungsschutzverbund daher gemeinsame Anstrengungen unternommen, um die mit diesem Konflikt in Zusammenhang stehenden nachrichtendienstlichen Aktivitäten, Cyberoperationen sowie Propaganda-, Desinformations- und Einflussnahmeaktivitäten in Deutschland zu beobachten und aufzuklären. Es besteht ein intensiver Austausch zwischen den Sicherheitsbehörden des Bundes und der Länder. Im besonderen Fokus stehen dabei die Desinformations- und Propagandaaktivitäten russischer Akteure. Nach einer Analyse des Institute for Strategic Dialogue (ISD) nutzen russische Staatsmedien, wie RT, angebliche „Faktenchecks", um deutsche „Desinformation" über Gaslieferungen aufzuzeigen. Kremlnahe Social Media-Accounts verbreiten ein inszeniertes Telefongespräch zwischen dem ukrainischen Präsidenten Selenskyj und seiner Frau, in dem der amerikanische Präsident Biden und Bundeskanzler Scholz verbal beleidigt werden. Die Verbreitung des gefälschten Telefonats soll Selenskyjs Besuch in Washington untergraben und Ressentiments gegenüber der Ukraine bei den westlichen Verbündeten schüren.

In Bezug auf die Debatten um die Haushaltsaufstellung 2024 in Deutschland nehmen russische Narrative zu einer instabilen politischen Lage in Deutschland zu. Kreml-nahe Medien berichten, in Deutschland würde ein neuer „Schattenkanzler" entstehen. Demnach würde „Der Finanzminister Christian Lindner ein Schattenkanzler werden, da die Mittel der Bundeskasse unter seiner Kontrolle stehen." Ferner wird die angespannte Haushaltssituation in Verbindung mit den deutschen Unterstützungsleistungen für die Ukraine gebracht, um das bekannte Narrativ zur abnehmenden westlichen Unterstützung der Ukraine weiter zu verbreiten.

Das auf Desinformation spezialisierte sogenannte Komikerduo „Vovan und Lexus" hat Ausschnitte aus einem Fakeanruf mit Bundeswirtschaftsminister Robert Habeck auf Social Media-Kanälen veröffentlicht. Ziel war es, Robert Habeck zu einem ukraine-kritischen Statement zu bewegen - was in diesem Fall nicht gelang. Russische Staatsmedien greifen die Fakeanrufe auf, um Deutschland zu diskreditieren. Demnach sei Robert Habeck „entgegen einer Warnung deutscher Geheimdienste auf den Prank reingefallen".

Für die Erkennung und Einordnung von Risiken sowie die Bewältigung von Herausforderungen, die eine illegitime Einflussnahme fremder Staaten auf Bund, Länder und Kommunen nach sich zieht sowie für eine wirksame Prävention, ist ein koordiniertes, gesamtstaatliches Zusammenwirken unerlässlich.

Russischer Motorradclub Night Wolves

Bei dem Motorradclub Night Wolves (Nachtwölfe) handelt es sich um den 1989 gegründeten größten Motorrad- und Rockerclub Russlands. Die Mitglieder vertreten nationalistische und christlich-orthodoxe Ansichten. Seit 2009 pflegen der Präsident der Night Wolves und der Russische Staatspräsident, Wladimir Putin, einen guten Kontakt. Seit mehreren Jahren gedenkt der Club am 9. Mai, dem „Tag des Sieges", mit Fahrten und Kranzniederlegungen den Opfern des Zweiten Weltkrieges. Abschluss und Höhepunkt der Fahrten sind die Veranstaltungen zur Erinnerung an das Kriegsende am Sowjetischen Ehrenmal in Berlin-Treptow.
Der Motorradclub ist in Chaptern organisiert. Im Jahr 2023 wurde ein Chapter in Deutschland gegründet. Geführt wird dieses durch das russische „Motherchapter" „ROSSIJA".
Aufgrund der Nähe zum russischen Präsidenten Putin liegt die Vermutung nahe, dass die Night Wolves politische Ziele Putins unterstützen und in seinem Auftrag handeln. Durch ihr medienwirksames Auftreten signalisieren sie Zustimmung für die russische Politik und könnten damit Einfluss auf die politische Meinungsbildung in Deutschland nehmen.

China

Um ihren Machtanspruch zu sichern und die wirtschaftlichen Ziele erreichen zu können, setzt auch die Volksrepublik China Geheimdienste ein. Von den vier chinesischen Geheimdiensten ist insbesondere das chinesische Ministerium für Staatssicherheit (MSS) für die Auslandsaufklärung zuständig. Es gilt als weltweit größter ziviler Geheimdienst.

Logo des MSS

Wesentliche Strategien chinesischer Nachrichtendienste

Die Volksrepublik China bedient sich ihrer Nachrichtendienste als Mittel zum Regimeerhalt. Übergeordnetes Ziel allen nachrichtendienstlichen Handelns ist die Aufrechterhaltung des Machtanspruchs

der Kommunistischen Partei Chinas (KPCh). China strebt eine aktive Gestaltung der internationalen Ordnung an und propagiert offen das Ziel, im Jahr 2049 – dem 100. Gründungsjahr der Volksrepublik – wirtschaftlich wie militärisch global führend zu sein. Um dieses Ziel zu erreichen, besteht ein allumfassender Informationsbedarf, den China offensiv auch mit nachrichtendienstlichen Mitteln deckt. Zu den wesentlichen nachrichtendienstlichen Akteuren zählen der nichtmilitärische In- und Auslandsnachrichtendienst MSS[205], der militärische Nachrichtendienst MID[206], das MÖS[207] sowie der technisch-militärische Nachrichtendienst NSD[208].

Gegenwärtig räumen chinesische Nachrichtendienste – neben den Themen um die Belt-and-Road-Initiative[209] – insbesondere den Entwicklungen im Sektor der Informationstechnologie (Cloud, Internet of Things, Quantentechnologien, Robotik sowie der 5G-Technologie) höchste Priorität ein. Dabei setzen die Dienste auch ausgeklügelte und technologisch anspruchsvolle Cyberoperationen zur Gewinnung von technologischem Know-how (auch für den eigenen Entwicklungsbedarf) ein.

Die Ziele chinesischer Spionage werden nach einer Nutzenkalkulation ausgewählt. Beabsichtigt wird vor allem der Vorteil für die eigene Nation durch Informationsgewinnung und -beschaffung. Die Schädigung des Gegners wird von den chinesischen Diensten als zweckdienliches Mittel in Kauf genommen, ist aber als solches oft selbst nicht Ziel des nachrichtendienstlichen Handelns.

China hat sich in Bezug auf den Ukraine-Krieg diplomatisch an die Seite Russlands gestellt. Das Land hat jedoch betont, dass es eine neutrale Position einnehme und sich für eine friedliche Lösung des Konflikts einsetze. Die Weigerung Chinas, den Angriffskrieg

205 Ministerium für Staatssicherheit = Inlandsnachrichtendienst mit Exekutivbefugnissen, Schwerpunkt: Beobachtung oppositioneller Bestrebungen.

206 Militärischer In- und Auslandsnachrichtendienst = Abschirmung gegen Aufklärungsversuche, Informationsgewinnung zu ausländischen Streitkräften.

207 Ministerium für öffentliche Sicherheit = Dem Polizeiministerium unterstellt, Bereitstellung nachrichtendienstlicher Spezialeinheiten.

208 technische-militärischer Nachrichtendienst = Spezialisiert auf Satellitenaufklärung und hochentwickelte Cyberoperationen gegen kritische Infrastrukturen.

209 Der Begriff bezeichnet die Neue Seidenstraße. Sie ist ein langfristiges Projekt der Kommunistischen Partei Chinas zum Aufbau von Infrastrukturen für Transport, Versorgung und Handel. Vorbild sind historische Routen zwischen China und dem Westen, die man erweitert und verändert.

Russlands zu verurteilen, hat bisher keine erkennbaren wirtschaftlichen Nachteile für die Volksrepublik zur Folge gehabt.

Iran

Die Geheimdienste der Islamischen Republik Iran sind eine wichtige Stütze für das dortige Regime. Das Ministry of Intelligence of the Islamic Republic of Iran (MOIS oder VAJA, Ministerium für Nachrichtenwesen der Islamischen Republik Iran) ist der zivile Auslandsgeheimdienst der Islamischen Republik Iran.

Die Ausspähung der Oppositionellengemeinde ist ein wesentlicher Aufgabenbereich der iranischen Nachrichtendienste. Die Hinweise erstreckten sich über die Beobachtung irankritischer Demonstrationen, bis hin zu konkreten Gefährdungssachverhalten gegenüber Einzelpersonen, die in Zusammenarbeit verschiedener Sicherheitsbehörden bearbeitet werden. Der Niedersächsische Verfassungsschutz nimmt derartige Hinweise sehr ernst und leitet entsprechende Aufklärungsmaßnahmen ein.

Logo des VAJA

Türkei

Der türkische In- und Auslandsnachrichtendienst „Milli Istihbarat Teskilati“ (MIT, „Nationaler Nachrichtendienst“) hat primär zur Aufgabe, den Machterhalt der türkischen Regierung sicherzustellen und Informationen zu beschaffen, die zur Vorbereitung politischer Entscheidungen hilfreich sind. Insoweit nehmen die Nachrichtendienste und Sicherheitsbehörden eine zentrale Rolle im Gefüge der türkischen Regierung ein.

Ein weiteres zentrales Thema ist die Oppositionellenausspähung, die in verschiedenste Bereiche hineinreicht. Hierbei bieten die Vielzahl türkischer Organisationen und Institutionen und die große türkeistämmige Gemeinde in der Bundesrepublik hinreichend Möglichkeiten, um an Informationen zu gelangen.

So hat es in den vergangenen Jahren Hinweise darauf gegeben, dass die türkische Religionsbehörde Diyanet über die Entsendung von Imamen in die DITIB-Moscheen Einfluss auf die Moscheegemeinden genommen haben soll. Die Imame sollen Informationen über

nicht-regimetreue Moscheebesucher an die Religionsbehörde gemeldet haben.

Außerdem besteht ein politischer und militärischer Konflikt zwischen der Türkei und der „Arbeiterpartei Kurdistans" (PKK)[210]. Die Türkei wirft der Bundesrepublik Deutschland vor, nicht in ausreichendem Maße gegen die PKK vorzugehen. Auch aus diesem Grunde dürfte die Türkei ein hohes Interesse an den hiesigen Aktivitäten der PKK-Anhängerinnen und -Anhänger in Niedersachsen haben. Es ist daher davon auszugehen, dass auch diese Aktivisten ausgespäht werden.

Darüber hinaus machte die türkische Regierung die nach dem Prediger Fetullah Gülen benannte „Gülen-Bewegung" für den Putschversuch von Teilen des türkischen Militärs im Jahr 2016 verantwortlich. Auch 2023 wurden in Niedersachsen durch den Verfassungsschutz Sensibilisierungsgespräche mit türkischen Oppositionellen und sachverhaltsaufklärende Maßnahmen durchgeführt.

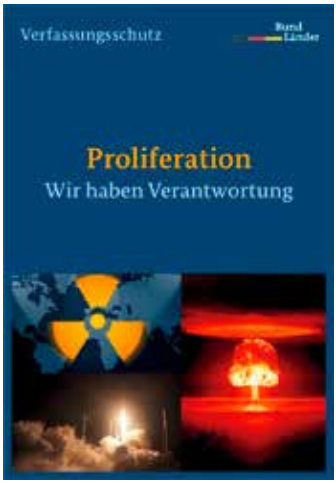
Wie türkische Nachrichtendienste vorgehen, wurde in einem Prozess vor dem Oberlandesgericht (OLG) Düsseldorf (Nordrhein-Westfalen) deutlich. Das OLG verurteilte einen türkischen Staatsangehörigen am 14.07.2022 u. a. wegen geheimdienstlicher Agententätigkeit zu einer Haftstrafe von einem Jahr und neun Monaten auf Bewährung. Der Verurteilte hatte Informationen von in Deutschland lebenden türkischen Oppositionellen an türkische Nachrichtendienste übermittelt. Außerdem verurteilte das OLG Düsseldorf einen deutschen Staatsangehörigen, den der Verurteilte als Helfer angeworben hatte, am 10.11.2022 u. a. wegen geheimdienstlicher Agententätigkeit zu einer Haftstrafe von neun Monaten auf Bewährung.

Für die Türkei, aber auch für die anderen genannten Länder gilt, dass es sich bei der Oppositionellenausspähung und der damit verbundenen nachrichtendienstlichen Informationsgewinnung um klassische Spionageaktivitäten handelt, die nach § 99 StGB strafbewährt sind. Sie stellt für fremde Nachrichtendienste ein wichtiges Instrument zur Informationsbeschaffung im Ausland dar.

210 Siehe hierzu auch Kapitel 5.4.

7.2 Proliferation

Proliferation ist die Weiterverbreitung von atomaren, biologischen und chemischen Waffensystemen und den dazugehörigen Trägersystemen. Wesentliches Merkmal der Proliferation ist, dass diese nicht von Einzelpersonen, sondern durch proliferationsrelevante Staaten [211] – unter Einbeziehung Ihrer Nachrichtendienste – betrieben wird. Die aktuell dynamischen Entwicklungen in den lokalen Krisen- und Konfliktherden, ebenso wie die geopolitischen Machtkämpfe autoritärer Regime, verdeutlichen das zunehmende Gefährdungspotenzial dieses Phänomens innerhalb der sicherheitspolitischen Weltlage.



Die Bundesrepublik Deutschland hat sich neben vielen anderen Staaten international dazu verpflichtet, den Einsatz und die Verbreitung von Massenvernichtungswaffen zu verhindern, um damit das friedliche Zusammenleben der Völker sicherzustellen.

Da Massenvernichtungswaffen und entsprechende Trägertechnologien nicht komplett auf dem Weltmarkt zu beschaffen sind, richtet sich das Interesse der proliferationsrelevanten Staaten auf den Erwerb einzelner Produkte.

Im Mittelpunkt stehen dabei die sogenannten Dual-Use-Güter (einschließlich Software und Know-how), die sowohl im zivilen aber auch im militärischen Bereich Anwendung finden können. Bei dem Erwerb solcher Güter ist es Ziel, eine militärische Nutzung durch die Beschaffung für einen vermeintlich zivilen Einsatzzweck zu verschleiern. Durch den Einsatz von Tarnfirmen sowie durch falsche Angaben über die Ware selbst, ihren tatsächlichen Bestimmungsort und -zweck, ist es oft sehr aufwändig, geheimdienstlich gesteuerte Beschaffungsaktivitäten zu erkennen.

211 Es handelt sich um Länder, von denen zu befürchten ist, dass von dort aus ABC-Waffen in einem bewaffneten Konflikt eingesetzt werden oder ihr Einsatz zur Durchsetzung politischer Ziele angedroht wird.

Niedersachsen ist erfolgreicher Standort zahlreicher innovativer Unternehmen und Forschungseinrichtungen. Die hier entwickelten und produzierten Güter sowie deren Technologien können teilweise zur Herstellung oder Weiterentwicklung von Massenvernichtungswaffen verwendet werden. Erfahrungen haben gezeigt, dass Unternehmen und Forschungseinrichtungen proliferationsrelevante Absichten oft nicht erkennen. Grundsätzlich gilt, dass die Umgehung von Exportbestimmungen eine Ordnungswidrigkeit bzw. einen Straftatbestand nach dem Außenwirtschaftsgesetz, der Außenwirtschaftsverordnung und ggf. dem Kriegswaffenkontrollgesetz darstellt.

Emerging Technologies

Einen zunehmenden Stellenwert in der Proliferationsbekämpfung nehmen die Entwicklungen technischer Innovationen – sogenannter Emerging Technologies (EMT) – ein, die von zahlreichen Staaten priorisiert werden, um sich einen Wettbewerbsvorteil zu verschaffen. Beispielhaft können die Entwicklung von Quantencomputern und die Einsatzmöglichkeiten von künstlicher Intelligenz (KI) genannt werden. Besonders problematisch ist dies, da insbesondere EMT mit einem zivil-militärischen „Dual Use"-Charakter das Potenzial haben, zukünftige militärische Konflikte in einem Ausmaß zu beeinflussen, das dem Effekt von Massenvernichtungswaffen ähnelt.
Aufgrund der geltenden Gesetzeslage bezüglich der Exportkontrolle für EMT kann der Verfassungsschutz i. d. R. nur durch Sensibilisierung von Politik und Unternehmen gegensteuern.

Volksrepublik China

Die Anstrengungen der Volksrepublik China im Bereich der Verbreitung von Massenvernichtungswaffen unterscheiden sich grundlegend von denen anderer Staaten. Es gibt in Deutschland keine signifikanten Beobachtungen hinsichtlich chinesischer Bestrebungen, Wissen oder Güter im Zusammenhang mit ABC-Waffen und Trägertechnologie zu erlangen. China hat bereits erhebliche Fortschritte auf technologischem Gebiet gemacht und ist daher weitgehend autark.
Im Bereich der EMT arbeitet die Volksrepublik mit Hochdruck an ihrem „Sprung an die Weltspitze". Dazu nutzt China intensiv den

deutschen Markt und die deutsche Wissenschaftslandschaft. Die Übertragungskanäle, wie beispielsweise der Erwerb von Unternehmen oder Kooperationen in Forschung und Wissenschaft sind äußerst vielfältig. Diese Situation generiert eine Anfälligkeit Deutschlands für den Abfluss hochtechnologischer Güter und entsprechendem Fachwissen. Dem wird durch intensive Aufklärung und Sensibilisierung betroffener Unternehmen entgegengewirkt.

Russische Föderation

Als Reaktion auf den russischen Angriffskrieg hat die Europäische Union seit Ende Februar 2022 gegen die Russische Föderation mehrere Sanktionspakete verhängt, die über die bisherigen Beschränkungen deutlich hinausgehen. Diese umfassen nicht nur weitreichende finanzielle Sanktionen, sondern beinhalten auch ein Verbot für die Lieferung sämtlicher Güter und Technologien, die dazu dienen könnten, die militärische und technologische Stärke Russlands zu erhöhen oder die Entwicklung des Verteidigungs- und Sicherheitssektors zu fördern. Es ist zu erwarten, dass Russland trotz oder gerade wegen dieser Sanktionen weiterhin intensive Bemühungen zur Beschaffung von Dual-Use-Produkten unternehmen wird.

Ausblick/Fazit

Der Niedersächsische Verfassungsschutz leistet Prävention durch konsequente Aufklärung und Sensibilisierungsgespräche. Er steht den niedersächsischen Wirtschaftsunternehmen, Behörden und Forschungseinrichtungen als vertraulicher Ansprechpartner zur Verfügung.

Zur Aufdeckung und Verhinderung von proliferationsrelevanten Aktivitäten arbeitet der Niedersächsische Verfassungsschutz eng mit anderen Sicherheitsbehörden zusammen.

7.3 Cyberabwehr

Die Abhängigkeit unserer Gesellschaft von Informations- und Kommunikationstechnologien steigt. Die dadurch verursachte Verwundbarkeit moderner Gesellschaften stellt eine große sicherheitspolitische Herausforderung dar, denn der mögliche Schaden für Staaten, ihre Bevölkerung und ihre Volkswirtschaften im Falle der Beeinträchtigung von Informations- und Kommunikationsinfrastrukturen ist immens. Staat, Kritische Infrastrukturen[212], Wirtschaft, Wissenschaft und Bevölkerung sind auf das verlässliche Funktionieren dieser Technologien, insbesondere des Internets, angewiesen. Zeitgleich werden Cyberangriffe zahlreicher, komplexer und professioneller. Häufig kann bei Angriffen weder auf die Identität noch auf die Motivation des Angreifers geschlossen werden; kriminelle, terroristische, militärische und/oder nachrichtendienstliche Hintergründe sind denkbar. Die für solche Angriffe häufig genutzten hoch entwickelten Schadprogramme abzuwehren und zurückzuverfolgen, erfordert eine enge Kooperation der beteiligten Sicherheitsbehörden. Fremde Staaten bedienen sich gezielter Cyberangriffe, um Informationen zu erlangen und das erworbene Wissen zu ihrem Vorteil zu nutzen. Täglich gibt es bundesweit eine Vielzahl an Cyberangriffen, mit dem Ziel der Verschlüsselung und der anschließenden Erpressung der Betroffenen[213]. Auf den einschlägigen Seiten für die Internetsicherheit, wie, z. B.: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html werden die Angriffe statistisch dargestellt. Neben den auch im Jahr 2023 fortgesetzten Angriffen auf Großunternehmen sind in Niedersachsen diverse kleinere und mittelständische Unternehmen, politische Entscheidungsträger oder auch Privatpersonen betroffen. Das verdeutlicht, welch hohen Stellenwert die IT-Sicherheit in jedem Bereich hat.

212 Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen von hoher Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden (siehe Internetseite des Bundesamtes für Sicherheit in der Informationstechnik, www.bsi.bund.de).

213 Auch bekannt als Einsatz von Ransomware (aus dem englischen: ransom für „Lösegeld").

Eine große Gefahr für Unternehmen und Behörden stellen nach wie vor „Advanced Persistant Threats“[214] dar. Diese zielgerichteten Cyberangriffe durch fortgeschrittene, gut organisierte und professionell ausgestattete Angreifer, die Anweisungen und Unterstützung in der Regel von Regierungen erhalten könnten, verlaufen typischerweise in mehreren Phasen und sind sehr komplex in der Vorbereitung und Durchführung. Ziel eines solchen Angriffs ist es, sich möglichst lange unentdeckt in fremden IT-Systemen zu bewegen, um sensible Daten auszuleiten oder anderweitig Schäden anzurichten. Im Gegensatz zu vielen anderen Cyberkriminellen verfolgen diese Angreifer ihre Ziele jedoch grundsätzlich langfristig, meist über mehrere Monate oder Jahre hinweg. Sie stimmen ihre Aktivitäten auf die Sicherheitsmaßnahmen ihrer anvisierten Opfer ab und greifen diese oft mehrfach an. Die Bearbeitung solcher Cyberangriffe stellt aufgrund der Anonymität des Angriffs und der nicht erkennbaren Motivation der Angreifer für die Sicherheitsbehörden eine große Herausforderung dar.

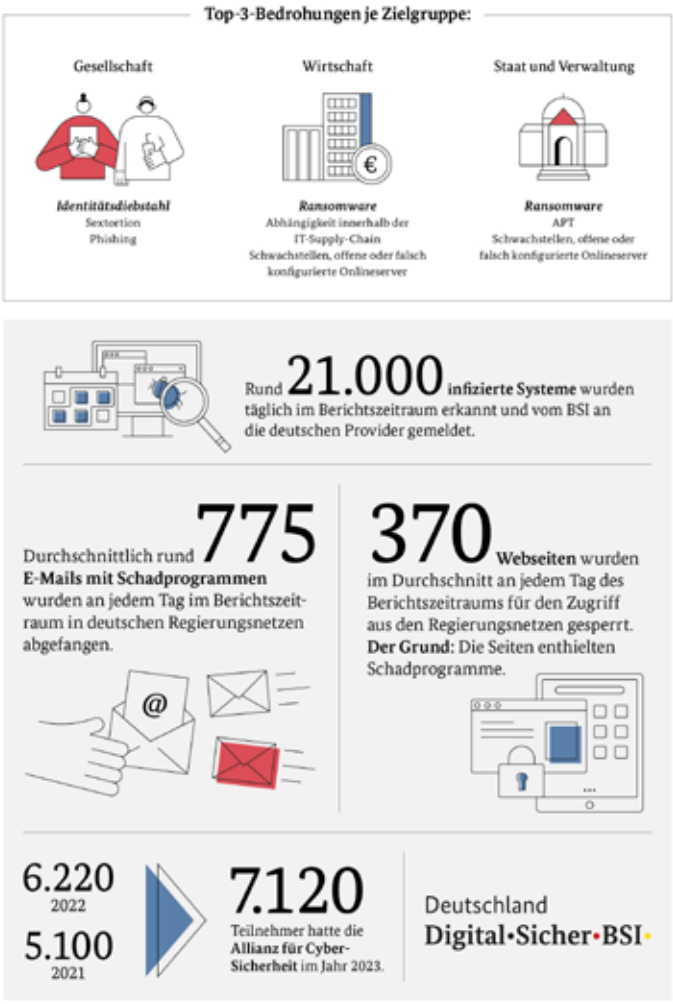
Die Abgrenzung zwischen Cybercrime und Cyberspionage ist häufig sehr schwierig, da auch bei einem Sachverhalt mit einem augenscheinlich in erster Linie bestehenden finanziellen Interesse des Angreifers, wie dem Einsatz von Ransomware, staatliche Akteure im Vorfeld an der Kompromittierung beteiligt gewesen sein können. Denn auch einem staatlichen Akteur kann eine Verschlüsselung der Systeme des Opfers zur Verschleierung der Aktivitäten und finanziellen Bereicherung dienen.

Neben direkten Cyberangriffen zum Zweck der Spionage oder Sabotage können häufig kompromittierte Systeme festgestellt werden, die als Bestandteil eines Botnetzes[215] von dem jeweiligen

214 Bei „Advanced Persistant Threats“ handelt es sich um zielgerichtete Cyberangriffe auf spezifisch ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer persistent (= andauernd) Zugriff auf ein Opfersystem verschafft und in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aufseiten der Angreifer aus und sind i. d. R. schwierig festzustellen (siehe Internetseite des Bundesamtes für Sicherheit in der Informationstechnik, www.bsi.bund.de).

215 Ein Botnet oder Botnetz, besteht aus gekaperten IT-Systemen, deren Besitzer und Nutzer in aller Regel nichts davon wissen, dass ihre Rechner ferngesteuert werden. Die heimliche Übernahme des Rechners beginnt mit einer Malware-Infektion. Die Schadsoftware ermöglicht es dem Angreifer, die Kontrolle über das System zu übernehmen, der Computer agiert wie ein Roboter oder kurz Bot. Gesteuert werden die gekaperten Computer meistens über sogenannte Command-and-Control-Server (C2-Server), welche wiederum vom Angreifer gesteuert werden.

Akteur gesteuert werden. Hierbei handelt es sich meist um kompromittierte Systeme von Unternehmen, Behörden oder gar Privatpersonen. Häufig will der Angreifer ohne Wissen des Betroffenen seine IP-Adresse für weitere Angriffe nutzen. Die



potenziellen Opfer müssen sich nicht notwendigerweise in Deutschland befinden. Beim Aufbau eines Botnetzes geht es hauptsächlich um Verschleierungsaktivitäten und Stärkung der eigenen Ressourcen in Form von Rechenkapazität durch die Vernetzung mehrerer PCs.

Eine andere Art der staatlich gesteuerten Angriffe zielte auf Politiker, die im Bundestag, im Landtag oder auch in den Kommunalparlamenten tätig sind oder waren. Dort wurde durch einen mutmaßlich ausländischen Cyberakteur versucht, E-Mail-Konten zu übernehmen, um anschließend, möglicherweise durch eine Desinformationskampagne, Einfluss nehmen zu können.

Eine weitere im Jahr 2023 vermehrt festgestellte Angriffsmethode staatlicher Akteure sind Supply Chain-Angriffe[216], deren Intention die Manipulation oder Kompromittierung von Lieferketten darstellt. Ein solcher Angriff kann auf verschiedene Arten erfolgen, u. a. durch die Injektion von Schadsoftware in Hardware oder Software während des Herstellungsprozesses, die Kompromittierung von Lieferanten- oder Herstellerdatenbanken oder die Unterwanderung von Drittanbieterdiensten. Z. B. war ein Unternehmen betroffen, dessen Telekommunikationssoftware Opfer eines Supply Chain-Angriffes geworden ist. Die Manipulation durch die Softwarebibliothek eines Drittanbieters erfolgte mutmaßlich durch einen staatlichen Akteur. Somit waren alle Systeme, die diese Software nutzen, potenziell verwundbar. Auch Systeme niedersächsischer Unternehmen waren betroffen.

Ein weiterer Punkt, der im Jahr 2023 die Sicherheitsbehörden beschäftigte, ist die voranschreitende Entwicklung Künstlicher Intelligenz (KI). Deren Nutzung kann potenziell sowohl positive als auch negative Auswirkungen auf die Sicherheit der Gesellschaft haben. Im Rahmen der Funktion als Frühwarnsystem für Politik und Gesellschaft ist es Aufgabe des Verfassungsschutzes, die Gefahren solcher Entwicklungen zu bewerten. Im Bereich der KI-Technologie existieren bereits konkrete Verwendungsmöglichkeiten für staatliche Akteure. Zu nennen sind hier Desinformationskampagnen, die mittels KI gezielt gefälschte Nachrichten, Videos oder Bilder generieren. Weitere Verwendungsmöglichkeiten dieser Technologie,

216 Bei Supply Chain-Angriffen werden Viren oder andere Schadsoftware über einen Lieferanten oder Drittanbieter verbreitet. Z. B. kann ein Keylogger auf einem USB-Laufwerk bei einem großen Einzelhändler eingeschleust werden und dann Tastenanschläge protokollieren, um Passwörter von Mitarbeiterkonten zu ermitteln.

die auch staatlichen Akteuren neue Handlungsmöglichkeiten eröffnen oder bereits vorhandene Vorgehensweisen vereinfachen oder verbessern, sind zukünftig zu erwarten.

7.4 Hilfe für Betroffene

Personen, die Opfer eines Anwerbungsversuchs fremder Geheimdienste oder eines elektronischen Angriffs mit vermutetem nachrichtendienstlichem Hintergrund geworden sind, wird geraten, sich an das

Niedersächsisches Ministerium für Inneres und Sport
Verfassungsschutzabteilung
Postfach 44 20
30044 Hannover
Telefon 0511 6709-0

zu wenden.
Weitere Informationen können Sie auch dem Flyer „Spionage – (k)ein Thema?!“ entnehmen, den Sie sowohl auf unserer Internetseite herunterladen, als auch über die vorstehenden Kontaktdaten bestellen können.