Spionageabwehr/ Proliferation/ Elektronische Angriffe

8. Spionageabwehr/Proliferation/ Elektronische Angriffe

8.1 Spionageaufkommen in Niedersachsen

Der Arbeitsbereich Spionageabwehr im Niedersächsischen Verfassungsschutz hat den gesetzlichen Auftrag, alle Informationen über sicherheitsgefährdende oder geheimdienstliche Aktivitäten zu sammeln und Spionage sowie Proliferation[123] zu verhindern. Da Niedersachsen als erfolgreicher Wirtschaftsstandort potenzielles Ziel von Spionageaktivitäten fremder Geheim- oder Nachrichtendienste[124] ist, gilt es ihn vor derartigen Aktivitäten zu bewahren. Zudem geht es darum, den Schutz der in Niedersachsen lebenden Bürgerinnen und Bürger zu gewährleisten.

Hauptträger der Spionageaktivitäten in der Bundesrepublik Deutschland sind nach wie vor die Russische Föderation, die Volksrepublik China, aber auch der Iran. Die Schwerpunkte ihrer Aktivitäten orientieren sich an den politischen Vorgaben und wirtschaftlichen Prioritäten.
Aufgrund desolater Sicherheitslagen in ihren Heimatländern und damit verbundener existenzieller Bedrohung 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 sowie in Syrien, 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 Nachrichtendienstmitarbeiter können dort als Diplomaten getarnt tätig werden und Informationen beschaffen oder sie leisten Unterstützung bei geheimdienstlichen Operationen ihrer Zentralen.

123 Proliferation ist die Weiterverbreitung von ABC-Waffen und Trägersystemen; siehe auch Kapitel 8.2.

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

Eine Vielzahl von Informationen, die für fremde Geheim- oder Nachrichtendienste interessant erscheinen und früher nur mit klassischen 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 auch von einer geheim- oder nachrichtendienstlichen oder staatlichen Beteiligung auszugehen.

Im Umkehrschluss bedeutet dies jedoch nicht, dass die klassischen Spionageaktivitäten ausgedient haben.
Im Jahr 2019 traten im Arbeitsbereich Spionageabwehr im Niedersächsischen Verfassungsschutz entsprechende Verdachtsfälle auf.
Für den Putschversuch von Teilen des türkischen Militärs am 15. und 16.07.2016 machte die türkische Regierung die nach dem Prediger Fetullah Gülen benannte „Gülen-Bewegung" verantwortlich.
Der türkische Innenminister Soylu sorgte im März 2019 in diesem Zusammenhang in Europa und damit auch in Deutschland für Verunsicherung, als er öffentlich erklärte, dass mutmaßliche „Terroristen im Ausland" sein Land spalten wollten, um dann aber trotzdem in die Türkei zu kommen und dort Urlaub zu machen. Soylu erklärte dazu: „… Sollen sie ruhig kommen, die werden verhaftet und weg! …"
Indirekt setzte er damit deutsche Touristen mit Terroristen gleich. Kurz nach Bekanntwerden relativierte die türkische Regierung die Aussagen. Ein Sprecher erklärte sie sogar zur Falschmeldung.
Da davon ausgegangen werden kann, dass der türkische Nachrich-

tendienst „Millî Istihbarat Teşkilâtı“ (MIT) auch in Niedersachsen insbesondere Oppositionelle der vom türkischen Staat als „Fetullahistische Terrororganisation“ (FETÖ) bezeichneten „Gülen-Bewegung“ ausspäht, führten Mitarbeiter des Niedersächsischen Verfassungsschutzes auch im Jahr 2019 zahlreiche Sensibilisierungsgespräche mit möglicherweise betroffenen Personen. Konkrete Spionagetätigkeiten wurden bislang allerdings nicht festgestellt.

Im Rahmen einer international abgestimmten Reaktion auf den Anschlag auf Sergej Skripal[125] und dessen Tochter am 04.03.2018 in Großbritannien erklärte das deutsche Auswärtige Amt Ende März 2018 vier an der Botschaft der Russischen Föderation akkreditierte Diplomaten zur Persona non grata und forderte sie auf, Deutschland zu verlassen. Anfang 2019 reagierten die Außenminister der EU-Staaten mit einem Einreiseverbot und Vermögenssperren gegen die Spitze des russischen Militärgeheimdienstes GRU[126].
Insbesondere baltische Staaten beklagen seit langem eine gegen sie gerichtete mediale Agitation Russlands. Es soll z. B. suggeriert werden, dass dort schlechtere Zustände als in Russland herrschen. Damit wird versucht, den russischsprachigen Teil der Bevölkerung im Sinne der russischen Regierung zu beeinflussen und der Versuch einer Destabilisierung unternommen. Nach Aussagen des Generalstabschefs der russischen Streitkräfte[127] muss sich Krieg nicht auf rein militärische Mittel beschränken. Die sogenannte „Gerassimow-Doktrin“ versteht z. B. das Mittel der Desinformation als Teil hybrider Kriegsführung zur Destabilisierung von anderen Staaten. Diese Aktivitäten werden als sicherheitsgefährdend i. S. des § 3 Abs. 1 Nr. 2 NVerfSchG eingeordnet.
Im Februar 2019 hat das US-amerikanische Unternehmen Facebook mehrere Accounts eines in Berlin ansässigen Internet-Senders gesperrt. Der Sender gehört mehrheitlich einer Videoagentur, die Ableger des weltweit operierenden, staatlichen russischen Senders

125 Sergej Skripal ist ein ehemaliger Oberst des russischen Militärgeheimdienstes GRU, der zum britischen Auslandsgeheimdienst MI6 übergelaufen ist.

126 GRU steht für Glawnoje Raswedywatelnoje Uprawlenije.

127 Waleri Gerassimow ist der Chef des russischen Generalstabs, der die These vertritt, dass Kriege gegen andere Staaten nicht nur auf dem Schlachtfeld stattfinden, sondern dass militärische Mittel gleichberechtigt neben nicht-militärischen Mitteln z. B. auf dem Gebiet der Politik, Wirtschaft oder Informationstechnik stehen.

„RT“ (früher „Russia Today“) ist. Seit mehreren Jahren verbreiten Akteure der Russischen Föderation auf vielfältige Weise prorussische Propaganda und Desinformation. Auch soziale Netzwerke sind dabei wichtige Werkzeuge geworden.

Iranisches Nachrichtenministerium (MOIS)

Bereits am 01.07.2018 wurde der 46-jährige iranische Staatsangehörige Assadollah A. aufgrund eines Europäischen Haftbefehls im Landkreis Aschaffenburg verhaftet. A. war seit 2014 als 3. Botschaftsrat an der iranischen Botschaft in Wien akkreditiert und soll im März 2018 ein in Antwerpen lebendes Ehepaar beauftragt haben, einen Sprengstoffanschlag auf die jährliche „Große Versammlung“ einer iranischen Auslandsopposition am 30.06.2018 in Frankreich zu verüben.

Nach vorliegenden Erkenntnissen war A. Mitarbeiter des iranischen Nachrichtenministeriums Ministry of Intelligence and Security (MOIS). Zu den Aufgaben des MOIS gehört in erster Linie die Beobachtung und Bekämpfung oppositioneller Gruppierungen innerhalb und außerhalb des Irans.[128]

Anfang Januar 2019 hat der Europäische Rat daraufhin eine Abteilung des MOIS auf die EU-Terrorliste gesetzt. Die Maßnahmen richten sich konkret gegen einen iranischen Diplomaten sowie einen ehemaligen Generaldirektor des iranischen Nachrichtendienstministeriums und sind Reaktionen der Europäischen Union auf diverse Vorfälle in Europa mit mutmaßlichem staatsterroristischem Hintergrund aus dem Iran.

Ende Januar 2019 hat die Bundesregierung zudem ein Landeverbot für eine iranische Fluggesellschaft in Deutschland verhängt. Das Auswärtige Amt begründete das Verbot ebenfalls mit deutschen Sicherheitsinteressen.

China

Im Zusammenhang mit der Demokratiebewegung in der chinesischen Sonderverwaltungszone Hongkong kommt es auch in Deutschland zu Demonstrationen, welche die dortige Situation thematisieren. Die chinesische Administration reagiert auf gegen

128 DER GENERALBUNDESANWALT beim Bundesgerichtshof, Pressemitteilung 36/2018 vom 11.07.2018.

sie gerichtete Protestaktionen besonders sensibel. So wurde z. B. der Empfang eines Sprechers der Protestbewegung durch Bundesaußenminister Maaß heftig kritisiert.
Entsprechend bleibt auch die Beobachtung und Kontrolle der Oppositionsbewegung im Ausland ein Schwerpunkt chinesischer Nachrichtendienste. Wir gehen daher davon aus, dass die chinesischen Behörden in Niedersachsen durchgeführte Aktionen beobachten und an der Identifizierung von Demonstrationsanmeldern oder -teilnehmern interessiert sind. Ebenfalls kann nicht ausgeschlossen werden, dass erkannte Protagonisten vom chinesischen Staat in Deutschland unter Druck gesetzt, bedroht oder eingeschüchtert werden.

Deutscher Staatsbürger versorgt jordanischen Geheimdienst mit Informationen

Mit Urteil vom 22.10.2019 hat der 3. Strafsenat (Staatsschutzsenat) des Thüringer Oberlandesgerichts einen 34-jährigen deutschen Staatsangehörigen wegen geheimdienstlicher Agententätigkeit (§ 99 Abs. 1 Satz 1 Nr. 1 StGB) zu einer Freiheitsstrafe verurteilt und die Vollstreckung der Strafe zur Bewährung ausgesetzt.
Der Beklagte versorgte zwischen 2016 und 2018 eine für den jordanischen Geheimdienst arbeitende Person mit Informationen und Lichtbildern zu deutschen Staatsbürgern, die im Umfeld der vom „Deutschsprachigen Islamkreis Hildesheim e. V." unterhaltenen Moschee (DIK-Moschee) in Hildesheim[129] verkehrten und dem salafistischen und jihadistischen Spektrum angehörten.
Im Rahmen der Hauptverhandlung hat der Angeklagte die Anklagevorwürfe im Wesentlichen bestätigt.
Im Zentrum der Strafzumessungserwägungen des Senates standen die für eine Agententätigkeit atypischen Umstände des festgestellten Tatgeschehens, nach denen von den ausspionierten Personen selbst eine erhebliche Gefahr für die Sicherheit der Bundesrepublik Deutschland ausging und die Motivation des Angeklagten bei der Tatbegehung maßgeblich von dem Willen der Bekämpfung dieser Gefährder getragen war. Der Angeklagte hat auf Einlegung einer Revision verzichtet.[130]

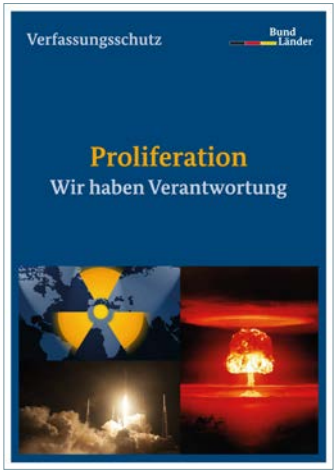
129 Die Hildesheimer DIK-Moschee war von dem Verein „Deutschsprachiger Islamkreis Hildesheim e. V." (DIK) betrieben worden. Der Verein ist am 14.03.2017 vom Niedersächsischen Ministerium für Inneres und Sport verboten worden.

130 Medieninformation des Thüringer Oberlandesgerichts vom 22.10.2019, Aktenzeichen OLG: 3 St 3 BJs 20/17.

8.2 Proliferation

Wesentliches Merkmal der Proliferation – also der Weiterverbreitung von ABC-Waffen und Trägersystemen – ist, dass sie nicht von Einzelpersonen, sondern von sogenannten proliferationsrelevanten Staaten wie dem Iran, Nordkorea, Pakistan und Syrien unter Einbeziehung ihrer Geheimdienste betrieben wird.

Da einsatzfähige ABC-Waffen- und Trägersysteme nicht in Gänze auf dem Weltmarkt zu beschaffen sind, richtet sich das Interesse dieser Staaten grundsätzlich auf den Erwerb von Produkten, die den Fortbestand und die Weiterentwicklung der bereits vorhandenen Waffenbestände gewährleisten. Im Mittelpunkt stehen dabei solche Ausfuhrprodukte, die als sogenannte Dual-use-Güter sowohl im zivilen als auch im militärischen Bereich Anwendung finden können. Ziel ist, bei dem Erwerb solcher Güter, eine militärische Nutzung durch die Beschaffung für einen vermeintlich zivilen Einsatzzweck zu verschleiern. Durch den Einsatz von Tarnfirmen bzw. -organisationen sowie durch falsche Angaben über die Ware selbst, ihren tatsächlichen Bestimmungsort und -zweck ist es oftmals sehr aufwändig, geheimdienstlich gesteuerte Beschaffungsaktivitäten zu erkennen. Der Export dieser Dual-use-Güter unterliegt strengen Ausfuhrbeschränkungen, um eine Nutzung für militärische Zwecke zu unterbinden. Grundsätzlich gilt, dass die Umgehung von Exportbestimmungen eine Ordnungswidrigkeit bzw. einen Straftatbestand nach dem Außenwirtschaftsgesetz, der Außenwirtschaftsverordnung und ggf. dem Kriegswaffenkontrollgesetz darstellt. Die Bundesrepublik Deutschland versucht, der Proliferation durch eine restriktive Exportkontrolle entgegen zu wirken.



Großes Interesse besteht an der Beschaffung von Gütern und Informationen aus niedersächsischen Hochtechnologieunternehmen. Die proliferationsrelevanten Staaten bemühen sich zudem um den Erwerb von Wissen, um dieses für den Betrieb von Programmen zur Herstellung von eigenen Massenvernichtungswaffen nutzen zu können.

Der Niedersächsische Verfassungsschutz unterhält Kontakte zu zahlreichen niedersächsischen Unternehmen und wissenschaftlichen Forschungseinrichtungen, die proliferationsrelevante Güter entwickeln, herstellen und vertreiben. Es hat sich eine vertrauensvolle Zusammenarbeit mit dem Ziel entwickelt, das Proliferationsrisiko einzudämmen. Durch den gegenseitigen Informationsaustausch können Proliferationshandlungen erkannt und die Lieferung proliferationsrelevanter Güter bzw. der illegale Know-how-Transfer unterbunden werden. Durch konsequente Aufklärung und Sensibilisierungsgespräche wird ein wesentlicher Beitrag zur Proliferationsbekämpfung geleistet.

8.3 Elektronische Angriffe mit vermutetem nachrichtendienstlichem Hintergrund

Die Abhängigkeit unserer Gesellschaft von Informations- und Kommunikationstechnologien steigt. Die dadurch verursachte Verwundbarkeit moderner Gesellschaften stellt eine der größten sicherheitspolitischen Herausforderungen dar, denn der mögliche Schaden für Staaten, ihre Bevölkerung und ihre Volkswirtschaften im Falle der Beeinträchtigung von Informationsinfrastrukturen ist immens. Staat, Kritische Infrastrukturen[131], Wirtschaft, Wissenschaft und Bevölkerung sind auf das verlässliche Funktionieren dieser Technologien, insbesondere des Internets, angewiesen.

Elektronische Angriffe werden zahlreicher, komplexer und professioneller. Meist 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

131 Kritische Infrastrukturen 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).

enge Kooperation der beteiligten Sicherheitsbehörden. Fremde Staaten bedienen sich gezielter elektronischer Angriffe, um Informationen zu erlangen und das erworbene Wissen zu ihrem Vorteil zu nutzen.

Zuletzt hat es in Niedersachsen und bundesweit elektronische Angriffe mit Verschlüsselungstrojanern gegeben. Neben den im Jahr 2019 fortgesetzten Angriffen auf Großunternehmen sind in Niedersachsen diverse kleinere und mittelständische Unternehmen betroffen. Das verdeutlicht, welch hohen Stellenwert die IT-Sicherheit hat.

Die höchste Gefahr für Unternehmen und Behörden stellen aktuell „Advanced Persistant Threats“[132] dar. Diese zielgerichteten elektronischen Angriffe durch fortgeschrittene, gut organisierte und professionell ausgestattete Angreifer verlaufen typischerweise in mehreren Phasen und sind sehr komplex in der Vorbereitung und Durchführung. Ziel eines solchen Angriffes ist es, sich möglichst lange unentdeckt in fremden IT-Systemen zu bewegen, um sensible Daten auszuleiten oder anderweitig Schäden anzurichten.

Die Bearbeitung solcher elektronischer Angriffe ist aufgrund der Anonymität des Angriffs und der nicht erkennbaren Motivation der Angreifer für die Sicherheitsbehörden die große Herausforderung der kommenden Jahre.

Der Niedersächsische Verfassungsschutz steht niedersächsischen Wirtschaftsunternehmen als Ansprechpartner zur Verfügung. Bei elektronischen Angriffen mit vermutetem nachrichtendienstlichem Hintergrund wird Beratung angeboten. Fälle von „Cybercrime“, bei denen ein solcher Verdacht ausgeschlossen werden konnte, werden in Absprache und nur mit dem Einverständnis des Betroffenen an die Strafverfolgungsbehörden abgegeben.

Insgesamt hat der Niedersächsische Verfassungsschutz im Jahr 2019 25 Vorgänge zu elektronischen Angriffen bearbeitet. Dabei handelt es sich um erkannte Cyberangriffe auf niedersächsische Unternehmen.

132 Bei Advanced Persistant Threats handelt es sich um zielgerichtete Cyber-Angriffe 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 in der Regel schwierig festzustellen (siehe Internetseite des Bundesamtes für Sicherheit in der Informationstechnik, www.bsi.bund.de).

Der Verfassungsschutz arbeitet im Rahmen der Cyber-Sicherheitsstrategie für Niedersachsen mit dem Computer Emergency Response Team der niedersächsischen Landesverwaltung (N-CERT) zusammen und ist darüber hinaus auf Bundesebene mit dem Nationalen Cyber-Abwehrzentrum (NCAZ) und anderen Behörden vernetzt sowie Multiplikator der Allianz für Cybersicherheit.

8.4 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.