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[136] zu verhindern. Dabei geht es insbesondere darum, den Schutz der in Niedersachsen lebenden Bürgerinnen und Bürger zu gewährleisten. Da Niedersachsen als erfolgreicher Wirtschaftsstandort potenzielles Ziel von Spionageaktivitäten fremder Geheim- oder Nachrichtendienste[137] ist, gilt es ihn vor derartigen Aktivitäten zu bewahren.

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. Auch Deutschland ist Ziel

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

137 Im Gegensatz zu Geheimdiensten unterliegen Nachrichtendienste einer rechtsstaatlichen Kontrolle und haben keine polizeilichen Befugnisse.

von Flüchtlingsbewegungen, die ihren Ursprung vor allem in Afghanistan, im Irak sowie in Syrien 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.
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.
Auch im Jahr 2018 bearbeitete der Arbeitsbereich Spionageabwehr im Niedersächsischen Verfassungsschutz entsprechende Verdachtsfälle.
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. In der Folge wurden türkische Listen mutmaßlicher Gülen-Anhänger in Deutschland bekannt, auf denen auch niedersächsische Bürger verzeichnet waren.
Da davon ausgegangen werden kann, dass der türkische Nachrichtendienst „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 2018 diverse Sensibilisierungsgespräche mit möglicherweise betroffenen Personen. Konkrete Spionagetätigkeiten wurden bislang allerdings nicht festgestellt.
Ein Vorfall im Sommer belegt abermals das russische Interesse, Erkenntnisse über deutsche Sicherheitsbehörden zu gewinnen. Nach einem Landgang in St. Petersburg (Russland) wurde erneut ein nie-

dersächsischer Polizeibeamter während einer privaten Ostseekreuzfahrt bei der Ausreise aus Russland von Sicherheitskräften zu dienstlichen Hintergründen befragt.

Im Rahmen einer international abgestimmten Reaktion auf den Anschlag auf Sergej Skripal 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.

Im März 2017 wurde der pakistanische Staatsangehörige Syed Mustufa H. vom Berliner Kammergericht schuldig gesprochen. Ihm konnte nachgewiesen werden, den ehemaligen Präsidenten der Deutsch-Israelischen Gesellschaft (DIG) für den Iran ausspioniert zu haben[138].

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[139].

Am 07.08.2018 wurde ein 33-jähriger deutscher Staatsangehöriger aufgrund eines Haftbefehls des Ermittlungsrichters des Bundesgerichtshofes vom 19.06.2018 wegen des Verdachts der geheimdienstlichen Agententätigkeit (§ 99 Abs. 1 Nr. 1 StGB) verhaftet.

Nach den Ergebnissen der Ermittlungen stand der Beschuldigte im Jahr 2016 in Verbindung mit einem jordanischen Geheimdienst. In dessen Auftrag soll er Informationen über die DIK-Moschee[140] in Hildesheim gesammelt und an seine Auftraggeber in Jordanien weitergegeben haben. Dabei soll der Beschuldigte auch Erkenntnisse zu mehreren Perso-

138 Urteil des Kammergerichts Berlin, Az. 3 StE 8/16-1.

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

140 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 Innenministerium verboten worden.

nen geliefert haben, die seiner Einschätzung nach in den Jschihad nach Syrien ziehen wollten oder aber bereits dorthin ausgereist waren[141].
Das Thüringer Oberlandesgericht hob den Haftbefehl im November 2018 mit der Begründung wieder auf, die Aktivitäten des Mannes hätten sich nicht gegen die Bundesrepublik Deutschland gerichtet. Der Bundesgerichtshof hat allerdings den Prozess gegen den mutmaßlichen Agenten zugelassen.[142]

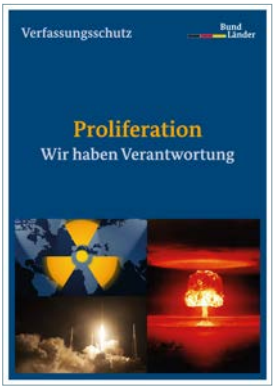
8.2 Proliferation

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 komplett 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.

141 DER GENERALBUNDESANWALT beim Bundesgerichtshof, Pressemitteilung 44/2018 vom 08.08.2018.

142 Bundesgerichtshof, Pressemitteilung Nr. 60/2018 vom 08.05.2018.

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 hat den Kontakt zu niedersächsischen Firmen und wissenschaftlichen Forschungseinrichtungen weiter ausgebaut. Die konsequente Aufklärung sowie Sensibilisierungsgespräche leisten einen wesentlichen Beitrag zur Proliferationsbekämpfung.

8.3 Elektronische Angriffe mit vermutetem nachrichtendienstlichem Hintergrund

Die Abhängigkeit der Gesellschaft von Informations- und Kommunikationstechnologien steigt. Die dadurch verursachte Verwundbarkeit moderner Gesellschaften ist eine der größten sicherheitspolitischen Herausforderungen, denn der mögliche Schaden für Staaten, ihre Bevölkerung und ihre Volkswirtschaften im Falle der Beeinträchtigung von Informationsinfrastrukturen ist immens. Staat, Kritische

Infrastrukturen[143], 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 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 bundesweit – auch in Niedersachsen – elektronische Angriffe mit Verschlüsselungstrojanern gegeben. Neben den im Jahr 2018 fortgesetzten Angriffen auf Großunternehmen sind in Niedersachsen auch 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“[144] 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.

143 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).

144 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 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 2018 41 Vorgänge zu elektronischen Angriffen bearbeitet. Dabei handelt es sich um erkannte Cyberangriffe auf niedersächsische Unternehmen. Mit den betroffenen Unternehmen wurde seitens der Verfassungsschutzbehörde Kontakt aufgenommen, um diese Angriffe aufzuklären und weitere Aktionen zu verhindern.
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.