Spionageabwehr / Proliferation / Cyberabwehr

7. Spionageabwehr / Proliferation / Cyberabwehr

7.1 Spionageaufkommen in Niedersachsen

Das Sachgebiet Spionageabwehr im Niedersächsischen Verfassungsschutz hat den gesetzlichen Auftrag, alle Informationen über sicherheitsgefährdende oder geheimdienstliche Aktivitäten zu sammeln und Spionage sowie Proliferation[122] zu verhindern. Da Niedersachsen als erfolgreicher Wirtschaftsstandort potenzielles Ziel von Spionageaktivitäten fremder Geheim- oder Nachrichtendienste[123] 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 von Aktivitäten fremder Geheim- und Nachrichtendienste weisen nicht ausschließlich einen Niedersachsenbezug auf. Die 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, aber auch der Iran. 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

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

123 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.

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 (z. B. welcher Angriffsweg und welche Infrastruktur genutzt werden) auch von einer geheim- oder nachrichtendienstlichen bzw. staatlichen Beteiligung auszugehen.
Im Umkehrschluss bedeutet dies jedoch nicht, dass die klassischen Spionageaktivitäten ausgedient haben. Im Jahr 2022 traten im Sachgebiet Spionageabwehr im Niedersächsischen Verfassungsschutz entsprechende Verdachtsfälle auf.

Nachfolgend werden exemplarisch einige Fälle dargestellt, die nicht ausschließlich einen Niedersachsenbezug aufweisen müssen. Im Vordergrund steht daher der sensibilisierende Präventivcharakter. Die Bearbeitungsschwerpunkte der Spionageabwehr lagen 2022 bei den Ländern Russland und China.

Russland

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. In den vergangenen Jahren fand eine Umorientierung zum staatsnahen Patriotismus statt. Seit 2009 pflegen der Präsident der Night Wolves und der Russische Staatspräsident, Wladimir Putin, ein gutes Verhältnis. Putin verlieh ihm im Februar 2013 eine Ehrenmedaille für seine „patriotischen Verdienste".

Seit mehreren Jahren gedenkt der Club am 9. Mai, dem „Tag des Sieges", mit Fahrten und Kranzniederlegungen den Opfern des Zweiten Weltkrieges. Hierbei wird das Andenken derjenigen geehrt, die beim Kampf gegen den Faschismus gefallen sind. Abschluss und Höhepunkt der Fahrten sind die Veranstaltungen zur Erinnerung an das Kriegsende am Sowjetischen Ehrenmal in Berlin-Treptow.

Analysten gehen von weltweit einer vierstelligen Zahl von Mitgliedern und Unterstützerinnen und Unterstützern aus. Der Motorradclub ist in Chaptern organisiert. Geführt werden diese durch das „Motherchapter" „ROSSIJA".

Aufgrund der Nähe zu Putin liegt die Vermutung nahe, dass die Night Wolves politische Ziele des russischen Staatspräsidenten unterstützen und in seinem Auftrag handeln. Durch ihr medienwirksames Auftreten signalisieren sie Zustimmung für die russische Politik und nehmen damit möglicherweise Einfluss auf die politische Meinungsbildung in Deutschland.

Verstoß gegen das Außenwirtschaftsgesetz durch ein niedersächsisches Unternehmen

Im August 2022 wurde im Rahmen von Exekutivmaßnahmen u. a. eine niedersächsische Chemiefirma durchsucht. Dem Unternehmen werden in den vergangenen Jahren mehrere Verstöße gegen das Außenwirtschaftsgesetz vorgeworfen. Hierbei standen Verantwortliche des Unternehmens im Verdacht, Güter nach Russland ausgeführt zu haben, ohne dabei über die entsprechenden Genehmigungen zu verfügen.

Der Niedersächsische Verfassungsschutz war an Personenermittlungen und an Informationserhebungen zum niedersächsischen Unternehmen beteiligt. Die Ermittlungen der Exekutivbehörden dauern derzeit noch an.

Einflussnahme durch russische Staatsmedien

Vor dem Hintergrund des russischen Angriffskrieges auf die Ukraine wurden im Verfassungsschutzverbund Sonderauswertungen eingerichtet, um die mit diesem Konflikt in Zusammenhang stehenden nachrichtendienstlichen Aktivitäten, Cyberoperationen sowie Propaganda-, Desinformations- und Einflussnahmebemühungen in Deutschland zu beobachten und aufzuklären. Im besonderen Fokus standen Desinformations- und Propagandaaktivitäten russischer Medien.

China

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[124], der militärische Nachrichtendienst MID[125], das MÖS[126] und der Technische Militärische Nachrichtendienst NSD[127].

Gegenwärtig räumen chinesische Nachrichtendienste – neben den Themen um die Belt-and-Road-Initiative[128] – insbesondere den Entwicklungen im Sektor der Informationstechnologie (Cloud, Internet

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

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

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

127 Technischer militärischer Nachrichtendienst = Spezialisiert auf Satellitenaufklärung und hochentwickelte Cyberoperationen gegen kritische Infrastrukturen.

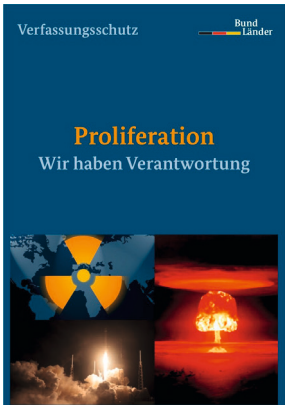
128 Der Begriff bezeichnet die Neue Seidenstraße. Sie ist ein langfristiges Projekt der Kommunistischen Partei Chinas zum Aufbau von Infrastrukturen für Transport, Versorgung und Handel. Vorbild sind historische Routen zwischen China und dem Westen, die man erweitert und verändert.

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 schlichten 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.

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 Staaten – unter Einbeziehung Ihrer Nachrichtendienste – betrieben wird.

Die aktuell dynamischen Entwicklungen in den lokalen Krisen- und Konfliktherden, ebenso wie die geopolitischen Machtspiele autoritärer Regime, verdeutlichen das zunehmende Gefährdungspotenzial 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 das 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.

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. Der Niedersächsische Verfassungsschutz leistet Prävention durch Aufklärung und steht als vertraulicher Ansprechpartner zur Verfügung.

Zur Aufdeckung und Verhinderung von proliferationsrelevanten Aktivitäten arbeitet der Niedersächsische Verfassungsschutz eng mit anderen Sicherheitsbehörden zusammen. Somit wird auch auf lokaler Ebene ein Beitrag mit internationaler Bedeutung geleistet.

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[129], Wirtschaft, Wissenschaft und

129 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).

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. Zuletzt hat es in Niedersachsen und bundesweit eine Vielzahl an Cyberangriffen gegeben, die mit dem Ziel der Verschlüsselung und der anschließenden Erpressung des Betroffenen[130] durchgeführt wurden. Neben den auch im Jahr 2022 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.

Eine große Gefahr für Unternehmen und Behörden stellen aktuell „Advanced Persistant Threats“[131] dar. Diese zielgerichteten Cyberangriffe durch fortgeschrittene, gut organisierte und professionell ausgestattete Angreifer, die ihre Anweisungen und Unterstützungen 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

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

131 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 in der Regel schwierig festzustellen (siehe Internetseite des Bundesamtes für Sicherheit in der Informationstechnik, www.bsi.bund.de).

oder Jahre hinweg. Sie stimmen ihre Aktivitäten auf die Sicherheitsmaßnahmen ihrer anvisierten Opfer ab und greifen diese oft mehrfach an. Die Bearbeitung solcher Cyberangriffe ist aufgrund der Anonymität des Angriffs und der nicht erkennbaren Motivation der Angreifer für die Sicherheitsbehörden eine große Herausforderung der kommenden Jahre.

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 anschließende Verschlüsselung der Systeme des Opfers, der Verschleierung der Aktivitäten und der Zielrichtung des Angriffs dienen.

Seit Jahresbeginn 2022, insbesondere seit Kriegsbeginn in der Ukraine, ist ein erhöhtes Hinweisaufkommen im Bereich Cyberabwehr festzustellen. Dies könnte mit einer erhöhten Alarmbereitschaft bei Cyberangriffen mit nachrichtendienstlichem Hintergrund liegen, da mehr Aufmerksamkeit und niedrigere Meldeschwellen als zuvor bestehen. Durch die hieraus resultierende höhere Anzahl der Sachverhaltsüberprüfungen konnten mehr Cyberangriffe validiert werden.

Neben direkten Cyberangriffen zum Zweck der Spionage oder Sabotage können häufig kompromittierte Systeme festgestellt werden, die als Bestandteil eines Botnetzes[132] von dem jeweiligen Akteur gesteuert werden. Hierbei handelt es sich meist um kompromittierte Systeme von Unternehmen, Behörden oder gar Privatpersonen.

Der Angreifer will ohne Wissen des Betroffenen dessen IP Adresse für weitere Angriffe nutzen. Die potenziellen Opfer müssen sich

132 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.

nicht notwendigerweise in Deutschland befinden. Beim Aufbau eines Botnetzes geht es hauptsächlich um Verschleierungsaktivitäten.
Ein konkreter, inzwischen öffentlich bekannter Fall nach diesem Muster betraf verschiedene niedersächsische Unternehmen. Die eingesetzte „Cyclops Blink Malware“ des Akteurs „Sandworm“ wird dem Russischen Nachrichtendienst „GRU“ zugeordnet. Der Akteur „Sandworm“ ist nach aktueller Einschätzung maßgeblich an Cyberangriffen gegen ukrainische Ziele beteiligt.
Bei einer anderen Art der staatlich gesteuerten Angriffe zielte der Angreifer auf Politiker, die im Bundestag, im Landtag oder auch in den Kommunalparlamenten tätig sind oder waren ab. Dort wurde durch einen mutmaßlichen ausländischen Cyberakteur versucht, E-Mail-Konten zu übernehmen, um anschließend, möglicherweise durch eine Desinformationskampagne, Einfluss nehmen zu können.
Konkrete erfolgreiche Angriffe auf kritische Infrastrukturen in Niedersachsen konnten bislang nicht festgestellt werden. Lediglich „Cyber-Kollateralschäden“ hatten spürbare Folgen, so der Ausfall des Satellitennetzwerks KA-SAT, der mutmaßlich im Zusammenhang mit dem Russland-Ukraine-Krieg stand. Bundesweit waren mindestens 3.000 Windräder, die über den Satellitenanbieter ferngewartet werden können, zeitweise nicht mehr erreichbar. Die Versorgungssicherheit war trotzdem gewährleistet.

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.