Spionageabwehr / Proliferation / Cyberabwehr

8.1 Sicherheitslage in Niedersachsen: Spionage und hybride Bedrohungen nehmen zu

8.1.1 Überblick

Deutschland ist als wirtschaftlich stärkstes EU-Mitglied, zweitgrößter Netto-Zahler der NATO und eine der führenden Wirtschaftsmächte weltweit ein besonders interessantes Ziel für ausländische Geheimdienste. Spionage richtet sich dabei nicht nur gegen Politik und Verwaltung, sondern auch gegen Wirtschaft, Wissenschaft und das Militär. Die aktuelle weltpolitische Lage ist dabei oft ausschlaggebend: Machtverschiebungen zwischen Europa, den USA, Russland und China sowie der weiterhin andauernde russische Angriffskrieg gegen die Ukraine haben die Bedrohungen für Deutschland und somit auch für Niedersachsen weiter verstärkt.

Hinzu kommen sogenannte hybride Bedrohungen – also Mischformen aus klassischer Spionage, Sabotage, Cyberangriffen und Desinformation. Gerade Regionen mit besonderer strategischer Bedeutung, wie die niedersächsische Küste mit ihren Häfen, Energieanlagen und militärischen Einrichtungen, stehen hierbei im Fokus. Berichte über Drohnenüberflüge oder verdächtige Aktivitäten zeigen, dass auch hier versucht wird, Informationen zu sammeln und/oder die Reaktionsfähigkeit der Sicherheitsbehörden zu testen. Die Gefährdung für Deutschland entsteht somit aus einem komplexen Zusammenspiel unterschiedlicher Interessen und Methoden. Sie reicht von Spionage oder Sabotage über wirtschaftliche Einflussnahme bis hin zu Cyberangriffen – und betrifft damit auch direkt die Menschen und Unternehmen in Niedersachsen. Diese verschiedenen Aktivitäten haben auch zum Ziel, die öffentliche Meinung zu beeinflussen, das Vertrauen in demokratische rechtsstaatliche Institutionen zu untergraben, politisch Verantwortliche zu diffamieren und Ängste innerhalb der Bevölkerung zu schüren.

8.1.2 Sicherheitsarchitektur

Im Rahmen der jeweiligen nationalen Sicherheitsarchitektur unterhalten zahlreiche Staaten Nachrichtendienste, deren Aufgabe in der Sammlung und Auswertung relevanter Informationen, auch mittels nachrichtendienstlicher Mittel, besteht.
Insbesondere in totalitären Systemen agieren diese Dienste als Instrumente der Machtprojektion und führen auch aktive Maßnahmen durch. Dieses hybride Spektrum umfasst u. a. die politische Einflussnahme, Sabotageakte bis hin zur Durchführung von Attentaten. Einzelne Dienste verfügen zudem über paramilitärische Einheiten für verdeckte Operationen und Kommandounternehmungen.
Obwohl die klassische Spionage im öffentlichen Diskurs mitunter teilweise als ein Phänomen vergangener Epochen betrachtet wird, hat sie auch im Zeitalter der globalen digitalen Vernetzung und des rapiden technologischen Fortschritts sowie im Kontext des völkerrechtswidrigen Angriffs Russlands auf die Ukraine weiterhin eine große Relevanz für Sicherheitsbehörden von Bund und Ländern. Darüber hinaus bleibt die Gewinnung und Führung menschlicher Quellen (Human Intelligence) eine zentrale operative Methode.

In der Bundesrepublik Deutschland sind der Auslandsnachrichtendienst [Bundesnachrichtendienst (BND)], der Inlandsnachrichtendienst (Verfassungsschutz) sowie der militärische Nachrichtendienst [Bundesamt für den Militärischen Abschirmdienst (BAMAD)] mit der Informationsbeschaffung betraut.

Nachrichtendienste unterliegen in Rechtsstaaten der Fach- und Rechtsaufsicht ihrer übergeordneten Dienststellen, da sie – wie jede staatliche Gewalt – an Recht und Gesetz gebunden sind. Aufgrund ihrer verdeckten Arbeitsweise und des Interesses von Regierungsstellen an der Informationsgewinnung und Analyseergebnissen wird eine Aufsicht durch Exekutivbehörden selbst oft nicht als hinreichend erachtet. Die Kontrolle wird daher durch parlamentarische Gremien ergänzt. Diese kann durch Debatten, Aktuelle Stunden oder auch durch parlamentarische Anfragen in und aus den jeweiligen Parlamenten erfolgen.[184]

184 Siehe auch Kapitel 1.6.

360-Grad-Blick der Verfassungsschutzbehörden

Das Sachgebiet Spionageabwehr im Niedersächsischen Verfassungsschutz hat den gesetzlichen Auftrag, alle Informationen über sicherheitsgefährdende oder geheimdienstliche Aktivitäten zu erheben, zu analysieren und Spionage sowie Proliferation[185] zu verhindern. Niedersachsen ist als erfolgreicher Wirtschaftsstandort potenzielles Ziel von Spionageaktivitäten fremder Geheim- oder Nachrichtendienste[186].

8.1.3 Prävention

Als weitere wichtige Aufgabe leisten die Fachbereiche Spionageabwehr, Proliferationsbekämpfung, Wirtschaftsschutz und Cyberabwehr des Niedersächsischen Verfassungsschutzes Präventionsarbeit in Niedersachsen. Ziel ist es, Unternehmen, Behörden und Forschungseinrichtungen vor Informationsabfluss, Manipulation und Sabotage durch Extremisten oder ausländische Dienste zu schützen. So werden die entsprechenden Mitarbeitenden über mögliche Angriffe informiert und sensibilisiert. Des Weiteren beobachtet der Niedersächsische Verfassungsschutz aktuelle Entwicklungen und gibt konkrete Handlungsempfehlungen. Das Präventionsangebot reicht von öffentlichen Veranstaltungen und Beiträgen auf Sicherheitskonferenzen bis hin zu direkten Gesprächen mit Vertretenden der jeweiligen Zielgruppe. Ergänzend dazu werden die Herausforderungen und aktuellen Themen der hybriden Bedrohungen in Fachvorträgen auf Wirtschaftsschutztagungen sowie durch Informationsschreiben an potenziell Betroffene herangetragen. Durch einen regelmäßigen Austausch ist der Niedersächsische Verfassungsschutz ein verlässlicher Ansprechpartner für die Wirtschaft.

Der Niedersächsische Verfassungsschutz nimmt aktuelle Gefahren u. a. durch hybride Bedrohungen sehr ernst. Deshalb wurden die Bereiche

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

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

Wirtschaftsschutz und Spionageabwehr personell erheblich verstärkt, um hybriden Bedrohungen aktiv und nachhaltig zu begegnen.
Um schnell und wirksam reagieren zu können arbeitet der Niedersächsische Verfassungsschutz eng mit anderen Sicherheitsbehörden in Niedersachsen, in den Bundesländern und auf Bundesebene zusammen. Es gibt regelmäßige Besprechungen, gegenseitige Hospitationen und spezielle Meldedienste, über die Informationen schnell weitergegeben werden können. So soll die Sicherheit in Niedersachsen effektiv und nachhaltig gestärkt werden.

Die Hauptakteure der klassischen Spionageaktivitäten in der Bundesrepublik Deutschland sind nach wie vor die Russische Föderation, die Volksrepublik China und die Islamische Republik Iran. Die Schwerpunkte der Interessen dieser Länder orientieren sich an den politischen Vorgaben und wirtschaftlichen Prioritäten der jeweiligen Regierungen.

Aufgrund der zum Teil desolaten Sicherheitslagen in ihren Heimatländern und der damit verbundenen existenziellen Bedrohungen sucht eine große Zahl von Menschen weiterhin 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 darüber hinaus 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. Nach der Schließung von Auslandsvertretungen, wie z. B. im Fall von Russland oder dem Iran, spielen soziale Netzwerke oder reisende Agenten

bei der Anbahnung von Kontakten oder der Abschöpfung von Informationen eine wichtige Rolle.

Eine Vielzahl von Informationen, die für fremde Geheim- oder Nachrichtendienste interessant erscheinen und früher nur mit klassischen Spionagetätigkeiten zu erheben waren, sind heutzutage mit wenig Aufwand und fast ohne Aufdeckungsrisiko auf virtuellem Wege zu erlangen. Manche Hinweise deuten darauf hin, dass bei bestimmten Angriffen auch staatliche Stellen oder Geheimdienste beteiligt sein könnten. Da Angreifer häufig dieselben technischen Mittel und Vorgehensweisen nutzen, lassen sich diese in vielen Fällen erkennen und bestimmten Akteuren zuordnen.

8.1.4 Schwerpunkte der Spionageabwehr in Niedersachsen

Russland

Logo des SWR

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.

Als Unterstützer der Ukraine steht Deutschland und somit auch Niedersachsen im Fokus ausländischer, insbesondere russischer

Geheimdienste und sieht sich in regional unterschiedlicher Intensität mit hybriden Bedrohungen konfrontiert.

So zielen russische Hacker auf deutsche Regierungsstellen, Unternehmen und Kritische Infrastrukturen (KRITIS)[187] ab, um sensible Daten zu stehlen oder Systeme zu stören. Auch gab es Fälle, in denen russische Staatsbürger verdächtig waren, sich Zugang zu militärischen Einrichtungen oder sensiblen Bereichen zu verschaffen, um dort Informationen zu erheben, die im Falle eines sich verschärfenden Konflikts für die russische Seite nützlich sein könnten. Darüber hinaus hat der Einsatz von Drohnen zur mutmaßlichen Ausspähung von Bundeswehr-Standorten und anderen strategischen Zielen deutlich zugenommen.

Low-Level-Agenten

Bei den sogenannten Low-Level-Agenten, die oft als Handlanger fungieren und für russische Auftraggeber Propaganda betreiben, Ziele ausspähen oder Sabotageaktionen ausführen, handelt es sich um Personen, die für russische Geheimdienste oder sonstige staatliche Organe tätig werden, ohne diesen selbst anzugehören. Die oft (klein-)kriminellen Akteure werden häufig über soziale Medien oder Messengerdienste angeworben und gesteuert. Der nachrichtendienstliche Hintergrund des Auftraggebers bleibt ihnen dabei mutmaßlich häufig verborgen – auch aufgrund von undurchsichtigen Auftragsketten mit zwischengeschalteten Mittelsmännern.
„Low-Level-Agenten" sind eine latente Gefahr. Sie sind nicht oder nur oberflächlich nachrichtendienstlich ausgebildete Täter, die gegen Bezahlung oder aus anderen Motiven mit konkreten, i. d. R. einfach auszuführenden Spionage- und Sabotagehandlungen beauftragt werden. Häufig wird ihnen nicht einmal bewusst sein, dass sie für einen fremden Staat handeln und verfolgen i. d. R. rein wirtschaftliche Interessen. Dieses Vorgehen ermöglicht dem russischen Geheimdienst im Zielland zu agieren, ohne eine Aufdeckung und Festnahme der eigenen Mitarbeitenden zu riskieren.

187 Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen von essenzieller 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).

So ließ die Bundesanwaltschaft 2025 drei ukrainische Staatsangehörige festnehmen, weil sie sich gegenüber russischen staatlichen Stellen zu Brand- und Sprengstoffanschlägen auf den Gütertransportverkehr in Deutschland bereit erklärt haben sollen. Dies ist nur ein Beispiel für das hohe Gefährdungspotenzial, das von dem Einsatz fremdstaatlich gesteuerter „Low-Level-Agenten" ausgeht.

Schutz der Kritischen Infrastruktur (KRITIS)

Der russische Angriffskrieg gegen die Ukraine hat dazu geführt, dass KRITIS wie Energieanlagen, Häfen oder Kommunikationsnetze stärker in den Fokus der niedersächsischen Sicherheitsbehörden genommen werden. Solche Einrichtungen gelten grundsätzlich als mögliche Ziele für Spionage, Cyberangriffe oder politisch motivierte Straftaten.

Um Gefahren frühzeitig zu erkennen, erstellen Polizei und Verfassungsschutz regelmäßig Bedrohungsanalysen und passen Schutzmaßnahmen an die jeweilige Lage an. Für die niedersächsische Küstenregion liegen zwar derzeit keine konkreten Hinweise auf Angriffe vor, dennoch bleibt sie wegen ihrer maritimen Bedeutung und Nähe zu wichtigen Infrastrukturen besonders sensibel.

Unterseekabel, Pipelines und Hafenanlagen stehen im Zentrum der Aufmerksamkeit. Russische Schiffe – darunter auch die sogenannte Schattenflotte – sind weiterhin in Nord- und Ostsee präsent und werden von deutschen Sicherheitsbehörden genau beobachtet, da von ihnen ausgehende Spionage- oder Sabotagehandlungen nicht ausgeschlossen werden können.

Alle deutschen Sicherheitsbehörden stellen sich kontinuierlich aktiv auf die sich stets verändernde Sicherheitslage und die mit dem Russland-Ukraine-Konflikt zusammenhängenden Herausforderungen ein.[188]

188 Siehe auch Kapitel 2.2.

8.1.5 Festnahmen, sicherheitsrelevante Vorfälle und sonstige Maßnahmen mit Bezug nach Niedersachsen

China

Logo des MSS

Um ihren Machtanspruch zu sichern und die eigenen wirtschaftlichen Ziele erreichen zu können, setzt die Volksrepublik China Geheimdienste ein. Von den vier chinesischen Geheimdiensten ist insbesondere das chinesische „Ministerium für Staatssicherheit" (MSS) für die In- und Auslandsaufklärung zuständig.[189] Es gilt als weltweit größter ziviler Geheimdienst.

Die Volksrepublik China bedient sich ihrer Geheimdienste als Mittel zum Regimeerhalt. Übergeordnetes Ziel allen geheimdienstlichen Handelns ist die Aufrechterhaltung des Machtanspruchs der Kommunistischen Partei Chinas. 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 umfassender Informationsbedarf, den China offensiv auch mit geheimdienstlichen Mitteln deckt. Zu den wesentlichen geheimdienstlichen Akteuren zählen neben dem nichtmilitärischen MSS, der militärische Geheimdienst MID[190], das MÖS[191] sowie der technisch-militärische Geheimdienst NSD[192].

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

189 Geheimdienst mit Exekutivbefugnissen, Schwerpunkt: Beobachtung oppositioneller Bestrebungen.

190 Militärischer In- und Auslandsgeheimdienst = Abschirmung gegen Aufklärungsversuche, Informationsgewinnung zu ausländischen Streitkräften.

191 Ministerium für öffentliche Sicherheit = Dem Polizeiministerium unterstellt, Bereitstellung geheimdienstlicher Spezialeinheiten.

192 Technisch-militärischer Geheimdienst = Spezialisiert auf Satellitenaufklärung und hochentwickelte Cyberoperationen gegen Kritische Infrastrukturen.

Gegenwärtig räumen chinesische Geheimdienste, neben den Themen um die Belt-and-Road-Initiative[193] – insbesondere den Entwicklungen im Sektor der Informationstechnologie (Cloud, Internet of Things, Quantentechnologien, Robotik, 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. Die Informationsbeschaffung dient in erster Linie dem Profit der eigenen Nation. Die Schädigung des Gegners wird von den chinesischen Diensten als zweckdienliches Mittel in Kauf genommen, ist aber oft selbst nicht Ziel des geheimdienstlichen Handelns.

Logo des VAJA

Iran

Die Geheimdienste der Islamischen Republik Iran sind eine wichtige Stütze für das dortige Regime. Das Ministerium für Nachrichtenwesen (MOIS oder VAJA) ist der zivile Auslandsgeheimdienst des Iran.

Die Ausspähung von Oppositionellen ist eine zentrale Aufgabe für die iranischen Geheimdienste, wobei die Aktivitäten von der Beobachtung von Demonstrationen bis zur Bedrohung konkreter Personen reichen. In Niedersachsen führt der Verfassungsschutz in solchen Fällen gemeinsam mit weiteren Sicherheitsbehörden Aufklärungs- und Schutzmaßnahmen durch.

193 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.

Hinweise

Für Hinweise auf Spionageaktivitäten oder andere sicherheitsgefährdende Vorkommnisse steht der Niedersächsische Verfassungsschutz als vertrauensvoller Ansprechpartner unter folgender Erreichbarkeit zur Seite:
E-Mail: Kontakt@mi.niedersachsen.de

In dringenden Fällen – insbesondere, wenn Gefahr für Leib und Leben besteht – ist die Polizei unter der Notrufnummer 110 zu alarmieren.

Weitere Informationen zum Thema Spionage können Sie auch dem Flyer „Spionage – (k)ein Thema?!" entnehmen, den Sie auf unserer Internetseite herunterladen können.

8.2 Proliferation

Proliferationsbekämpfung umfasst Maßnahmen zur Eindämmung der Verbreitung atomarer, biologischer und chemischer Waffensysteme sowie der hierfür benötigten Trägersysteme.
Sie beschränkt sich aber mittlerweile nicht nur hierauf, sondern beinhaltet auch die unkontrollierte Verbreitung und Weitergabe von digitalen Werkzeugen, Technologien oder Software, die für Cyberoperationen genutzt werden können.

Die Bundesrepublik Deutschland hat sich, ebenso wie zahlreiche andere Staaten, international verpflichtet, die Verbreitung und den Einsatz von Massenvernichtungswaffen zu verhindern, um Frieden und Stabilität zu sichern. Den Verfassungsschutzbehörden obliegt der Aufgabenbereich der Proliferationsbekämpfung. Sie leisten somit einen bedeutenden Beitrag zum friedlichen Zusammenleben der Völker.

Proliferation geht i. d. R. nicht von Einzelpersonen aus, sondern wird von Staaten betrieben, häufig unter Einbindung ihrer Geheim- oder Nachrichtendienste. Dabei handelt es sich um Akteure, bei denen die Gefahr besteht, dass sie ABC-Waffen in bewaffneten Konflikten einsetzen oder deren Einsatz zur Durchsetzung politischer Ziele

androhen. Die aktuellen Entwicklungen in internationalen Krisen- und Konfliktregionen sowie das machtpolitische Agieren autoritärer Regime erhöhen die sicherheitspolitischen Risiken und unterstreichen die Relevanz wirksamer Gegenmaßnahmen.

Da entsprechende Waffen- und deren Trägersysteme nicht vollständig frei verfügbar sind, konzentrieren sich proliferationsrelevante Staaten häufig auf den Erwerb einzelner Bauteile und Komponenten. Im Mittelpunkt stehen dabei sogenannte Dual-Use-Güter, also Produkte, Technologien, Software und Fachwissen, die sowohl für zivile als auch für militärische Zwecke geeignet sind. Proliferationsbestrebungen zielen darauf ab, den militärischen Nutzen solcher Güter hinter einem zivilen Verwendungszweck zu verschleiern. Der Einsatz von Deck- und Tarnfirmen, fingierte Geschäftsbeziehungen, gezielt irreführenden Waren- und Endverbleibsangaben oder Umweglieferungen über vermeintlich unkritische Drittstaaten, die als Zwischenstation oder Verschleierungsplattform fungieren, sowie verdeckte Beschaffungswege erschweren die Identifizierung und Aufklärung entsprechender Aktivitäten erheblich, insbesondere wenn sie durch staatliche Geheim- oder Nachrichtendienste gesteuert werden.

In den vergangenen Jahren hat sich das Aufgabenspektrum der Proliferationsabwehr deutlich erweitert und umfasst mittlerweile auch den Bereich der sogenannten Emerging Technologies (EMT). Darunter fallen neuartige technologische Entwicklungen und Hochinnovationen, die, unabhängig von klassischem ABC-Bezug, das Potenzial besitzen, militärische Fähigkeiten und Konfliktdynamiken in einer Weise zu verändern, die in ihrer Wirkung mit strategischen Waffensystemen vergleichbar sein können.

Dazu zählen z. B. Fortschritte in der Künstlichen Intelligenz (KI), autonom agierende Systeme, Quantentechnologien, neuartige Sensorik oder biotechnologische Verfahren. Deren sicherheitsrelevante Einsatzmöglichkeiten werden oft erst während der Entwicklungsphase erkannt. Bestehende Exportkontroll- und Regulierungssysteme decken diese Bereiche bislang nur teilweise ab und technologische Entwicklungen schreiten deutlich schneller voran als die Anpassung rechtlicher Rahmenbedingungen. Der Prävention kommt somit

eine wachsende Bedeutung zu. Der Niedersächsische Verfassungsschutz trägt diesem Umstand Rechnung und hat sich zum Ziel gesetzt, Forschungseinrichtungen und Unternehmen frühzeitig für die sicherheitsrelevanten Aspekte von EMT zu sensibilisieren. Durch gezielte Risikoaufklärung und den intensiven Austausch mit exponierten Unternehmen und Forschungseinrichtungen soll verhindert werden, dass neue Schlüsseltechnologien unbemerkt in die Hände von Staaten gelangen, die sie für destabilisierende oder militärische Zwecke missbrauchen könnten.

Niedersachsen ist ein Wirtschafts- und Wissenschaftsstandort mit einer Vielzahl hochinnovativer Unternehmen und Forschungsinstitutionen. Viele der hier entwickelten oder produzierten Technologien, Komponenten und Materialien besitzen ein erhebliches Dual-Use-Potenzial und können bei missbräuchlicher Anwendung zur Herstellung, Modernisierung oder Funktionssteigerung von Massenvernichtungswaffen beitragen.

Staaten, die entsprechende Fähigkeiten anstreben, versuchen deshalb zunehmend Zugang zu diesen Gütern zu erlangen. Für die Beschaffung werden oft nachrichtendienstliche Strukturen und Vorgehensweisen genutzt, um geltende Exportbestimmungen zu umgehen.

In der Praxis zeigt sich immer wieder, dass deutsche Unternehmen und Forschungseinrichtungen die sicherheitsrelevanten Hintergründe solcher Anfragen nicht oder erst zu spät erkennen. Die Gefahr eines unbeabsichtigten Beitrags zu Proliferation ist real und betrifft insbesondere hochspezialisierte Nischenbranchen sowie Forschungsfelder mit komplexen technischen Inhalten. Neben den erheblichen Risiken, die aus einer möglichen Mitwirkung an der Weiterverbreitung von Massenvernichtungswaffen entstehen, sind Verstöße gegen exportkontrollrechtliche Vorgaben auch rechtlich erheblich: Die unerlaubte Ausfuhr oder Weitergabe kontrollierter Güter kann je nach Schwere als Ordnungswidrigkeit oder Straftat geahndet werden, u. a. nach dem Außenwirtschaftsgesetz, der Außenwirtschaftsverordnung und gegebenenfalls dem Kriegswaffenkontrollgesetz.

Im Rahmen der Proliferationsbekämpfung sind internationale Sanktionen gegen Staaten wie Russland, Iran oder Nordkorea wichtige Instrumente zur Exportkontrolle und zum Schutz von Know-how. Neben Exportbeschränkungen in den Bereichen Finanzen, Transport und Energie stehen insbesondere proliferationsrelevante Güter, konventionelle Waffen und Hochtechnologieprodukte im Fokus der Maßnahmen. Oftmals versuchen sanktionierte Staaten, die Verbote zu umgehen.
Im Zusammenhang mit dem Russland-Ukraine-Krieg hat die EU zahlreiche Sanktionen gegen Russland verhängt, wodurch die Beschaffung von Rüstungsgütern sowie Dual-Use-Produkten für russische Akteure deutlich erschwert werden soll.

Bestehende Netzwerke zu niedersächsischen Unternehmen und Forschungseinrichtungen konnten weiter ausgebaut werden

Eine vertrauensvolle Zusammenarbeit baut Berührungsängste ab, stärkt Informationswege und sensibilisiert Verantwortliche für potenzielle Risiken im eigenen Arbeitsumfeld. Die etablierte Zusammenarbeit zwischen dem Niedersächsischen Verfassungsschutz und niedersächsischen Unternehmen sowie Forschungseinrichtungen hat zu einer größeren Aufmerksamkeit gegenüber auffälligen Anfragen, ungewöhnlichen Geschäftsbeziehungen oder sicherheitsrelevanten Forschungskooperationen geführt. Dies trägt dazu bei, dass verdächtige Vorgänge erkannt und dem Niedersächsischen Verfassungsschutz gemeldet werden, was wiederum die Qualität und Quantität des Hinweisaufkommens verbessert. Die gewachsenen Netzwerke bilden damit eine wichtige Grundlage für eine wirksame Proliferationsabwehr in Niedersachsen.

Im Rahmen der Proliferationsbekämpfung hat sich gezeigt, dass sich die Beschaffungsbemühungen der Volksrepublik China deutlich von den Aktivitäten anderer Staaten, die an Massenvernichtungswaffen oder deren Trägersystemen interessiert sind, unterscheiden. Anders als klassische Proliferationsakteure ist China aufgrund seines enormen technologischen Entwicklungsstands im Bereich der ABC-Waffentechnologien weitgehend autark und auf internationale Beschaffungswege kaum angewiesen. Zugleich verfolgt China ambitionierte Ziele im Bereich der sogenannten EMT.

Die wesentlichen Beschaffungsbemühungen beziehen sich daher auf zentrale Zukunftstechnologien. Um eine globale Führungsrolle im Hochtechnologiebereich zu erreichen, nutzt die Volksrepublik gezielt den Zugang zu deutschen Unternehmen, Forschungseinrichtungen und wissenschaftlichen Netzwerken. China setzt dabei ein breites Spektrum an Vorgehensweisen ein, um Zugang zu sensiblen Technologien, Expertise und Schlüsselkompetenzen zu erlangen. Dazu zählt der Erwerb kompletter Unternehmen ebenso wie langfristig angelegte wissenschaftliche Kooperationen, Forschungsstipendien, Joint Ventures oder die gezielte Rekrutierung von Fachkräften. Ergänzend tritt die gezielte Pflege persönlicher Beziehungen zu politischen, wirtschaftlichen oder wissenschaftlichen Entscheidungsträgerinnen und -trägern hinzu, um Einflusskanäle aufzubauen und strategische Interessen zu platzieren. Viele dieser Aktivitäten bewegen sich im Rahmen legaler wirtschaftlicher oder wissenschaftlicher Kooperationen und unterliegen weder internationalen Sanktionen noch den klassischen Exportkontrollmechanismen, was ihre sicherheitsrelevante Bewertung zusätzlich erschwert. Deutschland ist aufgrund seiner technologischen Spitzenposition und seiner offenen Forschungsstrukturen in besonderer Weise gefährdet. Es besteht die Gefahr, dass wertvolles Know-how, Forschungsergebnisse oder Hochtechnologie unbemerkt abfließen. Der Dual-Use-Charakter zahlreicher Schlüsseltechnologien, etwa in der KI, Robotik, Sensorik, Halbleitertechnologie, Quantenforschung oder modernen Biotechnologie, verschärft die Lage.

Proliferationsrelevante Staaten entsenden aber auch regelmäßig Gastwissenschaftlerinnen und -wissenschaftler an deutsche, darunter auch niedersächsische, Hochschulen und Forschungseinrichtungen. Im Einzelfall ist zu prüfen, ob ein möglicher Bezug zu Beschaffungsbemühungen für Programme zur Herstellung von Massenvernichtungswaffen besteht. Bei Bedarf sensibilisiert der Niedersächsische Verfassungsschutz die betreuenden Wissenschaftlerinnen und Wissenschaftler für entsprechende Risiken und informiert diese über aktuelle Entwicklungen. Der Niedersächsische Verfassungsschutz engagiert sich präventiv, indem er gezielte Informations- und Aufklärungsarbeit leistet und als vertraulicher Ansprechpartner für Unternehmen, Forschungseinrichtungen und Wissenschaftler zur Verfügung steht.

Proliferationsabwehr ist eine Gemeinschaftsaufgabe. Nur wenn Verdachtsmomente früh identifiziert werden und Wissen geteilt wird, lassen sich Risiken minimieren und gefährliche Entwicklungen unterbinden. Daher arbeitet der Verfassungsschutz eng mit weiteren Sicherheitsbehörden auf Landes- und Bundesebene zusammen, um verdächtige Vorgänge zu identifizieren, Informationen zu bündeln und koordinierte Gegenmaßnahmen einzuleiten.

Auf diese Weise trägt der Niedersächsische Verfassungsschutz aktiv zur Aufdeckung und Unterbindung proliferationsrelevanter Aktivitäten bei und leistet auf lokaler Ebene einen bedeutenden Beitrag zur internationalen Sicherheit.

8.3 Cyberabwehr

Die Abhängigkeit unserer Gesellschaft von Informations- und Kommunikationstechnologien steigt. Die dadurch verursachte Verwundbarkeit moderner Gesellschaften stellt eine große sicherheitspolitische Herausforderung dar. Der mögliche Schaden für Staaten, ihre Bevölkerung und ihre Volkswirtschaften im Falle der Beeinträchtigung von Informations- und Kommunikationsinfrastrukturen ist immens. Staat, Kritische Infrastrukturen, Wirtschaft, Wissenschaft und Bevölkerung sind auf das verlässliche Funktionieren dieser Technologien, insbesondere des Internets, angewiesen. Cyberangriffe werden 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 geheim- bzw. nachrichtendienstliche Hintergründe sind denkbar. Die für solche Angriffe häufig genutzten hoch entwickelten Schadprogramme abzuwehren und zurückzuverfolgen, erfordert eine enge Kooperation der Sicherheitsbehörden.

Auch 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.[194] Auf den einschlägigen Seiten für die Internetsicherheit, wie z. B. auf der Internetseite des Bundesamtes für Sicherheit in der Informationstechnik (BSI; https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html) werden die Angriffe statistisch dargestellt. Neben den im Jahr 2025 fortgesetzten Angriffen auf Großunternehmen waren in Niedersachsen diverse kleinere und mittelständische Unternehmen, politische Parteien, Nichtregierungsorganisationen oder auch Privatpersonen betroffen. Das verdeutlicht, welch hohen Stellenwert die IT-Sicherheit in allen Bereichen hat.

Eine große Gefahr für Unternehmen und Behörden stellen nach wie vor „Advanced Persistant Threats"[195] dar. Diese zielgerichteten Cyberangriffe durch gut organisierte und professionell ausgestattete Hacker, die Anweisungen und Unterstützung i. d. R. von Regierungen erhalten können, 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 grundsätzlich langfristig, meist über mehrere Monate oder Jahre hinweg. Sie stimmen ihre Aktivitäten auf die Sicherheitsmaßnahmen ihrer anvisierten Opfer ab und greifen diese häufig 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.

Im Rahmen einer Studie des Branchenverbands der deutschen Informations- und Telekommunikationsbranche (Bitkom e. V.) aus dem Jahr 2025 wurden durch Cyberangriffe geschädigte Unternehmen befragt. Die Befragung ergab einen signifikanten Anstieg

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

195 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 System verschafft und 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).

staatlich gesteuerter Cyberangriffe[196]. Im Jahr 2023 gaben nur sieben Prozent der Befragten an, von einem Cyberangriff von einem ausländischen Nachrichtendienst betroffen gewesen zu sein, im Jahr 2025 waren es 28 Prozent. Diese Steigerung kann auf den Umstand einer erhöhten Sensibilität und der verbesserten Möglichkeiten zur Zuordnung von staatlichen Akteuren im Cyberraum zurückgeführt werden. Ein tatsächlicher Anstieg von Cyberangriffen durch ausländische Nachrichtendienste ist im Hinblick auf die aktuelle weltpolitische Lage allerdings wahrscheinlich.

Die Abgrenzung zwischen Cybercrime und Cyberspionage, also Cyberangriffe durch ausländische Nachrichtendienste ist i. d. R. schwierig, da auch bei 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 zur finanziellen Bereicherung dienen.

Des Weiteren liegen vermehrt Hinweise vor, die darauf schließen lassen, dass ausländische Geheimdienste im Kontakt zu bislang vorwiegend finanziell motivierten Ransomware-Gruppierungen stehen. Aus einer Veröffentlichung von als authentisch bewerteten Kommunikationsdaten der russischen Ransomware-Gruppierungen „Black Basta" untereinander, gehen Verbindungen zum russischen Geheimdienst FSB hervor, die darauf hindeuten, dass führende Mitglieder der Gruppierung in Kontakt zu russischen staatlichen Stellen standen.[197] Das macht deutlich, dass russische Ransomware Gruppierungen wie „Black Basta" mit hoher Wahrscheinlichkeit auch Teil der hybriden Bedrohungen durch Russland sind. Die Einschätzung, dass solche Akteure von staatlichen russischen Stellen geduldet werden, besteht bereits seit einigen Jahren. Die

196 https://www.bitkom.org/sites/main/files/2025-09/bitkom-pressekonferenz-wirtschaftsschutz-cybercrime.pdf.

197 https://www.spiegel.de/netzwelt/web/ransomware-gruppe-black-basta-wie-ein-mutmasslicher-erpresser-aus-russland-der-justiz-entkam-a-df47e7f1-69de-4d60-bc34-af22e6e8fc05.

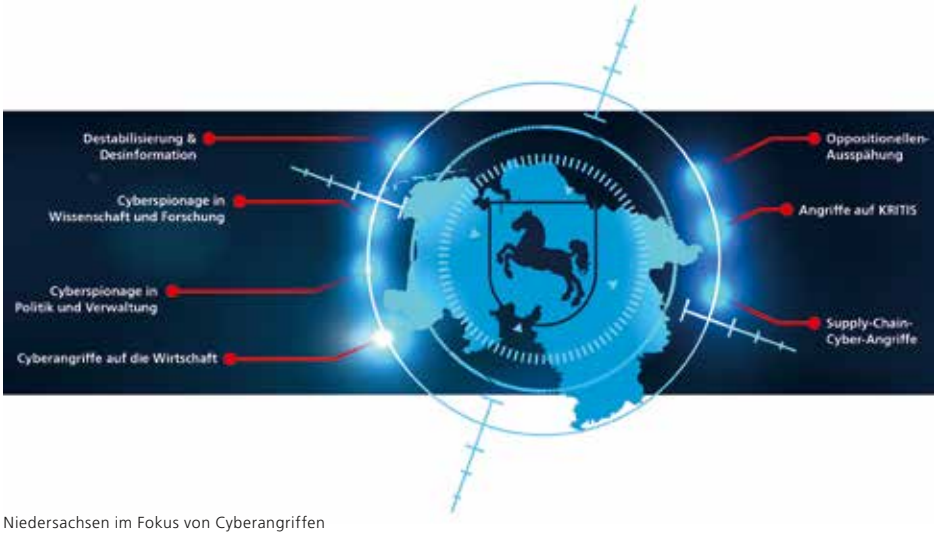
geleakten Informationen vermitteln jedoch den Eindruck, dass solche Gruppierungen wahrscheinlich sogar aktiv durch russische Stellen unterstützt und gesteuert werden. Angesichts der aktuellen politischen Lage erscheint eine Schwächung der deutschen Wirtschaft zudem zielführend für Russland.

Abgesehen von Ransomware-Gruppierungen gibt es auch sogenannte Hacktivismus-Gruppierungen. Dabei handelt es sich um Einzelpersonen oder koordinierte Kollektive, die Hacking-Techniken anwenden, um politische, soziale oder ideologische Anliegen zu fördern. Im Gegensatz zu gewöhnlichen Cyberkriminellen geht es ihnen nicht um finanziellen Profit, sondern um Aufmerksamkeit. Hierzu nutzen Hacktivismus-Gruppierungen häufig DDoS-Angriffe[198], die die Verfügbarkeit von Webseiten beeinträchtigen, indem gezielt eine Überlastung durch massenhafte Anfragen durch verschiedene vom Angreifer kontrollierte Systeme verursacht wird. Solche Angriffe führen i. d. R. keinen großen Schaden herbei, da die Angreifer dadurch keinen Zugriff auf die Daten der Betroffen erlangen. Prorussische Hacktivismus-Gruppierungen nutzen solche DDoS-Angriffe in erster Linie als Werkzeug der Propaganda, die darauf abzielt, gesellschaftliche Verunsicherung zu stiften und das Vertrauen in staatliche Institutionen zu untergraben. Daneben gibt es auch Hacktivismus-Gruppierungen wie „Z-Pentest Alliance“, die für ihre Angriffe auf KRITIS im Europäischen Raum, insbesondere in den Bereichen Energie und Wasser, bekannt sind. Dabei kompromittieren die Angreifer IT-Systeme, indem sie sich Zugriff auf Steuerungssysteme oder vertrauliche Daten verschaffen. Dieses Vorgehen ist deutlich kritischer zu bewerten. In Niedersachsen griff diese Gruppierung im Jahr 2025 auch Unternehmen im Energiesektor an. Das Ausmaß des Schadens war überschaubar, da es sich um kleine Anlagen handelte, die nicht dem KRITIS-Bereich zugeordnet werden.

198 Ein DDoS-Angriff („Distributed Denial of Service“) ist ein Cyberangriff, bei dem ein Ziel wie ein Server oder eine Website mit einer Flut von gefälschtem Internetverkehr überlastet wird. Angreifer nutzen dafür eine große Anzahl infizierter Computer, ein sogenanntes Botnetz, um das Ziel lahmzulegen. Dies führt dazu, dass legitime Nutzer keinen Zugriff mehr auf den Dienst haben.

Neben direkten Cyberangriffen zum Zweck der Spionage oder Sabotage werden von der Cyberabwehr im Niedersächsischen Verfassungsschutz häufig kompromittierte Systeme festgestellt, die als Bestandteil eines Botnetzes[199] gesteuert werden. Betroffen waren meist Systeme von Unternehmen, Behörden, Parteien oder Privatpersonen. Häufig wollen die Angreifenden ohne Wissen der Betroffenen deren IP-Adresse für weitere Angriffe, z. B. im Rahmen eines DDoS-Angriffs, nutzen. Beim Aufbau eines Botnetzes geht es hauptsächlich um Verschleierungsaktivitäten und die Stärkung der eigenen Ressourcen in Form von Rechenkapazität durch die Vernetzung mehrerer PCs.

Nordkoreanische Akteure veröffentlichten im Jahr 2025 Stellenanzeigen oder schrieben aktiv Personen mit Jobangeboten an. Das Interesse an einer vermeintlich lukrativen Stelle wurde so ausgenutzt, um Betroffene zur Ausführung von maliziöser Software



Niedersachsen im Fokus von Cyberangriffen

199 Ein Botnet oder Botnetz besteht aus gekaperten IT-Systemen, deren Nutzer in aller Regel nicht 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.

zu bringen. Hierzu suggerierte der Akteur der Interessentin oder dem Interessenten z. B. eine bestimmte Software zum Öffnen von Dokumenten zu benötigen, bei der es sich dann z. B. um eine modifizierte Version eines PDF-Readers handelt, die Schadsoftware auf das System der Betroffenen nachlädt. Eine andere Vorgehensweise, die sogar auf Personen mit IT-Expertise abzielt, ist die Bereitstellung von Programmierrätseln (sogenannte Coding Challenges), die der potenzielle Bewerber lösen soll, um Fähigkeiten unter Beweis zu stellen. Die Dateien, die im Rahmen dieser Aufgaben bereitgestellt werden, enthalten jedoch ebenfalls maliziöse Komponenten, die bei unbedachter Ausführung Schadsoftware nachladen. Falls das betroffene System an ein Unternehmens- oder Hochschulnetzwerk angebunden ist, breitet sich die Malware auch darauf aus. Im Anschluss versuchen die Akteure Know-how zu stehlen, Kryptowährung zu erbeuten sowie personenbezogene Informationen zu erlangen, die als neue Identität für weitere Angriffe verwendet werden kann.

Eine weitere besonders effektive Angriffsmethode staatlicher Akteure sind „Supply-Chain-Angriffe“[200], die Lieferketten manipulieren oder kompromittieren soll. 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. Die Detektion solcher Angriffe stellt auch Systeme niedersächsischer Unternehmen vor große Herausforderungen, da die Anzahl von Abhängigkeiten zu Softwarebibliotheken und eingesetzten Programmen stetig zunimmt.

Die Sicherheitsbehörden beschäftigt zudem die voranschreitende Entwicklung von KI, deren Nutzung sowohl positive als auch negative Auswirkungen auf die Sicherheit haben kann. Als Frühwarnsystem für Politik und Gesellschaft ist es Aufgabe des Verfassungsschutzes, die Gefahren solcher Entwicklungen zu bewerten. Staatliche

200 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.

Akteure verwenden KI-Technologie bereits für Desinformationskampagnen, indem gezielt gefälschte Nachrichten, Videos oder Bilder generiert werden. Seit dem Jahr 2025 kann auch vermehrt Schadsoftware festgestellt werden, die mithilfe diverser KI-Technologien entwickelt wurde oder KI im Rahmen ihrer Funktionsweise nutzt[201]. Aufgrund dessen ist zu befürchten, dass künftig das Erkennen von maliziöser mittels KI-generierter Software noch komplexer wird, da so z. B. Phishing-Mails automatisiert und zielgerichteter auf einzelne Betroffene zugeschnitten werden können.

201 https://www.heise.de/news/KI-gestuetzte-Cyberangriffe-Experten-beobachten-zunehmenden-LLM-Einsatz-10539423.html