Spionageabwehr / Proliferation / Cyberabwehr

7. Spionageabwehr / Proliferation / Cyberabwehr

7.1 Spionageaufkommen in Niedersachsen

Der Fachbereich Spionageabwehr im Niedersächsischen Verfassungsschutz hat den gesetzlichen Auftrag, alle Informationen über sicherheitsgefährdende oder geheimdienstliche Aktivitäten zu sammeln und Spionage sowie Proliferation[142] zu verhindern. Da Niedersachsen als erfolgreicher Wirtschaftsstandort potenzielles Ziel von Spionageaktivitäten fremder Geheim- oder Nachrichtendienste[143] ist, gilt es ihn vor derartigen Aktivitäten zu bewahren. Zudem geht es darum, den Schutz der in Niedersachsen lebenden Bürgerinnen und Bürger zu gewährleisten. Auch wenn die im Folgenden aufgeführten Beispiele von Aktivitäten fremder Geheim- und Nachrichtendienste nicht immer einen Niedersachsenbezug aufweisen, muss davon ausgegangen werden, dass es derartige Aktivitäten auch in Niedersachsen gibt. Die Beispiele sollen daher 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 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.

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

143 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.

Fremde Geheim- oder Nachrichtendienste sind in unterschiedlicher Personalstärke u. a. an den jeweiligen amtlichen Vertretungen (z. B. Botschaften, Generalkonsulate = Legalresidenturen) in Deutschland präsent und unterhalten dort Stützpunkte. Geheim- und Nachrichtendienstmitarbeitende können dort, als Diplomatinnen und Diplomaten getarnt, tätig werden und Informationen beschaffen oder sie leisten Unterstützung bei geheimdienstlichen Operationen ihrer Zentralen.
Eine Vielzahl von Informationen, die für fremde Geheim- oder Nachrichtendienste interessant erscheinen und früher nur mit klassischen 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 werden genutzt) auch von einer geheim- oder nachrichtendienstlichen oder staatlichen Beteiligung auszugehen.

Im Umkehrschluss bedeutet dies jedoch nicht, dass die klassischen Spionageaktivitäten ausgedient haben. Im Jahr 2021 traten im Fachbereich Spionageabwehr im Niedersächsischen Verfassungsschutz entsprechende Verdachtsfälle auf.

Nachfolgend werden exemplarisch einige Fälle dargestellt, die nicht unbedingt einen Niedersachsenbezug aufweisen müssen, aber genau so auch in Niedersachsen hätten passiert sein können. Im Vordergrund steht daher der Präventivcharakter, um die Unternehmen

und die Bevölkerung durch die Schilderung dieser Fälle zu sensibilisieren. Die Bearbeitungsschwerpunkte der Spionageabwehr lagen 2021 bei den Ländern Türkei, Russland und China.

Türkei

Am 17.09.2021 nahm die Polizei in Düsseldorf einen türkischen Staatsangehörigen wegen des Verdachts der geheimdienstlichen Agententätigkeit fest. In seinem Zimmer hatte ein Hotelmitarbeiter eine Waffe festgestellt und daraufhin die Polizei informiert. Es bestand der Verdacht der Verabredung zu einem Verbrechen. Nach Angaben der Staatsanwaltschaft entdeckten die Einsatzkräfte scharfe Munition sowie handschriftliche Aufzeichnungen über türkischstämmige Personen.
Gegen den 40-Jährigen ermittelt nun die Bundesanwaltschaft. Es gebe „zureichende tatsächliche Anhaltspunkte" dafür, dass der Mann Informationen über Personen, die mutmaßlich der Gülen-Bewegung angehören, gesammelt habe, um sie an den türkischen Nachrichtendienst „Millî Istihbarat Teşkilâtı" (MIT) zu übermitteln.

Die türkische Regierung macht die nach dem Prediger Fetullah Gülen benannte „Gülen-Bewegung" für den Putschversuch von Teilen des türkischen Militärs am 15. und 16.07.2016 verantwortlich. Anlässlich der Einweihung des neuen Dienstgebäudes des türkischen Geheimdienstes MIT am 06.01.2020 stellte der türkische Staatspräsident Erdoğan in Ankara lobend heraus, dass der MIT die Strukturen der als „Fetullahistische Terrororganisation" (FETÖ) bezeichneten „Gülen-Bewegung" aufgedeckt habe. Erdoğans Rede bot auch einen Ausblick auf das, was der MIT mittel- und langfristig plane. Zukünftig hätten Computer-Netzwerk-Operationen zur Identifikation Oppositioneller und seitens der Türkei als Terrorverdächtige bewerteter Personen Priorität.
Mitarbeiterinnen und Mitarbeiter des Niedersächsischen Verfassungsschutzes führten daher im Jahr 2021 mehr als 170 Sensibilisierungsgespräche mit möglicherweise betroffenen Personen. Konkrete Spionagetätigkeiten wurden bislang allerdings nicht festgestellt.

Russland

Einflussnahme durch russische Staatsmedien

Im Vorfeld der Bundestagswahl wurden zahlreiche Informationen zu politischen Themen über russische Medien verbreitet, mutmaßlich um auf die Meinungsbildung der Wählerinnen und Wähler Einfluss zu nehmen. Vorrangig waren die TV-Sender RT DE (deutscher Ableger des früheren „Russia Today") sowie der Radiosender bzw. das Nachrichtenportal SNA News[144] aktiv.

Die Reichweite derartiger „Nachrichten" kann in der Regel nur schwer gemessen werden. Auswirkungen auf die öffentliche Meinung, auf soziale Netzwerke und den politischen Willensbildungsprozess sind dadurch kaum abschätzbar.

Freiheitsstrafe wegen geheimdienstlicher Agententätigkeit

Der für Staatsschutzsachen zuständige 1. Strafsenat des Kammergerichts in Berlin hat einen 56-Jährigen wegen geheimdienstlicher Agententätigkeit für den russischen Militärgeheimdienst GRU zu einer Freiheitsstrafe von zwei Jahren verurteilt.[145]

Demnach soll der deutsche Staatsbürger sensible Informationen über das Bundestagsgebäude an den russischen Geheimdienst verraten haben. Als Mitarbeiter eines Unternehmens, welches schon mehrfach beauftragt wurde, die Sicherheit von elektronischen Geräten im Bundestagsgebäude zu überprüfen, hatte er Zugriff auf Dateien mit den Grundrissen der Liegenschaft des Bundestages. Diese Liegenschaftspläne, aus denen sich etwa die Lage und Nummern von Büroräumen ergeben, soll er im Jahr 2017 auf einen Datenträger übertragen und diesen einem Mitarbeiter in der russischen Botschaft in Berlin geschickt haben, der hauptamtlich für den russischen Militärgeheimdienst GRU tätig gewesen sei. Nach eigenen Angaben sei der Angeklagte nicht vom russischen Geheimdienst angeworben worden, er habe „aus eigenem Antrieb" gehandelt.

Der Angeklagte soll ein Politoffizier in der DDR gewesen sein. Seit 1983 soll er in der Nationalen Volksarmee (NVA) gedient und dort seine Kameraden in der Kaserne bespitzelt haben. Unter einem

144 SNA News firmierte bis Dezember 2020 unter der Bezeichnung „Sputnik News Agency".

145 Pressemitteilung PM 35/2021 des Kammergerichts Berlin vom 28.10.2021.

Decknamen war er als Inoffizieller Mitarbeiter (IM) für das Ministerium für Staatssicherheit (Stasi) der DDR tätig und stieg dann zum Führungs-IM auf. Ihm soll eine Zukunft bei der Stasi offen gestanden haben, die durch den Fall der Mauer verhindert wurde. Durch die Tätigkeit bei der Stasi könnte der Angeklagte gewusst haben, an welche Mitarbeiter er sich bei der russischen Botschaft wenden muss, um Informationen an den GRU weiterzuleiten.

Russischer Universitätsmitarbeiter wegen Spionageverdacht angeklagt

Der Generalbundesanwalt hat einen aus Russland stammenden Universitätsmitarbeiter festnehmen lassen[146], der Informationen aus dem Umfeld einer deutschen Hochschule an einen russischen Geheimdienst weitergegeben haben soll. Der Beschuldigte sei demnach dringend verdächtig, für einen russischen Geheimdienst tätig gewesen zu sein. Seine Wohnung und Dienststätte sind durchsucht worden. Am 09.12.2021 hat die Bundesanwaltschaft vor dem Oberlandesgericht München Anklage erhoben.[147]

Der 29-Jährige war den Ermittlern zufolge wissenschaftlicher Mitarbeiter an einem naturwissenschaftlich-technischen Lehrstuhl der deutschen Hochschule. Seit Oktober 2020 habe er sich mindestens dreimal mit einem Angehörigen eines russischen Auslandsgeheimdienstes getroffen. Zumindest bei zwei dieser Treffen habe er gegen Bargeld Informationen „aus dem Herrschaftsgebiet der Universität" weitergegeben.

Zum Forschungsbereich des Beschuldigten ist bekannt, dass dieser Doktorand der Professur für Mechanical Engineering war und Forschungen zu hybriden Werkstoffsystemen für den Leichtbau durchgeführt habe. Dadurch hatte er Zugang zu speziellem Know-how in innovativen Technologien, das für fremde Nachrichtendienste von besonderem Interesse ist.

China

Soziale Netzwerke wie Facebook, LinkedIn und Xing bieten vielfältige Möglichkeiten, sich mit bekannten Personen stärker zu vernetzen, neue Kontakte zu knüpfen oder sich in beruflicher Hinsicht

146 Pressemitteilung des Generalbundesanwaltes beim Bundesgerichtshof vom 21.06.2021.

147 Pressemitteilung des Generalbundesanwaltes beim Bundesgerichtshof vom 27.01.2022.

weiterzuentwickeln. Mit nur wenigen „Klicks“ lassen sich hier Informationen zu Biografien, wirtschaftlichen Verhältnissen, politischen Interessen und zum sozialen Umfeld von Nutzern abrufen.
Aufgrund dieser zumeist für jedermann einsehbaren persönlichen Daten sind soziale Netzwerke längst auch in den Fokus ausländischer Nachrichtendienste gerückt. Insbesondere chinesische Nachrichtendienste nutzen Netzwerke wie LinkedIn, um Personen mit für sie interessantem Profil zu identifizieren und im Anschluss als nachrichtendienstliche Quellen zu werben.
Über die Methodik chinesischer Nachrichtendienste, mittels Fake-Profilen insbesondere Mitarbeiterinnen und Mitarbeiter von deutschen und europäischen Behörden für eine Zusammenarbeit zu gewinnen, hat der Verfassungsschutz bereits 2017 informiert. Die seinerzeit benannten Fake-Profile wurden kurz darauf von der Firma LinkedIn gesperrt und gelöscht. Nichtsdestotrotz stellt der Verfassungsschutzverbund auch nachfolgend Anwerbungsversuche chinesischer Nachrichtendienste mittels Fake-Profilen insbesondere im Netzwerk LinkedIn fest.
Der Niedersächsische Verfassungsschutz rät bei solchen Fallmustern, derartige Kontaktanfragen zu ignorieren und der Verfassungsschutzbehörde mitzuteilen. In jedem Fall kann ein Kontaktversuch als Indikator gesehen werden, in den Fokus eines fremden Nachrichtendienstes geraten zu sein.

Anklageerhebung und Festnahme wegen mutmaßlicher geheimdienstlicher Agententätigkeit

Die Bundesanwaltschaft hat am 20.05.2021 vor dem Staatsschutzsenat des Oberlandesgerichts (OLG) München Anklage gegen einen deutschen Staatsangehörigen wegen geheimdienstlicher Agententätigkeit (§ 99 Abs. 1 Nr.1, Abs. 2 Satz 1 StGB i.V.m. § 1 Abs. 1 Nr. 4 NATO-Truppenschutzgesetz) erhoben[148]. Am 05.07.2021 erfolgte die Festnahme. Grundlage hierfür war der zuvor ergangene Haftbefehl des OLG München.
Der 75-jährige Politologe und pensionierte Mitarbeiter einer Stiftung soll fast ein Jahrzehnt lang für China spioniert haben. Anlässlich einer Vortragsreise nach Schanghai im Juni 2010 traten Angehörige eines

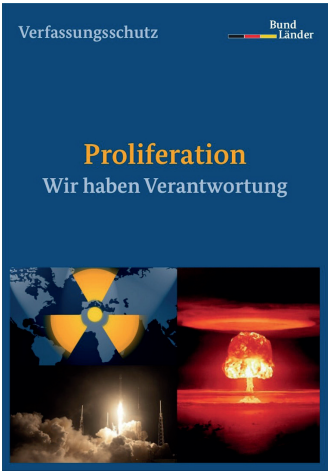
148 Pressemitteilung des Generalbundesanwaltes beim Bundesgerichtshof vom 06.07.2021.

chinesischen Nachrichtendienstes mit dem Angeschuldigten in Kontakt, um ihn für eine Mitarbeit zu gewinnen. Bis November 2019 soll er dem chinesischen Geheimdienst im Vorfeld und Nachgang von Staatsbesuchen oder multinationalen Konferenzen sowie zu bestimmten aktuellen Fragestellungen regelmäßig Informationen beschafft haben. Durch die hochrangigen politischen Ansprechpartner konnte der Beschuldigte bestimmte wichtige Informationen einholen.
Als Gegenleistung wurde ihm dafür laut Anklage die Reise zu den jeweiligen Treffen mit den chinesischen Nachrichtendienstmitarbeitern einschließlich eines Rahmenprogramms finanziert. Auch ein Honorar soll er erhalten haben.
Der Haftbefehl gegen den mutmaßlichen Spion wurde am 06.07.2021 durch den Staatsschutzsenat des OLG München außer Vollzug gesetzt.

Demokratiebewegung in China

Im Zusammenhang mit der Demokratiebewegung in der chinesischen Sonderverwaltungszone Hongkong gab es auch in Deutschland Demonstrationen, welche die dortige Situation thematisieren, allerdings nicht in Niedersachsen. Die chinesische Administration reagiert auf gegen sie gerichtete Protestaktionen besonders sensibel. Entsprechend bleibt auch die Beobachtung und Kontrolle der Oppositionsbewegung im Ausland ein Schwerpunkt chinesischer Nachrichtendienste. Es ist davon auszugehen, dass die chinesischen Behörden auch in anderen Zusammenhängen in Niedersachsen durchgeführte Aktionen beobachten und an der Identifizierung von Demonstrationsanmeldenden oder -teilnehmenden interessiert sind. Ebenfalls kann nicht ausgeschlossen werden, dass erkannte Protagonisten vom chinesischen Staat in Deutschland unter Druck gesetzt, bedroht oder eingeschüchtert werden.

7.2 Proliferation



Wesentliches Merkmal der Proliferation – also der Weiterverbreitung von atomaren, biologischen und chemischen Waffensystemen (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.

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 Informationsinfrastrukturen ist immens. Staat, Kritische Infrastrukturen[149], 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

149 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).

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 2021 fortgesetzten Angriffen auf Großunternehmen sind in Niedersachsen diverse kleinere und mittelständische Unternehmen betroffen. Das verdeutlicht, welch hohen Stellenwert die IT-Sicherheit hat.

Die größte Gefahr für Unternehmen und Behörden stellen aktuell „Advanced Persistant Threats“[150] dar. Diese zielgerichteten elektronischen Angriffe 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 Angriffes ist es, sich möglichst lange unentdeckt in fremden IT-Systemen zu bewegen, um sensible Daten auszuleiten oder anderweitig Schäden anzurichten.
Im Gegensatz zu vielen anderen Cyberkriminellen verfolgen diese Angreifer ihre Ziele jedoch grundsätzlich langfristig, meist über mehrere Monate oder Jahre hinweg. Sie stimmen ihre Aktivitäten auf die Sicherheitsmaßnahmen ihrer anvisierten Opfer ab und greifen ein und dasselbe Opfer oft mehrfach an.
Die Bearbeitung solcher elektronischen 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 nachrichtendienstlichen Hintergrund wird Beratung angeboten. Fälle von „Cybercrime“, bei denen ein solcher Verdacht ausgeschlossen werden konn-

150 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).

te, werden in Absprache und nur mit dem Einverständnis der oder des Betroffenen an die Strafverfolgungsbehörden abgegeben.

Auch im Jahr 2021 hat der Niedersächsische Verfassungsschutz Hinweise zu möglichen elektronischen Angriffen zum Nachteil von Personen, Institutionen und Einrichtungen bearbeitet. Mehrere Angriffswellen zielten auf Politiker, die im Bundestag, im Landtag oder auch in den Kommunalparlamenten tätig sind oder waren. Dort wurde durch einen mutmaßlichen ausländischen Cyberakteur versucht, E-Mail-Konten zu übernehmen, um anschließend, möglicherweise durch eine Desinformationskampagne, im Vorfeld der Bundestagswahl 2021 Einfluss nehmen zu können.
Ein weiteres Tätigkeitsfeld der Cyberabwehr war die Bearbeitung von Schwachstellen in E-Mail-Servern eines weltweit führenden Software-Anbieters. Anfang des Jahres 2021 wurden mehrere Schwachstellen bekannt, die aktiv ausgenutzt wurden. Zahlreiche Sensibilisierungsgespräche mit den Betroffenen wurden geführt, um einen größeren Schaden 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[151].

151 Die Allianz für Cybersicherheit wurde 2012 vom Bundesamt für Sicherheit in der Informationstechnik (BSI) gegründet und verfolgt das Ziel, die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken. Aktuell gehören ihr 4.088 Unternehmen, 122 Partner und 97 Multiplikatoren an.

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.