Spionageabwehr/ Proliferation/ Elektronische Angriffe

8. Spionageabwehr/Proliferation/ Elektronische Angriffe

8.1 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[149] zu verhindern. Da Niedersachsen als erfolgreicher Wirtschaftsstandort potenzielles Ziel von Spionageaktivitäten fremder Geheim- oder Nachrichtendienste[150] 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.

Hauptträger der klassischen Spionageaktivitäten in der Bundesrepublik Deutschland sind nach wie vor die Russische Föderation, die Volksrepublik China, aber auch der Iran. Die Schwerpunkte ihrer Aktivitäten orientieren sich an den politischen Vorgaben und wirtschaftlichen Prioritäten.

Aufgrund desolater Sicherheitslagen in ihren Heimatländern und damit verbundener existenzieller Bedrohung sucht eine große Zahl von Menschen Zuflucht und Schutz in Europa. Insbesondere Deutschland ist Ziel von Flüchtlingsbewegungen, die ihren Ursprung vor allem in Afghanistan, im Irak sowie in Syrien, aber auch in den Ländern Zentral- und Westafrikas haben. Mit der sich vergrößernden Exilgemeinde ist die Ausforschung oppositioneller Aktivitäten zur wichtigen Zielvorgabe für fremde Dienste in Deutschland geworden.

Fremde Geheim- oder Nachrichtendienste sind in unterschiedlicher Personalstärke u. a. an den jeweiligen amtlichen Vertretungen (z. B.

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

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

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 2020 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 passiert sein können. Im Vordergrund steht daher der Präventivcharakter, um die Unternehmen und die Bevölkerung durch die Schilderung dieser Fälle zu sensibilisieren.

Türkei

Die türkische Regierung machte 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 „Millî Istihbarat Teşkilâtı" (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.
Mitarbeiter des Niedersächsischen Verfassungsschutzes führten im Jahr 2020 mehr als 160 Sensibilisierungsgespräche mit möglicherweise betroffenen Personen. Konkrete Spionagetätigkeiten wurden bislang allerdings nicht festgestellt.

Russland

Die Bundesanwaltschaft hat am 18.06.2020 vor dem Staatsschutzsenat des Kammergerichts in Berlin Anklage gegen den russischen Staatsangehörigen Vadim K. erhoben.[151] Der Angeschuldigte ist des Mordes (§ 211 StGB) zum Nachteil des am 23.08.2019 in Berlin getöteten russisch-georgischen Staatsangehörigen Tornike K. hinreichend verdächtig. Vadim K. soll am 23.08.2019 in der Parkanlage Kleiner Tiergarten in Berlin Moabit den 40-jährigen georgischen Staatsangehörigen tschetschenischer Abstammung Tornike K. mit Schüssen aus einer Kurzwaffe gezielt getötet haben. In der Anklageschrift wird dargelegt, dass staatliche russische Stellen verdächtigt werden, dem Angeschuldigten den Auftrag erteilt zu haben, Tornike K. zu liquidieren, da er sich gegen den russischen Staat gewendet habe. Die gegen die russischen Staatsstrukturen vorgebrachten Anschuldigungen werden vom Kreml als unbegründet zurückgewiesen. Der Prozess begann am 07.10.2020 vor dem Kammergericht Berlin.
Insbesondere baltische Staaten beklagen seit langem eine gegen sie gerichtete mediale Agitation Russlands. Es soll z. B. suggeriert

151 Pressemitteilungen des Generalbundesanwaltes beim Bundesgerichtshof vom 04.12.2019 und 18.06.2020 sowie des Kammergerichts Berlin vom 02.09.2020.

werden, dass dort schlechtere Zustände als in Russland herrschen. Damit wird versucht, den russischsprachigen Teil der Bevölkerung im Sinne der russischen Regierung zu beeinflussen und die politischen Verhältnisse zu destabilisieren. Nach Aussagen des Generalstabschefs der russischen Streitkräfte[152] muss sich Krieg nicht auf rein militärische Mittel beschränken. Die sogenannte „Gerassimow-Doktrin" versteht z. B. das Mittel der Desinformation als Teil hybrider Kriegsführung zur Destabilisierung von anderen anderer Staaten.
Diese Aktivitäten werden als sicherheitsgefährdend i. S. des § 3 Abs. 1 Nr. 2 NVerfSchG eingeordnet.
Alekxej Nawalny, russischer Oppositionspolitiker und bekannter Kritiker des russischen Präsidenten, ist am 20.08.2020 auf einem Flug von Sibirien nach Moskau zusammengebrochen. In Omsk wurde er daraufhin zunächst in einer Klinik behandelt, bevor er am 22.08.2020 nach Berlin in die Charité ausgeflogen wurde. Befunde deutscher Stellen weisen auf eine Vergiftung und auf Parallelen zu früheren Vergiftungsfällen mit russischen Bezügen hin. Der Kreml zweifelt die Aussagefähigkeit der Ergebnisse an und inszenierte sich im Gegenzug als Opfer einer westlichen Diffamierungskampagne. Auch hier soll mit Desinformationen eine alternative Realität konstruiert werden.

Iran

Der Staatsschutzsenat des Oberlandesgerichts Koblenz hat am 23.03.2020 einen 51 Jahre alten Zivilangestellten der Bundeswehr wegen Landesverrats in einem besonders schweren Fall (§ 94 Abs. 1, 2 StGB) zu einer Freiheitsstrafe von sechs Jahren und zehn Monaten verurteilt. Gegen seine mitangeklagte Ehefrau hat der Senat wegen Beihilfe zum Landesverrat (§§ 94 Abs. 1, 27 Abs. 1 StGB) eine Freiheitsstrafe von zehn Monaten verhängt, deren Vollstreckung zur Bewährung ausgesetzt wurde.
Das Gericht hat es als erwiesen angesehen, dass der Angeklagte in einer Kaserne in Daun (Rheinland-Pfalz) als Übersetzer Staatsgeheimnisse militärischer Art an Mitarbeiter eines iranischen Nachrichtendienstes weitergab. Seine Ehefrau hat ihn bei dieser Verratstätigkeit unterstützt.

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

Konkret habe sich der Angeklagte spätestens ab dem 28.01.2013 in mindestens acht Fällen mit Verbindungsleuten eines iranischen Nachrichtendienstes in verschiedenen europäischen Städten getroffen, um Informationen, die er auf Datenträgern gespeichert hatte (z. B. Lagepläne der Bundeswehr über militärische Situationen und Analysen des Bundesministeriums der Verteidigung zu bestimmten Ländern und Themengebieten), weiterzugeben.[153]

Als Staatsterrorismus wird der von Staaten ausgeübte oder gesteuerte Terrorismus bei der Verfolgung ihrer außen- oder innenpolitischen Ziele verstanden. Konkret handelt es sich um Straftaten gegen das Leben, die körperliche Unversehrtheit und die persönliche Freiheit nach den §§ 211, 212, 234, 234a, 239 und / oder 239b StGB, wenn anzunehmen ist, dass die Tat durch eine oder im Auftrag einer fremden Macht begangen worden ist.

Der Verfassungsschutz geht davon aus, dass der iranische Geheimdienst „Ministry of Intelligence and Security" (MOIS) und die operativ tätige Spezialeinheit der iranischen Revolutionsgarden (Quds Force) in diesem Zusammenhang auch mögliche Zielpersonen in Europa und auch Deutschland ausforschen.

Bestätigt wurden die Aktivitäten der Quds Force in Deutschland bereits am 27.03.2017 durch ein Urteil des Kammergerichts Berlin gegen einen pakistanischen Staatsangehörigen. Dieser hatte nach Feststellung des Gerichts im Auftrag der „Quds Force" unter anderem den damaligen Vorsitzenden der Deutsch-Israelischen Gesellschaft ausgespäht und war deswegen zu einer Haftstrafe von vier Jahren und drei Monaten verurteilt worden.

Daneben hat auch ein aktuelles Urteil eines Gerichts in Dänemark gegen einen norwegischen Staatsangehörigen iranischer Abstammung Bedeutung, welches einer Agenturmeldung zufolge am 26.06.2020 ergangen ist. Das Gericht stellte in dem Urteil fest, dass der Angeklagte, der zu sieben Jahren Haft verurteilt wurde, im Auftrag eines iranischen Nachrichtendienstes einen in Dänemark lebenden Aktivisten der separatistischen Unabhängigkeitsbewegung „Arab Struggle Movement for the Liberation of Ahwaz" (ASMLA) ausgespäht habe, wodurch dessen Tötung durch einen iranischen Geheimdienst ermöglicht werden sollte.

153 Pressemeldung des Oberlandesgerichtes Koblenz zum Az. 2 StE 7/19 Geh. und Az. 2 StE 11/19 (2) Geh. vom 23.03.2020.

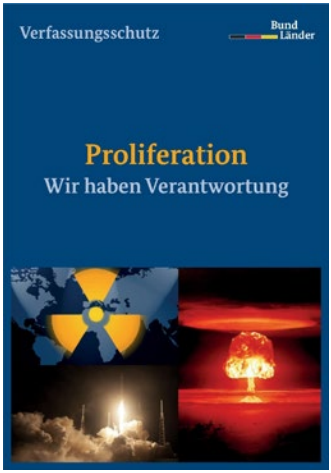
Trotz der Enttarnung mutmaßlicher iranischer Anschlagsplanungen ist davon auszugehen, dass iranische Geheimdienste auch zukünftig nicht auf staatsterroristische Aktionen im Europa verzichten werden.

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 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 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 weiterhin Anwerbungsversuche chinesischer Nachrichtendienste mittels Fake-Profilen insbesondere im Netzwerk LinkedIn fest.
Der Niedersächsische Verfassungsschutz rät bei solchen Fallmustern, derartige Kontaktanfragen zu ignorieren und vielmehr der Verfassungsschutzbehörde mitzuteilen. In jedem Fall kann ein Kontaktversuch als Indikator gesehen werden, in den Fokus eines fremden Nachrichtendienstes geraten zu sein.
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 Be-

hörden 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.

8.2 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.

8.3 Elektronische Angriffe mit vermutetem nachrichtendienstlichen Hintergrund

Die Abhängigkeit unserer Gesellschaft von Informations- und Kommunikationstechnologien steigt. Die dadurch verursachte Verwundbarkeit moderner Gesellschaften stellt eine der größten sicherheitspolitischen Herausforderungen dar, denn der mögliche Schaden für Staaten, ihre Bevölkerung und ihre Volkswirtschaften im Falle der Beeinträchtigung von Informationsinfrastrukturen ist immens. Staat, Kritische Infrastrukturen[154], Wirtschaft, Wissenschaft und Bevölkerung sind auf das verlässliche Funktionieren dieser Technologien, insbesondere des Internets, angewiesen.

154 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).

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

Die höchste Gefahr für Unternehmen und Behörden stellen aktuell „Advanced Persistant Threats“[155] 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 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.

155 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).

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

Auch im Jahr 2020 hat der Niedersächsische Verfassungsschutz Hinweise zu möglichen elektronischen Angriffe zum Nachteil von Personen, Institutionen und Einrichtungen bearbeitet. Mehrere Angriffe zielten auf Bildungseinrichtungen. Auch die Sensibilisierung von Forschungseinrichtungen, die mit der Entwicklung von Impfstoffen befasst sind, stellte ein Tätigkeitsfeld dar.

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[156].

156 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.

8.4 Hilfe für Betroffene

Personen, die Opfer eines Anwerbungsversuchs fremder Geheimdienste oder eines elektronischen Angriffs mit vermutetem nachrichtendienstlichen 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.