Spionageabwehr und Wirtschaftsschutz

Spionageabwehr und Wirtschaftsschutz 229

Spionage – Auftraggeber, Ziele und Methoden 232
Aufklärung und Abwehr von Proliferation 240
Wirtschaftsspionage 244

Das Interesse ausländischer Nachrichtendienste an Informationen über politische Vorhaben und Ziele, Verhandlungspositionen und Strategien sowie wirtschaftliche Planungen und militärische Potenziale in Deutschland und Nordrhein-Westfalen war im Jahr 2016 weiterhin hoch. Beleg dafür sind zahlreiche Versuche ausländischer Nachrichtendienste, Kontakt mit Gesprächspartnern in der nordrhein-westfälischen Politik und Wirtschaft aufzunehmen. Im Berichtsjahr war zudem zu beobachten, dass ausländische Nachrichtendienste verstärkt Beschäftigte von Behörden ansprechen, um Informationen abzugreifen.

Beschaffungsstellen in einschlägigen Staaten bemühten sich zudem, proliferationsrelevante Güter verdeckt in Nordrhein-Westfalen einzukaufen. Dies sind in der Regel sogenannte Dual-use-Produkte, die sich sowohl für zivile als auch für militärische Zwecke nutzen lassen. Getarnt werden die nicht zugelassenen Beschaffungen üblicherweise über ein auf mehrere Länder verteiltes Netzwerk aus Tarnfirmen und Strohmännern. Der eigentliche Empfänger soll dabei unerkannt bleiben. Die Spionageabwehr konnte im Berichtsjahr 32 dieser Beschaffungsversuche beobachten. In der überwiegenden Zahl der Fälle konnte eine Auslieferung verhindert werden.

Die Zahl gezielter und qualitativ hochwertiger Cyberangriffe auf deutsche Unternehmen lag im Jahr 2016 erneut auf einem hohen Niveau. Die Angreifer hatten es dabei auf Unternehmensnetzwerke und Kontrollsysteme der Industrie abgesehen. Im Fokus stehen insbesondere klei-

ne und mittlere Unternehmen, die sich häufig durch innovative Produkte und ein besonderes Know-how auszeichnen. Die Unternehmensleitungen sind gefordert, einen ausreichenden Schutz gegen elektronische Angriffe zu implementieren und die Beschäftigten auf allen Ebenen für die Gefahren zu sensibilisieren. Mit der Veranstaltungsreihe „Unternehmenssicherheit ist Chefsache“ richtete sich der nordrhein-westfälische Verfassungsschutz zusammen mit den Kooperationspartnern der Sicherheitspartnerschaft NRW daher gezielt an Entscheider in Unternehmen. Die ersten vier sogenannten Entscheider-Dialoge fanden im Herbst 2016 mit sehr guter Resonanz in unterschiedlichen Regionen des Landes statt. Neben dieser Reihe konnte der Verfassungsschutz mit zahlreichen Einzelgesprächen und Vorträgen in Unternehmen, Verbänden und Organisationen auch im Jahr 2016 seine intensive Beratungs- und Sensibilisierungsarbeit fortführen.

Spionage – Auftraggeber, Ziele und Methoden

Spionage bietet Regierungen die Möglichkeit, sich einen Informationsvorsprung zu verschaffen, um eigene politische, wirtschaftliche, wissenschaftliche oder militärische Ziele im In- und Ausland zu erreichen. Sie verschafft sich Zugang zu Informationen, die eine Einschätzung politischer Positionen und wirtschaftlicher Wettbewerbsfähigkeit des jeweiligen Staates sowie der militärischen Leistungsfähigkeit gegnerischer Bündnisse ermöglichen. Deutschland steht wegen seiner politischen und wirtschaftlichen Bedeutung im besonderen Fokus ausländischer Nachrichtendienste.

Beschaffungsbemühungen zielen auf unautorisierten Transfer wissenschaftlich-technischen Know-hows sowie auf Informationen über politische Vorhaben, Krisenmanagement und Handlungsstrategien ab. Wegen seines politischen Gewichts innerhalb der Bundesrepublik besteht auch an Nordrhein-Westfalen ein großes nachrichtendienstliches Interesse. Zudem ist das Land ein herausragender Innovations- und Wirtschaftsstandort mit mehr als 70 Universitäten und Fachhochschulen sowie mehr als 50 Technologiezentren.

Methoden der Spionage

Fast 90% der für Nachrichtendienste interessanten Informationen lassen sich offen über das Internet und andere Medien, durch den Besuch von Messen, bei gegenseitigen Delegationsbesuchen sowie durch geschickte Gesprächsführung mit Informations- und Wissensträgern erlangen. Dazu müssen nicht einmal aufwändige nachrichtendienstliche Operationen durchgeführt werden.

An die verbleibenden rund zehn Prozent versuchen Nachrichtendienste mit verdeckten Methoden zu gelangen. Das Spektrum reicht von der Herbeiführung und Kultivierung zunächst unverdächtiger Kontakte mit dem Ziel einer direkten oder indirekten Abschöpfung der Kontaktpersonen bis hin zu einer konspirativen Vorgehensweise, bei der Personen beispielsweise mit falschem Namen und Angaben zum eigenen Lebenslauf (sogenannte Legende) aktiv sind. Es kommt dabei in der Regel nicht auf die Hierarchieebene der Zielpersonen an. Manchmal geht es lediglich darum, Zugang zu einem interessanten Bereich zu erhalten. In selteneren Fällen zielen Nachrichtendienste auch darauf ab, einen belastenden Umstand – ein sogenanntes Kompromat – zu schaffen, mit dem der jeweilige Informations- und Wissensträger erpressbar gemacht werden soll. Diese Methode wird vorrangig im Ausland, beispielsweise bei Geschäftsreisenden, angewendet.

Nachrichtendienste nutzen zur Spionage aber auch die vielfältigen Möglichkeiten, die sich durch die rasanten Entwicklungen in der Informations- und Kommunikationstechnologie sowie durch die zunehmende Vernetzung und Digitalisierung ergeben. Elektronische Angriffe auf Rechnersysteme mit hochsensiblen Daten bieten hohe Erfolgsaussichten und lassen sich mit geringem Entdeckungsrisiko durchführen. Typische Angriffsmethoden sind das verdeckte Einschleusen von Schadsoftware (Trojanern) über E-Mails, über manipulierte Downloads („Drive-by-downloads“), über präparierte Datenträger oder auf dem Umweg über privates, aber beruflich genutztes Equipment von Mitarbeitern („Bring-your-own Devices“, beispielsweise USB-Sticks, Smartphones, Tablets). Außenstehenden gelingt es auf diesen Wegen, in Systeme einzudringen und Daten zu entwenden oder Systeme zu manipulieren. Mit dem digital operierenden „Spion 4.0“ lässt sich zudem bereits seit längerem eine neue Qualität in der Spionage feststellen.

Der Mensch stellt jedoch stets die größte Sicherheitslücke dar. Diese lässt sich auch durch eine noch so ausgefeilte materielle Absicherung über Firewalls, Anti-Viren-Programme, Passwortschutz oder Zugangsregelungen nicht schließen. Nachrichtendienste setzen über sogenanntes „Social Engineering“ an dieser Stelle an. Sie versuchen das Vertrauen eines Unternehmensangehörigen zu gewinnen, um über diesen Kontakt Zugang zu Systemen zu erhalten. Erkenntnisse belegen, dass aber auch der Spion am Kopierer und mit der Kamera am Zielobjekt weiterhin im Einsatz ist. Wachsamkeit sollte daher auch in diesem Punkt weiter bestehen.

Die Zahl nachrichtendienstlichen Personals in sogenannten Legalresidenturen im Bundesgebiet ist auch im europäischen Vergleich anhaltend hoch. Dies verdeutlicht und belegt das hohe Interesse an Informationen aus Deutschland. Legalresidenturen sind getarnte Stützpunkte ausländischer Nachrichtendienste, insbesondere in den diplomatischen und konsularischen Vertretungen, bei staatsnahen Unternehmen oder bei Medienagenturen. Von dort aus entwickelt das nachrichtendienstliche Personal über eigens bereitgestellte Tarndienstposten die geheimdienstlichen Aktivitäten.

Der Einsatz von sogenannten Illegalen dient ebenfalls der Verschleierung nachrichtendienstlicher Tätigkeiten. Dabei handelt es sich um Personen, die als Nachrichtendienstoffiziere von der Zentrale des ausländischen Nachrichtendienstes unter einer Falschidentität eingeschleust werden und häufig über viele Jahre in Deutschland unauffällig leben. Unter diesem Deckmantel führen sie teilweise aufwendige nachrichtendienstliche Operationen aus.

Erkenntnisse der Spionageabwehr

Die Spionageabwehr des nordrhein-westfälischen Verfassungsschutzes beobachtet im Rahmen einer 360-Grad-Aufklärung eine Vielzahl hier tätiger ausländischer Nachrichtendienste. Hauptakteure sind die Nachrichtendienste der Russischen Föderation, der Volksrepublik China, der

Islamischen Republik Iran und der Türkei. Die Beschaffungsbemühungen der Dienste richten sich nach wie vor auf die klassischen Zielbereiche Politik, Militär und Wirtschaft.

Im Jahr 2016 wurden erneut zahlreiche Kontaktversuche ausländischer Nachrichtendienste mit Gesprächspartnern in Nordrhein-Westfalen aus Politik und Wirtschaft bekannt. Die nordrhein-westfälische Spionageabwehr führt Sensibilisierungsgespräche mit potenziellen oder aktuellen Gesprächspartnern erkannter Nachrichtendienstoffiziere. In den Fällen, in denen ein Gesprächspartner von sich aus eine nachrichtendienstliche Verstrickung annimmt, wird geraten, mit der Spionageabwehr ein Gespräch zu führen.

Russische Föderation

Die russische Regierung setzt auch weiterhin auf die zielgerichtete Beschaffung von Informationen und Gütern durch ihre Nachrichtendienste. Als elementarer Bestandteil der russischen Sicherheitsarchitektur unterstützen sie wirksam bei der Vorbereitung und Realisierung politischer Vorhaben im In- und Ausland. Sie genießen im russischen Staatsgefüge einen hohen Stellenwert, Führungspositionen werden entsprechend besetzt.

Die Nachrichtendienste der russischen Föderation interessieren sich für politische Strategien sowohl auf nationaler, als auch auf europäischer Ebene. Ein besonderes Augenmerk liegt auf der Energiepolitik.

Die mit dem Ukraine-Konflikt einhergehenden Sanktionen der Europäischen Union schränken die russische Wirtschaft stark ein. Das Land hält dennoch an seinem Ziel fest, wirtschaftlich zu einer der fünf größten Volkswirtschaften aufzusteigen. Diese Zielvorgabe ist mit dem Streben verbunden, die russische Rüstungsproduktion wieder zu einem herausragenden Wirtschaftsfaktor zu machen und gleichzeitig Russland wieder als militärischen Machtfaktor zu unterstreichen. Die Nachrichtendienste haben den Auftrag, bei der Umsetzung zu unterstützen.

An einen Teil der nachrichtendienstlich interessanten Informationen gelangen die russischen Nachrichtendienste über offen zugängliche Quellen. Sie werten dazu beispielsweise Medien und das Internet aus. Schützenswerte Informationen werden nach gezielter Kontaktaufnahme zu Wissensträgern aus Politik und Wirtschaft bei Gesprächen abgeschöpft, die beispielsweise beim Besuch von Messen und Fachkongressen oder bei gegenseitigen Delegationsbesuchen geführt werden. Kontaktaufnahmen finden dabei häufig unter Legende oder unter Vorspiegelung einer zum Kontakt passenden vordergründigen Interessenlage statt. Im Berichtsjahr 2016 hat es auch in Nordrhein-Westfalen wieder Hinweise auf derartige Kontaktversuche gegeben. In diplomatischen und konsularischen Vertretungen, den sogenannte Legalresidenturen, sind Angehörige der Nachrichtendienste getarnt eingesetzt. Das gilt zudem für einige russische Unternehmen, die ihren Sitz in Deutschland haben, darunter auch in Nordrhein-Westfalen. Die nach wie vor hohe Personalstärke lässt auf die Bedeutung dieser Einrichtungen schließen.

An Informationen, die über menschliche Quellen nicht zu beschaffen sind, versuchen die russischen Nachrichtendienste über elektronische Angriffe heranzukommen. Dies gilt auch für das Berichtsjahr 2016, in dem die Dienste mit hoher Professionalität erneut Cyber-Angriffe gegen Behörden und Wirtschaftsunternehmen in Deutschland ausgeführt haben. Mit Social Engineering sorgfältig vorbereitet finden Trojaner oftmals zielsicher ihren Weg in die Rechnersysteme und ziehen dort die benötigten Informationen ab.

Kostenloses Angebot des Verfassungsschutzes

Zur Sensibilisierung vor den Gefahren nachrichtendienstlicher Tätigkeit führt der nordrhein-westfälische Verfassungsschutz auf Wunsch und auch unabhängig von konkreten Verdachtsfällen Informationsveranstaltungen für interessierte Unternehmen und Organisationen durch. Im Einzelfall berät er vertraulich, wenn sich Anhaltspunkte für den Verdacht eines Angriffs durch einen fremden Nachrichtendienst ergeben.
Anfragen mit der Bitte um Kontaktaufnahme können an kontakt.verfassungsschutz@im1.nrw.de gerichtet werden.

Vor besondere Herausforderungen stellt die deutschen Abwehrbehörden eine Strategie, bei der nicht nur die klassische Spionage im Vordergrund steht: Die sogenannte hybride Kriegsführung schließt aktive Desinformationskampagnen sowie gezielte Cyber-Angriffe ein. Die Spionageabwehr beobachtet seit längerem russische Propaganda- und Desinformationsaktivitäten, bei denen zielgerichtet Meinungsbildung und Entscheidungsprozesse in Politik und Gesellschaft beeinflusst werden sollen. Es wird dabei unter anderem versucht, gesellschaftliche Gruppierungen in Deutschland für die Ziele Russlands zu instrumentalisieren. Das manipulative Interesse bezieht sich vorrangig auf innenpolitische Themen, aber auch auf außenpolitische strategische Planungen. Elektronische Angriffe dienen der Sabotage sogenannter kritischer Infrastrukturen. Die sind Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen wie beispielsweise zur Wasser- und Stromversorgung oder zur Bereitstellung öffentlicher Dienstleistungen. Der flächendeckende Stromausfall in der West-Ukraine im Dezember 2015, der das öffentliche Leben weitgehend zum Stillstand brachte, wird auf einen solchen Cyber-Angriff zurückgeführt. Die Anwesenheit und der Einsatz ungekennzeichneter, militärisch agierender Truppen ergänzt diese Strategie im jeweiligen Krisengebiet.

Die russischen Nachrichtendienste sind klassisch dreigeteilt gegliedert in einen Inlands-, Auslands- und militärischen Nachrichtendienst, wobei sich die Zuständigkeiten im Einzelfall überschneiden. Die folgenden Dienste sind auch in Deutschland aktiv:

- Inlandsnachrichtendienst – FSB
  Der FSB ist unter anderem für die zivile und militärische Spionageabwehr zuständig sowie für

die Bekämpfung von Terrorismus und organisierter Kriminalität. Zur Aufgabenerfüllung führt er auch Einsätze im Ausland aus. Aufgrund der Zuständigkeit für den Grenzschutz ist der Dienst zur Kontrolle aller ein- und ausreisenden Personen berechtigt.

- Ziviler Auslandsnachrichtendienst – SWR
  Der SWR ist vorrangig für die Aufklärung in den Bereichen Politik, Wirtschaft, Wissenschaft und Technologie zuständig. Zudem forscht er die Arbeitsmethoden und Aktivitäten fremder Nachrichtendienste aus. Der Dienst leistet elektronische Aufklärung und wirkt bei der Bekämpfung der Proliferation und des Terrorismus mit. Operationen werden zentral aus Moskau oder aus den Legalresidenturen im Ausland geführt.

- Militärischer Auslandsnachrichtendienst – GRU
  Der GRU ist direkt dem Verteidigungsministerium unterstellt. Seine Aufgaben umfassen die Aufklärung des gesamten militärischen Bereichs. Neben der NATO gehört dazu auch die deutsche Bundeswehr. Von besonderem Interesse sind für die GRU die Rüstungsindustrie sowie alle weiteren militärisch nutzbaren Technologien.

Volksrepublik China

Trotz rückläufiger Wirtschaftszahlen verfolgt die chinesische Regierung weiterhin das Ziel, sich als führende Wirtschaftsmacht an der Weltspitze zu etablieren. Das Land will bis zum Jahr 2020 nicht mehr von ausländischen Technologien abhängig zu sein. Darüber hinaus will China seinen politischen und militärischen Einfluss ausbauen. Die vor allem maritime Aufrüstung dient sowohl der Durchsetzung umstrittener Gebietsansprüche im Südchinesischen Meer als auch der Sicherung von See- und Handelswegen zu den Rohstoffen in Afrika und Südamerika. Die chinesische Regierung ist zudem bemüht, innerstaatliche Konflikte in einigen Provinzen und mit Oppositionellen im In- und Ausland zu unterdrücken. In diesen Bereichen lässt sich die chinesische Staatsführung durch ihre Nachrichtendienste auf vielfältige Weise unterstützen.

Nordrhein-Westfalen mit seinen hochinnovativen kleinen und mittleren Unternehmen sowie seinen zahlreichen Universitäten, Fachhochschulen, Forschungseinrichtungen und Technologie- und Gründerzentren steht besonders im Fokus nachrichtendienstlicher Aktivitäten. Wie Russland und Iran nutzt China die klassische Methode, Angehörige des eigenen Nachrichtendienstes mit Hilfe von diplomatischen und konsularischen Vertretungen, sogenannten Legalresidenturen, zu tarnen. Es bedient sich für den illegalen Wissenstransfer teilweise aber auch der Hilfe hier dauerhaft lebender Chinesen oder von Gastwissenschaftlern, Studenten und Praktikanten, die sich vorübergehend in Deutschland aufhalten. Zahlreiche Hinweise lassen zudem den Schluss zu, dass chinesische Nachrichtendienste nach wie vor bemüht sind, mit Hilfe elektronischer Angriffe Informationen zu beschaffen.

Neben Beschaffungsbemühungen in den Bereichen Politik, Wirtschaft, Wissenschaft und Militär wirken die Nachrichtendienste vor allem bei der Bekämpfung der nachfolgenden Bestrebungen und Vereinigungen mit:

- Demokratiebewegung,
- Anhänger eines unabhängigen Taiwan,
- Anhänger eines unabhängigen Tibet,
- Falun-Gong Anhänger und
- turkstämmige (muslimische) Uiguren.

Diese Bestrebungen und Vereinigungen werden von der kommunistischen Partei Chinas (KPCH) als Bedrohung ihrer Macht betrachtet und als die „Fünf Gifte“ bezeichnet. Eine Verfolgung findet im In- und Ausland statt.

Die nachrichtendienstlichen Aufgaben werden von drei Ministerien und einer Regierungsorganisation wahrgenommen, wobei sich die Zuständigkeiten teilweise überschneiden:

- Ministry of State Security – MSS
  Der zivile In- und Auslandsnachrichtendienst ist innerhalb Chinas zuständig für die Bekämpfung möglicher Gefährder der territorialen Einheit und der inneren Ordnung, vor allem der „Fünf Gifte“. Das MSS hat hierfür die Befugnisse einer Polizeibehörde. Es nimmt darüber hinaus die Aufgaben der Spionageabwehr wahr. Dazu beobachtet es nicht nur die im Land lebenden offiziellen Vertreter fremder Nationen, sondern generell die Bürger fremder Staaten. Im Ausland führt das MSS eigene Spionageoperationen durch, bemüht sich um Informationen aus den Bereichen Politik, Wirtschaft und Wissenschaft und forscht oppositionelle chinesische Gruppen aus.

- Ministry of Public Security – MPS
  Die auch als „Ministerium für öffentliche Sicherheit“ (MÖS) bezeichnete Behörde ist für die Gewährleistung der öffentlichen Sicherheit und Ordnung zuständig. Die Überwachung des Straßenverkehrs oder die allgemeine Verbrechensbekämpfung gehören zum vorrangigen Aufgabenbereich. Das MPS überwacht aber auch allgemein das öffentliche Leben, um möglichen Gefahren für das Machtmonopol der Kommunistischen Partei Chinas entgegenzutreten. Eine zentrale Methode ist die Kontrolle des Internets, der klassischen Medien sowie der sich in China aufhaltenden Ausländer. Das MPS operiert nicht nur auf eigenem Hoheitsgebiet, sondern sammelt auch im Ausland Informationen über Personen und Organisationen, die von der KPCH wegen regierungskritischer Aktivitäten als staatsfeindlich eingestuft werden. Da das Ministerium bei der Wahrnehmung seiner Aufgaben außerhalb der polizeilichen Zuständigkeiten nachrichtendienstliche Mittel einsetzt, wird es zu den Nachrichtendiensten gezählt.

- Military Intelligence Departement – MID
  Die militärische In- und Auslandsaufklärung liegt in der Zuständigkeit der Volksbefreiungsarmee. Sie schützt die eigenen Streitkräfte unter anderem vor gegnerischen Ausspähversuchen. Wie alle militärischen Nachrichtendienste beschafft das MID im Ausland militärisch bedeutsame Informationen, die beispielsweise Erkenntnisse über die Fähigkeiten und die Bewaffnung fremder Streitkräfte liefern oder die für die Verteidigungs- und Bündnispolitik relevant sind. Weitere Aufgabenfelder sind technische Spionage, Fernmeldeaufklärung, Cyberspionage, Telekommunikationsüberwachung und IT-Sicherheit im militärischen Bereich.

- Büro 610
  Vor dem Hintergrund der wachsenden Meditationsbewegung „Falun Gong“ wurde 1999 das unmittelbar an das Zentralkomitee der KPCH angebundene „Büro 610“ geschaffen. Diese Organisation ist für die Aufklärung und Bekämpfung der regimekritischen Bewegung Falun Gong zuständig. Das „Büro 610“ operiert außerhalb einer Ministeriumsstruktur auch im Ausland mit nachrichtendienstlichen Mitteln und ist daher als weitere nachrichtendienstliche Organisation anzusehen. Justiz, Polizei und Verwaltung arbeiten ihm zu. Der Name nimmt Bezug auf die Gründung des Büros am 10. Juni 1999.

Islamische Republik Iran

Im Jahr 2016 gingen die wesentlichen nachrichtendienstlichen Aktivitäten des Iran in Nordrhein-Westfalen vom zivilen In- und Auslandsnachrichtendienst „Ministry of Information and Security“ (MOIS) aus. Traditionell ist die Überwachung und Bekämpfung der iranischen Opposition im In- und Ausland Aufgabenschwerpunkt des MOIS. Daneben interessieren sich die iranischen Nachrichten- und Sicherheitsdienste aber auch für Informationen aus den Bereichen Politik, Militär und Wirtschaft. Entsprechende nachrichtendienstlich gesteuerte Aktivitäten konnten im Berichtsjahr auch in Nordrhein-Westfalen festgestellt werden.

Die bereits für 2015 beschriebene Intensivierung der Ausforschungsbemühungen des MOIS gegen die oppositionelle „Volksmodjahedin Iran-Organisation“ (MEK) beziehungsweise ihren politischen Arm, den „Nationalen Widerstandrat Iran“ (NWRI), war auch im Jahr 2016 festzustellen. Der iranische Nachrichtendienst hielt weiterhin an der Strategie fest, die MEK durch gezielte Propaganda zu diskreditieren.

Türkei

Der türkische Nachrichtendienst „Millî Istihbarat Teşkilâtı“ (MIT) ist sowohl für die In- als auch Auslandsaufklärung zuständig. Dabei ist er im Gegensatz zu den deutschen Nachrichtendiensten mit umfangreichen Polizeibefugnissen ausgestattet.

Der MIT unterhält in Deutschland Legalresidenturen in offiziellen Repräsentanzen. In Nordrhein-Westfalen befinden sich vier von insgesamt 15 türkischen Generalkonsulaten auf deutschem Boden (Düsseldorf, Essen, Hürth und Münster). Mit mehr als 530.000 türkischen Staatsangehörigen und einer erheblich größeren Anzahl Personen mit türkischem Migrationshintergrund ist Nordrhein-Westfalen einer der weltweiten Schwerpunkte der türkischen Diaspora und somit auch Operationsgebiet türkischer Nachrichtendienste.

Eine der Hauptaufgaben des MIT im Ausland ist die Aufklärung und Ausspähung Oppositioneller. Dazu gehören neben den kurdischen Gruppierungen wie der **Arbeiterpartei Kurdistans (PKK)** vor allem die linksextremistischen Organisationen **Revolutionäre Volksbefreiungspartei-Front (DHKP-C)**, die „Marxistisch-Leninistische Kommunistische Partei“ (MLKP) und neuerdings vor allem die nach dem Prediger Fetullah Gülen benannte „Gülen-Bewegung“. Letztere wird von türkischer Regierungsseite für den Putschversuch durch Teile des türkischen Militärs am 15. und 16. Juli 2016 verantwortlich gemacht.

Es kann davon ausgegangen werden, dass der MIT auch in Nordrhein-Westfalen eine intensivierte Aufklärung der vom türkischen Staat als „Fetullahistische Terrororganisation“ (FETÖ) bezeichneten Organisation betreibt.

Jubel nach dem gescheiterten Putschversuch in der Türkei am 16. Juli 2016

Aufklärung und Abwehr von Proliferation

Unter Proliferation wird die Weiterverbreitung atomarer, biologischer oder chemischer Massenvernichtungswaffen beziehungsweise der zu ihrer Herstellung verwendeten Produkte sowie entsprechender Waffenträgersysteme einschließlich des dafür erforderlichen Know-hows verstanden. Bei proliferationsrelevanten Staaten wie Iran, Nordkorea, Syrien oder Pakistan steht zu befürchten, dass Massenvernichtungswaffen in Konflikten eingesetzt oder als politisches Druckmittel genutzt werden.

Bis heute ist es den genannten Staaten nicht gelungen, die zur Weiterentwicklung der eigenen Programme erforderlichen Güter ausschließlich im eigenen Land herzustellen. Nordrhein-Westfalen als starker Wirtschaftsstandort mit einer Vielzahl relevanter Unternehmen und Forschungseinrichtungen stand im Jahr 2016 daher weiterhin im Fokus proliferationsrelevanter Beschaffungsstellen.

Fallzahlen im Jahr 2016

Aus der Einigung im Nuklearkonflikt zwischen den fünf ständigen Mitgliedern des Sicherheitsrats und Deutschland sowie dem Iran resultierte mit dem „Implementation Day“ im Januar 2016 die Lockerung der Sanktionen gegen den Iran. In der Folge war ein starker Rückgang entsprechender iranischer Beschaffungsversuche zu verzeichnen. Dieser spiegelt sich in den vorliegenden Fallzahlen wider. So konnte die Spionageabwehr im Berichtsjahr 32 Beschaffungsversuche beobachten, die definitiv oder mit hoher Wahrscheinlichkeit zugunsten eines Proliferationsprogramms unternommen wurden. Diese Zahl stellt einen signifikanten Rückgang der in Nordrhein-Westfalen identifizierten sensiblen Einkaufsbemühungen gegenüber dem bis dahin bestehenden Höchstwert aus dem Jahr 2015 (141) dar.

Der Iran stellt dennoch weiterhin den Bearbeitungsschwerpunkt in der Proliferationsabwehr dar. Die Nachfrage nach relevanten Gütern für die iranischen Raketenprogramme bildet die überwiegende Mehrheit der hier bekannt gewordenen Fälle. Daneben wurden beispielsweise erneut mehrere pakistanische Beschaffungsversuche festgestellt. In der überwiegenden Zahl der Fälle erfolgte keine Auslieferung der jeweiligen Waren, da der Verfassungsschutz die betroffenen Unternehmen rechtzeitig warnen konnte oder bereits sensibilisierte Firmen verdächtige Anfragen als solche erkannten und nicht bedienten.

Ausländische Staaten versuchen über verschleierte Transportwege sogenannte Dual-use-Güter für militärische Zwecke zu beschaffen.

Proliferationsrelevante Güter

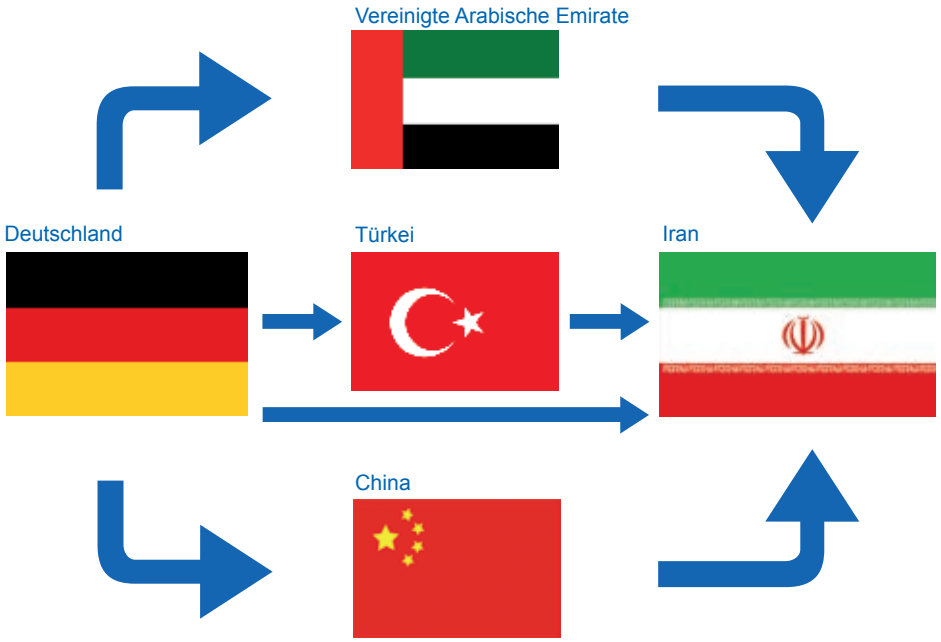
Gegenstand proliferationsrelevanter Anfragen sind in der Regel sogenannte Dual-use-Güter, also Produkte, die sowohl im zivilen als auch im militärischen Bereich verwendbar sind. Diese Güter bieten Einkaufsstellen die Möglichkeit, gegenüber Herstellern oder Händlern anstatt der tatsächlich vorgesehenen Endverwendung eine angeblich geplante zivile Nutzung anzugeben, um so die Lieferbereitschaft zu erhöhen.

Im Jahr 2016 nutzten die Proliferationsstaaten diesen Vorteil, indem sie auf eine Verwendung in der zivilen Forschung oder in der Öl-, Gas- und Stahlindustrie verwiesen. Als Belege wurden unter anderem gefälschte Endverbleibszertifikate oder sonstige scheinbar offizielle Dokumente vorgelegt. Im Berichtsjahr fielen nahezu sämtliche als proliferationsrelevant identifizierte Geschäftsanbahnungen in die Dual-use-Kategorie. Die Produktspanne erstreckte sich von kleinsten Ersatzteilen und elektronischen Komponenten bis hin zu kompletten industriellen Maschinen.

Beschaffungswege

Neben der Benennung einer angeblich zivilen Nutzung hat sich auch die Angabe falscher Endverwender als häufig genutzte Methode zum Erwerb proliferationsrelevanter Güter erwiesen. Dabei werden regelmäßig nicht nur vorgeschobene Unternehmen als Empfänger der Waren ausgegeben; oftmals wird zudem versucht, das eigentliche Zielland der Lieferung zu verschleiern.

In 2016 nutzten die Proliferationsstaaten dazu erneut umfangreiche Beschaffungsnetzwerke.



Routen proliferationsrelevanter Waren in den Iran

Diese bestehen aus Tarnfirmen und Strohmännern in unterschiedlichen Staaten. Sie versuchen, Güter über sogenannte Umgehungslieferungen zu beschaffen. Grundsätzlich können entsprechende Einkäufer hierzu jedes beliebige Land nutzen. Erfahrungsgemäß befinden sich die klassischen „Umgehungsstaaten“ aber in geographischer Nähe zum Zielland. Für Iran sind dies beispielhaft die Vereinigten Arabischen Emirate, die Türkei und China.

Aufklärung durch den Verfassungsschutz NRW

Der Verfassungsschutz NRW ist selbst vor dem Hintergrund der oben beschriebenen sinkenden Fallzahlen um eine kontinuierliche Ausweitung der Aufklärungsbemühungen bestrebt. Neben der Bearbeitung konkreter Verdachtsfälle und der Identifizierung von Beschaffungsnetzwerken führte die Spionageabwehr im Jahr 2016 erneut zahlreiche Sensibilisierungen in Form von Vorträgen und Einzelberatungen durch. Dabei wurden in 41 Veranstaltungen und Firmengesprächen über 120 Unternehmen in Nordrhein-Westfalen erreicht. Diese Präventionsarbeit der Spionageabwehr erhöht die Sensibilität in der Wirtschaft und führt durch ein zusätzliches Hinweisaufkommen zu einer stetigen Verbesserung der Proliferationsbekämpfung.

Ziele der Sensibilisierungen durch den Verfassungsschutz NRW sind Aufklärung und präventive Verhinderung möglicher Proliferationsgeschäfte. Die Gesprächspartner werden auf Gefahren illegaler Lieferungen sowie die einschlägigen Beschaffungsmethoden hingewiesen. In konkreten Einzelfällen bietet der Verfassungsschutz eine individuelle und vertrauensvolle Beratung, bei der Probleme und Fragen der Unternehmen stets vertraulich behandelt werden. Umgekehrt profitiert die Spionageabwehr von dem Austausch mit der Wirtschaft, über den Hinweise auf Anbahnungen mit möglichem Proliferationshintergrund gewonnen werden können.

Kontakt aufnehmen / Hinweise geben

Über die Rufnummer 0211 871 2821 und die E-Mail-Adresse kontakt.verfassungsschutz@im1.nrw.de kann ein Gesprächstermin mit der Spionageabwehr vereinbart werden.

Wirtschaftsspionage

Auch im Jahr 2016 konnten zahlreiche Angriffe auf das Know-how deutscher Unternehmen verzeichnet werden. Den deutschen Unternehmen entstehen hierdurch jährlich Schäden in Höhe von etwa 50 Milliarden Euro. Man kann von einer hohen Dunkelziffer ausgehen, weil Firmen Angriffe nicht bemerken oder sie aus Sorge um Image-Schäden nicht melden. Angriffsziele sind insbesondere kleine und mittlere Unternehmen. Sie verfügen häufig über sehr innovative Produkte und ein großes Know-how, sind sich jedoch oftmals der Gefahren nicht in vollem Umfang bewusst. Dabei sind schon lange nicht mehr nur Schlüsselbranchen, sondern mittlerweile nahezu alle Wirtschaftsbereiche von Spionage betroffen. Umfragen haben gezeigt, dass jedes zweite Unternehmen bereits Opfer eines Spionageversuches wurde.

In sehr vielen Staaten weltweit existieren gesetzliche Grundlagen, die den jeweiligen Nachrichtendiensten die Durchführung von Wirtschaftsspionage erlauben. Im Fokus der Spionageabwehr stehen insbesondere Länder wie China und Russland, aber auch viele andere Staaten betreiben Wirtschaftsspionage. In den vergangenen Jahren verdichteten sich die Erkenntnisse bei der Spionageabwehr des Verfassungsschutzes NRW, dass auch der Iran über ein eigenes Cyberprogramm verfügt. Es ist an exponierter Stelle innerhalb der sogenannten Revolutionsgarden angesiedelt. Insgesamt konnte im Jahr 2016 eine gegenüber den Vorjahren erneut deutlich erhöhte Zahl von qualitativ hochwertigen Cyberangriffen auf deutsche Unternehmen festgestellt werden. Ziel der Angriffe waren Unternehmensnetzwerke und Kontrollsysteme der Industrie.

Wirtschaftsspionage und Konkurrenzausspähung

Grundsätzlich lässt sich zwischen Wirtschaftsspionage und Konkurrenzausspähung, die oftmals auch als Industriespionage bezeichnet wird, unterscheiden. Unter Konkurrenzspionage versteht man die Ausspähung von Unternehmen durch einen Wettbewerber. Wirtschaftsspionage hingegen ist die staatlich gelenkte oder gestützte, von ausländischen Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben. In den Methoden unterscheiden sich beide Phänomene jedoch kaum.

Methoden der Wirtschaftsspionage

Die häufigste Angriffsvariante bestand im Jahr 2016 erneut darin, eine personalisierte E-Mail mit angehängter Schadsoftware zu versenden. Bei dieser Schadsoftware handelte es sich in der Regel um hochentwickelte Spionageprogramme, die speziell auf die IT-Infrastruktur des angegriffenen Unternehmens zugeschnitten waren. Nach Infektion verblieb die Schadsoftware oftmals über einen langen Zeitraum im Unternehmensnetz und übertrug unbemerkt Unternehmensdaten an den Angreifer. Diese von ausländischen Nachrichtendiensten genutzte Angriffsmethode führt zu einer fortgeschrittenen und andauernden Bedrohung des Unternehmensnetzwerkes. Sie wird als Advanced Persistent Threat (APT) bezeichnet.

Die zunehmende Digitalisierung von Produktionsprozessen, die unter dem Stichwort Industrie 4.0 zusammengefasst wird, bietet ausländischen Nachrichtendiensten neue Ansatzpunkte für mögliche Angriffe. In der Industrie 4.0 verzahnt sich die Produktion auf intelligente Weise mit modernster Informations- und Kommunikationstechnik. Das bringt große Vorteile und ermöglicht die kostengünstige Herstellung maßgeschneiderter Produkte nach individuellen Kundenwünschen und in hoher Qualität.

Letztendlich werden alle Prozesse digitalisiert und miteinander vernetzt. Dieser hohe Grad an Vernetzung und eine ungenügende Absicherung machen ein IT-Netzwerk allerdings auch leichter angreifbar. Gelingt es Wirtschaftsspionen an einer Stelle in ein solches Netzwerk einzudringen, erhalten sie häufig Zugang zu nahezu allen relevanten Bereichen. Darunter befinden sich Stellen, an denen sensible Unternehmensdaten gespeichert sind oder sich Steuerprozesse für die Produktion befinden. Daten können abfließen oder Produktionsprozesse sabotiert werden. Wirtschaftsspione setzen alles daran, über einen möglichst langen Zeitraum unentdeckt zu bleiben. Professionelle Spionageangriffe werden daher oftmals überhaupt nicht oder erst nach sehr langer Zeit entdeckt.

Smartphones als Angriffsziel

Es wurde aber nicht nur die IT von Unternehmen angegriffen, auch geschäftlich genutzte Smartphones waren das Ziel von Angriffen. Smartphones bieten nahezu die gleiche Funktionalität wie Computer, verfügen jedoch häufig nur über minimale Sicherheitsvorkehrungen und sind daher sehr leicht angreifbar. Im Bereich der Wirtschaftsspionage werden die mobilen Telefone mit professioneller Schadsoftware so infiziert, dass sie beispielsweise wie Wanzen funktionieren. Nimmt man ein solches Gerät mit in eine vertrauliche Besprechung, wird der gesamte Inhalt an den Angreifer übertragen. Es können alle Gespräche mitgehört und die auf dem Gerät gespeicherten Daten ausgelesen werden.

Social Engineering als beliebte Methode

Erheblich gestiegen ist im letzten Jahr der Einsatz von Social Engineering insbesondere zur Vorbereitung technischer Angriffe auf Unternehmensnetzwerke. Beim Social Engineering werden gezielt die Hilfsbereitschaft, Gutgläubigkeit oder auch Naivität von Mitarbeiterinnen und Mitarbeitern ausgenutzt, um einen Zugriff auf fremde IT-Netzwerke zu erhalten.

Systematischer Schutz des Unternehmens

Bei Angriffen spielt der „Faktor Mensch“ fast immer eine entscheidende Rolle. Eine regelmäßige Sensibilisierung und Schulung aller Mitarbeiter hilft, Angriffe mit Methoden von Social Engineering abzuwehren. Die Absicherung der eingesetzten IT nach dem aktuellen Stand der Technik ist zudem zwingend erforderlich. Bei der zunehmenden Komplexität eingesetzter IT-Systeme ist jedoch ein vollständiger Schutz kaum zu erreichen. Daher sind Unternehmen gefordert, für den Fall eines erfolgreichen Angriffs frühzeitig einen Notfallplan zu erstellen und in Übungen zu proben. Eine regelmäßige Sicherung aller Systeme über Backup-Routinen bildet eine wesentliche Säule eines erfolgreichen Notfallplans.

Unternehmenssicherheit ist Chefsache

Der Verfassungsschutz NRW empfiehlt Unternehmen dringend ein ganzheitliches Sicherheitskonzept. Dabei ist Unternehmenssicherheit mehr als reine IT-Sicherheit. Sie gehört in professionelle Hände und sollte von einer eigenen Organisationseinheit oder bei kleinen Unternehmen zumindest von speziell ausgebildeten Fachkräften vorangetrieben werden. Wichtig ist, dass der Prozess Unternehmenssicherheit, der auch die Themen Notfallmanagement und Prävention enthalten sollte, von der Führung eines Unternehmens ausgeht und top-down in das Unternehmen hineingetragen wird.

Der Verfassungsschutz NRW hat die Geschäftsführung der Sicherheitspartnerschaft Nordrhein-Westfalen inne. Gemeinsam mit der nordrhein-westfälischen Polizei, dem Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie, den Industrie- und Handelskammern NRW und der Allianz für Sicherheit in der Wirtschaft NRW hat er im Jahr 2016 die Veranstaltungsreihe „Unternehmenssicherheit ist Chefsache“ ins Leben gerufen. Im Berichtsjahr fanden die ersten vier Veranstaltungen in Bonn, Essen, Münster und Harsewinkel statt. Die Veranstaltungen richten sich gezielt an Entscheidungsträger in Unternehmen, um diese für die wichtigen Belange des Wirtschaftsschutzes zu sensibilisieren. Die als Entscheider-Dialog konzipierten Veranstaltungen wurden sehr gut angenommen. Das Dialogformat gab den Anwesenden die Möglichkeit, neben dem vertieften Informationsangebot das persönliche Gespräch mit den anwesenden Experten zu suchen.

Die Veranstaltungsreihe „Unternehmenssicherheit ist Chefsache“ spricht gezielt Entscheidungsträger in Unternehmen an.

Wirtschaftsschutzexperten des Verfassungsschutzes NRW geben aber auch außerhalb dieser Reihe konkrete Hilfestellungen. Sie stehen beispielsweise für kostenlose Sensibilisierungsvorträge zur Verfügung. Diese zeigen auf, welchen Bedrohungen Unternehmen aller Branchen und Größenordnungen durch Wirtschaftsspionage ausgesetzt sind, informieren über die wichtigsten Angriffsstrategien und stellen Schutzstrategien für Unternehmen vor. Im Jahr 2016 hielten Mitarbeiter des Verfassungsschutzes NRW 51 Vorträge mit rund 1.900 Teilnehmern, zudem wurden diverse Gespräche in Unternehmen geführt.

Auf Nachfrage besucht der Verfassungsschutz NRW zudem Unternehmen vor Ort, um praktische Hilfestellung bei der Erstellung eines Sicherheitskonzeptes zu geben.

Anfragen zu Vorträgen und Beratungsgesprächen

Anfragen können unbürokratisch per E-Mail an wirtschaftsschutz@im1.nrw.de oder telefonisch an 0211 871 2821 gerichtet werden.