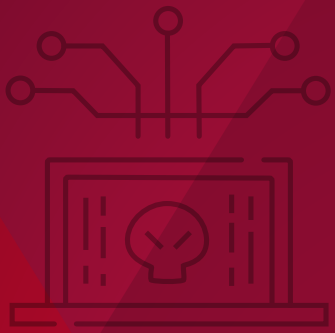
Bundesamt für
Verfassungsschutz

Spionage, Cyberangriffe & Co.

Bedrohungen durch fremde Nachrichtendienste



Spionage, Cyberangriffe & Co.

Bedrohungen durch fremde Nachrichtendienste

Inhalt

Kapitel 1
Deutschland als Ziel fremder Mächte 6

Kapitel 2
Interessen fremder Nachrichtendienste 7

2.1 Regierungen und ihre Nachrichtendienste 7
2.2 Die Betätigungsfelder im Kurzüberblick 8
2.3 Operationsgebiet Deutschland 10
2.4 Fremde Nachrichtendienste in Deutschland 10
2.4.1 Russische Föderation 11
2.4.2 Volksrepublik China 12
2.4.3 Islamische Republik Iran 14
2.4.4 Republik Türkei 15
2.4.5 Sonstige Staaten 16

Kapitel 3
Aktivitäten fremder Nachrichtendienste 18

3.1 Spionage 18
3.2 Cyberangriffe 20
3.3 Einflussnahme 22
3.4 Sabotage 24
3.5 Staatsterrorismus 25
3.6 Proliferation 26

Kapitel 4
Abwehrarbeit des Verfassungsschutzes 28

4.1 Spionageabwehr 30
4.2 Cyberabwehr 31
4.3 Proliferationsabwehr 32
4.4 Prävention in Wirtschaft, Wissenschaft, Politik und Verwaltung . . 33

Kapitel 5
Ausblick 35

Glossar 37

Kapitel 1

Deutschland als Ziel fremder Mächte

Die Welt der Spionage erscheint schillernd, doch fremde Nachrichtendienste agieren im Verborgenen. Ihr Ziel ist es, sensible Informationen zu erlangen. Sie sind aber auch in Sabotage, Einflussnahme und Desinformation verwickelt oder in Versuche involviert, Komponenten und Know-how zur Herstellung von Massenvernichtungswaffen zu beschaffen. Die Cyber- und Spionageabwehr des Bundesamtes für Verfassungsschutz (BfV) hat die Aufgabe, verborgenes wie illegales Handeln fremder Mächte in und gegen Deutschland aufzuklären und zu unterbinden.

Kapitel 2

Interessen fremder Nachrichtendienste

2.1 Regierungen und ihre Nachrichtendienste

Für Regierungen nahezu aller Staaten sind sensible Informationen aus dem Ausland von entscheidender Bedeutung, um eigene politische Leitlinien zu entwickeln, rechtzeitig auf globale Krisen reagieren oder weltpolitische Ambitionen durchsetzen zu können.

Diplomatinnen und Diplomaten sammeln auf legalen Wegen frei verfügbare Informationen, um ihre Regierungen über aktuelle Ereignisse und längerfristige Entwicklungen im jeweiligen Gastland zu unterrichten und um die Beziehungen ihrer Heimatstaaten mit diesem zu fördern. Viele Regierungen geben sich mit der Beschaffung offen verfügbarer Informationen allerdings nicht zufrieden. Sie streben danach, Erkenntnisse aus anderen Staaten zu erlangen, die nicht für die Öffentlichkeit bestimmt

sind. Hier beginnt die Welt der →*Spionage*, und als zentrale Akteure kommen fremde Nachrichtendienste ins Spiel. Dabei kann es sich um rein zivile Nachrichtendienste, Dienste mit Polizeibefugnissen oder militärische Nachrichtendienste handeln.

Die heute gegen Deutschland gerichteten Betätigungsfelder fremder Nachrichtendienste sind zahlreich: Ihr verdecktes Vorgehen zur Informationsbeschaffung und illegitimen →*Einflussnahme*, zum illegalen Waffen- und Know-how-Erwerb sowie zu →*Sabotage* oder gar zu Zwecken des →*Staatsterrorismus* stellt den Verfassungsschutz vor große Herausforderungen. Hinzu kommt, dass sich die Handlungsoptionen fremder Nachrichtendienste durch die Entwicklung neuer Technologien und die fortschreitende Digitalisierung deutlich erweitern.

2.2 Die Betätigungsfelder im Kurzüberblick

Spionage zur Informationsbeschaffung

Mit Spionage beschaffen Nachrichtendienste geheim gehaltene Informationen anderer Staaten aus Bereichen wie Politik und Verwaltung, Militär, Wirtschaft und Wissenschaft. Das können Pläne von Regierungen, Funktionsweisen von Waffensystemen, Strategien von Unternehmen oder wissenschaftliche Erkenntnisse von Forschungsinstituten sein. Die Informationsbeschaffung erfolgt auf verschiedenen Wegen. Dazu gehören sowohl die Heranziehung frei zugänglicher Informationen, etwa von Presseartikeln oder Internetbeiträgen (→*Open Source Intelligence – OSINT*), als auch der Einsatz menschlicher Quellen (→*Human Intelligence – HUMINT*). Sie erfolgt unter anderem auch durch das Abfangen elektronischer Signale (→*Signals Intelligence – SIGINT*).

Cyberangriffe auf Systeme und Netzwerke

Mit →*Cyberangriffen* können Nachrichtendienste in der digitalisierten Welt aus sicheren Basen im eigenen Land heraus in anderen Ländern spionieren. Sie greifen einzelne Computer oder ganze Netzwerke an und verschaffen sich dauerhaften Zugang. So sammeln sie Informationen oder eröffnen sich Möglichkeiten, durch Sabotage Schaden anzurichten.

Einflussnahme, Propaganda und Desinformation

Mit Einflussnahmeoperationen wollen Nachrichtendienste illegitim auf Menschen in politischen oder wirtschaftlichen Entscheidungspositionen im Sinne ihrer Staatsführung einwirken. Außerdem versuchen sie, mit →*Propaganda* vermeintliche Vorzüge autoritärer oder gar diktatorischer Staaten in der Öffentlichkeit herauszustellen, um diese als Alternative zur offenen Gesellschaft und zum demokratischen Rechtsstaat erscheinen zu lassen. Mit →*Desinformation* in der Medienwelt sowie in sozialen Medien wollen sie in der Bevölkerung Zweifel an der demokratischen Ordnung und der Funktionsfähigkeit von Politik und Verwaltung wecken.

Sabotage gegen die Infrastruktur

Mit Sabotage können Nachrichtendienste sogenannte →*Kritische Infrastrukturen (KRITIS)* wie Verkehrseinrichtungen, Kraftwerke, Pipelines, Krankenhäuser oder Informations- und Kommunikationseinrichtungen stören oder massiv beschädigen. KRITIS haben eine zentrale Bedeutung für das gesellschaftliche Leben, die Versorgungssicherheit und die staatliche Funktionsfähigkeit. Eine Bedrohung entwickelt sich bereits in der Phase der Vorbereitung möglicher Anschläge gegen KRITIS oder andere Stellen in Form einer vorbereitenden Ausspähung durch fremde Nachrichtendienste.

Staatsterrorismus bis hin zu Mord

Mit Staatsterrorismus begehen Nachrichtendienste einiger Staaten besonders schwere Verbrechen. Dieser kann erfolgen, um die deutsche Regierung zu einem bestimmten Handeln zu zwingen, richtet sich jedoch zumeist gegen Oppositionelle, die vor den Diktaturen ihrer Heimatländer nach Deutschland geflohen sind und „zum Schweigen gebracht“ werden sollen. Dazu erfolgen massive, das Leben von Menschen zerrüttende Bedrohungen, aber auch Entführungen oder sogar Mordanschläge (→*Transnationale Repression – TNR*).

Proliferation zum Bau von Massenvernichtungswaffen

Mit →*Proliferation* reagieren einige Staaten auf internationale Beschränkungen im Bereich der (Weiter-)Entwicklung von chemischen, biologischen, radiologischen und nuklearen Massenvernichtungswaffen (CBRN-Waffen)[1]. Sie versuchen, auf illegale Weise CBRN-Waffen, für deren Ein-

1 Für diese war früher die Bezeichnung ABC-Waffen gebräuchlich.

satz benötigte Raketen und andere Trägersysteme beziehungsweise Wissen zu deren Herstellung zu beschaffen. Dabei setzen verschiedene Staaten auch ihre Nachrichtendienste ein, die in Beschaffungsnetzwerke eingebunden sind.

2.3 Operationsgebiet Deutschland

Verschiedene fremde Nachrichtendienste richten ihre Aktivitäten gegen Deutschland. Als bevölkerungsreichstes Mitglied der EU, Partner im Verteidigungsbündnis NATO, weltweit vernetzte Wirtschaftsmacht und nicht zuletzt als wichtiger Standort von Forschung und Entwicklung ist Deutschland für sie ein attraktives Ziel. Es ist als freie und weltoffene Gesellschaft besonders angreifbar, da ausländische Nachrichtendienste diese Offenheit für ihre Zwecke missbrauchen. Als Schutzraum und Zufluchtsort politisch Verfolgter und Heimat für Eingewanderte leben in Deutschland unterschiedliche Bevölkerungsgruppen mit Migrationshintergrund, die aus verschiedenen Gründen im Blickfeld der Nachrichtendienste ihrer Herkunftsländer stehen und unter Umständen TNR ausgesetzt sind.

2.4 Fremde Nachrichtendienste in Deutschland

Der Großteil der gegen Deutschland gerichteten Spionage, Cyberangriffe und sonstigen nachrichtendienstlichen Aktivitäten geht von vier Staaten aus: der Russischen Föderation, der Volksrepublik China, der Islamischen Republik Iran sowie der Republik Türkei. Darüber hinaus agieren sowohl Nachrichtendienste menschenrechtsfeindlicher Diktaturen wie der Demokratischen Volksrepublik Korea (Nordkorea) oder der Arabischen Republik Syrien, aber auch aus rechtsstaatlichen Demokratien gegen Deutschland. Im verdeckten Kampf um sensible Informationen oder Einfluss betätigen sich jedoch nicht nur mit Deutschland rivalisierende Staaten, sondern auch solche, zu denen ein gutes Verhältnis besteht.

2.4.1 Russische Föderation

In Russland haben die Nachrichtendienste traditionell eine zentrale Funktion innerhalb des Staates und sind wesentliche Einrichtungen der Sicherheitsarchitektur. Ein Teil der aktuellen politischen Machtelite war in der Vergangenheit für sie tätig. So leitete der ehemalige KGB[2]-Offizier Wladimir Putin in den 1990er-Jahren den zivilien Inlandsnachrichtendienst FSB[3], bevor er in das Präsidentenamt gelangte. Unter den Bedingungen der autoritären Herrschaft Putins dienen die – auch für Mordanschläge verantwortlichen – Nachrichtendienste im Inneren der Machterhaltung des Regimes und im Äußeren zur Informationsbeschaffung sowie zur rücksichtslosen Durchsetzung seiner Interessen.

Die russischen Nachrichtendienste betätigen sich seit Jahrzehnten mit hohem nachrichtendienstlichem Aufwand in und gegen Deutschland. Aktiv sind dabei neben dem FSB der zivile Auslandsnachrichtendienst SWR[4] und der Militärnachrichtendienst GRU[5]. Im Kontext der in der Vergangenheit vielfältigen deutsch-russischen Beziehungen interessieren sie sich seit Jahrzehnten für ein breites Themenspektrum aus Politik und Verwaltung, Militär, Wirtschaft und Wissenschaft. Nach der ersten völkerrechtswidrigen russischen Besetzung ukrainischer Gebiete im Jahr 2014 und den daraufhin erlassenen Sanktionen der EU rückten die Außen-, Sicherheits-, Verteidigungs- sowie Energiewirtschaftspolitik Deutschlands in den Fokus russischer Spionage und Cyberangriffe. Parallel dazu erfolgen Maßnahmen zur Einflussnahme auf Politik und Gesellschaft in Deutschland, unter anderem mittels Propaganda und Desinformation.

Arbeitsintensität, Umfang und Komplexität des nachrichtendienstlichen Handelns der Russischen Föderation haben mit dem Angriffskrieg gegen die Ukraine deutlich zugenommen. Dieser Herausforderung begegnete die Bundesregierung unter anderem mit der Ausweisung zahlreicher russischer Nachrichtendienstangehöriger, die als diplomatisches Personal

2 Komitet Gossudarstwennoi Besopasnosti (auf Deutsch: Komitee für Staatssicherheit), ehemaliger sowjetischer In- und Auslandsnachrichtendienst sowie Geheimpolizei (1954–1991).

3 Federalnaja Slushba Besopasnosti (auf Deutsch: Föderaler Dienst für Sicherheit).

4 Slushba Wneschnej Raswedki (auf Deutsch: Dienst der Außenaufklärung).

5 Glawnoje Raswedywatelnoje Uprawlenije (auf Deutsch: Hauptverwaltung für Aufklärung).

getarnt in den sogenannten →*Legalresidenturen* tätig waren. Das BfV beobachtet sorgfältig, auf welche Weise die russischen Dienste diesen Verlust zu kompensieren suchen.

Die **Bundesregierung** hat auf Russlands Angriffskrieg gegen die Ukraine mit humanitärer, politischer, wirtschaftlicher und militärischer Unterstützung für das angegriffene Land reagiert. Seitdem versuchen russische Nachrichtendienste, ihren erhöhten Informationsbedarf insbesondere über die Unterstützungsleistungen sowie die politischen Entscheidungswege in Deutschland, der EU, der NATO und anderen internationalen Einrichtungen mit Agenten und Cyberangriffen zu decken. Im Fokus stehen die Ausbildung ukrainischer Soldaten in Deutschland, internationale Waffentransporte in die Ukraine, die deutsche Energiepolitik oder gegen Russland gerichtete Sanktionen der EU. Russland hat außerdem Interesse daran, die öffentliche Meinung sowie politische Meinungsträgerinnen und -träger gegen die Unterstützung der Ukraine zu beeinflussen sowie Sabotageaktionen vorzubereiten und durchzuführen.

2.4.2 Volksrepublik China

Die Nachrichtendienste der Volksrepublik China dienen dem Machterhalt der Kommunistischen Partei Chinas (KPCh). Für die Entwicklung des Landes zur Weltmacht betreibt die Staats- und Parteiführung den Aufbau einer vom Ausland unabhängigen Wirtschaft und forciert den Ausbau der Armee. Bei dieser Großmachtpolitik spielen die Nachrichtendienste mit ihrer Informationsbeschaffung eine wesentliche Rolle. Außerdem bekämpfen die chinesischen Behörden auch verschiedene oppositionelle Gruppen, insbesondere die nach mehr Unabhängigkeit strebenden

ethnischen Minderheiten der Uiguren und Tibeter, die regimekritische Falun-Gong-Bewegung, die Demokratiebewegung und die Befürworter einer Eigenstaatlichkeit der Insel Taiwan. Darüber hinaus steht auch die Hongkonger Demokratiebewegung im Fokus und es werden die Anhängerinnen und Anhänger der „White Paper-Bewegung“ bekämpft, die 2022/2023 die repressiven Maßnahmen der KPCh in Zeiten der Coronapandemie kritisierten.

Die Volksrepublik China zählt bereits heute mit ihrer Wirtschaftskraft, ihren wissenschaftlich-technischen Fähigkeiten und ihren modernen Streitkräften zu den einflussreichsten Nationen der Welt. Der von Staatspräsident Xi Jinping verfolgte „**chinesische Traum**“ soll bis Mitte des 21. Jahrhunderts zum Status einer Weltmacht führen. Mit dieser Zielsetzung ist das Land ein strategischer Rivale der USA; zugleich will es die regelbasierte Weltordnung in seinem Sinne neu prägen. Zudem vertritt China seine Interessen im Ausland auch aggressiv, etwa gegenüber dem demokratischen Taiwan oder im Streit mit seinen Nachbarn um Inseln im Südchinesischen Meer.

China betreibt hauptsächlich Spionage und Einflussnahme im politischen Raum mittels Agenten und Cyberangriffen, setzt für das Ziel einer globalen Führungsrolle seine nachrichtendienstlichen Ressourcen jedoch auch gegen Wirtschaft und Wissenschaft ein. Im Zentrum der Wissenschaftsspionage steht der Know-how-Transfer, welcher auch mit anderen Mitteln wie Austausch- oder Kooperationsprogrammen verfolgt wird.

Die Beziehungen zwischen Deutschland und China sind einerseits von intensiven Wirtschaftsverbindungen und andererseits einer politischen Systemrivalität geprägt. Diese besteht zwischen der kommunistischen Diktatur Chinas und der rechtsstaatlichen Demokratie Deutschlands, deren Leitbild die Menschenwürde ist.

In Deutschland sind der zivile In- und Auslandsnachrichtendienst MSS[6] sowie das auf die Unterdrückung von Regierungsgegnerinnen und -gegnern konzentrierte MPS[7] aktiv. Neben diesen betätigen sich der allgemeine Militärnachrichtendienst MID[8] sowie der auf Fernmeldewesen und den Cyberraum spezialisierte technische militärische Nachrichtendienst NSD[9]. Deren Aktivitäten können der chinesischen Regierung auch zur Begleitung strategischer Investitionen in deutsche Spitzentechnologien sowie Unternehmen von besonderer Relevanz für die globalen Machtambitionen des Landes und bei der Anwerbung von Wissensträgerinnen und -trägern aus Wissenschaft und Militär nützlich sein.

2.4.3 Islamische Republik Iran

Die seit der Islamischen Revolution von 1979 durchgängig autokratisch von einem schiitischen „Obersten Führer“ regierte Islamische Republik Iran verfügt als Regionalmacht am erdöl- und erdgasreichen Persischen Golf über eine geopolitisch wichtige Position. Sie ist insbesondere im Nahen und Mittleren Osten militärisch aktiv, unterstützt Terroristen und betreibt selbst Staatsterrorismus. Gleichzeitig unterhält Iran ein Atomwaffenprogramm, weshalb er umfangreichen Sanktionen insbesondere der EU und der USA unterliegt. Das Land hat eine grundlegend feindselige Haltung gegenüber den USA und strebt die Vernichtung des Staates

6 Ministry of State Security (auf Deutsch: Ministerium für Staatssicherheit).
7 Ministry of Public Security (auf Deutsch: Ministerium für Öffentliche Sicherheit).
8 Military Intelligence Directorate (auf Deutsch: Direktion des Militärgeheimdienstes).
9 Network Systems Department (auf Deutsch: Ressort für Netzwerksysteme).

Israel an. Im Inneren begeht der iranische Sicherheitsapparat regelmäßig schwere Menschenrechtsverletzungen, darunter Folter und Tötungen gegen Regimegegnerinnen und -gegner.

In Deutschland operiert der zivile Nachrichtendienst VAJA[10], der international unter der Bezeichnung MOIS[11] bekannt ist. Als militärische Parallelstruktur zur regulären Armee sind die Revolutionsgarden mit ihrem Nachrichtendienst IRGC-IO[12] sowie der militärischen Spezialeinheit Quds Force[13] ebenfalls nachrichtendienstlich gegen Deutschland tätig.

Ein Schwerpunkt iranischer nachrichtendienstlicher Aktivitäten ist die Bekämpfung oppositioneller Gruppierungen und Einzelpersonen im In- und Ausland. Diese Gruppierungen gelten aus Sicht der Machthaber Irans als Gefährdung für den Fortbestand des Regimes. Die iranischen Nachrichtendienste spüren weltweit mit hoher Aggressivität im Ausland lebende Regierungsgegnerinnen und -gegner auf und bekämpfen diese rücksichtslos. Gefährdet sind auch Personen mit deutscher und iranischer Doppelstaatsangehörigkeit.

Wegen der Konfrontation mit den westlichen Staaten ist Iran auch verstärkt an deutscher Außen- und Sicherheitspolitik sowie an militärischen Belangen interessiert. Iranische Nachrichtendienste richten ihre Arbeit außerdem gegen (pro-)israelische sowie (pro-)jüdische Ziele in Deutschland.

2.4.4 Republik Türkei

Mit der Türkei ist ein Staat in Deutschland nachrichtendienstlich aktiv, der im Gegensatz zu Russland, China und Iran seine Regierung in freien

10 Vezarat e Ettela'at-e Jomhouri-ye Eslami-ye Iran (auf Deutsch: Ministerium für Nachrichtenwesen der Islamischen Republik Iran).

11 Ministry of Intelligence (auf Deutsch: Ministerium für Nachrichtenwesen).

12 Islamic Revolutionary Guard Corps Intelligence Organization (auf Deutsch: Nachrichtendienst der Armee der Wächter der Islamischen Revolution).

13 Auch: al-Quds-Einheit, Quds-Brigaden oder Sepah-Qods. Die Bezeichnung der Einheit wird von dem arabischen Namen für Jerusalem „al-Quds" abgeleitet.

Wahlen bestimmt. Doch der Umstand, dass die Türkei als NATO-Mitglied ein militärischer Verbündeter sowie als EU-Beitrittskandidat ein enger Kooperationspartner Deutschlands ist, verhindert nicht, dass die türkische Regierung zur Wahrung ihrer Interessen und Informationsbedürfnisse Aufklärung in Deutschland betreibt. Dazu tragen die türkischen Nachrichtendienste und Sicherheitsbehörden entscheidend bei. Da in Deutschland mehrere Millionen türkeistämmige Menschen leben, bestehen vielfältige Beziehungen zwischen diesen und der türkischen Gesellschaft. Die türkischen Nachrichtendienstangehörigen spähen tatsächliche oder vermutete Gegnerinnen und Gegner der türkischen Regierung aus. Das betrifft vor allem die „Arbeiterpartei Kurdistans" (PKK)[14], die in der Türkei mit terroristischen und paramilitärischen Mitteln gegen den Staat kämpft und sich in Deutschland innerhalb der kurdischen Szene um Unterstützende und Geldmittel für die Gesamtorganisation bemüht. Darüber hinaus steht die in den letzten Jahren vom türkischen Staat als Bedrohung erachtete Gülen-Bewegung im Fokus. Zur Vorbereitung politischer Entscheidungen interessieren sich türkische Nachrichtendienste außerdem unter anderem für Informationen über die Politik der deutschen Regierung in der EU und der NATO.

2.4.5 Sonstige Staaten

Zur breiten Gruppe der weiteren in Deutschland nachrichtendienstlich aktiven Staaten zählt die von einer kommunistischen Diktatur beherrschte Demokratische Volksrepublik Korea (Nordkorea). Sie verfügt einerseits über Atomwaffen sowie weitreichende Raketen und ist andererseits eines der isoliertesten Länder der Welt. Aufgrund ihrer Atomwaffenpolitik unterliegt sie umfangreichen Sanktionen der Vereinten Nationen, die die nordkoreanische Wirtschaft stark belasten. Das Hauptinteresse des herrschenden Regimes ist sein Machterhalt, wozu es sich auf mehrere Nachrichtendienste stützt: den zivilen Nachrichten- und Sicherheitsdienst MSS[15], den Militärnachrichtendienst RGB[16] sowie den Nach-

14 Auf Kurdisch: „Partiya Karkerên Kurdistan".

15 Ministry of State Security (auf Deutsch: Ministerium für Staatssicherheit).

16 Reconnaissance General Bureau (auf Deutsch: Generalbüro für Aufklärung).

richtendienst der Staatspartei UFD[17], die alle auch in Deutschland agieren. Ihre Arbeitsschwerpunkte sind die Gewährleistung der Sicherheit nordkoreanischer Vertretungen im Ausland sowie die umfassende Überwachung nordkoreanischer Staatsbürgerinnen und -bürger hierzulande. Hinzu kommen die nachrichtendienstliche Aufklärung Deutschlands mittels Cyberangriffen und die Unterstützung der umfassenden Proliferationsaktivitäten des Regimes beziehungsweise die Beschaffung dafür benötigter Devisen.

In den letzten Jahren ergingen zu Spionagefällen verschiedene Gerichtsurteile, die Tätigkeiten weiterer Nachrichtendienste in Deutschland belegen. Zu diesen gehören Dienste aus Ägypten, Syrien, Marokko, Vietnam, Pakistan oder Indien. Dabei handelt es sich häufig um Fälle von TNR. Bei der Bearbeitung illegaler nachrichtendienstlicher Tätigkeiten betraf es mit den USA in einem Fall sogar einen der engsten Verbündeten Deutschlands. So wurde 2016 ein zuvor von US-amerikanischen Nachrichtendienstangehörigen als sogenannter Maulwurf geführter Angehöriger des Bundesnachrichtendienstes (BND) zu einer achtjährigen Haftstrafe verurteilt.

Bei den Nachrichtendiensten aus dem Nahen und Mittleren Osten ist die Ausspähung und Diskreditierung von in Deutschland lebenden Regierungsgegnerinnen und -gegnern ein zentrales Aufgabengebiet. Dabei bemühen sie sich sowohl um die Anwerbung menschlicher Quellen als auch um erfolgreiche Cyberangriffe. Es besteht ebenso die Gefahr, dass außereuropäische Regionalkonflikte wie beispielsweise zwischen Saudi-Arabien und Iran oder zwischen Indien und Pakistan auch mit nachrichtendienstlichen Mitteln in Deutschland ausgetragen werden. Menschliche Quellen kommen dabei genauso zum Einsatz wie moderne technische Mittel sowie Aktivitäten im Cyberraum.

17 United Front Department (auf Deutsch: Zentralabteilung Vereinigte Arbeitsfront).

Kapitel 3

Aktivitäten fremder Nachrichtendienste

3.1 Spionage

Die Informationsbeschaffung durch Spionage ist der klassische Arbeitsschwerpunkt aller fremden Nachrichtendienste, die in oder gegen Deutschland arbeiten. Sie beinhaltet das illegale Ausspähen sensibler und/oder geheimer Informationen aus den Bereichen Politik und Verwaltung, Militär, Wirtschaft und Wissenschaft.

Durch Informationszugänge in diesen Bereichen erhoffen sich ausländische Nachrichtendienste Vorteile für ihre eigenen Regierungen.

Spionage und Einflussnahme, darunter auch die Anwerbung menschlicher Quellen, finden heutzutage sowohl in der realen als auch in der virtuellen Welt statt.
Probate Mittel der **Informationsgewinnung in der realen Welt** sind etwa Besuche von Handelsmessen oder die Teilnahme an öffentlichen Vortragsveranstaltungen, Tagungen und Diskussionsrunden. Hier können fremde Nachrichtendienste nicht nur wertige Sachinformationen gewinnen, sondern vor allem ihr Netzwerk an Gesprächspartnerinnen und -partnern erweitern, das bei Bedarf auch ohne engere nachrichtendienstliche Anbindung abgeschöpft werden kann.
Soziale Medien spielen für die **Informationsgewinnung in der virtuellen Welt** eine sehr große Rolle, da hier eine Vielzahl an persönlichen Daten gesammelt werden kann, die dann wiederum für weitere operative Zwecke nutzbar sind. Gerade freiwillig offenbarte Informationen zu Ausbildungen, Arbeitsstellen, Familie, Freunden, Kollegen oder Hobbys sind wertvolle „Schätze“ für fremde Nachrichtendienste: Mit diesen identifizieren sie Personen, die als menschliche Quellen zu Spionage- und Einflussnahmezwecken in Frage kommen. Zudem gibt es Versuche der Anwerbung und Instruktion durch fremde Nachrichtendienste über soziale Medien.

Dazu werben sie Personen mit Zugang zu sensiblen Informationen an. Sie identifizieren zunächst, welche Personen interessante Zugänge besitzen und Ansatzpunkte für den Aufbau einer Zusammenarbeit bieten. Danach sprechen psychologisch geschulte Nachrichtendienstangehörige die Zielpersonen im Rahmen einer zunächst unverfänglichen Kontaktaufnahme an, um sodann über einen längeren Zeitraum ein immer persönlicher werdendes Verhältnis aufzubauen. Bereits in diesem Stadium schöpfen sie durch eine geschickte Gesprächsführung auf unauffällige Weise Informationen ab. Im für sie optimalen Fall entwickelt sich das Verhältnis so, dass sich die Wissensträgenden zu einer festen Zusammenarbeit verpflichten.

Das Knüpfen von Kontakten ist ausländischen Nachrichtendiensten am

einfachsten auf dem jeweils eigenen Staatsgebiet möglich: Aus Deutschland eingereiste Geschäftsleute oder Touristinnen und Touristen können dort problemlos überwacht und gegebenenfalls angesprochen werden. Für den Einsatz in Deutschland werden die Mitarbeiter ausländischer Nachrichtendienste häufig als diplomatisches Personal getarnt, damit sie mit diplomatischer Immunität ausgestattet innerhalb der eigenen Botschaft oder in ihren Konsulaten sogenannte Legalresidenturen bilden. Dies schützt sie zwar vor einer möglichen Verhaftung, ihnen droht jedoch die Ausweisung, sollten sie bei illegalen Tätigkeiten erwischt werden. Riskanter ist im Vergleich dazu die Tarnung als Mitarbeitende staatlich beeinflusster Einrichtungen, wie beispielsweise Presseagenturen oder Luftfahrtgesellschaften.

Botschafts- und Konsulatsgebäude sind außerdem potenzielle Standorte für Abhöranlagen und bieten so eine weitere Möglichkeit der illegalen Informationsgewinnung.

3.2 Cyberangriffe

Ausländische Nachrichtendienste können mit hoch qualifizierten Computerexperten aufwendig Cyberangriffe gegen einzelne Rechner oder gesamte Computernetzwerke durchführen, um Informationen abzuschöpfen, Daten zu verändern oder Betriebsabläufe zu stören. Sie können auch Hardware zerstören, IT-Netzwerke zusammenbrechen lassen oder den Betrieb von Unternehmen oder Einrichtungen wie beispielsweise Rathäuser oder Hospitäler beeinträchtigen. Im Vergleich zur traditionellen Arbeitsweise mit eigens dafür angeworbenen Menschen bieten Cyberangriffe eine Reihe von Vorteilen:

Sie sind
- ortsunabhängig,
- relativ kostengünstig und
- für die durchführenden Personen risikoarm.

Ein weiterer Nutzen besteht darin, dass die Verantwortlichen ihren nachrichtendienstlichen Hintergrund verschleiern können, indem sie sich den Anschein einer nicht staatlichen Gruppe geben, die keinem Nachrichtendienst angehört. Generell ist für

hochqualifizierte und langfristig handelnde Angreifer im Cyberraum die Bezeichnung →*Advanced Persistent Threat (APT)* geläufig. Deren Attacken entwickeln sich über einen längeren Zeitraum derart umfassend, dass sie regelrechte Angriffswellen bilden können.

Angriffsvektor bezeichnet den Angriffsweg und die Angriffstechnik, die ein unbefugter Eindringling nehmen kann, um ein fremdes Computersystem zu kompromittieren und für eigene Zwecke zu missbrauchen.
Phishing bezeichnet generell den Versuch, in der elektronischen Kommunikation persönliche Daten illegal zu „angeln" und für unzulässige Zwecke zu verwenden. Durch gefälschte E-Mails, Webseiten oder Anrufe sollen Daten wie zum Beispiel Zugangsdaten, Passwörter, Kreditkartennummern erlangt werden.
Spear-Phishing ist einer der am häufigsten verwendeten Angriffsvektoren und stellt eine Variante des Phishings dar, die insbesondere von APTs verwendet wird. Die Phishing-Mail wird für eine Einzelperson oder einen kleinen Personenkreis maßgeschneidert. Durch die Verwendung zuvor recherchierter Informationen und Insiderwissen soll die E-Mail täuschend echt wirken, um an vertrauliche Daten des potenziellen Opfers zu gelangen oder ein bestimmtes Verhalten auszulösen.

Bei nachrichtendienstlich verursachten Cyberangriffen wird (wie bei Attacken von Cyberkriminellen) in der Regel eine Schadsoftware in einen Zielcomputer oder in ein Netzwerk eingeschleust.

Nach erfolgreichen Cyberangriffen nutzen ausländische Nachrichtendienste auch die Möglichkeit, gestohlene Daten zu veröffentlichen oder beispielsweise Social-Media-Konten der betroffenen Personen oder Organisationen zu kapern und zur Verbreitung von Falschinformationen zu missbrauchen.

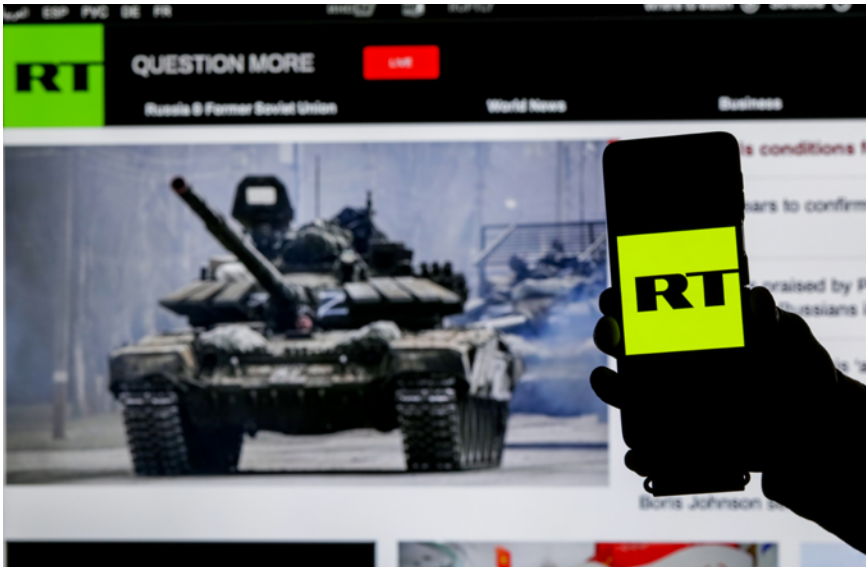
Bei **Hack and Leak** kompromittieren die Angreifer zunächst das Computernetzwerk des Opfers und leiten erbeutete Daten aus. In einem zweiten Schritt werden die gestohlenen Daten dann teilweise verfälscht und gezielt veröffentlicht, um die öffentliche Wahrnehmung im eigenen Sinne zu beeinflussen. Dabei wird häufig auf einen strategisch günstigen Zeitpunkt für die Veröffentlichung gewartet, beispielsweise im Vorfeld von Wahlen. Die Veröffentlichung erfolgt in der Regel nicht durch die Manipulierenden selbst, sondern über Dritte (zum Beispiel über Webseiten oder Akteure in sozialen Medien), um eine Zuordnung zu erschweren.
Bei **Hack and Publish** kompromittieren die Angreifer legitime Social-Media-Konten oder Nachrichtenseiten, um darüber anschließend falsche Informationen zu verbreiten. Die auf solche Weise erscheinenden Falschinformationen werden oft parallel über weitere Verbreitungswege wie zum Beispiel Blogs, andere soziale Medien oder E-Mails an Medienunternehmen gestreut.

3.3 Einflussnahme

Verschiedene Staaten versuchen, Politik und Gesellschaft in Deutschland auf eine Art zu beeinflussen, die über eine legitime Verbreitung eines positiven Bildes des eigenen Staates oder die transparente Beziehungspflege zu Politikerinnen und Politikern hinausgeht. In diesen Fällen handelt es sich um eine unzulässige Einflussnahme. Diese zielt darauf ab, im Verborgenen oder unter Vortäuschung falscher Tatsachen, Einfluss auf Entscheidungs- und Funktionstragende anderer Staaten auszuüben, den offenen politischen Willensbildungsprozess – besonders vor Wahlen – zu manipulieren, das Vertrauen der Bevölkerung in die Stabilität und Integrität der Institutionen und Mechanismen der Demokratie zu schwächen oder Werte und Bündnisse demokratischer Staaten zu untergraben. Dazu gehört unter anderem, die Rolle unabhängiger Medien in Frage zu stellen. Diese Form der unzulässigen Beeinflussung kann aber

auch der Unterstützung strategischer und wirtschaftspolitischer Ziele, dem Propagieren der Überlegenheit des eigenen Gesellschaftsmodells oder dem Ausbau einer Machtposition dienen. Dazu setzen fremde Staaten ebenfalls ihre jeweiligen Nachrichtendienste neben anderen Stellen (wie beispielsweise Staatsmedien) ein.

Einflussnahme erfolgt – in Verbindung mit Desinformation – insbesondere im digitalisierten Informationsraum. Seit Beginn des russischen Angriffskriegs gegen die Ukraine im Februar 2022 erfolgt dieses Vorgehen seitens Russlands ausgesprochen aggressiv und hat deshalb nicht nur weitere Aufmerksamkeit erfahren, sondern auch Gegenmaßnahmen zur Folge. Für solche Angriffe auf die Demokratie können fremde Staaten durch Cyberangriffe gestohlene Daten für Propagandakampagnen und die Desinformation der Öffentlichkeit nutzen. Über die Staatsmedien hinaus spielen im virtuellen Raum aber auch Influencerinnen und Influencer eine wichtige Rolle. In der Welt von Politik und Wirtschaft pflegen ausländische Nachrichtendienste zudem verdeckte Beziehungen zu einflussreichen Personen, um so Themen im Sinne ihres Herkunftslandes zu platzieren. Dazu können auch Begünstigungen wie Geld, Auslandsreisen oder exklusive Kontakte beitragen.



Hybride Bedrohungen sind gekennzeichnet durch die Anwendung konventioneller und nicht konventioneller Mittel im gesamten zivil-militärischen Spektrum zwischen Diplomatie und Krieg unter (meist) gezielter Verschleierung der eigenen Urheberschaft. Ziel ist es, das gesamtgesellschaftliche und politische Gefüge nachhaltig zu stören oder zu beeinflussen und damit eigene aggressive und offensive Zielsetzungen zu verfolgen. Dazu gehört es auch, demokratische Prozesse nachhaltig zu delegitimieren.
Bezogen auf Deutschland fallen unter diese Kategorie Desinformation, Cyberangriffe oder die Ausübung von Druck (beispielsweise bei der künstlichen Verknappung von Energieressourcen bezogen auf Gas im Jahr 2022). Hybride Einflussakteure greifen aktuelle gesellschaftliche Themen auf, deuten diese in ihrem Sinne um und verbreiten ihre Narrative. Daneben können Sabotagehandlungen, die beabsichtigte Steuerung von Migrationsströmen oder die Unterstützung von Organisierter Kriminalität Bestandteile hybriden Handelns sein.

3.4 Sabotage

Sabotage bezeichnet Angriffe unter anderem auf Einrichtungen, die lebenswichtig für das Funktionieren eines Staates oder den Schutz seiner Bevölkerung sind. Dazu gehören militärische Einrichtungen oder KRITIS wie etwa Hafenanlagen, Kraftwerke, Erdgaspipelines oder Datenkabel. Attacken können sowohl digital durch Cyberangriffe als auch klassisch durch Brand- oder Sprengstoffanschläge, beispielsweise durch sogenannte →*Innentäter*, erfolgen. Dabei geht den Angriffen durch eine fremde Macht eine nachrichtendienstliche Ausforschung voraus.

3.5 Staatsterrorismus

Zum Handlungsfeld einiger Nachrichtendienste gehört auch Staatsterrorismus. Er umfasst Schwerverbrechen, um einzelne Menschen zu schädigen, die Öffentlichkeit oder eine gesellschaftliche Gruppe in Schrecken zu versetzen oder eine Regierung zu einem bestimmten Handeln zu zwingen. Zum Staatsterrorismus gehören Entführungen oder (Sprengstoff-)Anschläge sowie die vorbereitenden Ausspähungen. Die Täterschaft für derartige Verbrechen kann wegen der sie begleitenden professionellen Tarnung häufig nicht lückenlos mit öffentlich präsentierbaren Beweisen belegt werden. Jedoch kann bei Terrorakten, bei denen der Nutzen für einen Staat ersichtlich und deren Tatausführung äußerst aufwändig ist, ein nachrichtendienstlicher Hintergrund angenommen werden.

2019 ermordete ein russischer Staatsbürger einen in Berlin lebenden Asylbewerber, der für die Unabhängigkeit Tschetscheniens von Russland gekämpft hatte. In seinem Urteil stufte das Berliner Kammergericht 2021 die Tat als Staatsterrorismus ein.

Ein weiterer Fall von Staatsterrorismus betrifft einen Gegner der iranischen Diktatur, der durch das iranische Justizsystem 2023 zum Tode verurteilt wurde. Der in Iran geborene deutsche Staatsbürger arbeitete aus dem Ausland gegen das iranische Regime und war zuvor während einer Reise aus Dubai entführt und in Iran inhaftiert worden.

3.6 Proliferation

Proliferation ist die Verbreitung von chemischen, biologischen, radiologischen und nuklearen Massenvernichtungswaffen (CBRN-Waffen), entsprechenden Trägersystemen (beispielsweise Raketen) sowie von Gütern und Know-how zu deren Herstellung. Zur Fabrikation solcher Waffen können auch handelsübliche Maschinen, Messgeräte und Materialien dienen, die im zivilen Bereich an zahlreichen Stellen eingesetzt werden. Sie werden deshalb auch Dual-Use-Güter genannt und unterliegen in Deutschland besonderen Kontroll- und Ausfuhrregelungen. Auch deren Weiterverbreitung fällt unter den Begriff der Proliferation.

Mehrere Staaten wie Iran, Nordkorea oder Pakistan streben die Herstellung beziehungsweise Weiterentwicklung von CBRN-Waffen an, werden aber durch bestehende Beschränkungen und Sanktionen daran gehindert. Um diese zu umgehen, setzen sie Forschungsinstitute, Unternehmen und ihre Nachrichtendienste ein. Die Beschaffung von Dual-Use-Gütern erfolgt dabei häufig über Drittländer durch sogenannte Umgehungsausfuhren unter Einsatz von Tarnfirmen oder mit falschen Angaben hinsichtlich des Verwendungszwecks. Der Finanztransfer läuft bei derartigen Geschäften über breit gefächerte Firmen- und Bankennetzwerke,

um so die Herkunft des Käufers zu verschleiern.[18]

Auch der Bereich der Emerging Technologies (EMT) ist proliferationsrelevant. Bei EMT handelt es sich um neueste Technologiefelder wie Quantentechnologie, künstliche Intelligenz (KI) und Biotechnologie, die einen zukünftigen militärischen Nutzwert versprechen, zu denen aber aufgrund ihres innovativen Charakters noch kein abschließendes Regelwerk existiert. Ausländische Nachrichtendienste können dabei Kooperationen von Forschungseinrichtungen ihres Staates mit deutschen Hochschulen oder Forschungsinstituten für einen Wissenstransfer missbrauchen. Dies schließt den Einsatz eigener Doktoranden und sonstiger Gastwissenschaftler im Rahmen des international üblichen wissenschaftlichen Austausches ausdrücklich mit ein.

Im Bereich der EMT arbeitet vor allem China mit Hochdruck an seinem „Sprung an die Spitze" – unter vielfältiger Nutzung des deutschen Marktes und der deutschen Wissenschaftslandschaft.

18 Dazu wird auch das außerhalb der regulierten Finanzwirtschaft existierende Hawala-Finanzsystem genutzt. Es ist ein Überweisungssystem, das seine Wurzeln im frühmittelalterlichen Handelswesen des Nahen und Mittleren Ostens hat und international die anonyme Überweisung von Bargeld ermöglicht.

Kapitel 4

Abwehrarbeit des Verfassungsschutzes

Weltweit verteidigen sich Staaten gegen die Aktivitäten fremder Nachrichtendienste durch den Einsatz abwehrender Dienste. In Deutschland erfolgt dies durch den Verfassungsschutz, in erster Linie über das BfV. Es arbeitet als nationale Zentralstelle eng mit den in den einzelnen Bundesländern bestehenden Landesbehörden für Verfassungsschutz (LfV) zusammen. Dieser Verfassungsschutzverbund klärt dabei nicht nur die Bemühungen der genannten Nachrichtendienste aus Russland, China, Iran und der Türkei auf, sondern im Rahmen eines Rundumblicks („360°-Bearbeitung“) auch die Tätigkeiten anderer fremder Nachrichtendienste. Die Ergebnisse leitet das BfV der Bundesregierung zu, die diese als Grundlage für ihre politische Entscheidungsfindung nutzt.

In Abhängigkeit von der Entwicklung eines Falles kooperiert das BfV auch mit den anderen deutschen Nachrichtendiensten Bundesamt für den Militärischen Abschirmdienst (BAMAD) und BND und arbeitet eng mit weiteren Bundesbehörden wie dem Bundeskriminalamt (BKA) und der Bundespolizei (BPol) zusammen. Der Generalbundesanwalt (GBA) nimmt die Funktion als Staatsanwaltschaft des Bundes ein und betreut Verfahren, die Staatsschutzdelikte sowie Straftaten nach dem Völkerstrafgesetzbuch berühren. In Zusammenarbeit mit weiteren Sicherheitsbehörden wie dem Zollkriminalamt (ZKA) und dem Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) leisten das BfV und die LfV außerdem Proliferationsabwehr.

Zusammenarbeit ist eine unerlässliche Grundlage für eine erfolgreiche Abwehrarbeit gegen die Aktivitäten ausländischer Nachrichtendienste. Deswegen arbeitet die →*Cyber-* und →*Spionageabwehr* des BfV nicht nur mit deutschen (Sicherheits-)Behörden zusammen, sondern kooperiert auch mit Nachrichtendiensten anderer Staaten. Darüber hinaus tauscht sich die **Cyber- und Spionageabwehr** auch mit nicht staatlichen Stellen wie etwa Unternehmen, Hochschulen oder Forschungseinrichtungen aus.
In Deutschland sind alle Nachrichtendienste mit Cyber- und Spionageabwehr beschäftigt. Grundsätzlich ist dafür das **BfV** zuständig. Daneben unterhalten auch die meisten **LfV** eine eigene Cyber- und Spionageabwehr. Das BfV und die LfV arbeiten dabei eng zusammen. Dem **BAMAD** obliegt die Sicherheit des Geschäftsbereichs des Bundesministeriums der Verteidigung, inklusive der Bundeswehr. Der **BND** sammelt bedeutende außen- und sicherheitspolitische Informationen über das Ausland und unterrichtet die Bundesregierung. Wegen seiner Tätigkeit ist der BND Ziel von Gegenspionage und betreibt daher im Rahmen der Eigensicherung deren Abwehr.

4.1 Spionageabwehr

Die Spionageabwehr hat das Ziel, Ausspähversuche fremder Nachrichtendienste bereits in einem frühen Stadium zu erkennen, zu analysieren und schließlich zu unterbinden. Dabei will sie unter anderem aufklären, wo nachrichtendienstliche Strukturen bestehen, welche Personen daran beteiligt sind, für welche Bereiche sich fremde Nachrichtendienste interessieren und welche Methoden diese anwenden. Anhaltspunkte dafür bieten die Beobachtung der Legalresidenturen an den diplomatischen Vertretungen, aber auch die Bearbeitung der Reisewege bereits erkannter Mitarbeiter fremder Nachrichtendienste. Darüber hinaus nutzt die Spionageabwehr weitere Wege der Erkenntnisgewinnung. Eine besondere Herausforderung ergibt sich dabei aus dem Umstand, dass ausländische Nachrichtendienste häufig aus ihren Herkunftsländern heraus agieren und die Reisefreiheit innerhalb der EU ausnutzen. Auch deshalb hat die Zusammenarbeit mit nationalen und internationalen Partnern, insbesondere den Nachrichtendiensten der EU-Mitgliedsstaaten, eine große Bedeutung.

Die Beobachtung und Analyse der Ausforschungstätigkeit fremder Nachrichtendienste lassen Rückschlüsse auf deren Aufgabenprofil und somit auf die Absichten ihrer Regierungen zu. Dies dient im Rahmen der Spionageabwehr auch zur Früherkennung von Einflussnahme auf die deutsche Gesellschaft durch Propaganda und Desinformation. Eine daraufhin erfolgende Unterrichtung von Politik und Öffentlichkeit kann die Wirkung der Einflussaktivitäten auf die politische Meinungs- und Willensbildung eingrenzen.

Bei der Bekämpfung von Sabotage und Staatsterrorismus kann die anhaltende Beobachtung ausländischer Nachrichtendienste Hinweise auf Vorbereitungshandlungen erbringen. Dies ermöglicht es dem Verfassungsschutz, gefährdete Personen sowie die für Gefahrenabwehr zuständigen Stellen zu unterrichten. Sofern entsprechende Straftaten erfolgen, tragen die zuvor erarbeiteten Erkenntnisse über Strukturen, Personen, Ziele und Methoden verdächtigter Dienste zur Tataufklärung durch Polizei und Justiz bei.

Auf Grundlage der dabei gewonnenen Erkenntnisse sowie anderer Hinweise bewertet das BfV die aktuelle Bedrohungslage, beteiligt sich am Gemeinsamen Extremismus- und Terrorismusabwehrzentrum (GETZ) und informiert unter anderem die Regierung sowie die Öffentlichkeit. Sofern sich die Erkenntnisse der Spionageabwehr derart verdichten, dass sie auf Straftaten hindeuten, kann das BfV den GBA in Kenntnis setzen, damit dieser den Sachverhalt als Ermittlungsbehörde juristisch prüft. Der GBA eröffnet dann gegebenenfalls ein Ermittlungsverfahren, bei dem zur polizeilichen Aufklärung das BKA oder die in den einzelnen Bundesländern bestehenden Landeskriminalämter (LKÄ) einbezogen werden.

Das **GETZ** ist eine Kooperations- und Kommunikationsplattform für Polizei und Nachrichtendienste auf Bundes- und Länderebene zur Bekämpfung von Rechts- und Linksextremismus/-terrorismus, sowie auslandsbezogenem Extremismus und zur Spionageabwehr. Es handelt sich um keine eigenständige Behörde, sondern das GETZ bündelt die Fachkompetenzen aller beteiligten Behörden für einen möglichst lückenlosen und schnellen Informationsfluss.

4.2 Cyberabwehr

Die Cyberabwehr umfasst alle Maßnahmen zur Wahrung oder Erhöhung der Cybersicherheit. Sie richtet sich gegen alle ausländischen staatlich gesteuerten Cyberangriffe auf deutsche Ziele, identifiziert Angreifer, klärt deren Vorgehensweisen auf und warnt gefährdete Stellen. Auch in diesem Bereich kooperiert die Cyber- und Spionageabwehr des BfV eng mit den LfV und anderen Stellen wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie internationalen Partnern. Zudem engagiert sich das BfV im Nationalen Cyber-Abwehrzentrum (Cyber-AZ), einer Kooperations-, Kommunikations- und Koordinierungs-Plattform aller relevanten deutschen Behörden für Cybersicherheit.

Die Cyberabwehr des BfV hat drei Kernaufgaben:

- staatlich gesteuerte Cyberangriffe erkennen (**Detektion**),
- erkannte Cyberangriffe analysieren und zuordnen (**Attribution**) sowie
- weitere staatlich gesteuerte Cyberangriffe verhindern (**Prävention**).

Die Ergebnisse der Attribution von Cyberangriffen sind dabei wichtige Bestandteile für mögliche Strafverfahren gegen Täter und Grundlage für mögliche politische Reaktionen der Bundesregierung gegen verantwortliche Stellen. Die von der Cyberabwehr gewonnenen Erkenntnisse dienen darüber hinaus der Prävention zukünftiger Angriffe, indem das BfV beispielsweise gefährdete Bereiche informiert. Mit den Informationen über mögliche Angriffe können diese das Ausmaß ihrer Gefährdung erkennen und eigenverantwortlich entsprechende Schutzmaßnahmen einleiten. In diesem Sinne veröffentlicht das BfV anlassbezogene Warnhinweise wie den „BfV Cyber-Brief", führt Sensibilisierungsgespräche mit betroffenen Stellen durch und beteiligt sich an Informationsveranstaltungen.

Bundesamt für Verfassungsschutz

Köln, 31. August 2023

BfV Cyber-Brief
Nr. 02/2023

Gruppierungen APT 15 und APT 31 nutzen Heimnetzwerkgeräte für staatlich gesteuerte Cyberangriffskampagnen

4.3 Proliferationsabwehr

Die Proliferationsbekämpfung besitzt eine besonders große Bedeutung für die internationale Sicherheit, da sie sich gegen die illegale Weiterverbreitung von CBRN-Waffen und dazugehörigem technologischem Wissen richtet. So ist von einigen Staaten zu befürchten, dass sie zur Durchsetzung politischer Ziele mit dem Einsatz von Massenvernichtungswaffen drohen oder diese sogar in einem bewaffneten Konflikt einsetzen würden. Sol-

che Staaten bemühen sich um die Beschaffung dafür benötigter Güter unter Umgehung der strengen deutschen und europäischen Exportkontrollbestimmungen.

Der Verfassungsschutzverbund klärt derartige Versuche auf und trägt dadurch zu ihrer Verhinderung bei. Dabei ist für die Proliferationsabwehr der Austausch und die Zusammenarbeit mit anderen nationalen Behörden wie dem ZKA und dem BAFA sowie mit internationalen Partnern unverzichtbar. Sofern durch die Aufklärungsarbeit kriminelle Aktivitäten bewiesen werden können, übermittelt das BfV die Erkenntnisse an die Strafverfolgungsbehörden. Zudem sensibilisiert die Proliferationsabwehr Unternehmen sowie Bildungs- und Forschungseinrichtungen.

4.4 Prävention in Wirtschaft, Wissenschaft, Politik und Verwaltung

Die öffentliche Präventionsarbeit des BfV informiert Wirtschaft und Wissenschaft sowie Politik und Verwaltung über Gefahren, die von Spionage und Cyberangriffen wie auch von Extremismus und Terrorismus ausgehen. Der Fokus liegt auf Herausforderungen für strategisch bedeutsame Wirtschafts- und Technologiebereiche wie beispielsweise Chiphersteller, die Sicherheits- und Verteidigungswirtschaft sowie die Energiebranche.

Dazu veröffentlicht das BfV auf seiner Webseite beziehungsweise in gedruckter Form unterschiedliche Publikationen. Die „Informationsblätter zum Wirtschaftsschutz“ stellen überblicksartig Themen mit allgemeiner Bedeutung vor. Die Formate „Sicherheitshinweis für die Wirtschaft“ und „Sicherheitshinweis für Politik & Verwaltung“ weisen zielgruppenorientiert bestimmte Branchen und Einrichtungen auf aktuelle Bedrohungen hin. Mit der Heftreihe „SPOC“ informiert das BfV in Form eines zeitgemäßen Magazins Wirtschaft und Wissenschaft, aber auch die breite Öffentlichkeit über aktuelle Entwicklungen in der Sicherheitslandschaft.

Im Internet stellt das BfV der Öffentlichkeit auch über seinen Kanal im sozialen Netzwerk X (vormals Twitter) Informationen zur Verfügung.

Zudem engagiert sich das BfV in der „Initiative Wirtschaftsschutz“[19], in der dessen Erkenntnisse sowie die Expertise der Sicherheitsbehörden BKA, BSI und BND mit dem Wissen mehrerer Wirtschaftsvereinigungen verbunden werden. Dieser Austausch stärkt die Widerstandsfähigkeit des Wirtschafts- und Wissenschaftsstandorts Deutschland. Das BfV trägt darüber hinaus durch eine internationale, insbesondere europäische Vernetzung der Präventionsarbeit zu einem höheren Sicherheitsniveau bei.

19 www.wirtschaftsschutz.info.

Kapitel 5

Ausblick

Nationalstaaten werden auch in Zukunft ihre Interessen mit dem Einsatz eigener Nachrichtendienste verfolgen. Internationale Konfliktlagen, militärische Konfrontationen, wirtschaftliche Verwerfungen und wissenschaftliche Innovationen fördern diese Bereitschaft. Deshalb werden fremde Nachrichtendienste auch zukünftig ihre Bemühungen fortsetzen, in Deutschland zu spionieren, Cyberangriffe durchzuführen oder Einflussnahmeaktivitäten auszuüben, Sabotage oder Staatsterrorismus zu betreiben sowie sensitive Produkte und Technologien illegal zu beschaffen. Darüber hinaus können grundlegende Entwicklungen im Bereich der EMT wie Quantentechnologie, KI, Hyperschalltechnik, Überwachungstechnologien oder Biotechnologie nicht nur das wirtschaftliche, politische und gesellschaftliche Umfeld wesentlich verändern, sondern sie besitzen auch ein militärisches Potenzial. Sie werden deshalb künftig eine

erhebliche Bedeutung für die Sicherheit Deutschlands haben.

Die sich verändernden geopolitischen Gegebenheiten sowie die stetige Weiterentwicklung im Bereich neuer Technologien stellen die Cyber- und Spionageabwehr des BfV fortlaufend vor neue Herausforderungen. Diese wird auch weiterhin Strukturerkenntnisse zu fremden Nachrichtendiensten erarbeiten, deren Mitarbeitende und ihre Aufträge enttarnen sowie versuchen, Kontaktpersonen und Quellen aufzudecken. Nur so können illegale nachrichtendienstliche Tätigkeiten dauerhaft kontrolliert und unterbunden werden.

Das BfV beobachtet permanent neue Entwicklungen und weist Politik und Verwaltung sowie Wirtschaft und Wissenschaft auf damit verbundene Risiken hin. Es trägt auf diese Weise zur Abwehr möglicher Gefahren bei. Im Verbund mit nationalen und internationalen Partnern leistet es mit seiner Cyber-, Spionage- und Proliferationsabwehr so einen wichtigen Beitrag zum Schutz unserer Demokratie.

Glossar

→ ***Advanced Persistent Threat (APT)***

„Advanced Persistent Threat“ (auf Deutsch: fortgeschrittene andauernde Bedrohung) bezeichnet einen komplexen, zielgerichteten und effektiven Angriff auf IT-Strukturen durch einen gut ausgebildeten und ressourcenstarken Angreifer.

→ ***Seite 21***

→ ***Cyberabwehr***

Der Begriff umfasst alle Maßnahmen mit dem Ziel der Wahrung oder Erhöhung der Cybersicherheit. Die Cyberabwehr des Verfassungsschutzes ist zuständig für alle staatlich gesteuerten →*Cyberangriffe* gegen deutsche Ziele. Sie hat die Aufgabe, solche Attacken zu erkennen, sie einem staatlichen Akteur zuzuordnen sowie gefährdete Stellen zu sensibilisieren.

→ ***Seite 29***

→ ***Cyberangriff***

Ein Cyberangriff ist eine gezielte Attacke auf Computer oder Computernetzwerke. Beispiele für Auswirkungen von erfolgreichen Cyberangriffen sind die Störung von Betriebsabläufen, der Abfluss von Informationen, die Verweigerung von Zugängen sowie die Manipulation, Beschädigung oder Zerstörung von Hardware, Daten, Netzwerken oder technischen Systemen.

→ ***Seite 8***

→ ***Desinformation***

Desinformation ist die Verbreitung falscher oder irreführender Informationen, um Einzelpersonen, Gruppen oder die öffentliche Meinung als Ganzes zu beeinflussen. Eine Desinformation liegt vor, wenn sie nach objektiven Maßstäben inhaltlich unzutreffend ist, der Urheber dies weiß und sie dennoch mit dem Ziel der Beeinflussung verwendet. Gleiches gilt für das Verschweigen wesentlicher Teile einer Information. Desinformationsaktivitäten sollen Emotionen, Wahrnehmungen und Einstellungen verändern.

→ ***Seite 9***

→ ***Einflussnahme***

Staaten verfolgen ihre Interessen über eine Vielzahl zulässiger, meist diplomatischer Aktivitäten. Darüber hinaus gibt es aber auch unzulässige Einflussnahmeaktivitäten. Diese erfolgen eher im Verborgenen, unter Vortäuschung falscher Tatsachen und teilweise unter Einsatz von Nachrichtendiensten. Sie sollen auf Meinungs- und Willensbildungsprozesse sowie Entscheidungs- und Funktionsträger anderer Staaten einwirken, das Vertrauen der Bevölkerung in die Institutionen und die Mechanismen der Demokratie schwächen oder Bündnisse untergraben.

→ ***Seite 8***

→ ***Human Intelligence (HUMINT)***

HUMINT befasst sich mit dem Führen menschlicher Quellen. Personen, die Zugang zu wertvollen Informationen haben, sind für jeden Nachrichtendienst wichtig. Das Führen menschlicher Quellen hat auch in Zeiten der Digitalisierung nicht an Bedeutung verloren und gehört mit zu den anspruchsvollsten Tätigkeiten eines Nachrichtendienstes. HUMINT kann sowohl für die hauptamtlichen Mitarbeitenden als auch die Quellen mit hohen persönlichen Risiken verbunden sein. Daraus erwächst eine

besondere Verantwortung des Nachrichtendienstes für seine menschlichen Quellen.

→ ***Seite 8***

→ ***Innentäter***

Innentäter sind Personen, die aufgrund ihrer Betätigung innerhalb oder in der Nähe von schützenswerten Einrichtungen Informationen stehlen, →*Sabotage* betreiben oder Schutzmaßnahmen stören. Dazu zählen auch Mitarbeitende von Fremdfirmen, die an sicherheitsempfindlichen Stellen in der zu schützenden Einrichtung tätig sind. Motive dafür können im politisch-gesellschaftlichen oder persönlichen Umfeld sowie in krimineller Energie liegen.

→ ***Seite 24***

→ ***Kritische Infrastrukturen (KRITIS)***

KRITIS ist die Abkürzung für Kritische Infrastrukturen. Damit sind Anlagen, Systeme und Organisationen gemeint, die eine wichtige Bedeutung für die Aufrechterhaltung gesellschaftlicher Funktionen haben. Deren Ausfall hätte erhebliche Auswirkungen auf das Gemeinwesen, zum Beispiel in Form von Versorgungsengpässen und Gefährdung der öffentlichen Sicherheit. In Deutschland zählen mehrere Sektoren zu KRITIS, dazu gehören Einrichtungen aus den Bereichen Energieversorgung, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Siedlungsabfallentsorgung, Finanz- und Versicherungswesen, Staat und Verwaltung, Medien und Kultur.

→ ***Seite 9***

→ ***Legalresidenturen***

Legalresidenturen sind Stützpunkte eines ausländischen Nachrichtendienstes, abgetarnt in einer offiziellen Vertretung, zum Beispiel in einer Botschaft, einem Generalkonsulat oder in einer halboffiziellen Vertretung im Gastland (beispielsweise eine Nachrichtenagentur oder staatliche Fluggesellschaft).

→ ***Seite 12***

→ ***Open Source Intelligence (OSINT)***

OSINT ist die Informationsgewinnung aus offenen Quellen. Darunter fallen Presseerzeugnisse, Bücher oder Internetseiten.

→ ***Seite 8***

→ ***Proliferation***
Proliferation ist die Weiterverbreitung von Massenvernichtungswaffen und der dafür benötigten Trägertechnologien, des für deren Herstellung benötigten Wissens sowie der entsprechenden Produktionsmittel. Zudem versuchen einige Staaten, sich militärisch anwendbare EMT zu beschaffen. Massenvernichtungswaffen werden auch CBRN-Waffen genannt (chemische, biologische, radiologische und nukleare Waffen). Der Begriff ersetzt mittlerweile die früher gebräuchliche Bezeichnung ABC-Waffen (atomare, biologische und chemische Waffen). Zum Aufbau entsprechender Forschungs-, Entwicklungs- und Produktionsstätten können auch Maschinen, Messgeräte und Materialien dienen, die im zivilen Bereich an zahlreichen Stellen eingesetzt werden, sogenannte Dual-Use-Güter. Auch ihre Weiterverbreitung fällt unter den Begriff der Proliferation.
→ ***Seite 9***

→ ***Propaganda***
Mit Propaganda wollen Staaten die öffentliche Meinung anderer Staaten beeinflussen, um eine gewünschte Reaktion oder Haltung zu erzeugen. Maßgeblich ist nicht der Wahrheitsgehalt einer Nachricht, sondern die geschickte Auswahl beziehungsweise deren Manipulation.
→ ***Seite 9***

→ ***Sabotage***
Sabotage ist die bewusste Beeinträchtigung von militärischen oder politischen Prozessen oder von Produktionsabläufen. Dazu kann das Beschädigen oder Zerstören wichtiger Anlagen und Einrichtungen beispielsweise im Bereich →*KRITIS* zählen.
→ ***Seite 8***

→ ***Signals Intelligence (SIGINT)***
SIGINT ist die Auswertung von elektromagnetischen Signalen aller Art zur Gewinnung von Informationen. Dabei werden unterschiedliche Signale beziehungsweise Datenströme erfasst und nach bestimmten Inhalten durchsucht.
→ ***Seite 8***

→ ***Spionage***
Spionage ist das Erkunden von politischen Faktoren sowie der wirtschaftlichen, wissenschaftlichen und militärischen Potenziale eines anderen Staates mit verdeckten Mitteln.
→ ***Seite 8***

→ ***Spionageabwehr***

Spionageabwehr ist die Aufklärung und Abwehr von Aktivitäten fremder Nachrichtendienste in oder gegen Deutschland. Dazu gewinnt die Spionageabwehr Erkenntnisse über Strukturen, Aktivitäten, Akteure, Arbeitsmethoden und Zielobjekte dieser Nachrichtendienste.

→ ***Seite 29***

→ ***Staatsterrorismus***

Staatsterrorismus ist der im Auftrag einer fremden Macht – meist durch einen Nachrichtendienst – ausgeübte oder gesteuerte Terrorismus. Maßgebliche staatsterroristische Ziele können die Einflussnahme auf fremde Staaten, die Einschüchterung und Neutralisierung Oppositioneller, aber auch die Bestrafung von „Verrätern" oder Überläufern sein. Bei Staatsterrorismus können schwere Straftaten wie Mord, Totschlag oder Entführungen erfolgen.

→ ***Seite 8***

→ ***Transnationale Repression (TNR)***

Transnationale Repression (TNR) umfasst im Allgemeinen die von einer Reihe von Staaten außerhalb ihrer Landesgrenzen betriebenen Unterdrückungsmaßnahmen. Sie richten sich gegen im Ausland lebende Dissidenten oder sonstige von der Regierung des Heimatlandes als Gegner eingestufte Personen. Gängige Formen der TNR sind, über die Ausspähung von Dissidenten und anderen Regierungsgegnern (→*HUMINT*, →*Cyberangriffe*) hinaus, die Bedrohung und Verfolgung oppositioneller Gruppierungen (Denunziation, Unterwanderung, ostentative Observation, →*Desinformation* oder falsche Anschuldigung). So werden unterschiedliche, bewusst einschüchternde Drohkulissen aufgebaut. Im äußersten Fall kann es zu →*Staatsterrorismus* mit schwersten Gefahren für Leib und Leben kommen (Entführung, Mord). Die ausführenden Länder setzen dabei neben ihren Nachrichtendiensten auch andere staatliche Einrichtungen ein oder missbrauchen dafür mitunter auch internationale Amtshilfen.

→ ***Seite 9***

Impressum

Herausgeber
Bundesamt für Verfassungsschutz
Öffentlichkeitsarbeit
Merianstraße 100
50765 Köln
oeffentlichkeitsarbeit@bfv.bund.de
www.verfassungsschutz.de
Tel.: +49 (0)228 99 792-0
Fax: +49 (0)228 99 10 792-2915

Layout & Produktion
Bundesamt für Verfassungsschutz
Mediengestaltung und Druck
im ServiceCenter I

Stand
Januar 2025 (B-0031)

Diese Broschüre ist Teil der Öffentlichkeitsarbeit des Bundesamtes für Verfassungsschutz. Sie wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt. Sie darf weder von Parteien noch von Wahlwerbenden und Wahlhelfenden während eines Wahlkampfes zum Zwecke der Wahlwerbung verwandt werden.

Bildnachweis

S. 2: Designed by freepik | S. 2: berkahicon – freepik.com | S. 2: Ida Desi Mariana – freepik.com | S. 6: ccvision | S. 7: BeeBright – iStock | S. 12: IMAGO/ITAR-TASS | S. 14: picture alliance / REUTERS | JASON LEE | S. 15: ccvision.com | S. 18: geralt – pixabay | S. 23: picture alliance / ZUMAPRESS.com | Muhammed Ibrahim Ali | S. 25: picture alliance/dpa | Christoph Soeder | S. 26: picture alliance / Newscom | KCNA | S. 28: BfV | S. 35: ccvision | S. 37: patpitchaya auf iStock

Tom (25) und Miriam (27)
Arbeite gemeinsam mit uns
IM AUFTRAG DER DEMOKRATIE!
Bewirb dich und komm in unser Team.
Ob Ausbildung, Studium oder Direkteinstieg –
beim Verfassungsschutz erwarten dich vielfältige Einsatzmöglichkeiten.
Scannen für Jobangebote
Bundesamt für Verfassungsschutz
WERDE VERFASSUNGSSCHÜTZER*IN.
Mehr Informationen unter
verfassungsschutz.de/karriere

www.verfassungsschutz.de