durchführen, sind für den Anstieg der allgemeinen Cyberbedrohungslage in Deutschland verantwortlich. Ziel dieser hacktivistischen Akteure ist dabei bislang eher eine propagandistische Wirkung als tatsächliche nachhaltige Cybersabotage. Das BfV verfolgt Hinweise unter anderem von IT-Sicherheitsdienstleistern, nach denen Verbindungen prorussischer Hacktivisten zum russischen Staat und seinen Diensten bestehen. Zumindest von einer Tolerierung durch diesen ist auszugehen.

Cybercrime

Mutmaßlich russische Cybercrime-Akteure setzen für ihre kriminellen Handlungen vor allem Ransomware[188]-Angriffe gegen deutsche Stellen und Unternehmen ein. Auch wenn eine direkte Verbindung zu staatlichen Stellen Russlands in der Regel nicht klar belegbar ist, existieren Fälle, in denen die Opferauswahl im direkten Zusammenhang mit politischen Zielen Russlands steht. Insoweit ist eine Beeinflussung durch russische Nachrichtendienste wahrscheinlich beziehungsweise zumindest eine Tolerierung durch staatliche Stellen Russlands gegeben.

6. Gefährdungspotenzial

Eine zukünftige Intensivierung der hybriden Bedrohungen (vgl. Kap. I.) aus Russland für Deutschland ist eher wahrscheinlich. Dabei gehen die russischen Dienste opportunistisch vor und werden fortlaufend bewerten, inwiefern eine weitere Eskalation ihrer Aktivitäten für die Zielerreichung zweckdienlich ist. Das beständige gegen Deutschland und Europa gerichtete hybride Agieren birgt zudem die Gefahr einer Verschiebung hinsichtlich der Wahrnehmung, welches russische Verhalten als noch akzeptabel erscheint.

Von den russischen Nachrichtendiensten geht ein sehr hohes Gefährdungspotenzial aus. Seit Beginn des Angriffskriegs Russlands gegen die Ukraine 2022 und der in der Folge erlassenen Sanktionen der westlichen Staaten greift das Handeln staatlicher und nicht staatlicher russischer Stellen vermehrt ineinander, um dem intensiven Informationsbedürfnis der Führung sowie der Wahrnehmung Russlands im Sinne des Kreml Rechnung zu tragen. Dies führt zu einem intensiven Aufklärungsinteresse russischer

[188] Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (englisch: „ransom“) wieder freigeben.

Nachrichtendienste, offensiven Desinformationsaktivitäten sowie einer wachsenden Gefährdung durch Sabotagehandlungen.

Auf die Ausweisung russischer Diplomaten und die damit einhergehende Schwächung nachrichtendienstlicher Kapazitäten reagierten die russischen Nachrichtendienste pragmatisch. Sie bauen ihre Methoden zur Informationsbeschaffung weiter aus. Das umfasst neben den bisherigen Spionage- und Cyberoperationen zur Informationsgewinnung nun auch den niedrigschwelligen Einsatz von Low-Level-Agenten für Spionage oder Sabotage.

Der russische Staat verfolgt einen umfassenden Ansatz: Cyberangriffe ergänzen beziehungsweise bereiten klassische Aufklärungsaktivitäten vor, Spionage und Desinformation greifen ineinander. Eine Trennung zwischen realweltlichen und digitalen Maßnahmen erfolgt nicht. Während die russischen Nachrichtendienste im Inland unerwünschte Organisationen und oppositionelle Meinungen verfolgen, richten sich deren Aktivitäten im Ausland gegen ganz unterschiedliche Stellen.

Trotz umfassender Sanktionsmaßnahmen ist weiterhin mit der Fähigkeit und dem Willen russischer Nachrichtendienste zu komplexen Operationen in Europa zu rechnen. Die Entwicklung des Angriffskriegs gegen die Ukraine und die entsprechend angepassten nachrichtendienstlichen Aktivitäten haben einen Einfluss auf die Gefährdungslage in und für Deutschland. Das schlägt sich insbesondere in der erhöhten Gefährdung in Bezug auf Sabotageaktivitäten und darauf gerichtete Vorbereitungshandlungen nieder. Das Schadensausmaß von Sabotage – von cybergestützt bis hin zu physischen Sabotageakten – kann, je nach weiterem Konfliktverlauf, erheblich variieren. Es umfasst sogar das Risiko einer Gefährdung von Leib und Leben auch in Deutschland. Dabei kann es sich um unmittelbare Angriffe handeln oder mittelbare Kollateralschäden sowie Spill-over-Effekte, beabsichtigte oder unbeabsichtigte Folgen eines Cyberangriffs auf weiteren Ebenen als dem ursprünglich angegriffenen Bereich.

III. Nachrichten- und Sicherheitsdienste der Volksrepublik China

Die Nachrichtendienste Chinas sind mit umfangreichen Befugnissen ausgestattet und dienen maßgeblich dem Machterhalt der Kommunistischen Partei Chinas (KPCh) und der Verwirklichung ihrer politischen Ziele. Dazu gehört ihre Absicht, die Volksrepublik China bis 2049 zu einer Weltmacht – mindestens auf Augenhöhe mit den USA – zu entwickeln und einen globalen Führungsanspruch des Landes durchzusetzen („Chinese Dream"). Neben politischer Spionage sind die Nachrichtendienste am Umbau der Volkswirtschaft zu einer führenden Industrienation beteiligt. So setzen sie zahlreiche wirtschaftspolitische Masterpläne und Strategien zur Erlangung von Markt- und Technologieführerschaft in wesentlichen Sektoren mit um. Gleichzeitig wirken sie im Rahmen der „zivil-militärischen Fusion" aktiv am forcierten Aufbau der Volksbefreiungsarmee zu einer „Weltklasse-Armee" mit. Zudem sind die chinesischen Dienste in illegitime Einflussnahmeaktivitäten involviert, mit denen die KPCh versucht, die Interessen der Staats- und Parteiführung im Ausland in unlauterer Weise durchzusetzen.

1. Zielbereiche und Schwerpunkte der Informationsbeschaffung

Aufklärungsziele

Der Bedarf der Staats- und Parteiführung an Erkenntnissen über supranationale Einrichtungen wie die EU oder internationale Organisationen wie die Vereinten Nationen sowie über die Bündnispolitik des Westens ist angesichts der geopolitischen Ambitionen Chinas hoch. Dafür analysiert China beispielsweise den Umgang westlicher Staaten mit Russland infolge der anhaltenden russischen Aggression gegen die Ukraine oder die deutsche Außenpolitik in anderen Regionen mit zunehmendem Konfliktpotenzial. Ableitungen daraus sind im Hinblick auf die chinesischen Vereinigungsbestrebungen mit Taiwan für die kommunistische Parteiführung von großer Bedeutung. In Deutschland stehen Ziele in Politik und Verwaltung, Wirtschaft, Wissenschaft und Technik sowie Militär im Fokus chinesischer Dienste. Darüber hinaus werden oppositionelle Gruppen und Einzelpersonen überwacht und unter Druck gesetzt. In Politik und Verwaltung werden Informationen zu politischen Positionen Deutschlands mit Bezug

auf China gewonnen. Für die Realisierung seiner ambitionierten Industrie- und Militärpolitik nutzt der chinesische Staat Spionage in Wirtschaft und Wissenschaft, versucht, deutsche Unternehmen der Spitzentechnologie teilweise oder ganz aufzukaufen und wirbt gezielt Wissensträgerinnen und -träger mit relevantem Know-how an und ab. Erkenntnisse zu Struktur, Bewaffnung und Ausbildung der Bundeswehr stehen ebenso im Interesse chinesischer Dienste wie die Beschaffung moderner Waffentechnik aus der deutschen Sicherheits- und Verteidigungsindustrie oder auch militärisch nutzbare Hochtechnologien wie die Quantentechnologie.

2. Methodik der Informationsgewinnung

Aktivitäten aus Legalresidenturen

China verfügt über insgesamt fünf diplomatische Vertretungen in Deutschland – die Botschaft in Berlin mit ihrer Außenstelle in Bonn sowie Generalkonsulate in Düsseldorf (Nordrhein-Westfalen), Frankfurt am Main (Hessen), Hamburg und München (Bayern). Aus den chinesischen Legalresidenturen an diesen diplomatischen Vertretungen erfolgt überwiegend eine offene Informationsbeschaffung, einschließlich eines Monitorings von Medien und sonstigen offenen Publikationen. Daneben sammeln Angehörige der Legalresidenturen Informationen im Rahmen harmlos wirkender Kontaktpflege. Solche Gesprächsabschöpfung zielt auf aktive und ehemalige Verantwortliche aus Politik und Wirtschaft.

Zu den Aufgaben der Legalresidenturen gehören zudem Kontrolle und ideologische Steuerung der chinesischen Auslandsgemeinde in Deutschland. Durch eine enge institutionelle Anbindung chinesischer Unternehmen, Studierendenorganisationen, Landsmannschaften, Vereine und Institute soll linientreues Verhalten sichergestellt und die sogenannte Einheitsfront im Ausland gestärkt werden. Angehörige der Diaspora werden für Maßnahmen gegen chinesische Oppositionelle und zur propagandistischen Unterstützung der Politik der Staats- und Parteiführung instrumentalisiert. Zur Informationsgewinnung greifen die Legalresidenturen auf regimetreue Zuträger aus der Auslandsgemeinde zurück.

Angehörige chinesischer Medien

Die Nachrichtendienste setzen zur Informationsgewinnung auch in Deutschland tätige chinesische Auslandskorrespondentinnen und -korrespondenten zur offenen Gesprächsabschöpfung ein, denn Medienangehörige sind eng an die chinesische Botschaft

angebunden. Zudem nutzt der Staat ihre Kontaktnetzwerke sowie die Reichweite der von ihnen verfassten Beiträge, um in Deutschland KPCh-Narrative für ein positives Bild vom Land zu verbreiten.

Zentrale Steuerung und Anwerbung menschlicher Quellen

Nachrichtendienstliche Operationen zur verdeckten Informationsbeschaffung werden hauptsächlich unmittelbar aus den Büros der Dienste in China gesteuert. Bei Aufenthalten in China werden Zielpersonen aus Deutschland angesprochen und mit der Aussicht auf Entlohnung angeworben. Betroffen sind meist solche deutschen Staatsbürger, die entweder über hochwertige Zugänge verfügen oder eine aus Sicht der chinesischen Nachrichtendienste aussichtsreiche künftige Entwicklung versprechen. Initiiert werden können solche Werbungsmaßnahmen beispielsweise bei Veranstaltungen im akademischen Umfeld. Die in der Folge stattfindenden Treffs werden überwiegend in Drittländern oder in China durchgeführt, um operative Risiken in Deutschland zu reduzieren. Die Steuerung erfolgt meist persönlich, teilweise aber auch über webbasierte verschlüsselte Kommunikation, insbesondere über den chinesischen Messengerdienst WeChat.

Staatlich gesteuerter Know-how- und Technologietransfer nach China

China betreibt seit Jahren ein umfassendes System des Technologie- und Know-how-Transfers, um seine wirtschaftliche und militärische Entwicklung voranzutreiben. Die Staats- und Parteiführung strebt zum 100. Jahrestag der Gründung der Volksrepublik im Jahr 2049 eine globale Technologieführerschaft an. Dieses Ziel wird durch ein strategisches und ganzheitliches Vorgehen konsequent verfolgt, welches von gezielten Unternehmenserwerben über Joint Ventures bis hin zu Talentakquise-Programmen und Forschungskooperationen reicht. Dabei versucht China, seine Beschaffungsnetzwerke beständig weiterzuentwickeln, administrative Beschränkungen und Prüfungen beispielsweise im Visaverfahren flexibel zu umgehen und neue Methoden des Know-how-Transfers zu etablieren. Mit dem Ziel, militärische Überlegenheit in zukunftsrelevanten Technologien zu erlangen, fokussiert China auch die Nutzbarmachung von zivilen Erkenntnissen im Bereich des Militärs. Kernziele dieses Wissenstransfers sind Emerging and disruptive Technologies (EDT) wie Quantentechnologie, künstliche Intelligenz (KI) sowie Hyperschalltechnik wie auch Biotechnologie und Überwachungstechnologie. Es ist davon auszugehen, dass alle relevanten Erkenntnisse, die in der zivilen Forschung erlangt wurden, auch dem chinesischen Militär und dem Rüstungssektor zugänglich gemacht werden.

Forschungskooperationen und Gastwissenschaftler

Die Beschaffung von Technologie und Know-how erfolgt über nachrichtendienstliche Netze wie über verschiedene, überwiegend legale Wege. Zu diesen gehören wissenschaftliche Kooperationen mit deutschen Universitäten und (Spitzen-)Forschungseinrichtungen. Um gezielt rechtliche Grauzonen, ein weiterhin mangelndes Risikobewusstsein sowie die in Deutschland verfassungsrechtlich garantierte Wissenschaftsfreiheit auszunutzen, instrumentalisiert der chinesische Staat vor allem chinesische Gastwissenschaftlerinnen und -wissenschaftler im Sinne seiner Ambitionen. Diese bewegt er mit verschiedenen Mitteln zur Zusammenarbeit, dazu gehören finanzielle Zuwendungen und akademische oder berufliche Aufstiegschancen in China, aber auch vertraglich festgelegte Verbindlichkeiten, beispielsweise über die staatlichen Stipendien des China Scholarship Council (CSC), und nicht zuletzt auch politische oder nachrichtendienstliche Druckmittel.

Um Forschungs- oder Studienaufenthalte von Gastwissenschaftlerinnen und Gastwissenschaftlern in für China technologisch und militärisch relevanten Bereichen zu realisieren, werden auch bestehende deutsche Visabeschränkungen zur Verhinderung des Abflusses von relevantem Wissen gezielt umgangen.

Darüber hinaus liegt das chinesische Augenmerk auf deutschen und anderen nicht chinesischen Wissenschaftlerinnen und Wissenschaftlern, die über langjährig gewachsene Kennverhältnisse abgeschöpft oder mittels finanzieller Anreize zum Wissens- und Technologietransfer zugunsten Chinas bewegt werden.

Ausländische Direktinvestitionen

Im Jahr 2024 blieb Deutschland weiterhin eines der wichtigsten Ziele chinesischer Investitionen, auch wenn die Zahl chinesischer Unternehmensbeteiligungen und -übernahmen in Europa allgemein seit Jahren sinkt. Ausländische Direktinvestitionen, besonders im Industriesektor und im High-Tech-Bereich, ermöglichen es China, auf legalem Weg Zugriff auf Technologien oder geistiges Eigentum zu erlangen. Dadurch kann China Innovationsrückstände ausgleichen und einen technologischen Vorsprung erzielen. Zudem öffnen sie auch das Tor zu politischer Einflussnahme, Spionage und Sabotage. Ein sukzessiver Verkauf deutscher Unternehmen aus zukunftsträchtigen Branchen kann mittel- bis langfristig die Wettbewerbsfähigkeit des Industrie- und Technologiestandorts Deutschland nachhaltig beeinträchtigen. Zudem besteht das Risiko weiter wachsender Abhängigkeiten, welche im Falle

geopolitischer Konfliktlagen von China im eigenen Sinne ausgenutzt werden können.

3. Einflussnahme und Transnationale Repression

Um die Ambitionen der KPCh erfolgreich umsetzen zu können, versucht China, durch (häufig illegitime) Einflussnahmeaktivitäten in Politik, Gesellschaft und Wirtschaft im Ausland ein für sich wohlwollendes Umfeld zu erzeugen. Zudem verbreiten chinesische Stellen Desinformation und Propaganda, um die Politik der KPCh in ein positives Licht zu rücken und die vermeintliche Überlegenheit des chinesischen Ordnungsmodells hervorzuheben.

Vielfältiger Instrumentenkasten

Im politischen Bereich bemüht sich die chinesische Seite, gut vernetzte (aktive und ehemalige) Parlamentarier als „Lobbyisten" für ihre Interessen zu gewinnen. Gleichzeitig werden deutsche Abgeordnete (auch auf Länderebene), die offen die Politik der KPCh kritisieren, teilweise unter Druck gesetzt oder in Einzelfällen mit Sanktionsmaßnahmen belegt.

Im Bereich von Bildung und Forschung drohen Chinas Aktivitäten und Kooperationsformate die akademische Freiheit zu unterminieren. Die chinesischen Konfuzius-Institute dienen innerhalb der Einflussnahmestrategie der KPCh unter anderem dazu, ein makelloses Chinabild zu verbreiten und regimekritische Veranstaltungen oder Forschung an deutschen Hochschulen zu verhindern.

Zudem versuchen staatliche chinesische Akteure, führende Persönlichkeiten aus der deutschen Wirtschaft – unter Ausnutzung bestehender Abhängigkeiten einzelner deutscher Unternehmen vom chinesischen Markt – für die Durchsetzung der Interessen der KPCh zu instrumentalisieren. Bei „unerwünschtem" Verhalten ausländischer Unternehmen und Regierungen setzt die Staats- und Parteiführung zum Zweck der Abschreckung auf öffentlichkeitswirksame Sanktionierung und staatlich gesteuerte Boykotte in China.

TNR

Im Rahmen der Transnationalen Repression (TNR) (vgl. Kap. I) hat China in den vergangenen Jahren eine engmaschige extraterritoriale Infrastruktur aufgebaut, über die chinesische Einheitsfrontorganisationen Informationen sammeln. Hierzu zählen

unter anderem Diaspora-Vereine, Verbindungsstellen sowie eine gleichgeschaltete Diaspora-Presse. So können potenzielle „Abweichler“ identifiziert, in der chinesischstämmigen Gemeinschaft in Deutschland isoliert, eingeschüchtert oder unter Druck gesetzt werden. Seit 2023 gibt es immer wieder Fälle Transnationaler Repression gegen ursprünglich aus China stammende Oppositionelle, diese Entwicklung hat sich 2024 fortgesetzt.

4. Cyberangriffe

Im Jahr 2024 verübten mutmaßlich staatliche oder staatlich gesteuerte chinesische Cyberakteure zahlreiche Angriffe auf Unternehmen, Institutionen, Behörden und Privatpersonen in Deutschland. Cyberangriffe begleiten das Interesse Chinas an einer globalen Spitzenposition in Politik, Wirtschaft, Technologie und Militär.

Weiterentwicklung der Vorgehensweise

Unternehmen im Umfeld von Politik und Verwaltung standen 2024 intensiv im Fokus und wurden als Einfallstor für darauf aufbauende Angriffe genutzt. Die Vorgehensweise der Cyberspionageakteure erfuhr eine deutliche technische Weiterentwicklung, wodurch sie eine bislang kaum dagewesene Reichweite und Effektivität erreichten. Dabei spielen auch chinesische Gesetze sowie das Gesamtgefüge der chinesischen Cybersicherheitspolitik eine wesentliche Rolle.

Angriffe gegen IT-Dienstleister

Technisch äußerst komplexe Cyberangriffe richteten sich vor allem gegen IT-Dienstleister und andere Unternehmen, die mit der Betreuung von Behördennetzwerken betraut sind. Stärker in den Fokus gerieten auch wieder deutsche Unternehmen aus Schlüsselbranchen mit ihren Dienstleistern, beispielsweise im Bereich der Satellitenkommunikation oder aus der Luft- und Raumfahrt. Durch die Ausnutzung nicht öffentlich bekannter Soft- und Hardwareschwachstellen (Zero-Day-Exploits[189]) konnten die Angreifer tief in die Netzwerkinfrastruktur ihrer Ziele vordringen. So gelang es ihnen, sich über längere Zeit unbemerkt privilegierten Zugriff auf weitere interne Systeme zu sichern. Es ist davon auszugehen, dass nicht die Dienstleister selbst im Fokus standen, sondern über

[189] Eine Zero-Day-Schwachstelle ist eine bislang dem Hersteller nicht bekannte Sicherheitslücke, für die kein Sicherheitsupdate existiert. Die Ausnutzung von Zero-Day-Schwachstellen lässt zudem auf Angreifende schließen, denen große technische oder finanzielle Ressourcen zur Verfügung stehen.

deren Infrastruktur ein Vordringen in die Netzwerke von deren Kunden beabsichtigt war (Supply-Chain-Angriffe).

Begünstigt durch das im Juli 2021 in Kraft getretene chinesische „Schwachstellengesetz“[190] setzen chinesische Cyberakteure seit einigen Jahren auf solche Exploit-basierte Cyberangriffe. Sie erhalten durch das Gesetz einfacher und schneller Zugriff auf Schwachstellen – bevor diese geschlossen werden können. Die Ausnutzung solcher Schwachstellen für Cyberspionageoperationen chinesischer Nachrichtendienste ist eine zunehmend bedrohliche Entwicklung.

Einsatz von Verschleierungsnetzwerken

Chinesische Cyberakteure flankierten ihre Aufklärungs- und Angriffshandlungen mit verschiedenen Verschleierungsnetzwerken. Zunehmend komplexere Techniken und ein hoher Ressourceneinsatz belegen die beachtliche Weiterentwicklung von Angriffswerkzeugen und erschweren die Detektion von Angriffen. Zur weitestgehenden Abtarnung der Aktivitäten werden Endgeräte wie beispielsweise Heimrouter oder IoT-Geräte[191] in wachsender Anzahl durch Cyberangreifer infiltriert und in der Folge für Angriffskampagnen gegen Politik, Verwaltung, Wirtschaft und Einzelpersonen missbraucht. Die Kontrollübernahme über solche Geräte, die für den Einsatz in kleineren Unternehmen oder von Privatanwendern konzipiert sind, erfolgt auch durch das Ausnutzen von Zero-Day-Exploits.

Beispielhaft für einen schweren Cyberangriff über ein Verschleierungsnetzwerk steht das 2021 erfolgte Eindringen in das Netzwerk des Bundesamts für Kartographie und Geodäsie. Diesen Cyberangriff ordnete die Bundesregierung am 31. Juli 2024 staatlichen chinesischen Akteuren zu.

APT 15

Die seit mindestens 2010 aktive Cybergruppierung APT 15 verschafft sich seit Jahren in verschiedenen Ländern Zugänge zu sensiblen Einrichtungen und Informationen, unter anderem durch Verschleierungsnetzwerke. Im Fokus von APT 15 stehen

[190] Nach dem „Regulations on the Management of Network Product Security Vulnerabilities“-Gesetz müssen in- und ausländische Unternehmen neu entdeckte Sicherheitslücken in IT-Systemen umgehend der chinesischen Regierung mitteilen.

[191] Das Internet of Things (IoT, Internet der Dinge) ist ein Sammelbegriff für Technologien, die es ermöglichen, physikalische und virtuelle Objekte miteinander zu vernetzen und zusammenarbeiten zu lassen. Als IoT-Geräte können herkömmliche, mit dem Internet verbundene Haushaltsgegenstände bis hin zu professionellen Industriewerkzeugen infrage kommen.

Regierungsinstitutionen in europäischen Staaten; erfolgreich angegriffene Ziele wurden auch in Deutschland bekannt. Darüber hinaus erfolgten 2024 Aufklärungs- und Angriffshandlungen gegen Unternehmen aus der Luft- und Raumfahrtbranche, die sich durch fortwährende technische Weiterentwicklung sowie das intensive Ausnutzen von Zero-Day-Schwachstellen auszeichneten.

i-Soon-Leak

Unbekannte veröffentlichten im Februar 2024 einen Datensatz, der Details zu Kooperationen des chinesischen Cybersecurity-Unternehmens i-Soon (Shanghai Anxun Information Technology Company) mit dem chinesischen Sicherheitsapparat enthüllt. Die im Leak enthaltenen Produkt- und Servicelisten sowie Verträge belegen, dass i-Soon Cyberspionagesoftware an den chinesischen Nachrichtendienst MSS sowie die Volksbefreiungsarmee verkauft. Die Daten zeugen von einem komplexen System einer gleichsam industrialisierten chinesischen Cyberspionage durch privatwirtschaftliche Unternehmen. Im Ergebnis sind erheblich mehr Akteure als nur staatliche Cyberangreifer aktiv. Die Unterlagen geben Einblicke in die Arbeitsweisen privater Hackerfirmen und Schadsoftware-Anbieter und deren Verbindungen zum chinesischen Staat. Von den so bekannt gewordenen Schadprogrammen wurden einige seit geraumer Zeit von chinesischen Akteuren zur Cyberspionage gegen Ziele in Europa genutzt. Dieses Outsourcing staatlicher Cyberspionage erschwert die Rückverfolgung einzelner Kampagnen zu spezifischen Akteuren und eine öffentliche Attribution.

5. Gefährdungspotenzial

Zur dauerhaften Machtsicherung hat die KPCh unter Staats- und Parteichef XI Jinping die Kontrolle über nahezu alle Bereiche des Lebens in China weiter ausgebaut. China ist bestrebt, die internationale Ordnung entlang der Interessen seines Einparteiensystems zu beeinflussen und dabei auch die Grundfesten der regelbasierten Ordnung zu relativieren. Gleichzeitig schottet sich China gegen „schädliche westliche“ Einflüsse ab, um das Land nach dortiger Sichtweise so zur wirtschaftlichen und politischen Führungsnation aufzubauen. Diese Entwicklung geht mit einer umfassenden, langfristigen und systematischen Aufklärung der politischen, militärischen und wirtschaftlichen Interessen und Potenziale ausländischer Akteure, aber auch der Beobachtung und Unterdrückung

regimekritischer Strömungen im Ausland sowie Versuchen einher, Entscheidungsprozesse vielerorts im Sinne der Partei- und Staatsführung zu beeinflussen.

Deutschland ist aufgrund seiner herausragenden politischen, wirtschaftlichen und geopolitischen Rolle eines der bedeutendsten Aufklärungs-, Beschaffungs- und Einflussziele Chinas. Dies manifestiert sich aktuell in einer Zunahme staatlicher Spionage- und Einflussnahmeaktivitäten. Beispielhaft hierfür stehen verschiedene im Jahr 2024 durchgeführte Exekutivmaßnahmen in Deutschland. Im Rahmen mehrerer Ermittlungsverfahren des GBA wurden diverse Personen wegen des Verdachts geheimdienstlicher Agententätigkeit für einen chinesischen Nachrichtendienst verhaftet. In den meisten Fällen waren Vorfeldermittlungen des BfV ursächlich für die Maßnahmen.

Trotz der zur Schau gestellten Selbstgewissheit der chinesischen Regierung sieht sich der Parteistaat unverändert in seiner Sicherheit bedroht. Diese perzipierte Machtgefährdung manifestiert sich unter anderem in dem Versuch, jede Form von politischem Dissens im In- und Ausland im Keim zu ersticken. Dadurch sind die Freiheitsrechte der chinesischen Diaspora weltweit bedroht.

Um zukünftige Bedrohungsszenarien frühzeitig zu erkennen, sind die politischen sowie wirtschaftlichen Entwicklungen und die daraus resultierenden globalen Ambitionen Chinas gesamtheitlich im Blick zu behalten. China handelt bei seiner strategischen Ausrichtung planvoll und langfristig. Ähnlich angelegt ist auch die offensive Cyberstrategie, die durch umfangreichen Wissenstransfer einen wichtigen Beitrag zum Erreichen der Ziele des Landes leisten soll. Cyberspionageangriffe sind für China ein wesentliches Werkzeug zur verdeckten Informationsbeschaffung. Cyberoperationen dürften auch zukünftig hochprofessionell, von staatlichen wie nicht staatlichen Stellen und mit enormem Ressourcenaufwand umgesetzt werden. Das bedroht die digitale Souveränität Deutschlands und Europas, gerade auch angesichts der stetig wachsenden Digitalisierung, die Angreifern großflächige Cyberangriffe erleichtert.

IV. Nachrichtendienste der Islamischen Republik Iran

Die angespannte sicherheitspolitische Lage im Nahen und Mittleren Osten sowie innere Spannungen der Islamischen Republik Iran prägen die nachrichtendienstlichen Aktivitäten der Theokratie. Iran versteht sich als Regionalmacht – mit einer ausgeprägten antiwestlichen sowie antiisraelischen Stoßrichtung.

Vorgehen gegen Oppositionelle und Kritiker

Die Bekämpfung oppositioneller Gruppierungen und Einzelpersonen im In- und Ausland bildet einen Schwerpunkt iranischer nachrichtendienstlicher Aktivitäten. Für die Machthaber Irans gelten solche Gruppierungen als Gefährdung für den Fortbestand ihrer Herrschaft. Besonders deutlich zeigt sich dies in der wiederholten gewaltsamen Unterdrückung von Protesten durch das Regime.

Neben den USA sieht Iran insbesondere den Staat Israel, dessen Repräsentantinnen und Repräsentanten sowie exponierte Unterstützerinnen und Unterstützer als Feinde an. Hierzu zählen auch führende Vertreterinnen und Vertreter jüdischer Organisationen in der Diaspora. Deshalb gehören auch Ausspähungsaktivitäten gegen (pro-)israelische sowie (pro-)jüdische Ziele in Deutschland zum Tätigkeitsfeld der Spionage Irans.

Akteure

Hauptsächlich gehen die gegen Deutschland gerichteten Aktivitäten weiterhin vom Ministry of Intelligence (VAJA[192], zumeist MOIS abgekürzt) aus. In seinem Fokus stehen insbesondere die in Deutschland aktiven iranischen Oppositionsgruppen. Neben dem MOIS ist zudem die ebenfalls geheimdienstlich agierende Quds Force der Iranischen Revolutionsgarden[193] in Deutschland aktiv.

Staatsterrorismus

Nachrichtendienste der Islamischen Republik Iran setzen auch staatsterroristische Mittel zur Durchsetzung ihrer Ziele ein. Dabei handelt es sich maßgeblich um die Einschüchterung und Neutralisierung Oppositioneller, aber auch die Bestrafung von „Verrätern“ oder „Überläufern“. Daneben spielt auch Druck auf Politik und Öffentlichkeit anderer Staaten eine Rolle (vgl. Kap. I). Ausspähungsaktivitäten iranischer Nachrichtendienste dienen häufig der

[192] In Farsi: Vezarat-e Ettela'at-e Jomhouri-ye Eslami-ye Iran – VAJA.
[193] In Farsi: Sepah Pasdaran.

Vorbereitung staatsterroristischer Aktivitäten, darunter Entführung oder sogar Tötung der Zielperson.

Die Feststellungen in der Urteilsbegründung des OLG Düsseldorf (Nordrhein-Westfalen) vom 19. Dezember 2023 gegen einen Angeklagten – er erhielt eine Gesamtfreiheitsstrafe von zwei Jahren und neun Monaten wegen Verabredung einer schweren Brandstiftung und versuchter Brandstiftung – wurden in Politik und Öffentlichkeit in Europa als Beleg für das aggressive Vorgehen der Islamischen Republik Iran gewertet. In der Nacht zum 18. November 2022 hatte der Verurteilte in Bochum (Nordrhein-Westfalen) eine in der Nachbarschaft der dortigen Synagoge befindliche Schule mit einem Brandsatz beschädigt. Das Gericht hatte zum Hintergrund der Tat festgestellt, dass die Anschlagsplanung auf eine „staatliche iranische Stelle" zurückging. Diese Tat beweist, dass die Aktivitäten Irans über die Ausspähung der oppositionellen iranischen Diaspora deutlich hinausgehen und (pro-)jüdische und (pro-)israelische Interessen und Einrichtungen in Deutschland im Fokus iranischer Aktivitäten stehen.

Seit 2019 kam es im Rahmen aufwendiger Operationen der iranischen Nachrichtendienste wiederholt zu Entführungen von hochrangigen Zielpersonen aus dem oppositionellen Spektrum nach Iran. Auch in Deutschland lebende Personen können Opfer solcher Operationen werden, insbesondere bei Reisen in Anrainerstaaten Irans. Im Jahr 2020 wurde ein deutscher Staatsangehöriger, der zudem die iranische Staatsangehörigkeit besaß, bei einer Reise in ein Nachbarland Irans verschleppt.

Anbahnung/ Verhaftung bei Reisen nach Iran

Iranreisende müssen damit rechnen, im Land willkürlich verhaftet und angeklagt zu werden. Die iranischen Dienste nutzten auch 2024 offenbar bevorzugt nachrichtendienstliche Ansprachen mit dem Ziel einer Verpflichtung zur Zusammenarbeit. Dies gilt insbesondere für Personen, die iranische Stellen mit einer oppositionellen Gruppierung in Verbindung bringen oder bei denen sie Kontakte zu Personen aus der oppositionellen Szene vermuten. Betroffenen drohen mehrtägige Befragungen durch iranische Nachrichtendienste, bei denen erheblicher Druck auf sie ausgeübt wird. Zudem können dabei Mobilfunkgeräte und Informations- und Kommunikationshardware ausgelesen oder manipuliert werden. Ziel solcher oft unter Vorwand eingefädelter Verhöre ist es, Personen zu zwingen, oppositionelle Aktivitäten aufzugeben oder

sie nachrichtendienstlich zu verpflichten. Diesem Druck können sich Betroffene kaum entziehen.

Gefährdung von Doppelstaatern

Besonders gefährdet sind Personen mit deutscher und iranischer Staatsangehörigkeit. Das Regime behandelt diese grundsätzlich als iranische Staatsangehörige, da es Doppelstaatsangehörigkeiten rechtlich nicht anerkennt. Gleichzeitig nutzt Iran die zweite Staatsbürgerschaft zur Ausübung politischen Drucks. Es ist davon auszugehen, dass Iran auch weiterhin gezielt westliche Staatsangehörige unter konstruierten Vorwänden festnimmt und als Druckmittel in einer Art „Geiselpolitik" einsetzt. Dies dient der Durchsetzung seiner politischen Ziele, um beispielsweise den Austausch gegen im Ausland inhaftierte Personen zu erreichen.

Schließung von Generalkonsulaten

Im Dezember 2024 wurden auf Veranlassung der Bundesregierung – als Reaktion auf den Tod eines inhaftierten, zuvor entführten und nach einem Schauprozess zum Tode verurteilten deutsch-iranischen Staatsangehörigen in Iran – die drei iranischen Generalkonsulate in Frankfurt am Main (Hessen), München (Bayern) und Hamburg geschlossen. Ein Teil des diplomatischen Personals musste Deutschland verlassen. Iran verfügt somit nur noch über die Botschaft in Berlin als diplomatische Vertretung.

Cyberangriffe

Staatlich gesteuerte iranische Cyberakteure nutzen seit mindestens 2013 Cyberangriffe zur Informationsgewinnung; sie entwickeln ihre Fähigkeiten stetig weiter. In Deutschland fokussierten sich iranische Cyberspionageaktivitäten 2024 vorwiegend auf die hier beheimatete iranische Diaspora. Im Zielspektrum der Angriffskampagnen der APT-Gruppierung Charming Kitten standen Exiliraner, Oppositionelle, Regimekritiker, Journalisten und Einzelpersonen aus der Menschenrechtsbewegung sowie Frauenrechtsaktivistinnen, die sich öffentlich kritisch über Menschenrechtsverstöße in Iran geäußert hatten. Sie erfolgen vorwiegend mittels Spear-Phishing-Angriffen[194] und zeichnen sich durch ein aufwendiges Social Engineering[195] aus, das mit großer Ausdauer bis zur erfolgreichen Infektion der Kommunikationssysteme der

[194] Spear-Phishing-Angriffe werden besonders bei APTs verwendet. Dabei wird die Phishing-Mail für einen kleinen Empfängerkreis oder sogar nur für eine Einzelperson maßgeschneidert.

[195] Social Engineering ist eine manipulative Methode mit dem Ziel, Menschen zu einem bestimmten (sicherheitskritischen) Verhalten zu verleiten. Sie wird als Vorbereitung von weiterführenden Aktivitäten eingesetzt, wie z.B. Cyberangriffen oder Anwerbungsversuchen ausländischer Nachrichtendienste.

Angegriffenen durchgeführt wird. Dabei setzen iranische Cyberakteure neben frei verfügbarer auch zielgerichtet angepasste Schadsoftware ein.

Gefährdungspotenzial

Das in den letzten Jahren angestiegene Gefährdungspotenzial blieb auch 2024 hoch. Exponierte Einzelpersonen und Gruppierungen unterliegen grundsätzlich einer höheren Gefährdung. Es ist davon auszugehen, dass die Nachrichtendienste Interessen der Führung des Landes weiterhin mit allen Mitteln – auch durch Gewalttaten und sogar Tötungen – verfolgen werden.

Iranische Nachrichtendienste haben in Deutschland das vorrangige Ziel, die iranische Opposition in der Diaspora auszuforschen. Zudem bleiben aber auch (pro-)israelische beziehungsweise (pro-) jüdische Ziele in ihrem Zielspektrum. Im Bereich von Cyberangriffsoperationen werden iranische Akteure ihre Fähigkeiten weiter professionalisieren. Wegen der umfassenden Sanktionen und des wirtschaftlichen wie technologischen Mangels wird Iran zudem versuchen, Know-how, Informationen und Produkte mithilfe von Cyberspionage zu beschaffen.

V. Nachrichtendienste der Republik Türkei

Die türkischen Nachrichtendienste decken ein breites Aufklärungsportfolio ab, wobei ihr Arbeitsschwerpunkt in Deutschland die Oppositionellenausspähung (Transnationale Repression, TNR, vgl. Kap. I) ist. Vorrangiges Aufklärungsziel sind Organisationen, die die Türkei als extremistisch oder terroristisch einstuft, wie die „Arbeiterpartei Kurdistans“ (PKK), die auch in der EU und den USA als Terrororganisation gelistet ist, und die Bewegung des am 20. Oktober 2024 im US-Exil verstorbenen islamischen Predigers Fethullah Gülen (sog. Gülen-Bewegung oder „Hizmet“, in der Türkei auch „FETÖ“). Nachrichtendienstliches Aufklärungsinteresse besteht auch gegenüber Gruppen und Einzelpersonen, die in Opposition zur türkischen Regierung stehen und als „Staatsfeinde“ angesehen werden.

Methodik

In Deutschland bestehen für türkische Nachrichtendienste wegen der großen türkeistämmigen Gemeinde und der hohen Zahl türkischer Organisationen und Institutionen sowie der diplomatischen

Vertretungen im Bundesgebiet viele günstige Gelegenheiten zur verdeckten Informationsbeschaffung. Die Dienste beziehen ihre Informationen unter anderem von angeworbenen menschlichen Quellen oder anderen Personen, die eigeninitiativ Hinweise geben. In die Sammlung, Auswertung und Weiterleitung von Informationen – darunter auch an Strafverfolgungsbehörden in der Türkei – sind türkische Auslandsvertretungen in Deutschland eingebunden. Zahlreiche Festnahmen und Inhaftierungen sowie Aus- und Einreisesperren für Türkeireisende aus Deutschland dokumentieren das hohe Strafverfolgungs- und Handlungsinteresse türkischer staatlicher Stellen.

Staatliche Einflussnahme

Zusätzlich erfolgen Einflussnahmeaktivitäten von türkischen Organisationen auf türkeistämmige Gemeinschaften in Deutschland, die Auswirkungen auf den politischen Willensbildungsprozess oder Entscheidungsfindungen in Deutschland haben können.

Der größte staats- beziehungsweise regierungsnahe Interessenverband für Einflussnahme ist die 2004 gegründete Union Internationaler Demokraten (UID) mit Sitz in Köln (Nordrhein-Westfalen). Sie verfügt in Deutschland über ein erhebliches Mobilisierungspotenzial, welches auch bei den türkischen Parlaments- und Präsidentschaftswahlen im Mai 2023 zum Tragen kam. Ihre Verbindungen zur Türkei stellt die UID durch regelmäßige Treffen mit AKP-Funktionären und türkischen Regierungsmitgliedern zur Schau.

Im Umfeld dieser eng an Ankara angebundenen Personenzusammenschlüsse gründeten sich in der Vergangenheit immer wieder Parteien und Wählervereinigungen, um insbesondere Stimmen der türkisch-muslimischen Gemeinschaft in Deutschland zu gewinnen.

Gefährdungspotenzial

Die türkischen Nachrichtendienste setzen ihre Aktivitäten auf hohem Niveau fort, wobei Oppositionelle und Dissidenten für sie weiterhin eines der vorrangigen Aufklärungsziele in Deutschland bleiben. Ebenso ist zu erwarten, dass die Einflussnahmeaktivitäten türkischer staats- oder regierungsnaher Organisationen fortgeführt werden.

VI. Nachrichtendienste sonstiger Staaten

Im Sinne einer „360°-Bearbeitung“ richten sich die Aufklärungs- und Abwehraktivitäten der Cyber- und Spionageabwehr gegen illegale nachrichtendienstliche Aktivitäten jeglicher Staaten, die für ihre Zwecke menschliche Quellen, Cyberangriffe und andere technische Aufklärungsmittel nutzen. Spionageaktivitäten ausländischer Nachrichtendienste in oder gegen Deutschland werden in keinem Fall toleriert.

Nachrichtendienste Nordafrikas und des Nahen und Mittleren Ostens

Einen Schwerpunkt der „360°-Bearbeitung“ stellen die nachrichtendienstlichen Aktivitäten der Staaten Nordafrikas und des Nahen und Mittleren Ostens in Deutschland dar, darunter insbesondere von Syrien, Ägypten und Marokko. Zu ihrem Aufklärungsspektrum gehören vor allem die hier ansässigen Auslandsgemeinden, beispielsweise die syrische Diaspora, bei der es sich um die europaweit größte handelt. Die Nachrichtendienste versuchen, Oppositionelle in Deutschland auszuspähen oder als Extremisten zu diskreditieren. Die Methoden der Transnationalen Repression (TNR, vgl. Kap. I) reichen bis hin zu einer physischen Bedrohung.

Ägypten gilt als ein autoritäres Regime, das in Deutschland und insbesondere bei Reisen nach Ägypten vor Repressionen gegen Regimekritiker nicht zurückschreckt. In Einzelfällen können auch deutsche Mandatsträger betroffen sein.

Eine besondere Fallkonstellation ergibt sich mit Blick auf syrische Nachrichtendienste. Bis zum Sturz des Assad-Regimes im Dezember 2024 waren für sie – neben der syrienstämmigen Gemeinschaft in Deutschland – auch deutsche Gerichtsverfahren zur Aufarbeitung von Kriegsverbrechen im syrischen Bürgerkrieg relevant. Basierend auf dem Weltrechtsprinzip erfolgt eine juristische Aufarbeitung von Kriegsverbrechen in Syrien auch vor deutschen Gerichten. Syrische Dienste hatten ein Interesse, diese Verfahren gezielt auszuspähen und Zeugen einzuschüchtern, um so eine öffentliche juristische Aufklärung zu beeinträchtigen. Mit hoher Wahrscheinlichkeit wird es in den nächsten Jahren zu weiteren Gerichtsverfahren dieser Art kommen, die – in Abhängigkeit von der künftigen politischen Entwicklung – erneut in den Fokus syrischer Dienste geraten könnten. Dem Schutz dieser Verfahren vor nachrichtendienstlichen Operationen kommt daher eine besondere Bedeutung zu.

Nachrichtendienste aus Nordafrika und dem Nahen und Mittleren Osten haben in der Vergangenheit auch menschliche Quellen geführt, um in deutschen Behörden Informationen zu gewinnen. Darüber hinaus sind sie bestrebt, Politik, Medien und Verwaltungshandeln in Deutschland durch klandestine Methoden im Sinne ihrer Staatsführungen zu beeinflussen. Nationale politische Interessen oder außereuropäische Regionalkonflikte werden so auch hierzulande verfolgt und ausgetragen. Bei ihren Aufklärungsaktivitäten bedienen sich vorgenannte Nachrichtendienste modernster technischer Mittel.

Pakistanische Nachrichtendienste

Die pakistanischen Nachrichtendienste beobachten in Deutschland insbesondere oppositionelle Gruppierungen, vor allem Angehörige des Volkes der Belutschen, die in Afghanistan, Iran und Pakistan leben. Gleichzeitig versuchen sie, Einfluss auf die hiesige pakistanische und afghanische Diaspora zu nehmen sowie eine positive Wahrnehmung Pakistans in Deutschland zu erzeugen. Hierzu unterstützen die pakistanischen Nachrichtendienste regimefreundliche Propagandaveranstaltungen und Demonstrationen.

Indische Nachrichtendienste

Der Aufgabenschwerpunkt der indischen Nachrichtendienste in Deutschland liegt auf der Ausspähung separatistischer Sikh-Bewegungen, die als terroristische Vereinigungen eingestuft werden. Aber auch als illoyal gegenüber der gegenwärtigen Regierung angesehene Gruppen geraten zunehmend in den Fokus der Nachrichtendienste.

Die sich weltweit mehrenden Berichte über Transnationale Repression und Einflussnahme durch indische Stellen lassen sich aus Beobachtungen in Deutschland bestätigen. Das BfV konnte in den letzten zehn Jahren maßgeblich dazu beitragen, dass durch die Aufklärung solcher Aktivitäten mehrere Gerichte Agenten indischer Nachrichtendienste verurteilen konnten. In diesen Fällen wurde beispielsweise die Ausstellung von Reisepässen erst dann in Aussicht gestellt, wenn sich die Betroffenen auf eine Zusammenarbeit mit indischen Stellen eingelassen und Informationen an diese geliefert hatten.

Es ist davon auszugehen, dass Transnationale Repression gegen Separatisten und Regimekritiker auch hierzulande zunehmen wird. Aufgrund der wachsenden globalen politischen Bedeutung

Indiens sowie dessen wirtschaftlichen wie strategischen Ambitionen könnten die nachrichtendienstlichen Aufklärungsbemühungen in Deutschland auch in den Feldern Politik und Wirtschaft zunehmen.

Vietnamesische Nachrichtendienste

Die vietnamesischen Nachrichtendienste und das Militär sind feste Bestandteile des Sicherheits- und Repressionsapparats der Kommunistischen Partei Vietnams. Dissidenten und wegen mutmaßlicher Wirtschaftsstraftaten gesuchte Personen stehen auch in Deutschland im Fokus vietnamesischer Nachrichtendienste.

Ein Beispiel für deren Gefährdung ist der Fall des im Jahr 2017 von Deutschland nach Vietnam entführten vietnamesischen Managers Trịnh Xuân Thanh. Im August 2024 wurde der ehemalige Polizeigeneral To Lam, der damals als Minister für öffentliche Sicherheit nachweislich in dessen Entführung verstrickt war, zum Generalsekretär der Kommunistischen Partei Vietnams ernannt. Es ist davon auszugehen, dass der Verfolgungsdruck auf in Deutschland aufhältige vietnamesische Oppositionelle und Dissidenten weiter hoch bleibt.

Nordkoreanische Nachrichtendienste

Nordkoreanische Nachrichtendienste zielen darauf ab, im Ausland lebende Landsleute unter umfassender Kontrolle zu halten. So will das Regime in Pjöngjang Fälle von Flucht in den Westen wegen des damit verbundenen Prestige- und Talentverlustes unbedingt vermeiden. Nordkoreanische Nachrichtendienste gehen dabei mit großer Härte vor.

Die Nachrichtendienste Nordkoreas nutzen weltweit offensive Cyberoperationen für die Informationsgewinnung über diplomatische und politische Prozesse, zur Wirtschaftsspionage sowie zur Devisenbeschaffung. Eine wesentliche Rolle spielt dabei das Reconnaissance General Bureau (RGB), das wahrscheinlich für die Cyberangriffe der APT-Gruppierung Lazarus verantwortlich ist. Von Wirtschaftsspionage sind vornehmlich Unternehmen aus Bereichen betroffen, die die nordkoreanische Staatsführung im eigenen Land in besonderem Maße vorantreiben will. So erfolgten auch im Jahr 2024 weltweit Cyberspionageangriffe zur Erbeutung geschützten Know-hows insbesondere aus Unternehmen der Luft- und Raumfahrt- sowie der Antriebstechnologie, die für die Rüstung des Landes von Bedeutung sind. Als Angriffsvektor wurde dabei mehrfach erfolgreich Social Engineering angewendet.

Im Fokus der Cyberakteure stehen auch Personen, die sich mit der politischen und humanitären Lage auf der koreanischen Halbinsel befassen sowie internationale Organisationen wie die Vereinten Nationen, die mit der Verhängung, Durchsetzung und Evaluation internationaler Sanktionen gegen Nordkorea betraut sind.

Darüber hinaus setzt Nordkorea gezielt getarnte IT-Fachkräfte (sog. IT-Worker) ein, die ihre Dienstleistungen weltweit Unternehmen anbieten. Die durch die IT-Fachkräfte – zumeist in Kryptowährungen – erarbeiteten Erträge kommen dem nordkoreanischen Regime zugute und finanzieren unter anderem Rüstungsprogramme des Staats. Auch deutsche Firmen beschäftigten bereits nordkoreanische IT-Fachkräfte, die teils direkt aus Nordkorea heraus, teils aber auch außerhalb des Landes arbeiten. Da diese mitunter tiefe Einblicke und Zugänge in die IT-Systeme der Unternehmen erlangen, kann nicht ausgeschlossen werden, dass neben der Erwirtschaftung von (Krypto-)Devisen auch sensible Informationen abfließen und so (Cyber-)Spionageoperationen Nordkoreas unterstützt werden.

VII. Proliferation

Im Rahmen der Proliferationsabwehr nimmt das BfV Staaten in den Blick, von denen zu befürchten ist, dass sie CBRN-Waffen[196] in einem bewaffneten Konflikt einsetzen oder ihren Einsatz zur Durchsetzung politischer Ziele androhen. Staaten, die nach solchen Massenvernichtungswaffen streben, sind bei der Entwicklung und Herstellung der Waffen und Trägersysteme auch weiterhin auf den Weltmarkt und Deutschland angewiesen, obwohl einige selbst technologische Fortschritte verzeichnen. Allerdings verhindern die strengen deutschen und europäischen Exportkontrollbestimmungen solche Beschaffungsbemühungen auf dem regulären Markt.

Umgehungsversuche

Daher beschaffen diese Staaten Produkte und Komponenten über Drittländer (sogenannte Umgehungsausfuhren), schalten Tarnfirmen ein oder machen bei genehmigungspflichtigen Ausfuhren

[196] CBRN-Waffen bezeichnen chemische, biologische, radiologische und nukleare Waffen. Diese gelten als Massenvernichtungswaffen.

von Dual-Use-Gütern[197] falsche Angaben über den Verwendungszweck oder Endverwender. Finanztransfers, die solche Geschäfte begleiten, laufen über verzweigte Firmen- und Bankennetzwerke. So soll der Ursprung von Käufern verschleiert werden.

Islamische Republik Iran

Iran verstieß auch 2024 gegen maßgebliche Verpflichtungen aus der Wiener Nuklearvereinbarung von 2015 (Joint Comprehensive Plan of Action, JCPoA). Die EU hat daher das Teilembargo aufrechterhalten, welches die Weitergabe proliferationsrelevanter Güter an Iran verbietet sowie den Export von Waffen und Trägersystemen untersagt. Wegen des gewaltsamen Vorgehens der iranischen Sicherheitskräfte im Innern sowie der Unterstützung des russischen Angriffskriegs gegen die Ukraine hat die EU 2023 und 2024 weitere Sanktionen gegen das Land erlassen. Neben seinem Atomprogramm verfolgt Iran eines der umfangreichsten Raketenprogramme im Nahen und Mittleren Osten. Im Bereich der iranischen Trägertechnologie-/Raketenprogramme sind die Beschaffungsaktivitäten in Deutschland anhaltend hoch – mit steigender Tendenz. Die Militärschläge Irans im Rahmen der Spannungen im Nahen Osten zeigen, dass er bereit ist, seine politischen Ziele mit Einsatz seiner Armee durchzusetzen. Zusätzlich bedient sich Iran auch lokaler Stellvertreter wie der „Hizb-Allah“ oder anderer Milizen.

Russische Föderation

Trotz umfangreicher und beständig angepasster beziehungsweise erweiterter EU-Sanktionen setzt Russland seine proliferationsrelevanten Aktivitäten in Deutschland fort. Als Reaktion auf den russischen Angriffskrieg hat die EU seit Ende Februar 2022 Sanktionen gegen Russland erlassen, die unter anderem Finanzsanktionen sowie Einfuhr- und Einreisebeschränkungen gegen zahlreiche Güter, Institutionen und Einzelpersonen umfassen. Zentraler Bestandteil der Sanktionen ist das Verbot für die Lieferung von Dual-Use-Gütern (Anhang I der Dual-Use-Verordnung) sowie sämtlichen Gütern und Technologien, die zur militärischen und technologischen Stärkung Russlands oder zur Entwicklung des Verteidigungs- und Sicherheitssektors beitragen könnten (Anhang VII der RU-Embargo-Verordnung).[198]

[197] Dual-Use-Güter bezeichnen Produkte, die sowohl für zivile als auch für militärische Zwecke verwendet werden können.

[198] Nähere Informationen zu den beiden wichtigsten EU-Sanktionen gegen Russland VO (EU) 833/2014 und VO (EU) 269/2014 sind in den FAQ des BMWE und auf der Internetseite des BAFA www.bafa.de/DE/Aussenwirtschaft/Ausfuhrkontrolle/Embargos/Russland/russland_node.html verfügbar.

Neben Dual-Use-Gütern für CBRN-Waffen und militärische Raumfahrtprogramme zielten russische Beschaffungsbemühungen vermehrt in Richtung Quantentechnologie und maritime Güter. Insgesamt hat das BfV im Jahr 2024 im Vergleich zum Vorjahr eine nahezu gleichbleibende Anzahl proliferationsrelevanter Beschaffungsversuche unter Einbindung russischer Nachrichtendienste mit konkretem Deutschlandbezug verifiziert. Auch künftig ist mit einer anhaltend hohen Zahl proliferationsrelevanter Beschaffungsbemühungen Russlands zu rechnen.

Volksrepublik China

China arbeitet im Bereich der Emerging Technologies (EMT) mit Hochdruck an dem von der KPCh propagierten „Sprung an die Weltspitze" – auch unter vielfältiger Nutzung des deutschen Marktes und der deutschen Wissenschaftslandschaft. Dies geschieht durch die (Forschungs-)Güterbeschaffung im Rahmen regulärer Geschäftsbeziehungen, ausländische Direktinvestitionen oder Wissenschaftskooperationen. Häufig sind solche Beschaffungsaktivitäten weder Gegenstand von Sanktionen oder internationalen Restriktionen noch von nationalen beziehungsweise europäischen Exportbeschränkungen. Mit der Investitionsprüfung steht ein Instrument zur Überprüfung ausländischer Direktinvestitionen zur Verfügung.

Erkennbar ist in vielen Bereichen die Anfälligkeit Deutschlands für Abflüsse hiesiger Hochtechnologie. Da insbesondere EMT mit zivil-militärischem Dual-Use-Charakter das Potenzial haben, zukünftige militärische Auseinandersetzungen in einem Maße zu beeinflussen, das der Wirkung von Massenvernichtungswaffen nahekommt, ist diese Entwicklung mit Sorge zu betrachten. Am 20. Dezember 2024 hat der GBA Anklage gegen drei deutsche Staatsangehörige vor dem OLG Düsseldorf (Nordrhein-Westfalen) erhoben. Sie waren am 22. April 2024 in Bad Homburg (Hessen) und Düsseldorf festgenommen worden. Ihnen werden geheimdienstliche Tätigkeiten für den chinesischen Nachrichtendienst Ministerium für Staatssicherheit (MSS, vgl. Kap. X) und gewerbsmäßige Verstöße gegen das Außenwirtschaftsgesetz vorgeworfen. Über eine von ihnen betriebene Firma beschafften sie Informationen über militärisch nutzbare innovative Technologien, unter anderem bei Forschungseinrichtungen und mittels Kooperationsabkommen bei einer deutschen Universität. Dieser Fall belegt, dass China ein umfassendes und einzigartiges System des Technologie- und Know-how-Transfers zum Zwecke der militärischen Aufrüstung

betreibt. Das BfV steuert dem durch nachrichtendienstliche Aufklärung und Analyse mit anschließender Sensibilisierung von Politik und Unternehmen entgegen.

Islamische Republik Pakistan

Pakistan betreibt ein umfassendes militärisches Nuklear- und Trägertechnologieprogramm. Der Ausbau des eigenen Kernwaffenpotenzials durch die Entwicklung und Stationierung neuer nuklearfähiger Raketen sowie die Produktionssteigerung bei spaltbaren Materialien haben für Pakistan große Bedeutung.

Auch im Jahr 2024 waren in Deutschland – wie in zahlreichen anderen westlichen Ländern – proliferationsrelevante pakistanische Beschaffungsversuche festzustellen. Intensive verdeckte Bemühungen zur Fortentwicklung des pakistanischen Nuklear- und Trägertechnologieprogramms sind auch zukünftig zu erwarten.

Demokratische Volksrepublik Korea (Nordkorea)

Nordkorea verfügt über ein weit fortgeschrittenes, völkerrechtswidriges Kernwaffen- und Raketenprogramm. Der Besitz nuklear bestückter Raketen gilt dem Regime als herausragendes Element der Machterhaltung und -demonstration. Auch 2024 führte das Land zahlreiche Raketentests durch. Zudem lieferte Nordkorea weiterhin Waffen und Munition an Russland, stellte nordkoreanische Soldaten bereit für den Einsatz im russischen Angriffskrieg gegen die Ukraine und schloss im Juni 2024 ein umfassendes strategisches Partnerschaftsabkommen mit Russland. Die intensivierte Kooperation zwischen Nordkorea und Russland könnte zu einer Modernisierung des nordkoreanischen Militärs und möglicherweise auch dessen Waffenprogrammen führen. Welche Auswirkungen die zunehmende Bindung an Russland auf proliferationsrelevante Beschaffungsversuche in Deutschland haben wird, behält das BfV im Blick.

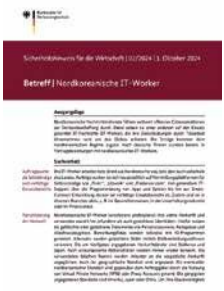
VIII. Prävention in Wirtschaft, Wissenschaft, Politik und Verwaltung

Mit seiner Präventionsarbeit trägt das BfV dazu bei, dass sich Wirtschaft, Wissenschaft sowie Politik und Verwaltung besser gegen Ausforschung, illegalen Wissens- und Technologietransfer, Sabotage sowie Bedrohungen durch Extremismus und Terrorismus schützen können.

Schwerpunkt russischer Angriffskrieg und chinesische Spionage

2024 bestimmten die sich aus dem Agieren Russlands im Zuge seines Angriffskriegs gegen die Ukraine ergebenen Bedrohungen weiterhin die Arbeit des Präventionsbereichs des BfV. Zudem prägten Gefährdungen durch Vorbereitungshandlungen für Sabotage sowie einzelne Sabotageakte die Sicherheitslage. Aber auch die umfassende Spionage Chinas und anderer Staaten stellte einen Schwerpunkt in der Präventionstätigkeit des Wirtschaftsschutzes dar.

Informationsangebote für Wirtschaft, Wissenschaft, Politik und Verwaltung



Das BfV veröffentlichte deshalb lagebezogen „Sicherheitshinweise für die Wirtschaft“ und sprach zudem einzelne Zielgruppen unmittelbar an. Mit dem Format werden deutsche Unternehmen, Verbände und politische Entscheidungsträgerinnen und -träger über einzelne Aspekte der aktuellen Bedrohungslage informiert. Weiterhin gibt das BfV Handlungsempfehlungen, beispielsweise zum Schutz vor nachrichtendienstlicher Anbahnung. Zuletzt veröffentlichte Ausgaben befassten sich mit dem Schutz vor Sabotage und mit der Gefährdung durch nordkoreanische IT-Fachkräfte.[199] Auch mit ausländischen Partnern – wie dem National Intelligence Service (NIS) der Republik Korea (Südkorea) – hat das BfV 2024 einen „Sicherheitshinweis zur Gefahr durch nordkoreanische Cyberaktivitäten gegen die Rüstungsbranche“ veröffentlicht.

Zusätzlich konnte mit dem „BfV CYBER INSIGHT“ ein Einblick in die offensive Vorgehensweise chinesischer Cyberspionage gegeben werden. Dabei handelt es sich um eine Analyse Anfang 2024 geleakter Dokumente einer chinesischen Firma, in der die Arbeit chinesischer Cybersicherheitsdienstleister für Chinas Nachrichtendienste nachvollziehbar wird (vgl. auch Abschnitt III, 4.).

Die „Informationsblätter zum Wirtschaftsschutz“ geben einen Überblick über relevante Sicherheitsthemen und dienen als Handreichung zur Sensibilisierung von Beschäftigten und der Leitungsebene von Unternehmen. Neu erschienen ist 2024 ein Blatt zu Extremismus als Gefahr für Wirtschaft und Wissenschaft.[200]

[199] Der „Sicherheitshinweis für die Wirtschaft“ wird auf www.verfassungsschutz.de und www.wirtschaftsschutz.info zur Verfügung gestellt sowie über den BfV-Kanal beim Kurznachrichtendienst X bekannt gemacht.

[200] Die „Informationsblätter zum Wirtschaftsschutz“ sind in deutscher und englischer Sprache erhältlich und werden auf www.verfassungsschutz.de und www.wirtschaftsschutz.info zur Verfügung gestellt.

Der präventive Wirtschaftsschutz ist ein zentrales Anliegen des gesamten Verfassungsschutzverbundes, weshalb hier eine enge Zusammenarbeit erfolgt. Darüber hinaus engagiert sich das BfV bei der Weiterentwicklung der durch das BMI koordinierten „Initiative Wirtschaftsschutz", in der staatliche Stellen und Wirtschaftsverbände zusammenarbeiten.

Prävention im Verbund

IX. Ermittlungsverfahren, Festnahmen und Verurteilungen

Im Jahr 2024 leitete der Generalbundesanwalt beim Bundesgerichtshof insgesamt 17 neue Ermittlungsverfahren wegen des Verdachts der geheimdienstlichen Agententätigkeit (§ 99 StGB) ein. 2024 wurden gegen elf Personen Haftbefehle wegen dieses Vorwurfs vollstreckt. Drei Personen wurden wegen geheimdienstlicher Agententätigkeit rechtskräftig verurteilt.

X. Strukturen und Aufgaben ausländischer Nachrichtendienste

1. Russische Föderation

SWR Slushba Wneschnej Raswedki	Ziviler Auslandsnachrichtendienst
Leitung:	Sergej Narischkin
Der SWR ist für Spionage in den Bereichen Politik, Wirtschaft, Wissenschaft und Technologie zuständig. Zu seinen Aufgaben gehören zudem die Ausforschung von Zielen und Arbeitsmethoden westlicher Nachrichten- und Sicherheitsdienste sowie die elektronische Fernmeldeaufklärung. Der SWR ist ebenfalls im Bereich von Cyberspionageoperationen aktiv, darunter gegen Hochwertziele westlicher Staaten, insbesondere im Hinblick auf das russische Erkenntnisinteresse für Außen- und Sicherheitspolitik. Zudem wirkt der Dienst an der Bekämpfung von Proliferation und Terrorismus mit.	

GRU Glawnoje Raswedywatelnoje Uprawlenije	Militärischer Auslandsnachrichtendienst
Leitung:	Admiral Igor Kostjukow
Zu den Aufgaben der GRU gehört die Beschaffung von Informationen in den Bereichen Militär und Sicherheitspolitik. Zu den Zielobjekten zählen die Bundeswehr, die NATO und andere westliche Verteidigungsstrukturen sowie militärisch nutzbare Technologien. Neben Cyberspionage führt die GRU auch (Cyber-)Sabotageoperationen durch. Mit den SpetsNaz verfügt die GRU über eine erhebliche personelle Komponente an militärischen Spezialeinheiten.	

FSB Federalnaja Slushba Besopasnosti	Inlandsnachrichtendienst
Leitung:	Armeegeneral Alexander Bortnikow
Zu den Aufgaben des FSB gehören die Spionageabwehr, die Beobachtung oppositioneller Gruppierungen sowie die Bekämpfung von Extremismus, Terrorismus und Organisierter Kriminalität. Zudem zählen der Schutz der russischen Industrie vor Wirtschaftsspionage, der Schutz ausländischer Investoren vor Wirtschaftskriminalität sowie die Sicherung der Staatsgrenzen zu seinen Aufgaben. Der FSB betreibt auch Gegenspionage im Ausland und ist in der Cyberspionage aktiv. Neben den nachrichtendienstlichen Aufgaben ist ein erheblicher Teil des Personals für den Grenzschutz zuständig.	

2. Volksrepublik China

MSS Ministry of State Security	Ziviler In- und Auslandsnachrichtendienst
Leitung:	Minister Chen Yixin
Das MSS ist sowohl mit Abwehraufgaben im Inland als auch mit offensiven Spionageaktivitäten im Ausland betraut. In Fragen der nationalen Sicherheit nimmt das MSS eine zentrale Rolle unter den chinesischen Diensten ein. Das Ministerium ist für die Bekämpfung von Gefahren für die staatliche Ordnung und Sicherheit zuständig und hierfür auch mit Polizeibefugnissen ausgestattet. In Deutschland bemüht es sich nachhaltig um Informationen aus den Bereichen Politik, Wirtschaft und Wissenschaft und klärt oppositionelle chinesische Gruppierungen auf. Das MSS ist auch im Bereich von Cyberspionageoperationen aktiv. Im Fokus stehen dabei Hochwertziele westlicher Staaten, insbesondere zu Themen der Außen- und Sicherheitspolitik.	

MID Military Intelligence Directorate	Militärischer In- und Auslands-nachrichtendienst
Das MID ist weltweit tätig. Es entsendet Militärattachés und unterhält Verbindungen zu ausländischen Streitkräften. Es ist für die Beschaffung von Informationen zuständig, die die äußere Sicherheit der Volksrepublik betreffen. Das MID konzentriert sich auf militärisch-strategische Aufklärungsziele – wie Struktur, Stärke und Ausrüstung fremder Streitkräfte. Spionageziele sind aber auch Politik sowie Wissenschaft und Technik mit militärischem Bezug.	

NSD Network Systems Department	Technischer militärischer Nachrichtendienst
Das NSD ist der Teilstreitkraft PLA Strategic Support Force (SSF) der Volksbefreiungsarmee unterstellt. Es betreibt weltweite Fernmeldeaufklärung und Cyberspionage und ist für Telekommunikationsüberwachung, IT-Sicherheit und Cyberabwehr im Militär zuständig. Zahlreiche gegen westliche Staaten aktive chinesische Cybergruppierungen werden mutmaßlich vom NSD gesteuert.	

MPS Ministry of Public Security	Ministerium für Öffentliche Sicherheit
Leitung:	Minister Wang Xiaohong
Das MPS ist zuständig für öffentliche Sicherheit und Ordnung und kann auf die Ordnungs- und Kriminalpolizei zurückgreifen. Ferner verfügt das MPS über nachrichtendienstliche Einheiten, die auch verdeckt im Ausland tätig sind und deren Aufgaben sich teilweise mit denen des MSS decken. Überdies kontrolliert und zensiert das MPS die Medien und den Internetverkehr. Mutmaßlich steuert das MPS chinesische Cyberspionageangriffe gegen im Ausland lebende chinesische Staatsangehörige und Dissidentinnen bzw. Dissidenten.	

IDCPC International Department of the Central Committee of the Communist Party of China	Internationale Abteilung des ZK der KPCh
Leitung:	Minister Liu Jianchao
Das IDCPC hat Ministeriumsrang und ist für den Dialog der KPCh mit ausländischen Parteien des gesamten politischen Spektrums zuständig. Darüber hinaus führt es verdeckte politische Einflussoperationen durch und nutzt auch nachrichtendienstliche Mittel zur Informationsbeschaffung.	

3. Islamische Republik Iran

VAJA/MOIS Ministry of Intelligence[201]	Ziviler In- und Auslandsnachrichtendienst
Leitung:	Minister Esmaeil Khatib
VAJA/MOIS ist wegen seiner Größe und Bedeutung für den Machterhalt der Regierung eines der mächtigsten Ministerien. In seiner Funktion als Minister hat der Leiter des VAJA/MOIS einen Sitz im Kabinett. Kernaufgabe ist die Ausspähung und Bekämpfung oppositioneller Bewegungen im In- und Ausland, auch durch Staatsterrorismus. Darüber hinaus werden im westlichen Ausland einschließlich Israel Informationen aus den Bereichen Außen- und Sicherheitspolitik, Wirtschaft und Wissenschaft beschafft.	

[201] In Farsi: Vezarat e Ettela'at-e Jomhouri-ye Eslami-ye Iran – VAJA.

IRGC-IO Islamic Revolutionary Guard Corps Intelligence Organization[202]	Militärischer In- und Auslandsnachrichtendienst
Leitung:	Mohammad Kazemi
Der Nachrichtendienst der Iranischen Revolutionsgarden ist sowohl für Spionage im Ausland als auch für Abwehraufgaben im Inland zuständig und so eine wichtige Säule der Herrschaftssicherung der iranischen Führung.	

Quds Force[203] (auch: al-Quds-Einheit, Quds-Brigaden oder Sepah-Qods)	Militärische Spezialeinheit
Leitung:	Brigadegeneral Ismail Ghaani
Die Spezialeinheit der Revolutionsgarden ist auf extraterritoriale und verdeckte militärische und staatsterroristische Operationen sowie auf nachrichtendienstliche Ausspähungen spezialisiert.	

4. Republik Türkei

Türkische Nachrichtendienste

Das Aufklärungsinteresse türkischer Nachrichtendienste in Deutschland gilt grundsätzlich allen Organisationen und Einzelpersonen, die in tatsächlicher oder mutmaßlicher Opposition zur gegenwärtigen türkischen Regierung stehen. Ihre vorrangigen Ziele sind die auch in der EU und den USA als Terrororganisation gelistete „Arbeiterpartei Kurdistans“ (PKK) und die Gülen-Bewegung. Weitere Aufklärungsziele bilden wirtschaftliche, politische, militärische und technologische Themen innerhalb Deutschlands und dessen Rolle innerhalb von EU und NATO.

[202] In Farsi: Sepah Pasdaran.

[203] In Farsi: Niru-ye Quds (diese Bezeichnung der Einheit wird von dem arabischen Namen für Jerusalem „al-Quds“ abgeleitet).

Geheim- und Sabotageschutz

Geheim- und Sabotageschutz

Zielsetzung

Der Geheimschutz dient dem Schutz von Informationen, die durch eine staatliche Stelle als Verschlusssache (VS)[204] eingestuft worden sind.

Der Sabotageschutz hat die Aufgabe, lebens- und verteidigungswichtige Einrichtungen vor Sabotagehandlungen durch sogenannte Innentäter zu schützen. Solche Einrichtungen sind entweder für die Funktionsfähigkeit des Staates unverzichtbar oder können im Sabotagefall die Gesundheit oder das Leben großer Teile der Bevölkerung erheblich gefährden.

Personeller Geheim- und Sabotageschutz

Wesentliches Element des personellen Geheim- und Sabotageschutzes sind Sicherheitsüberprüfungen nach dem Sicherheitsüberprüfungsgesetz (SÜG).

Das SÜG bestimmt, wann eine Sicherheitsüberprüfung erforderlich ist. Im Bereich des personellen Geheimschutzes ist demnach ein Zugang zu Verschlusssachen ausschlaggebend, die als VS-VERTRAULICH oder höher eingestuft sind. Beim vorbeugenden personellen Sabotageschutz ist die Tätigkeit an einer sicherheitsempfindlichen Stelle einer lebens- oder verteidigungswichtigen Einrichtung (festgeschrieben in der Sicherheitsüberprüfungsfeststellungsverordnung – SÜFV) maßgeblich.

Darüber hinaus sind Sicherheitsüberprüfungen auch auf einer spezialgesetzlichen Grundlage vorgesehen.[205]

Überprüfungsarten

Das SÜG sieht drei Überprüfungsarten vor:

- einfache Sicherheitsüberprüfung (Ü1),
- erweiterte Sicherheitsüberprüfung (Ü2),

[204] Nach § 4 Abs. 1 SÜG sind VS im öffentlichen Interesse, insbesondere zum Schutz des Wohles des Bundes oder eines Landes, geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse unabhängig von ihrer Darstellungsform. VS können auch Produkte und die dazugehörenden Dokumente sowie zugehörige Schlüsselmittel zur Entschlüsselung, Verschlüsselung und Übertragung von Informationen sein (Kryptomittel). Geheimhaltungsbedürftig im öffentlichen Interesse können auch Geschäfts-, Betriebs-, Erfindungs-, Steuer- oder sonstige private Geheimnisse oder Umstände des persönlichen Lebensbereichs sein.

[205] Zum Beispiel im Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel-10-Gesetz), im Satellitendatensicherheitsgesetz (SatDSiG), im Bundeskriminalamtgesetz (BKAG) sowie im Zollfahndungsdienstgesetz (ZFdG).

- erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen (Ü3).

Im Geheimschutz richtet sich die Art der Sicherheitsüberprüfung nach der Höhe des Geheimhaltungsgrades der Verschlusssachen, zu denen die betroffene Person Zugang erhalten soll.

Im Rahmen der Ü2 und Ü3 werden Überprüfungsmaßnahmen auch bei der sogenannten mitbetroffenen Person[206] durchgeführt. Für den Bereich des Sabotageschutzes erfolgt eine reduzierte Form der Ü2.

Grundlage jeder Sicherheitsüberprüfung ist die Sicherheitserklärung der betroffenen Person, welche die im SÜG festgelegten Angaben zu enthalten hat. Die Sicherheitsüberprüfung setzt die Zustimmung der betroffenen und gegebenenfalls der mitbetroffenen Person voraus.

Zulässig ist eine Sicherheitsüberprüfung nur, wenn vorgesehen ist, dass die betroffene Person in absehbarer Zeit eine sicherheitsempfindliche Tätigkeit aufnehmen oder weiterhin ausüben wird.

Sicherheitsrisiko

Ziel der Sicherheitsüberprüfung ist, festzustellen, ob eine Person die für die jeweilige sicherheitsempfindliche Tätigkeit erforderliche Zuverlässigkeit besitzt. Diese Voraussetzung ist nicht gegeben, wenn ein Sicherheitsrisiko festgestellt wird. Ein solches liegt vor, wenn tatsächliche Anhaltspunkte

- Zweifel an der Zuverlässigkeit bei der Wahrnehmung der sicherheitsempfindlichen Tätigkeit,
- eine besondere Gefährdung bei möglichen Anbahnungs- oder Werbungsversuchen[207] oder

[206] Mitbetroffene, in die Überprüfung einzubeziehende Person ist: die volljährige Ehegattin oder der volljährige Ehegatte, die Lebenspartnerin oder der Lebenspartner oder die volljährige Partnerin oder der volljährige Partner, mit der oder dem die betroffene Person in einer auf Dauer angelegten Gemeinschaft lebt (Lebensgefährtin oder Lebensgefährte).

[207] In Betracht kommen ausländische Nachrichtendienste, Vereinigungen im Sinne der §§ 129 bis 129b Strafgesetzbuch sowie extremistische Organisationen, die Bestrebungen im Sinne des § 3 Abs. 1 Bundesverfassungsschutzgesetz (BVerfSchG) verfolgen.

- Zweifel am Bekenntnis zur freiheitlichen demokratischen Grundordnung oder am jederzeitigen Eintreten für deren Erhaltung

dies begründen.

Die Feststellung eines Sicherheitsrisikos ist keine Sanktion, sondern setzt bei Zweifeln an der Zuverlässigkeit und Verstößen gegen die Verfassungstreuepflicht voraus, dass keine bzw. keine hinreichend positive Prognose über das künftige Verhalten der betroffenen Person möglich ist.

Zweifel an der Zuverlässigkeit

Zweifel an der Zuverlässigkeit können sich zum Beispiel aus Verstößen gegen Strafvorschriften oder Dienstpflichten, einem übermäßigen Alkoholkonsum, der Abhängigkeit oder dem Konsum von Betäubungsmitteln oder bestimmten Medikamenten sowie bei Vorliegen bestimmter psychischer Erkrankungen ergeben.

Nachrichtendienstliche Gefährdung

Eine nachrichtendienstliche Gefährdung kann sich vor allem aus verwandtschaftlichen Verbindungen in Staaten mit besonderen Sicherheitsrisiken ergeben. Die Feststellung des Sicherheitsrisikos lässt in diesem Fall nicht darauf schließen, dass die betroffene Person gegen Pflichten verstoßen würde. Auch wenn der maßgebliche Zweck der Feststellung eines Sicherheitsrisikos dem Schutz von Verschlusssachen dient, werden durch die Maßnahme die Person selbst und Verwandte oder Freunde, die in Risikostaaten leben, vor Anbahnungsversuchen und Repressalien geschützt. Auch eine Überschuldung oder Umstände, welche eine Person unbedingt vor Dritten verborgen halten will, bieten Angriffsflächen für eine mögliche Erpressbarkeit und können eine erhöhte nachrichtendienstliche Gefährdung begründen.

Zweifel an der Verfassungstreue

Zweifel an der Verfassungstreue sind regelmäßig gerechtfertigt, wenn eine Person Mitglied in einer extremistischen (Teil)Organisation ist, insbesondere, wenn sie sich aktiv oder auch propagandistisch für diese einsetzt. Dies gilt auch, wenn sie Dritten wegen ihres Geschlechtes, ihrer Abstammung, ihrer Sprache, ihrer Heimat und Herkunft, ihres Glaubens oder ihrer religiösen oder politischen Anschauungen die Anerkennung der gleichen Würde und Rechte wie anderen abspricht.

Stetige aktualisierte Neubewertung

Die Maßstäbe bei der Beurteilung möglicher Sicherheitsrisiken werden in Ansehung der national wie international zuletzt zunehmend angespannten Sicherheitslage stetig neu bewertet und angepasst. Der Angriffskrieg Russlands gegen die Ukraine wird zunehmend aggressiv geführt. Dies geht einher mit intensivierten Spionageaktivitäten und Anwerbungsversuchen der russischen Nachrichtendienste. Wie befürchtet, schreckt Russland zwischenzeitlich auch vor der Durchführung oder Veranlassung von Sabotageakten in Deutschland und anderen europäischen Staaten nicht mehr zurück. Kritische Infrastrukturen, etwa der Informations- und Kommunikationstechnik sowie der Energieversorgung, gilt es in besonderem Maße vor Sabotagehandlungen zu schützen.

Die gerade in sozialen Medien verstärkte Verbreitung antisemitischer Propaganda hält auch über ein Jahr nach dem terroristischen Angriff der HAMAS auf Israel am 7. Oktober 2023 und den anschließenden Geschehnissen im Nahen Osten weiter an. Auch die Ausdehnung des kriegerischen Konflikts auf den Libanon spielt hierbei eine Rolle.

Die Verbreitung etwaiger antisemitischer Stellungnahmen und auch bereits das Liken solcher Äußerungen können im Einzelfall ein Sicherheitsrisiko begründen.

Die Entscheidung, ob für eine Person eine Sicherheitsüberprüfung erforderlich ist und ob ein Sicherheitsrisiko vorliegt, trifft die zuständige Stelle. Dies ist im öffentlichen Bereich regelmäßig die Beschäftigungsbehörde, im nichtöffentlichen Bereich das Bundesministerium für Wirtschaft und Energie (BMWE), sofern nichts anderes bestimmt ist. In der Folge führt das BfV die für die jeweilige Überprüfungsart nach § 12 SÜG vorgesehenen Maßnahmen durch und nimmt damit eine wichtige Serviceaufgabe für diese Bedarfsträger wahr. Zusätzlich wirkt das BfV gemäß § 3 Abs. 2 SÜG bei der Geheimschutzbetreuung nichtöffentlicher Stellen mit, indem es zum Beispiel die Angaben der nichtöffentlichen Stellen unter Berücksichtigung der Erkenntnisse der Verfassungsschutzbehörden sicherheitsmäßig bewertet.

Maßnahmen der Sicherheitsüberprüfung

Zu den Maßnahmen zählen insbesondere die Berücksichtigung der Erkenntnisse der Verfassungsschutzbehörden des Bundes und der Länder und der anderen Nachrichtendienste des Bundes sowie von Polizei- und Justizbehörden. Zudem können bei allen

Überprüfungsarten öffentlich zugängliche Informationen zu der betroffenen Person im Internet recherchiert werden. Bei der Ü2 werden für die mitbetroffene Person die für die Ü1 und Ü2 vorgesehenen Maßnahmen (ohne Internetrecherche) ebenfalls durchgeführt. Bei der Ü3 werden – zusätzlich zu den Maßnahmen der Ü1 und Ü2 – die von der betroffenen Person angegebenen Referenzpersonen sowie weitere geeignete Auskunftspersonen befragt. Die im Rahmen des Sicherheitsüberprüfungsverfahrens festgestellten Erkenntnisse werden vom BfV auf ihre Sicherheitserheblichkeit geprüft und bei der Erstellung eines abschließenden Votums berücksichtigt. Auf dessen Grundlage entscheidet die Beschäftigungsbehörde beziehungsweise das BMWE über den Einsatz der überprüften Person in einer sicherheitsempfindlichen Tätigkeit.

Entwicklungen

Sicherheitsüberprüfungen sind ein geeignetes Mittel, um sensible Tätigkeiten nur an besonders zuverlässige Personen zu übertragen.

In den letzten Jahren ist der Kreis der zu überprüfenden Personen kontinuierlich ausgedehnt worden. Globalisierung und Migration führen dabei nicht selten zu einem erhöhten Überprüfungsaufwand, da Aufenthalte außerhalb Deutschlands ebenfalls mit eigenen Maßnahmen abzuklären sind.

Das BfV hat im vergangenen Jahr gem. § 3 Abs. 2 Nr. 1 und 2 BVerfSchG im Rahmen von 66.248 Sicherheitsüberprüfungen 88.194 Personen im Geheim- und Sabotageschutz überprüft. Das Überprüfungsaufkommen steigt kontinuierlich an. Das BfV trägt diesem Umstand mit der Konzeption, Pilotierung und Einführung weitgehend digitalisierter Arbeitsprozesse Rechnung. Die Anzahl der Sicherheitsüberprüfungen verteilt sich nahezu gleichmäßig auf Behördenmitarbeitende und Beschäftigte in Unternehmen.

Im Jahr 2024 wurden im Geheimschutz 16.483 Personen im Rahmen von einfachen Sicherheitsüberprüfungen (Ü1), 37.148 Personen im Rahmen von 23.537 erweiterten Sicherheitsüberprüfungen (Ü2) und 2.662 Personen im Rahmen von 1.563 erweiterten Sicherheitsüberprüfungen mit Sicherheitsermittlungen (Ü3) überprüft. Hinzu kamen 9.787 Überprüfungen im Bereich des vorbeugenden personellen Sabotageschutzes. Ferner wurden 14.878 Aktualisierungen von Sicherheitsüberprüfungen (Ü1 – Ü3 und Sabotageschutz) vorgenommen und hierbei 22.114 Personen überprüft.

Schulung und Sensibilisierung

Das BfV bietet den Geheim- und Sabotageschutzbeauftragten in Behörden[208] regelmäßig Schulungen an. Hierbei haben sich Videoseminare zu einem teilnahmestarken Format entwickelt. Im Rahmen dieser Veranstaltungen werden Entwicklungen in den Beobachtungsfeldern der Verfassungsschutzbehörden sowie rechtliche Themen behandelt. Gleichzeitig wird ein praxisorientierter Austausch gefördert. Daneben hat das BfV weitere Formate etabliert, um in Form von Präsenzveranstaltungen aktuelle fachliche Entwicklungen darzustellen und mit den am Überprüfungsverfahren beteiligten Behörden zu diskutieren.

[208] Die Geheim- beziehungsweise Sabotageschutzbeauftragten in Behörden sind in ihren jeweiligen Zuständigkeitsbereichen für die Durchführung der Bestimmungen des SÜG und der dazu ergangenen Regelungen verantwortlich. Sie nehmen Aufgaben im Zusammenhang mit der Durchführung von Sicherheitsüberprüfungen wahr und sorgen dafür, dass sicherheitsempfindliche Tätigkeiten nur nach Maßgabe des Gesetzes übertragen werden. Ferner treffen sie die abschließende Entscheidung über die Zulässigkeit der Betrauung mit einer sicherheitsempfindlichen Tätigkeit. Sie sind Ansprechstellen für die Bediensteten in allen Fragen des personellen Geheim- beziehungsweise Sabotageschutzes. Geheimschutzbeauftragte sind darüber hinaus für die Durchführung der Maßnahmen des materiellen Geheimschutzes verantwortlich.

„Scientology-Organisation“ (SO)

„Scientology-Organisation“ (SO)

Die „Scientology-Organisation“ (SO) strebt an, weltweit eine „scientologische Gesellschaft“ nach eigener Vorstellung zu errichten. Dabei beruft sie sich auf ein Gesellschaftsbild, welches auf den Schriften des Gründers und der Leitfigur Lafayette Ron Hubbard (1911–1986) basiert. In seinem erstmalig 1950 veröffentlichten Buch „Dianetik“ entwickelte Hubbard eine Methode, die er als „Technologie“, „Dianetik“ oder „Scientology“ bezeichnete. Diese soll dem Nutzer ermöglichen, sich von jeglichen psychischen und physischen Belastungen zu befreien und somit eine Wandlung zum perfekten Menschen („Clear“ oder „Nichtaberrierter“[209] genannt) zu vollziehen. Menschen, die nicht zu den „Clears“ beziehungsweise „Nichtaberrierten“ gehören, sollen innerhalb dieser „scientologischen Gesellschaft“ hingegen Grundrechte und die Menschenwürde abgesprochen werden.

Ideologie

Laut Hubbard ist „wahre Demokratie“ nur dann zu erreichen, wenn sich der Staat ausschließlich aus „Nichtaberrierten“ zusammensetzt. In diesem Kontext erachtet sich die SO selbst als Führungselite, die durch die Anwendung der Lehren Hubbards den Rest der Menschheit regieren sollte. Ein derartiges – die Demokratie ersetzendes – System einer exklusiv scientologischen Regierung ist mit dem Demokratieprinzip unvereinbar, da in einem solchen System die Staatsgewalt weder vom Volke ausginge noch durch eine ununterbrochene Legitimationskette an das Volk gebunden wäre. Die heutige SO distanziert sich nicht von den verfassungsfeindlichen Aussagen Hubbards. Sie verbreitet ihre Ideologie im Rahmen zahlreicher Publikationen, Veranstaltungen und Kurse, sowohl in Präsenz als auch im Internet, mit dem Ziel, eine Welt nach ausschließlich scientologischen Richtlinien zu schaffen.

Struktur

Die SO ist hierarchisch organisiert und unterhält diverse, weltweit agierende Unter- und Tarnorganisationen. In Deutschland existieren neben drei repräsentativen Zentren, den sogenannten Idealen Orgs, mehrere weitere Niederlassungen, die je nach Größe und Ausstattung als „Orgs“ beziehungsweise „Missionen“ bezeichnet werden. Zu diesen Einrichtungen zählen auch zwei sogenannte Celebrity Centres, die vornehmlich für prominente Persönlichkeiten

[209] Vgl. Hubbard, „Dianetik – Der Leitfaden für den menschlichen Verstand“, 3. überarbeitete Ausgabe, Kopenhagen 2007, S. 537 ff.

bestimmt sind. Die Organisation verfolgt weltweit einen aktiven Expansionskurs, die Anzahl der Mitglieder in Deutschland stagniert jedoch seit 2021 bei rund 3.600 Personen.

Strategie

Das primäre Ziel des Expansionskurses ist eine Maximierung finanzieller Mittel sowie – durch die Bekämpfung von Kritikern – die Errichtung einer scientologischen Gesellschaftsordnung im Sinne Hubbards. Dabei bemüht sich die SO in ihrer Außendarstellung, als sozial engagierte Organisation sowie unpolitische Religionsgemeinschaft wahrgenommen zu werden, und arbeitet gezielt darauf hin, dass dieser Status offiziell anerkannt wird. In einer Pressemitteilung anlässlich der Neueröffnung einer „Idealen Org“ in Paris (Frankreich) im April 2024 betonte die SO, dass „die Scientology-Kirche in Europa immer mehr staatliche Anerkennungen“ erfahre und beispielsweise in Großbritannien, den Niederlanden, Portugal, Schweden und Spanien „als gemeinnützige Religionsgemeinschaft anerkannt“ sei.[210]

Aktivitäten

Im gesamten Bundesgebiet ließen sich 2024 regelmäßig Kundgebungen, Informationsstände sowie Verteilaktionen der SO und insbesondere ihrer Unter- und Tarnorganisationen feststellen. Die im Zuge der Coronapandemie eingeführten kostenpflichtigen virtuellen Angebote mit Webinaren, Online-Briefings und weiteren Onlineveranstaltungen haben sich etabliert und wurden fortgeführt.[211] Diese nutzt die SO strategisch, um einem erweiterten Empfängerkreis niedrigschwellig scientologische Inhalte nahezubringen, neue Mitglieder zu werben, Finanzmittel zu generieren und zu expandieren.

Kampagnen

Um die strategischen Ziele voranzutreiben, starteten im Berichtsjahr mehrere Kampagnen. So präsentierte die Organisation unter dem Titel „Let´s better the world“[212] eine neue Plattform, die sämtliche Multimedia-Spots diverser SO-Kampagnen vereint, um ihre Vernetzung auszubauen.

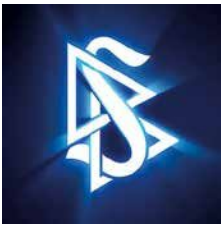
Während der Fußball-Europameisterschaft 2024 in Deutschland verteilte die Tarnorganisation „Sag NEIN zu Drogen – sag JA zum Leben“ im Rahmen einer bundesweiten Kampagne in großem Umfang Informationsmaterial und betrieb in mehreren deutschen

[210] Internetplattform „pressetext.com“ (16. September 2024).
[211] Homepage „Scientology Deutschland“ (18. November 2024).
[212] Homepage „Let´s better the world“ (26. November 2024).

Städten Informationsstände. Unter dem Deckmantel der Drogenprävention ist der SO-Bezug nur schwer erkennbar. So tarnt sie ihre Anwerbeversuche und verschleiert zunächst die Verbreitung ihrer Ideologie. Mithilfe ihrer Kampagnen will die SO neue Zielgruppen generieren und weitere Unterstützer gewinnen. Gleichzeitig soll mit derartigen Themen Akzeptanz für die SO geschaffen werden.

Auch im Jahr 2024 verteilte die SO-Tarnorganisation „The Way to Happiness“ bundesweit Broschüren in Briefkästen und an Passanten. Die Broschüre mit dem Titel „Glück versprühen & verspüren! – Der Weg zum Glücklichsein“ ist mit Smileys, Marienkäfern und vierblättrigen Kleeblättern bedruckt und wirkt somit wie eine Werbebroschüre, die auch ein jüngeres Publikum ansprechen könnte. Sie enthält allgemeine Vorschläge zum Glücklichsein, während der Bezug zur SO auch hier nicht sofort ersichtlich ist. Auf diese Weise sollen Adressen beschafft und eine Kontaktaufnahme zur SO erreicht werden, um so neue Mitglieder zu akquirieren.

„Scientology-Organisation“ (SO)



Gründung:	1954 in den USA 1970 erste Niederlassung in Deutschland
Sitz:	Los Angeles (USA) („Church of Scientology International“, CSI) München (Bayern) („Scientology Kirche Deutschland e.V.“, SKD)
Leitung/Vorsitz:	USA: David Miscavige Deutschland: Helmuth Blöbaum
Mitglieder/Anhänger in Deutschland:	3.600 (2023: 3.600)
Publikationen/Medien (Auswahl):	Streamingdienst: „Scientology Network“ Zeitungen/Zeitschriften: „Impact“ „International Scientology News“ „The Auditor“ „Source“ „Freewinds“ Broschüren: „Der Weg zum Glücklichsein“ „Wie man gute Entscheidungen trifft“ Podcast: „Tierische Abenteuer von Amandas Bauernhof“ Buch: „Fabelhafte Tiergeschichten“[213]

[213] Elyse Aronson-Van Breemen (alias Mz GOOSE), „Fabelhafte Tiergeschichten“, Orlando-Verlag 2001 (englischer Originaltitel: „The Happiness Fables“ 2016).

Teil-/Nebenorganisationen (Auswahl):	Drei „Ideale Orgs“, zwei „Celebrity Centres“ sowie weitere „Orgs“ und „Missionen“ „World Institute of Scientology Enterprises“ (WISE) „Kommission für Verstöße der Psychiatrie gegen Menschenrechte Deutschland e.V.“ (KVPM) „Sag NEIN zu Drogen – Sag JA zum Leben“ „Youth for Human Rights“ „NARCONON“ „CRIMINON“ „International Way to Happiness Foundation“

Die „Scientology-Organisation“ (SO) beabsichtigt, weltweit eine „scientologische Gesellschaft“ zu etablieren. Dieses Ideal der SO basiert dogmatisch auf den Schriften des Gründers und der Leitfigur Lafayette Ron Hubbard (1911–1986), die nach wie vor maßgeblich sind. In ihnen wird deutlich, dass in einer Gesellschaft nach scientologischen Vorstellungen wesentliche Grund- und Menschenrechte, wie beispielsweise die Menschenwürde und das Recht auf freie Entfaltung der Persönlichkeit, ebenso wenig gewährleistet sind wie das Recht auf Gleichbehandlung. Zur Erreichung dieses Ziels verfolgt die SO eine langfristig angelegte Strategie.

Anhang

Übersicht über Verbotsmaßnahmen des BMI gegen extremistische Bestrebungen im Zeitraum Januar 1990 bis Dezember 2024

(Soweit nicht anders gekennzeichnet, sind die Verbote unanfechtbar.)

Organisation	Datum der Verbotsverfügung/ des Verbotsvollzugs	Verbotsgründe	Phänomenbereich
„Nationalistische Front“ (NF)	26.11.1992	Vereinszweck gegen die verfassungsmäßige Ordnung gerichtet	RE
„Deutsche Alternative“ (DA)	08.12.1992	Vereinszweck gegen die verfassungsmäßige Ordnung gerichtet	RE
„Nationale Offensive“ (NO)	21.12.1992	Vereinszweck gegen die verfassungsmäßige Ordnung gerichtet	RE
„Arbeiterpartei Kurdistans“ (PKK)/„Nationale Befreiungsfront Kurdistans“ (ERNK) und Teilorganisationen, **„Föderation der patriotischen Arbeiter- und Kulturvereinigungen aus Kurdistan in der Bundesrepublik Deutschland e.V.“ (FEYKA-Kurdistan), „Kurdistan-Komitee e.V.“**	22.11.1993	Strafgesetzwidrigkeit, Gefährdung der inneren Sicherheit und öffentlichen Ordnung sowie außenpolitischer Belange Deutschlands	AE
„Wiking-Jugend e.V.“ (WJ)	10.11.1994	Vereinszweck gegen die verfassungsmäßige Ordnung gerichtet	RE
„Kurdistan Informationsbüro“ (KIB) alias **„Kurdistan Informationsbüro in Deutschland“**	20.02.1995	Ersatzorganisation des rechtskräftig verbotenen „Kurdistan-Komitee e.V.“	AE

RE = Rechtsextremismus
LE = Linksextremismus
ISiT = Islamismus/islamistischer Terrorismus
RuS = Reichsbürger und Selbstverwalter
AE = Auslandsbezogener Extremismus

Organisation	Datum der Verbots-verfügung/ des Verbots-vollzugs	Verbotsgründe	Phäno-men-bereich
„Freiheitliche Deutsche Arbeiterpartei“ (FAP)	22.02.1995	Vereinszweck gegen die verfassungs-mäßige Ordnung gerichtet	RE
„Revolutionäre Volksbefreiungspartei-Front“ (DHKP-C)	06.08.1998	Strafgesetzwidrigkeit und Gefähr-dung der inneren Sicherheit Ersatzorganisation der am 9. Februar 1983 rechtskräftig ver-botenen „Revolutionären Linken“ („Devrimci Sol“)	AE
„Türkische Volksbefreiungspartei-Front“ (THKP-C)	06.08.1998	Strafgesetzwidrigkeit und Gefähr-dung der inneren Sicherheit	AE
„Blood & Honour“ Division Deutschland (B&H) mit **„White Youth“**	12.09.2000	Vereinszweck gegen die verfassungs-mäßige Ordnung gerichtet Verstoß gegen den Gedanken der Völkerverständigung	RE
„Kalifatsstaat“ und 35 Teilorganisationen	08.12.2001 14.12.2001 13.05.2002 16.09.2002	Vereinszweck gegen die verfassungs-mäßige Ordnung gerichtet Verstoß gegen den Gedanken der Völkerverständigung Propagierung von Gewalt als Mittel zur Durchsetzung politischer Ziele	ISiT

RE = Rechtsextremismus
LE = Linksextremismus
ISiT = Islamismus/islamistischer Terrorismus
RuS = Reichsbürger und Selbstverwalter
AE = Auslandsbezogener Extremismus

Organisation	Datum der Verbots-verfügung/ des Verbots-vollzugs	Verbotsgründe	Phäno-men-bereich
„al-Aqsa e.V.“	31.07.2002	Verstoß gegen den Gedanken der Völkerverständigung (finanzielle Unterstützung der HAMAS und ihrer sogenannten Sozialvereine)	ISiT
„Hizb ut-Tahrir“ (HuT)	10.01.2003	Verstoß gegen den Gedanken der Völkerverständigung Befürwortung von Gewalt zur Durch-setzung politischer Belange	ISiT
„Yeni Akit GmbH“ Verlegerin der Europa-Ausgabe der türkisch-sprachigen Tageszeitung „Anadolu’da Vakit“	22.02.2005	Leugnung und Verharmlosung des Holocaust in volksverhetzender Weise Verbreitung antisemitischer/ antiwestlicher Propaganda	ISiT
„Bremer Hilfswerk e.V.“[214]	Selbstauf-lösung mit Wirkung vom 18.01.2005; Löschung im Vereins-register am 29.06.2005		ISiT
„YATIM-Kinderhilfe e.V.“	30.08.2005	Nachfolgeorganisation des rechts-kräftig verbotenen „al-Aqsa e.V.“	ISiT

[214] Das BMI hatte am 3. Dezember 2004 ein vereinsrechtliches Ermittlungsverfahren mit dem Ziel eines Verbots gegen das „Bremer Hilfswerk e.V.“ eingeleitet. Der Verein ist dem Verbot durch Selbstauflösung zuvorgekommen.

RE = Rechtsextremismus
LE = Linksextremismus
ISiT = Islamismus/islamistischer Terrorismus
RuS = Reichsbürger und Selbstverwalter
AE = Auslandsbezogener Extremismus

Organisation	Datum der Verbots-verfügung/ des Verbots-vollzugs	Verbotsgründe	Phäno-men-bereich
„Collegium Humanum“ (CH) mit **„Bauernhilfe e.V.“**	18.04.2008	Vereinszweck gegen die verfassungs-mäßige Ordnung gerichtet Zuwiderlaufen gegen Strafgesetze	RE
„Verein zur Rehabilitierung der wegen Bestreitens des Holocaust Verfolgten“ (VRBHV)	18.04.2008	Vereinszweck gegen die verfassungs-mäßige Ordnung gerichtet Zuwiderlaufen gegen Strafgesetze	RE
„Mesopotamia Broadcast A/S“, „Roj TV A/S“ **„VIKO Fernseh Produktion GmbH“**	13.06.2008 13.06.2008	Verstoß gegen den Gedanken der Völkerverständigung Teilorganisation von „Roj TV A/S“	AE
„al-Manar TV“	29.10.2008	Verstoß gegen den Gedanken der Völkerverständigung	ISiT
„Heimattreue Deutsche Jugend – Bund zum Schutz für Umwelt, Mitwelt und Heimat e.V.“ (HDJ)	09.03.2009	Vereinszweck gegen die verfassungs-mäßige Ordnung gerichtet Zuwiderlaufen gegen Strafgesetze Ideologische Indoktrinierung von Kindern und Jugendlichen mit natio-nalsozialistischem Gedankengut	RE
„Internationale Humanitäre Hilfsorganisation e.V.“ (IHH)	23.06.2010	Verstoß gegen den Gedanken der Völkerverständigung	ISiT

RE = Rechtsextremismus
LE = Linksextremismus
ISiT = Islamismus/islamistischer Terrorismus
RuS = Reichsbürger und Selbstverwalter
AE = Auslandsbezogener Extremismus

Organisation	Datum der Verbots-verfügung/ des Verbots-vollzugs	Verbotsgründe	Phäno-men-bereich
„Hilfsorganisation für nationale politische Gefangene und deren Angehörige e.V." (HNG)	30.08.2011	Vereinszweck gegen die verfassungs-mäßige Ordnung gerichtet Zuwiderlaufen gegen Strafgesetze	RE
„Millatu Ibrahim"	29.05.2012	Vereinszweck gegen die verfassungs-mäßige Ordnung gerichtet Verstoß gegen den Gedanken der Völkerverständigung	ISiT
„Dawa FFM" einschließlich der Teilorganisation **„Inter-nationaler Jugendverein – Dar al Schabab e.V."**	25.02.2013	Vereinszweck gegen die verfassungs-mäßige Ordnung gerichtet Verstoß gegen den Gedanken der Völkerverständigung	ISiT
„an-Nussrah"	25.02.2013	Teilorganisation des rechtskräftig verbotenen Vereins „Millatu Ibrahim"	ISiT
„DawaTeam Islamische Audios"	25.02.2013	Vereinszweck gegen die verfassungs-mäßige Ordnung gerichtet Verstoß gegen den Gedanken der Völkerverständigung	ISiT
„Waisenkinderprojekt Libanon e.V." (WKP) (Umbenennung in **„Farben für Waisenkinder e.V."** am 16.10.2014)	02.04.2014	Verstoß gegen den Gedanken der Völkerverständigung	ISiT

RE = Rechtsextremismus
LE = Linksextremismus
ISiT = Islamismus/islamistischer Terrorismus
RuS = Reichsbürger und Selbstverwalter
AE = Auslandsbezogener Extremismus

Organisation	Datum der Verbots-verfügung/ des Verbots-vollzugs	Verbotsgründe	Phäno-men-bereich
„Islamischer Staat“ (IS) alias **„Islamischer Staat im Irak“** alias **„Islamischer Staat im Irak und in Groß-Syrien“**	12.09.2014	Vereinszweck gegen die verfassungs-mäßige Ordnung gerichtet Verstoß gegen den Gedanken der Völkerverständigung	ISiT
„Tauhid Germany“ (TG)	26.02.2015	Ersatzorganisation des rechtskräftig verbotenen Vereins „Millatu Ibrahim“	ISiT
„Altermedia Deutschland“	04.01.2016	Vereinszweck gegen die verfassungs-mäßige Ordnung gerichtet	RE
„Weisse Wölfe Terrorcrew“ (WWT)	10.02.2016	Vereinszweck gegen die verfassungs-mäßige Ordnung gerichtet	RE
„Die Wahre Religion“ (DWR)	25.10.2016	Vereinszweck gegen die verfassungs-mäßige Ordnung gerichtet Verstoß gegen den Gedanken der Völkerverständigung	ISiT
„linksunten.indymedia“	14.08.2017	Vereinszweck und -tätigkeit gegen die verfassungsmäßige Ordnung gerichtet Zuwiderlaufen gegen Strafgesetze	LE
„Mezopotamien Verlag und Vertrieb GmbH“	01.02.2019	Teilorganisation der mit Verfügung des Bundesministeriums des Innern vom 22.11.1993 verbotenen PKK	AE

RE = Rechtsextremismus
LE = Linksextremismus
ISiT = Islamismus/islamistischer Terrorismus
RuS = Reichsbürger und Selbstverwalter
AE = Auslandsbezogener Extremismus

Organisation	Datum der Verbots-verfügung/ des Verbots-vollzugs	Verbotsgründe	Phäno-men-bereich
„MİR Multimedia GmbH“	01.02.2019	Teilorganisation der mit Verfügung des Bundesministeriums des Innern vom 22.11.1993 verbotenen PKK	AE
„Combat 18 Deutschland“ (C18 Deutschland)	06.12.2019	Vereinszweck und -tätigkeit gegen die verfassungsmäßige Ordnung gerichtet Zuwiderlaufen gegen Strafgesetze Verstoß gegen den Gedanken der Völkerverständigung	RE
„Geeinte deutsche Völker und Stämme“ (GdVuSt) einschließlich der Teil-organisation **„Osnabrücker Landmark“**	14.02.2020	Vereinszweck und -tätigkeit gegen die verfassungsmäßige Ordnung gerichtet Zuwiderlaufen gegen Strafgesetze Verstoß gegen den Gedanken der Völkerverständigung	RuS
„Hizb Allah“	26.03.2020	Verstoß gegen den Gedanken der Völkerverständigung Zuwiderlaufen gegen Strafgesetze	ISiT

RE = Rechtsextremismus
LE = Linksextremismus
ISiT = Islamismus/islamistischer Terrorismus
RuS = Reichsbürger und Selbstverwalter
AE = Auslandsbezogener Extremismus