



Bundesamt für
Verfassungsschutz

Spionage gegen Deutschland - Aktuelle Entwicklungen -



bfv-themenreihe

Impressum:

Herausgeber: Bundesamt für Verfassungsschutz
Presse- und Öffentlichkeitsarbeit
Merianstraße 100
50765 Köln
E-Mail: pressereferat@verfassungsschutz.de
<http://www.verfassungsschutz.de>

Layout und Satz: Bundesamt für Verfassungsschutz
IT 21.2 PrintCenter

Stand: November 2008

Dieser Text wird im Rahmen der Öffentlichkeitsarbeit des Bundesamtes für Verfassungsschutz herausgegeben. Er darf nicht in einer Weise verwendet werden, die als Parteinahme des Bundesamtes zu Gunsten einzelner politischer Gruppen verstanden werden könnte. Die Verteilung auf Wahlveranstaltungen, an Informationsständen von Parteien wie auch jede sonstige Verwendung zum Zwecke der Wahlwerbung ist untersagt. Den Parteien ist es gestattet, die Schrift zur Unterrichtung ihrer eigenen Mitglieder weiterzugeben.

Auszugsweise Wiedergabe mit Quellenangabe gestattet.

Inhalt	Seite
1. Vorbemerkung	4
2. Hauptträger von Spionageaktivitäten gegen Deutschland	5
2.1 Nachrichtendienste der Russischen Föderation	5
2.2 Nachrichtendienste der Volksrepublik China	7
3. Wirtschaftsspionage und Konkurrenzausspähung	9
4. Gegenmaßnahmen der Verfassungschutzbehörden in Zusammenarbeit mit der Wirtschaft	10

1. Vorbemerkung

Die Bundesrepublik Deutschland ist für die Nachrichtendienste einer Reihe von Staaten ein bedeutendes Aufklärungsziel, wegen ihrer geopolitischen Lage, ihrer wichtigen Rolle in EU und NATO und nicht zuletzt als Standort zahlreicher Unternehmen der Spitzentechnologie mit Weltmarktführung. Hauptträger der Spionageaktivitäten sind derzeit die Russische Föderation und die Volksrepublik China. Darüber hinaus sind auch Nachrichtendienste aus Ländern des Nahen und Mittleren Ostens sowie Nordafrikas zu nennen.

Die Nachrichtendienste dieser Staaten sind in unterschiedlicher Personalstärke an den amtlichen¹ bzw. halbamtlichen² Vertretungen ihrer Staaten in Deutschland präsent und unterhalten so genannte Legalresidenturen³. Die dort abgetarnt als „Diplomaten“ oder „Journalisten“ arbeitenden Nachrichtendienstmitarbeiter betreiben entweder selbst – offen oder verdeckt – Informationsbeschaffung oder leisten Unterstützung bei nachrichtendienstlichen Operationen, die direkt von den Zentralen der Dienste in den Heimatländern durchgeführt werden. Sofern solchen „Diplomaten“ statuswidrige Aktivitäten nachgewiesen werden, kann dies zur Ausweisung der betreffenden Personen aus Deutschland führen.

Die Schwerpunkte nachrichtendienstlicher Beschaffungsaktivitäten orientieren sich an aktuellen politischen Vorgaben oder volkswirtschaftlichen Prioritäten in den jeweiligen Staaten. Die Aufklärungsziele ausländischer Dienste reichen von der Informationsbeschaffung aus Politik, Wirtschaft und Militär bis hin zur Ausspähung und Unterwanderung in Deutschland ansässiger Organisationen und Personen, die in Gegnerschaft zu den Regierungen in ihrem Heimatland stehen. Einen zunehmend breiteren Raum nehmen für einige Dienste Aufklärungsziele in den Bereichen Wirtschaft, Wissenschaft und Forschung ein. Technologisch weniger entwickelte Staaten spähen in erster Linie technisches Know-how aus, um Kosten für Forschung und Entwicklung sowie mögliche Lizenzgebühren einzusparen. Hochentwickelte Staaten interessieren sich demgegenüber eher für Produktideen, komplexe Fertigungstechniken sowie für Unternehmens- und Marktstrategien.

Eine zunehmende Bedeutung gewinnen in diesem Zusammenhang internetbasierte Angriffe auf Computersysteme von Wirtschaftsunternehmen, aber auch von Regierungsstellen. Angesichts der Auswahl der Angriffsziele und der angewandten Methoden ist eine nachrichtendienstliche Steuerung oder Beteiligung in vielen Fällen sehr wahrscheinlich.

Darüber hinaus bemühen sich einige Länder darum, in den Besitz atomarer, biologischer und chemischer Massenvernichtungsmittel und der erforderlichen Trägersysteme zu gelangen. Die Staaten, die Proliferation betreiben, wie Iran und Nordkorea, versuchen, Kontrollmaßnahmen durch Lieferungen über Drittländer und durch die Beschaffung von so genannten „dual use“-Gütern⁴ zu umgehen.

1 Amtliche Vertretungen sind z.B. Botschaften oder Generalkonsulate eines Staates.

2 Halbamtliche Vertretungen sind z.B. Presseagenturen oder Fluggesellschaften eines Staates.

3 Als Legalresidentur bezeichnet man den Stützpunkt eines fremden Nachrichtendienstes, abgetarnt in einer amtlichen oder halbamtlichen Vertretung seines Landes im Gastland.

4 Hierunter versteht man Güter, die sowohl zu zivilen als auch zu militärischen Zwecken genutzt werden können.

2. Hauptträger von Spionageaktivitäten gegen Deutschland

2.1 Nachrichtendienste der Russischen Föderation

Die russischen Nachrichtendienste sind ein stabiler Faktor der nationalen Sicherheitsarchitektur; sie genießen bei der politischen Führung Rückhalt und hohes Ansehen. Die im In- und Ausland beschafften Informationen der Dienste werden bei der Vorbereitung von politischen Entscheidungen berücksichtigt. Sie tragen zur Erfüllung politischer Vorgaben bei und dienen nicht zuletzt dazu, neben den politischen auch die ökonomischen Interessen Russlands vor dem Hintergrund seiner erstarkenden Wirtschaftskraft weltweit voranzutreiben. Die russische Wirtschaft profitiert in erheblichem Maße davon, dass alle Dienste gesetzlich verpflichtet sind, Wirtschaftsspionage zu betreiben.

Insgesamt verfügen die russischen Nachrichtendienste über mehrere hunderttausend Mitarbeiter.

Trotz der gefestigten politischen und wirtschaftlichen Beziehungen zwischen Russland und Deutschland hält die russische Staatsführung daran fest, Spionage gegen unser Land zu betreiben. Im Mittelpunkt der Aufklärungsbemühungen steht nach wie vor der Bereich Politik, es folgen die Bereiche Militär, Wirtschaft, Wissenschaft und Technik.

Einen großen Teil ihres Informationsbedarfes decken die Dienste durch Auswertung offener Quellen (Internet und sonstige Medien, Teilnahme an Messen, öffentlichen Vortragsveranstaltungen usw.). Sie setzen jedoch auch konspirative Beschaffungsmethoden ein, um an besonders hochwertige geschützte Informationen zu gelangen (z.B. Führung von Agenten, elektronische Aufklärung).

Der Inlandsdienst FSB betreibt eine intensive Internetüberwachung in Russland. Zu diesem Zweck müssen alle russischen Anbieter von Internetzugängen dem FSB einen ständigen Zugriff auf den Datenverkehr ermöglichen, der in oder über Russland abgewickelt wird. Auch die Telefongesellschaften des Landes sind verpflichtet, dem Dienst einen permanenten Zugang zu Informationen über Telefonkunden und deren Telefongespräche zu gewähren. Dadurch erhält der FSB die Möglichkeit, Kontakte, deren Intensität sowie den Aufenthalt der Gesprächsteilnehmer zum Zeitpunkt der Telefonate festzustellen und die so gewonnenen Informationen für nachrichtendienstliche Zwecke zu nutzen. Ausländische Staatsangehörige in Russland müssen angesichts dieser Tatsache damit rechnen, bei Telefongesprächen oder bei der Nutzung des Internet in das Blickfeld des FSB zu geraten und gezielt geheimdienstlich überwacht zu werden.

Russische Dienste

- ziviler Auslandsaufklärungsdienst SWR
- militärischer Auslandsaufklärungsdienst GRU
- Inlandsnachrichtendienst FSB

<p>SWR (Akronym für Slushba Wneschnej Raswedkij)</p>	<p>Auslandsdienst (zivil) <u>Aufgaben:</u></p> <ul style="list-style-type: none"> • Aufklärung in den Bereichen Politik, Wirtschaft, Wissenschaft und Technik • Elektronische Fernmeldeaufklärung • Mitwirkung bei der Bekämpfung des internationalen Terrorismus • Bekämpfung der Proliferation • Ausforschung von Zielen / Arbeitsmethoden westlicher Nachrichtendienste <p><u>Personalumfang:</u> mehr als 13.000 Mitarbeiter</p>
<p>GRU (Akronym für Glawnoje Raswediwatelnoje Uprawlenije)</p>	<p>Auslandsdienst (militärisch) <u>Aufgaben:</u></p> <ul style="list-style-type: none"> • Aufklärung des gesamten sicherheitspolitischen und militärischen Spektrums, z.B. <ul style="list-style-type: none"> • Bundeswehr • NATO, sonstige westliche Verteidigungsstrukturen • Bereich militärisch nutzbarer Technologie <p><u>Personalumfang:</u> ca. 12.000 Mitarbeiter</p>
<p>FSB (Akronym für Federalnaja Slushba Besopasnosti)</p>	<p>Inlandsdienst <u>Aufgaben:</u></p> <ul style="list-style-type: none"> • Spionageabwehr (zivil und militärisch) • Extremismus-/Terrorismusbekämpfung • Bekämpfung Organisierter Kriminalität • Sicherung der Staatsgrenze, Grenzkontrolle • Fernmeldesicherheit im Bereich Telekommunikation und Sicherheit in der Informationstechnik <p><u>Personalumfang:</u> mindestens 350.000 Mitarbeiter</p>

2.2 Nachrichtendienste der Volksrepublik China

China versteht sich als sozialistischer Staat mit einem Machtmonopol der „Kommunistischen Partei Chinas“ (KPCh). Personen, die ihre Opposition zu Partei oder Regierung öffentlich äußern, setzen sich der Gefahr von Repressionen aus. Alle Aktivitäten, die sich aus Sicht der Staatsführung gegen die KPCh, die Einheit des Staates (z.B. durch Autonomiebestrebungen in Tibet) richten, werden rigoros verfolgt.

Zur Aufrechterhaltung der inneren Ordnung und der Stabilität des Regimes sowie zur Durchsetzung politischer und ökonomischer Interessen unterhalten Partei und Regierung einen gewaltigen Sicherheitsapparat. Mit dem Ministerium für Staatssicherheit (MSS) verfügt China über einen der weltweit größten Sicherheits- und Aufklärungsdienste.

Die guten Beziehungen zwischen China und Deutschland sowie die exportorientierte deutsche Wirtschaft begünstigen seit Jahren einen intensiven, in aller Regel aber auch einseitigen Abfluss von Know-how aus allen Hochtechnologiebereichen in Richtung China. Das Bestreben, bis zum Jahr 2020 den USA wirtschaftlich und militärisch auf Augenhöhe gegenüberzutreten zu können, soll durch Beschaffung von Spitzentechnologie aus dem Westen gelingen. Daher versucht China auch am Hochtechnologiestandort Deutschland auf vielfältigen Wegen entsprechendes Know-how zu beschaffen, um so die in vielen Bereichen noch bestehenden erheblichen Technologielücken zu schließen. Hierbei spielen die chinesischen Nachrichtendienste eine wichtige Rolle.

Die sich in Deutschland aufhaltenden chinesischen Fachkräfte, insbesondere postgraduierte Studenten, Austauschwissenschaftler, Praktikanten sowie bereits eingebürgerte Personen chinesischer Abstammung bilden aus chinesischer Sicht eine besonders gute Basis zur Informationsgewinnung. Dieser Personenkreis fühlt sich seiner Heimat häufig eng verbunden – das nutzen die Nachrichtendienste aus. Erleichtert wird die Informationsabschöpfung dieser so genannten Non-Professionals auch durch den hohen Organisationsgrad der chinesischen Diaspora in Deutschland, die sich in zahlreichen Vereinen - zumeist unter Förderung und Kontrolle der amtlichen chinesischen Vertretungen – zusammengeschlossen hat.

Zu einer besonderen Gefahr haben sich die E-Mail-basierten elektronischen Angriffe auf Netzwerke von Behörden und Unternehmen entwickelt. Sie erfolgen in der Regel unbemerkt und risikolos vom Boden des angreifenden Landes aus. Nach Einschätzung von Fachleuten haben die meisten der derzeit festgestellten elektronischen Angriffe ihren Ursprung in China, vieles deutet auf eine Steuerung durch chinesische Nachrichtendienste hin.

Chinesische Dienste

- ziviler In- und Auslandsaufklärungsdienst MSS
- militärischer In- und Auslandsaufklärungsdienst MID

<p>MSS (Ministry of State Security)</p>	<p>In- und Auslandsdienst (zivil) <u>Aufgaben:</u></p> <ul style="list-style-type: none">• Gewährleistung der Inneren Sicherheit (Überwachung von Oppositionellen und separatistischen Bewegungen)• Spionageabwehr• Weltweite Auslandsaufklärung, insbesondere in den Bereichen<ul style="list-style-type: none">• Politik• Wirtschaft• Wissenschaft und Technik• Forschung• Randbereiche des Militärwesens
<p>MID (Military Intelligence Department)</p>	<p>In- und Auslandsdienst (militärisch) <u>Aufgaben:</u></p> <ul style="list-style-type: none">• Weltweite Auslandsaufklärung mit menschlichen Quellen<ul style="list-style-type: none">• in allen Bereichen mit militärischem Bezug• in den Bereichen Politik und Wirtschaft• Überwachung von Oppositionellen und separatistischen Bewegungen• Aufklärung der weltweiten Telekommunikation und Fernmeldesicherheit der nationalen Netze• Kontrolle des diplomatischen Fernmeldeverkehrs der ausländischen Botschaften im Inland

3. Wirtschaftsspionage und Konkurrenzausspähung

Seit jeher gehört die Wirtschaft zu den klassischen Aufklärungszielen der Nachrichtendienste. Nicht zuletzt auch deshalb, weil eine funktionierende Ökonomie eine der Grundvoraussetzungen für die innere Stabilität von Staaten ist.

Angesichts der verschärften Konkurrenzsituation auf dem Weltmarkt gewinnen sowohl die Wirtschaftsspionage als auch ihre erfolgreiche Abwehr an Bedeutung. Dies gilt in besonderem Maße für ein Land wie Deutschland, das seinen Reichtum nicht in erster Linie Rohstoffen und Bodenschätzen verdankt, sondern den innovativen Fähigkeiten seiner Menschen und Unternehmen. Unser Land muss Maßnahmen treffen, um technologisches und unternehmerisches Know-how zu schützen. Es muss Konzepte entwickeln, die Ausspähungsgefahren minimieren und ein gemeinsames Handeln von Behörden und Unternehmen in Sicherheitsfragen gewährleisten. Die Verfassungsschutzbehörden leisten hierzu durch enge Zusammenarbeit mit Unternehmen und Wirtschaftsverbänden ihren Beitrag.

Die Regelungen in den Verfassungsschutzgesetzen erfordern eine Unterscheidung zwischen Wirtschaftsspionage und Konkurrenzausspähung. Unter Wirtschaftsspionage verstehen wir ausschließlich die staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben. Nur diese Art der Ausforschung fällt unter den Begriff der geheimdienstlichen Agententätigkeit, deren Aufklärung und Abwehr den Verfassungsschutzbehörden als gesetzliche Aufgabe zugewiesen ist. Konkurrenzausspähung (synonym werden die Begriffe Konkurrenzspionage oder Industriespionage verwandt) betreiben Unternehmen auf nationaler und internationaler Ebene untereinander. In der Praxis ähneln sich die Vorgehensweisen, sodass der Auftraggeber der jeweiligen Ausforschung oft erst in einem späteren Stadium identifiziert werden kann. Für die betroffenen Unternehmen ist die Unterscheidung zwischen Wirtschafts- und Konkurrenzspionage allenfalls akademischer Natur. Sie fordern immer wieder, dass den Verfassungsschutzbehörden im Interesse eines umfassenden staatlichen Wirtschaftsschutzes auch eine Zuständigkeit zur Abwehr von Konkurrenzspionage übertragen wird.

4. Gegenmaßnahmen der Verfassungsschutzbehörden in Zusammenarbeit mit der Wirtschaft

Die Spionageabwehr gehört zu den Kernkompetenzen des Verfassungsschutzes. Aufklärung und Analyse politischer und militärstrategischer Spionage fremder Staaten sind auch für die Abwehr von Wirtschaftsspionage von hohem Nutzen. Elementare Voraussetzung für eine erfolgreiche Gefahrenabwehr ist ein Problembewusstsein bei den gefährdeten Unternehmen (hierbei handelt es sich keineswegs nur um Großkonzerne, sondern auch um eine Vielzahl innovativer klein- und mittelständischer Unternehmen). Die „Global Player“ sind sich der Gefahren der Ausspähung durch fremde Nachrichtendienste oder Konkurrenten bewusst und haben in ihren Sicherheitsabteilungen Abwehrkonzepte und Programme entwickelt, die den Eintritt eines Schadensfalles verringern sollen. Kleinen und mittleren Unternehmen fehlen dagegen oft Erfahrung, personelle Ressourcen und finanzielle Möglichkeiten, um Firmengeheimnisse effektiv gegen unbefugten Zugriff zu schützen.

Die Bundesregierung räumt dem Schutz der heimischen Wirtschaft einen hohen Stellenwert ein. Vor diesem Hintergrund hat das Bundesministerium des Innern aktuell die „Rahmenregelung für die Zusammenarbeit mit der gewerblichen Wirtschaft auf Bundesebene in Sicherheitsfragen“ aktualisiert und weiterentwickelt. Im Ergebnis der Überarbeitung wurde der Kreis der zuliefernden Partner erweitert. Sie prüfen vorliegende Sicherheitserkenntnisse auf ihre Relevanz für die Wirtschaft, leiten diese nach Maßgabe der Kooperationskonzepte an die Wirtschaftsunternehmen weiter und stehen ihnen als Ansprechpartner und als Unterstützer z.B. bei Fachveranstaltungen zur Verfügung. Zusätzlich wurde im Rahmen einer Private-Public-Partnership der „Ressortkreis Wirtschaftsschutz“ gegründet, dem neben Vertretern verschiedener Bundesministerien auch Vertreter von Nachrichtendiensten des Bundes sowie Vertreter von Polizei- und Zollbehörden auf Bundesebene angehören. In diesem Gremium werden Informationen und Erkenntnisse der Bundesregierung zum Thema Wirtschaftsspionage gebündelt und bewertet. Im partnerschaftlichen Dialog mit der Wirtschaft sollen Gegenmaßnahmen entwickelt und koordiniert werden. Besonderer Wert wird dabei auf die Effizienz der Kommunikationswege und des Informationsaustausches zwischen den Sicherheitsbehörden und der Wirtschaft gelegt.

Dem Ressortkreis wird künftig eine gemeinsame Berichtsplattform zum verstärkten internen Informationsaustausch dienen. Gleichzeitig sollen damit auch die Information deutscher Unternehmen über Risiken der Wirtschaftsspionage und Möglichkeiten zu deren Abwehr intensiviert werden.

Die „Rahmenregelung“ ist im Übrigen die Basis der Kooperation zwischen der „Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V. (ASW)“⁵, dem

5 Die ASW fungiert als Zentralorganisation der Wirtschaft in Sicherheitsfragen. Sie wird getragen von den Spitzenorganisationen der deutschen Wirtschaft (DIHK, BDI, BDA), allen deutschen regionalen Sicherheitsverbänden (VSWn) sowie mehreren Branchenverbänden. Die Mitgliedsorganisationen der ASW repräsentieren über vier Millionen Unternehmen und Selbständige und vertreten deren gemeinsame Sicherheitsinteressen.

BfV und anderen staatlichen Institutionen.

Zielsetzung beider Strukturen ist es, die Strategien im Bereich des Wirtschaftsschutzes an die gestiegene Bedrohung anzupassen und künftig im engen Dialog stetig zu evaluieren. Dieses Konzept ist integraler Bestandteil der „Sicherheitspartnerschaft zwischen Staat und Wirtschaft“. Die erforderliche sicherheitspolitische Mitwirkungskomponente von Wirtschaftsunternehmen wurde so neu gestaltet.

Es liegt im gemeinsamen Interesse von Staat und Wirtschaft, dass die Verfassungsschutzbehörden ihre Erkenntnisse in Bezug auf Wirtschaftsspionage so detailliert wie möglich an deutsche Unternehmen weitergeben, um sie über die von fremden Diensten ausgehenden Gefahren zu informieren und in den Stand zu versetzen, Sicherheitsrisiken möglichst klein zu halten.

Das BfV als zentrale Nachrichtensammel- und Analysestelle übermittelt der ASW kontinuierlich Beiträge, die für die Sicherheit der Wirtschaft relevant sind. Es stellt zudem Analysen, Referenten und Hilfsmittel zur Verfügung, u.a. für Befragungen der Arbeitskreise der Sicherheitsbevollmächtigten der Wirtschaft oder für überregionale Fachveranstaltungen von Firmen. Darüber hinaus führen BfV und ASW gemeinsame Sicherheitssymposien mit unterschiedlichen Themenschwerpunkten durch. Um die bewährte Kooperation zu festigen und zu intensivieren, sind diverse weitere Maßnahmen geplant.

Im Rahmen der Öffentlichkeitsarbeit zur Abwehr von Wirtschaftsspionage hat das BfV sein Informationsangebot deutlich ausgeweitet. Neben der Einrichtung einer eigenen Rubrik im Internetangebot des BfV zählt hierzu ein erstmals im Oktober 2008 veröffentlichter Newsletter. In Zusammenarbeit mit den Landesbehörden für Verfassungsschutz wurde die Broschüre „Wirtschaftsspionage: Risiko für Ihr Unternehmen“ veröffentlicht. Zudem präsentierte man sich gemeinsam mit einem Stand auf der Messe „Security 2008“ in Essen.

Im BfV erarbeitete Sensibilisierungskonzepte sollen mit der ASW abgestimmt und gemeinsam auf spezielle Zielgruppen in der Wirtschaft zugeschnitten werden. Durch einen stetigen wechselseitigen Informationsaustausch über Angriffsmethoden fremder Nachrichtendienste oder konkurrierender Unternehmen können sicherheitsrelevante Informationen kanalisiert und den Wirtschaftsunternehmen zeitnah für strategische Entscheidungen zur Verfügung gestellt werden. Die Qualität der Beratungstätigkeit durch den Verfassungsschutz beruht in starkem Maße darauf, welche Informationen die durch Wirtschaftsspionage betroffenen Unternehmen dem Verfassungsschutz zur Verfügung stellen. Nur wenn Verdachts- und Schadensfälle mitgeteilt werden, können daraus qualifizierte Schlussfolgerungen gezogen und diese Erfahrungen zur Warnung, Beratung und Sensibilisierung der bislang noch nicht betroffenen Unternehmen genutzt werden.

Da wir besonders auf den Schutz unserer Quellen achten und - anders als die

Polizei - nicht dem Legalitätsprinzip unterliegen, können wir unseren Hinweisgebern Vertraulichkeit zusichern. Keine der Firmen, die sich wegen möglicher Ausforschungen an die Spionageabwehr wendet, muss befürchten, dass die zur Verfügung gestellten Informationen ohne ihr Wissen und Wollen publik gemacht werden und sich womöglich negativ auf das Firmenimage auswirken. Die Verfassungsschutzbehörden stehen jederzeit für Beratungsgespräche zur Verfügung.

Vor diesem Hintergrund werben wir immer wieder um Verständnis bei den deutschen Wirtschaftsunternehmen: Nicht nur fremde Nachrichtendienste sammeln eine Fülle von unterschiedlichen Informationsbruchstücken, um diese zu einem Gesamtbild über ihr Aufklärungsziel zusammenzufügen. Auch die Spionageabwehr benötigt detaillierte Informationen, aktuelle und profunde Kenntnisse über Methoden und Ziele der Angreifer, um Gefahrenanalyse betreiben und Abwehrstrategien entwickeln zu können. Ohne vertrauensvolle Zusammenarbeit zwischen Verfassungsschutzbehörden und Wirtschaftsunternehmen können wir dieses Ziel nicht erreichen.