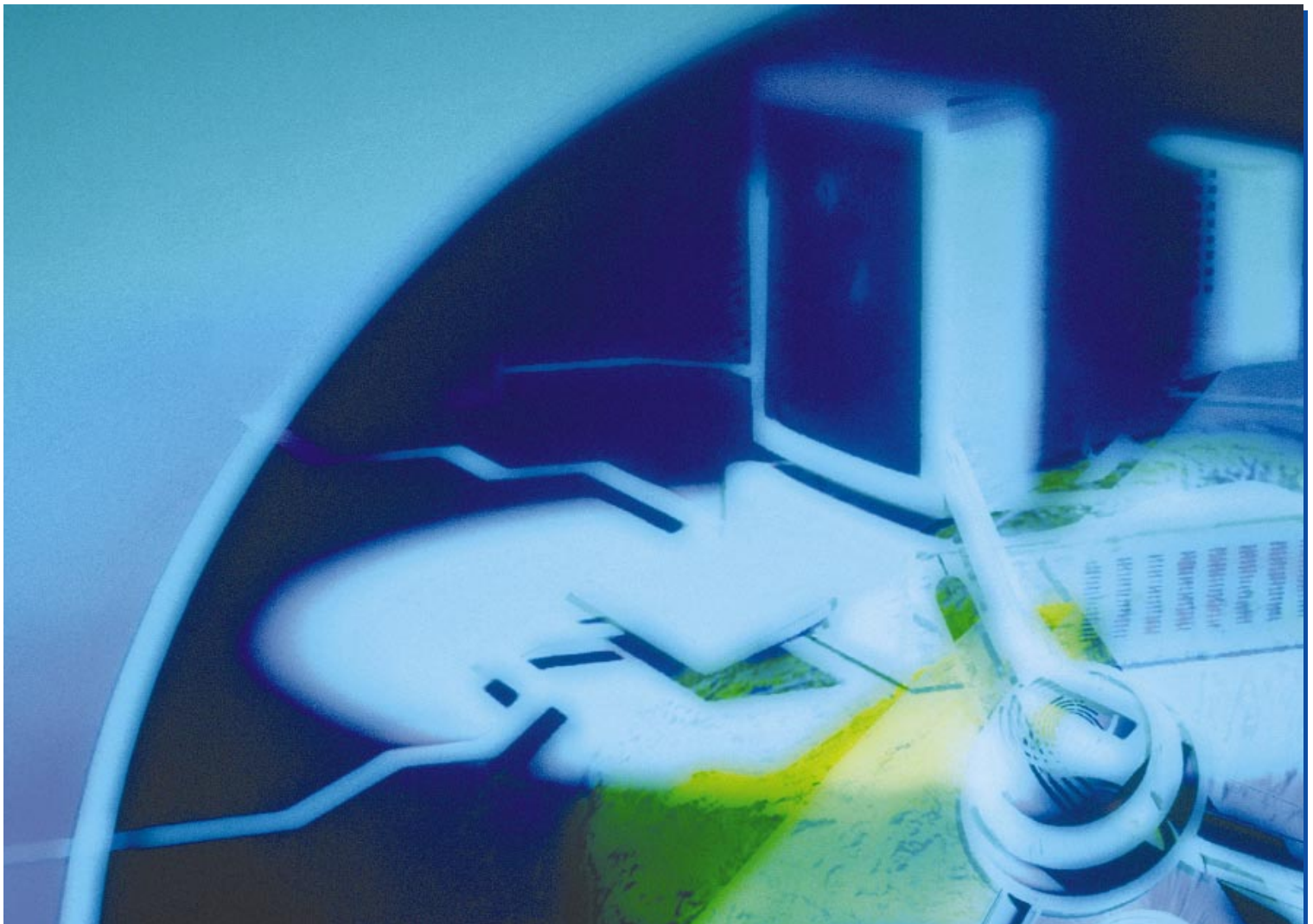


Wirtschaftsspionage

Information und Prävention

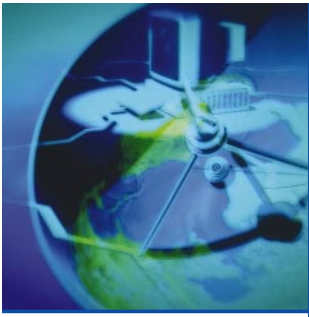


IMPRESSUM

Herausgeber:
Bundesamt für
Verfassungsschutz für die
Verfassungsschutzbehörden in
Bund und Ländern

Druck:
Vereinigte Verlagsanstalten,
Düsseldorf

Stand: Januar 2002



WIRTSCHAFTSSPIONAGE

Staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben. (Dieser Bereich nachrichtendienstlicher Tätigkeit ist Aufgabe der Spionageabwehr der Verfassungsschutzbehörden.)

KONKURRENZAUSSPÄHUNG

(umgangssprachlich Industriespionage)

Ausforschung, die ein (konkurrierendes) Unternehmen gegen ein anderes betreibt.

Hiervon abzugrenzen ist die

PROLIFERATION

d.h. Weiterverbreitung von Massenvernichtungswaffen bzw. der zu ihrer Herstellung verwendeten Produkte – einschließlich des dafür erforderlichen Know-how – sowie von entsprechenden Waffenträgersystemen.

Inhalt

1. Gefährdung der Wirtschaft	4
2. Das Know-how der deutschen Wirtschaft weckt Begehrlichkeiten	6
3. Nachrichtendienste als Träger der Wirtschaftsspionage	8
3.1 Slushba Wneschnej Raswedkij (SWR)	10
3.2 Glawnoje Raswedywatelnoje Uprawlenije (GRU)	11
3.3 Federalnaja Slushba Besopasnosti (FSB)	11
3.4 Federalnoje Agenstwo Prawitelstvennoj Swjasi i Informazij (FAPSI)	12
3.4 Guojia Anaquaanbu	13
3.5 Zhong Chan er Bu	13
3.7 Dienste von Krisenländern	13
4. Wirtschaftsspionage westlicher Dienste?	14
5. Methoden der Wirtschaftsspionage	16
5.1 Quellen im Objekt	18
5.2 Abschöpfungsquellen	18
5.3 Spionage aus Legalresidenturen	19
5.4 Tarnung als Mitarbeiter wirtschaftlicher Unternehmen	19
5.5 Gefährdung deutscher Unternehmen im Ausland	20
5.6 Austauschwissenschaftler und Praktikanten	21
5.7 Proliferation	21
6. Instrumente zur Bekämpfung von Wirtschaftsspionage und Konkurrenzausspähung	22
7. Goldene Regeln der Prävention	25
8. Ihre Ansprechpartner	26



1. Die Gefährdung der Wirtschaft durch Spionage



Unsere Unternehmen sind die tragende Säule des wirtschaftlichen Fortschritts und des Wohlstandes in Deutschland. Sie vor Angriffen fremder Nachrichtendienste zu schützen, ist eine wichtige Aufgabe des Verfassungsschutzes in Bund und Ländern. Aufgrund jahrzehntelanger Erfahrung auf dem Gebiet der Spionageabwehr ist dieser daher ein **kompetenter Gesprächspartner und Berater für die Wirtschaft.**

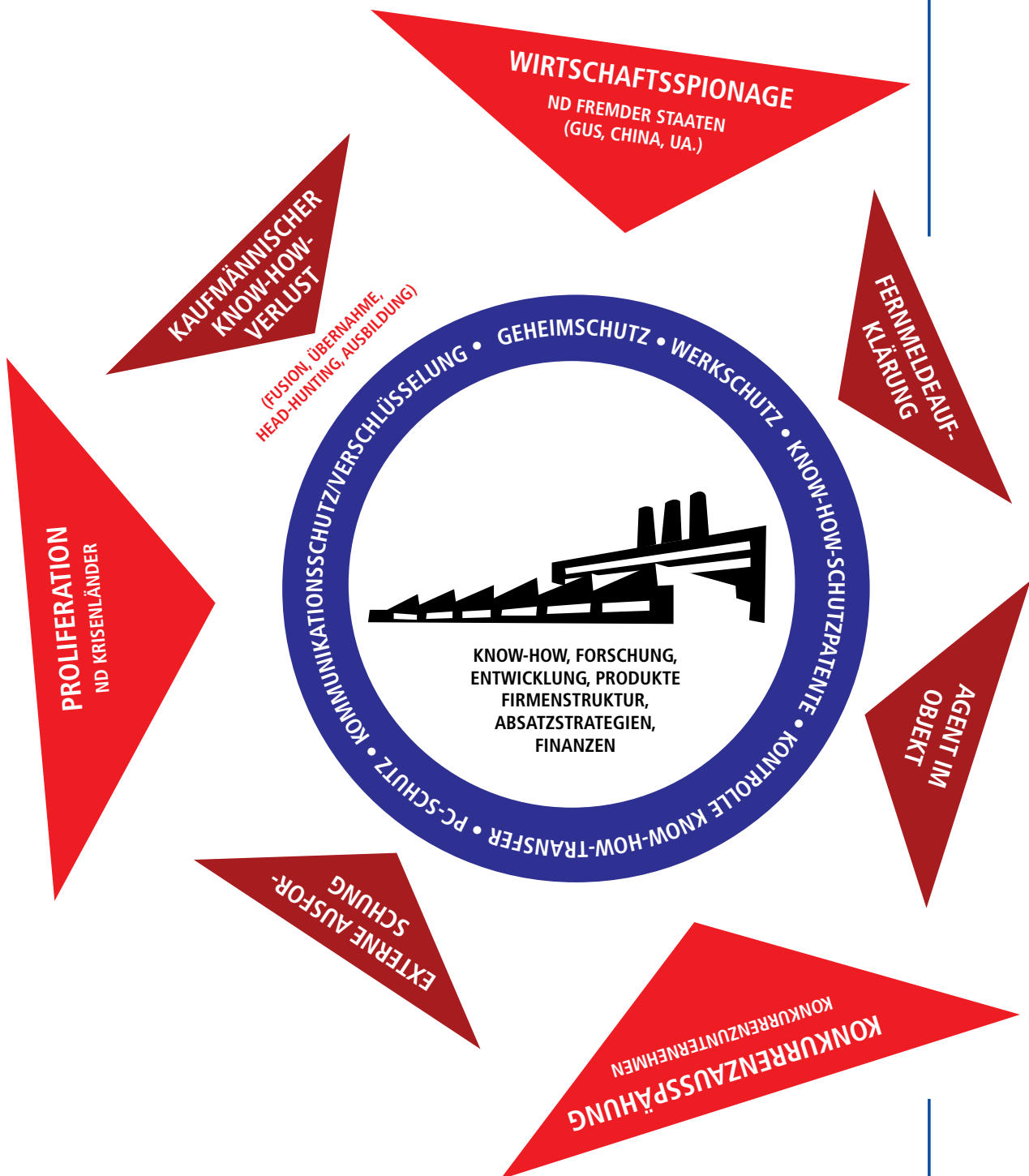
Bereits seit Jahren arbeitet der Verfassungsschutz bundesweit mit über 1500 Unternehmen im Rahmen des vorbeugenden Geheimschutzes erfolgreich zusammen - darüber hinaus aber auch mit einer Vielzahl weiterer Firmen in Beratungs-, Verdachts- und Spionagefällen.

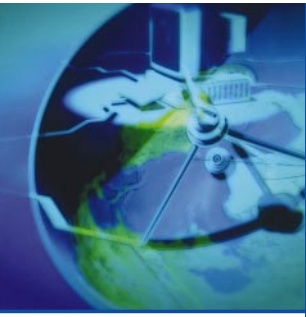
Der Verfassungsschutz kann den betroffenen Unternehmen aber nur helfen, wenn ihm vorhandene Verdachtsmomente **so frühzeitig wie möglich** mitgeteilt werden. Da die Verfassungsschutzbehörden im Gegensatz zur Polizei nicht dem Legalitätsprinzip¹ sondern dem Opportunitätsprinzip² unterliegen, können sie im Rahmen der gesetzlichen Möglichkeiten Hinweise vertraulich behandeln und der gewerblichen Wirtschaft partnerschaftliche Hilfe anbieten.

¹ Legalitätsprinzip: Gesetzmäßigkeitsgrundsatz; Strafverfolgungsbehörden sind prinzipiell verpflichtet, bei Vorliegen tatsächlicher Anhaltspunkte Straftaten zu verfolgen.

² Opportunitätsprinzip: Ermessensgrundsatz; eine Strafverfolgung kann unterbleiben.

Diese Broschüre will die Verantwortlichen in den Unternehmen für die Gefahren der Wirtschaftsspionage sensibilisieren, über Methoden und Ziele informieren und Hilfeleistung anbieten, um Schäden zu vermeiden.





2. Das Know-how der deutschen Wirtschaft weckt Begehrlichkeiten

Über die Bedeutung der Wirtschaftsspionage wird in den Medien und der Politik heftig diskutiert. Dies geschieht besonders vor dem Hintergrund der zunehmenden Globalisierung von Wirtschaft und Technologie bei gleichzeitiger Verschärfung des internationalen Wettbewerbs. Der Blick richtet sich dabei in erster Linie auf die Dienste der Nachfolgestaaten der ehemaligen Sowjetunion.

In Russland und der Ukraine sind die Dienste gesetzlich verpflichtet, die Wirtschaft ihres Landes zu unterstützen. Aber auch Nachrichtendienste anderer Staaten sollen angeblich Wirtschaftsspionage betreiben, um die eigene Wirtschaft zu fördern. Für die in den letzten Jahren wiederholt in der Öffentlichkeit auch gegen verbündete Staaten erhobenen Vorwürfe gibt es allerdings keinerlei Belege.


In der öffentlichen Diskussion wird häufig nicht zwischen Wirtschaftsspionage und der Konkurrenzausspähung ("Industriespionage") unterschieden. Es ist daher zunächst eine **Abgrenzung** erforderlich.

Bei **Konkurrenzausspähung** handelt es sich um die **Ausforschung, die ein (konkurrierendes) Unternehmen gegen ein anderes** betreibt.

Unter **Wirtschaftsspionage** ist demgegenüber **nur die staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben** zu verstehen. Dieser Bereich nachrichtendienstlicher Tätigkeit ist Aufgabe der Spionageabwehr der Verfassungsschutzbehörden.

Aufklärung und Gegenmaßnahmen schützen natürlich auch vor Konkurrenzausspähung.

Wirtschaftsspionage hat keine einheitlichen Ziele. Sie konzentriert sich auch nicht allein auf hochsensible Informationen oder Neuentwicklungen. Vielmehr richten sich die **Aufklärungsziele und Methoden nach dem jeweiligen technologischen Stand der handelnden Staaten**. So verfolgen hochentwickelte Industriestaaten gegenüber ihren Konkurrenten mit dem gleichen Standard andere Ziele als technologisch weniger entwickelte Staaten, die einen Rückstand aufholen und technisch gleichziehen wollen.



Die Interessen hochentwickelter Staaten richten sich insbesondere auf:

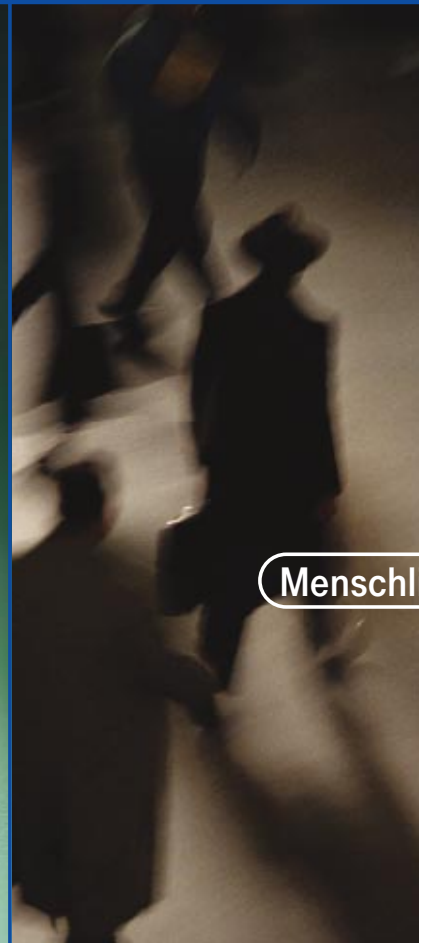
- Unternehmens- und Marktstrategien
- Wettbewerbsstrategien, Preisgestaltung und Konditionen, insbesondere bei großen Ausschreibungen
- Zusammenschlüsse und Absprachen von Unternehmen
- Informationen über Entscheidungsprozesse im Unternehmen
- Informationen über Manager und deren unmittelbare Mitarbeiter

Die Ziele technisch weniger entwickelter Staaten liegen eher in den folgenden Bereichen:

- Die Beschaffung von technischem Know-how, um Kosten für eigene Entwicklungen oder Lizenzgebühren zu sparen
- Beschaffung von Informationen über Fertigungstechniken, um auf dem Markt mit kostengünstigeren Nachbauten konkurrenzfähig zu sein



3. Nachrichtendienste als Träger der Wirtschaftsspionage



Auslandsaufklärung wird von fast allen Staaten der Welt betrieben, um politische Entscheidungen vorzubereiten oder weltwirtschaftliche Lagebilder zu erstellen. Neben offen zugänglichen Informationen werden hierzu auch verdeckt gewonnene nachrichtendienstliche Erkenntnisse z.B. aus der Fernmeldeaufklärung, von Satellitenfotos sowie aus der Abschöpfung menschlicher Quellen genutzt.



lische Quellen

Satellitenfotos

Einige **Auslandsaufklärungsdienste** haben aber auch die Aufgabe, die Wirtschaft ihres Landes unmittelbar zu unterstützen, indem sie für die Unternehmen ihres Heimatlandes Informationen beschaffen, die diesen sonst nicht oder nur mit erheblichem finanziellen Aufwand zugänglich wären. In einigen Ländern sind neben den Auslandsaufklärungsdiensten auch die **Inlandsdienste** - also die klassischen Abwehrdienste - mit dieser Aufgabe betraut.

In den letzten Jahren kommt der sogenannten **“Fernmelde- und elektronischen Aufklärung”** auch im Rahmen der Wirtschaftsspionage eine immer größere Bedeutung zu. Hierzu zählen das Abhören von Telefonen sowie das Mitlesen von Fernschreiben, Faxen und anderen Datenströmen. Die technischen Voraussetzungen sind schon lange gegeben, aber erst der Einsatz leistungsstarker Computer mit der Fähigkeit, durch automatisierte Suche nach Schlüsselworten eine bearbeitbare Vorauswahl zu treffen, ermöglicht den breiteren Einsatz dieses Spionageinstrumentes. Es darf dabei aber nicht übersehen werden, dass wegen der ungeheuren, kaum darstellbaren Masse der Datenströme eine lückenlose Überwachung nicht möglich ist.



Die weltweiten nachrichtendienstlichen Möglichkeiten zur Überwachung von Telekommunikation sind Realität. Jedem Nutzer moderner Kommunikationsmedien muss bei deren unverschlüsselter Benutzung bewusst sein, dass er abgehört werden kann und somit schutzbedürftige Informationen gefährdet sind. Ein individueller, auf die konkreten Bedürfnisse des Nutzers zugeschnittener **Schutz der Informationstechnik (IT) ist daher unerlässlich.**

Für seine Konzeption stehen als Ansprechpartner auch die Behörden für Verfassungsschutz zur Verfügung.

Einige der wichtigsten Dienste, die Wirtschaftsspionage betreiben, werden nachfolgend beispielhaft vorgestellt:

3.1 „Slushba Wneschnej Raswedkij“ (SWR)

Der zivile russische Aufklärungsdienst ist aus der 1. Hauptverwaltung des aufgelösten sowjetischen Staatssicherheitsdienstes KGB entstanden. Aufgabenschwerpunkte des Dienstes sind u.a. die politische, die wissenschaftlich-technologische und die ökonomische Aufklärung. Im Mai 2000 wurde die Leitung des Dienstes, der ca. 15.000 Mitarbeiter beschäftigt, dem Deutschlandexperten General Sergej Lebedew übertragen. Lebedew war im Zeitraum zwischen 1979 und 1995 über 13 Jahre als operativer Geheimdienststoffizier der sowjetischen - später russischen - Auslandsaufklärung auf diplomatischen Tarndienstposten bei russischen Auslandsvertretungen in Deutschland eingesetzt.



3.2 „Glawnoje Raswedywatelnoje Uprawlenije“ (GRU)

Die „Hauptverwaltung Aufklärung“, die am 5. November 1998 ihren achtzigsten Geburtstag feierte, ist als militärischer Auslandsaufklärungsdienst dem russischen Verteidigungsministerium unterstellt. Schwerpunktmäßig beschafft die GRU militärpolitische, strategische, taktische und geografische Informationen. Daneben versucht sie in den Zielländern Kenntnisse über militärisch nutzbare wissenschaftliche oder technologische Produkte oder Produktinformationen aus der Rüstungstechnik zu erlangen. Ebenfalls von Interesse sind Informationen über zivile Produkte mit militärischen Anwendungsmöglichkeiten. Die GRU beschäftigt derzeit etwa 12.000 Mitarbeiter.

3.3 „Federalnaja Slushba Besopasnosti“ (FSB)

Der russische Inlandsdienst „Föderaler Sicherheitsdienst“ ist über seine Abwehrzuständigkeiten hinaus gesetzlich befugt, Auslandsaufklärung zu betreiben.

Der FSB soll seit etwa März 2000 innerhalb Russlands eine umfangreiche Internet-Überwachung durchführen. Es ist daher nicht auszuschließen, dass er Kenntnis über die Internet-Kommunikation in Russland tätiger ausländischer Investoren, Firmen und deren Mitarbeiter hat. Dies schließt Pager-Nachrichten, E-Mails, Videokonferenzen und Telefonate ein. Eine besondere Gefährdung ergibt sich auch daraus: Es muss davon ausgegangen werden, dass der Überwachung durch den FSB auch jede Internet-Kommunikation unterliegt (SORM II[Ⓢ]), die über russische Provider abgewickelt wird. Da dies oftmals durch den User nicht beeinflussbar ist, kann nur eine generelle Sensibilität für diese Problematik und der Einsatz geeigneter Schutzprogramme vor Schaden bewahren.

Ⓢ Das russische Überwachungsgesetz SORM II (Sistema Operativno-Rozysknykh Meropriyatii) ist seit Juli 1998 in Kraft. Aufgrund des Gesetzes müssen Internetprovider auf eigene Kosten eine Überwachungsschnittstelle mit einer Glasfaserverbindung zum russischen Geheimdienst FSB einrichten. Dem FSB wird so die Echtzeitüberwachung des gesamten Internetverkehrs in und über Russland ermöglicht.



3.4 „Federalnoje Agenstwo Prawitelstvennoj Swjasi i Informazij“ (FAPSI)

Die russische “Föderale Agentur für Regierungsfernmeldewesen und Information” betreibt eine intensive Fernmeldeaufklärung.

Sie entstand aus verschiedenen Organisationseinheiten des aufgelösten KGB. Zu ihren Aufgaben gehört die planmäßige Überwachung, Aufzeichnung und Entschlüsselung des internationalen Fernmeldeverkehrs bzw. der drahtlosen Telekommunikation mit Hilfe moderner Nachrichtentechnik. Im Abwehrbereich ist der Dienst für technische Bereitstellung und den Betrieb wichtiger staatlicher Nachrichtenverbindungen, z.B. der Regierung und der Armee, sowie für Schutzmaßnahmen gegen Abhörversuche verantwortlich.

Auch in die kommerzielle Nutzung von Nachrichtentechnik ist FAPSI einbezogen. Sie erteilt Betreiberlizenzen für Kommunikationstechnik, ist für die Vergabe der Funkkanäle und Frequenzen, z.B. bei Banken und Industrieunternehmen, zuständig und muss den Einsatz von Verschlüsselungsverfahren genehmigen. Dazu wird im Rahmen “normaler” Geschäftsbeziehungen versucht, modernste Technik im Ausland zu beschaffen.

Bei Messen tritt FAPSI als Aussteller und Anbieter selbstentwickelter Produkte - vornehmlich Soft- und Hardware aus dem Bereich Datensicherheit und Verschlüsselung - auf. So können Kontakte zu Firmen und Unternehmen geknüpft werden, ohne dass die nachrichtendienstliche Zielrichtung erkennbar wird.

Unter Einbeziehung der dem Dienst unterstehenden russischen Fernmeldetruppen verfügt FAPSI über eine Personenstärke von ca. 120.000 Mitarbeitern.



3.5 „Guojia Anaqaanbu“

Das chinesische Ministerium für Staatssicherheit untersteht dem Staatsrat und ist als ziviler Dienst sowohl für die innere Sicherheit als auch für die Auslandsaufklärung zuständig.

Die Auslandsaufklärung beschafft weltweit Informationen u.a. auch aus den Bereichen Wissenschaft und Wirtschaft. Hierzu zählen auch Informationen, die nicht offen zugänglich und besonders sensibel sind. Ausgangspunkt solcher Spionageaktivitäten sind oftmals „Legalresidenturen“^④ in diplomatischen und konsularischen Vertretungen sowie Luftfahrtgesellschaften, Außenhandelsunternehmen, Presseagenturen, chinesische Firmen und deutsch-chinesische Jointventures.

3.6 „Zhong Chan Er Bu“

Der chinesische militärische Informationsdienst ist ständig bemüht, vielfältige Kontakte im Einsatzland zu knüpfen und Informationen zu sammeln, die u.a. für die Fortentwicklung der chinesischen Rüstung von Bedeutung sind.

3.7 Dienste von Krisenländern^⑤

Die Dienste der Krisenländer befassen sich hauptsächlich mit der Unterstützung der Proliferation und der Ausforschung der in Opposition zum jeweiligen Regime stehenden im Ausland lebenden Staatsangehörigen. Doch sind sie teilweise auch auf dem Gebiet der Wirtschaftsspionage tätig, wobei die Grenzen fließend sind. Die Dienste dieser Länder schöpfen durch Studenten, Austauschwissenschaftler, Praktikanten und die Teilnahme an Kongressen und Seminaren auch illegal Know-how ab.

^④ Legalresidenturen: zu Spionagezwecken missbrauchte diplomatische Einrichtungen oder unter staatlicher Kontrolle stehende Medien- und Wirtschaftseinrichtungen.

^⑤ Krisenländer: Es handelt sich um Länder, von denen zu befürchten ist, dass von dort aus ABC-Waffen in einem bewaffneten Konflikt eingesetzt werden oder ihr Einsatz zur Durchsetzung politischer Ziele angedroht wird. Derzeit Iran, Irak, Libyen, Syrien, Nordkorea, Pakistan, Indien (in der Literatur teilweise auch als Schwellenländer und/oder besorgniserregende Staaten bezeichnet).



4. Wirtschaftsspionage westlicher Dienste?



Meldungen und Berichte in den Medien sowie Äußerungen von Politikern gehen davon aus, dass auch westliche Länder Wirtschaftsspionage betreiben. Belege für eine Wirtschaftsspionage westlicher Dienste liegen bisher nicht vor. Weder in den Verfassungsschutzgesetzen des Bundes und der Länder noch in den Strafvorschriften wegen Spionage wird nach der Himmelsrichtung unterschieden, aus der diese Aktivitäten erfolgen. Die Abwehrbehörden sprechen daher auch von dem ihnen eigenen **“360°-Blick”**.

So wird seit Jahren über ein unter der Bezeichnung ECHELON bekanntes Fernmelde-Aufklärungssystem diskutiert, an dem mehrere Staaten beteiligt sein und mit dessen Hilfe insbesondere die USA ihre eigenen Unternehmen mit internen Daten ausländischer Unternehmen versorgen sollen. Der wegen dieser Vorwürfe eingesetzte Nichtständige Ausschuss des Europäischen Parlaments kommt in seinem Bericht vom 11.07.2001 zu dem Schluss, dass an der Existenz eines derartigen Fernaufklärungssystems und dessen Einsatz im Rahmen der strategischen Aufklärung nicht zu zweifeln sei. Bei aller Gefahr, die diese Art der Aufklärung für den Informationsaustausch per elektronischer IT bedeutet und vor der dringend Schutz benötigt wird, werden ECHELON nach Meinung des Ausschusses weit überschätzte Fähigkeiten zugeschrieben. Es gebe keinen belegten Fall für Wirtschaftsspionage; die USA seien auch aus rechtlichen und politischen Gründen gehindert, ihre einheimischen Unternehmen mit mehr oder weniger zufällig aufgefangenen Informationen zu versorgen.

Der Ausschuss ist des weiteren zu folgendem Ergebnis gelangt:

- Wirtschaftsspionage setze hauptsächlich vor Ort oder am mobilen Arbeitsplatz an, da sich mit wenigen Ausnahmen die gesuchten Informationen nicht durch Abhören der internationalen Telekommunikationsnetze finden ließen.
- Mit der strategischen Kontrolle internationaler Fernmeldeverkehre ließen sich für Wirtschaftsspionage bedeutsame Informationen nur als Zufallsfunde gewinnen.

Der Ausschuss hat darauf hingewiesen, dass ein Kommunikationsüberwachungssystem nur dann seine volle Wirksamkeit entfalten könne, wenn sensible Daten über Satellitenverbindungen nach außen gelangten wie zum Beispiel bei Videokonferenzen.

Die öffentliche Diskussion des Themas WIRTSCHAFTSSPIONAGE hatte zu einer Focussierung auf ECHELON geführt. Sensible Unternehmensdaten befinden sich jedoch in erster Linie in den Unternehmen selbst. Die ausschließliche Blickrichtung auf ECHELON birgt daher das Risiko, dass die hauptsächliche, auch vom Ausschuss so gesehene Gefahrenquelle, nämlich Spionage vor Ort oder am Arbeitsplatz durch sogenannte Innentäter, unterschätzt oder auch gar nicht zur Kenntnis genommen wird.

Die Spionageabwehr geht nach derzeitiger Kenntnislage davon aus, dass von westlichen Staaten keine systematische Wirtschaftsspionage gegen die Bundesrepublik Deutschland durchgeführt wird. Allen Verdachtshinweisen wird jedoch nachgegangen.



5. Methoden der Wirtschaftsspionage



Zu den Arbeitsmethoden der Aufklärungsdienste gehören sowohl die offene Informationssammlung wie auch die konspirative, verdeckte Nachrichtenbeschaffung. Heute lassen sich aus den der Allgemeinheit zur Verfügung stehenden Quellen Informationen beschaffen, die früher nur über Agenten zu erlangen waren. Dennoch wird nicht auf die klassischen Spionagemethoden verzichtet.

Bei ihren konspirativen Beschaffungsaktivitäten verschleiern die Geheimdienste ihre wahren Absichten und versuchen z.B. unter der Tarnung ihrer Mitarbeiter als Diplomaten, Geschäftsleute oder Journalisten an nachrichtendienstlich interessante Informationen zu gelangen. Zusätzlich erfolgt die verdeckte Informationsbeschaffung in den Zielländern durch geheime Mitarbeiter, die als Agenten für eine Verrats- oder Aufklärungstätigkeit angeworben wurden, oder es werden Nachrichtendienstmitarbeiter eingesetzt, die unter einer falschen Identität als sogenannte "Illegale" in das Zielland eingeschleust wurden. Die Informationsbeschaffung mit menschlichen Quellen wird ergänzt durch moderne Nachrichtentechnik, die bei der Fernmelde- und elektronischen Aufklärung sowie als Kommunikationsinstrument bei der Agentenführung eingesetzt wird.

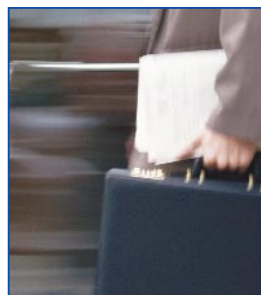
Offene Beschaffung

Auswertung von Veröffentlichungen, Internet und Datenbanken



Geheime Beschaffung

Einsatz von Agenten



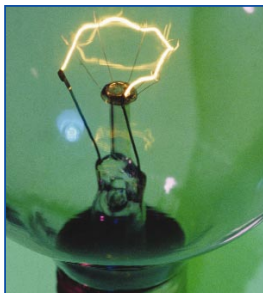
Besuch von öffentlichen Veranstaltungen
(z.B. Messen, Kongresse, Symposien etc.)



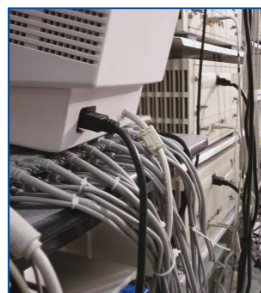
Überwachung von Telekommunikation



Teilnahme an Studiengängen oder wissenschaftlichen Projekten



Eindringen in Informationssysteme



Abschöpfung im Gespräch





5.1 Quellen im Objekt

Eine "Quelle", also einen Agenten in einem nachrichtendienstlich interessanten Objekt, zu führen, ist der Idealfall für einen Aufklärungsdienst.

Dabei wird entweder ein Mitarbeiter des Geheimdienstes als Agent in das Zielobjekt eingeschleust oder ein Mitarbeiter des Unternehmens wird als Agent geworben. Der letztere bietet deutliche Vorteile: Er kann sofort Informationen beschaffen, während der eingeschleuste Agent erst eine geeignete Position erreichen muss. Die Erfahrungen aus der Aufarbeitung der Aktivitäten der "Hauptverwaltung Aufklärung" des Ministeriums für Staatssicherheit der ehemaligen DDR haben gezeigt, dass nur ganz selten ideologische Gründe für den Verrat ausschlaggebend waren. Die Motive waren überwiegend Unzufriedenheit am Arbeitsplatz, Geldgier, Abenteuerlust und das Gefühl, etwas Besonderes zu sein. Daran hat sich nichts geändert.

5.2 Abschöpfquellen

Oft beschaffen Aufklärungsdienste die gewünschten Informationen durch "Abschöpfung" von Gesprächspartnern, ohne dass die "Quelle" bemerkt, dass sie ihr Wissen an einen Nachrichtendienst weitergibt. Diese Methode bietet beiden Seiten große Vorteile: Der als "Quelle" missbrauchte Gesprächspartner hat nie das Gefühl, etwas Unerlaubtes zu tun, der Empfänger braucht sich nicht als Nachrichtendienstler zu enttarnen. Ein Abendessen oder ein kleines Geschenk genügen häufig, um die geeignete Atmosphäre zu erzeugen, die nötige Aufmerksamkeit einzuschläfern und damit die gewünschte Mitteilungsbereitschaft zu fördern.

In unserer offenen Gesellschaft ist eine große Fülle auch sensibler Informationen auf dem offenen Markt erhältlich: in Fachzeitschriften, Dissertationen oder Produktbeschreibungen; man findet sie in öffentlichen Bibliotheken, in Datenbanken, auf Industriemessen oder im Internet usw.. Oft schon versetzt eine gründliche Auswertung informativer Veröffentlichungen die Nachrichtendienste in die Lage, Gesamtbilder ihrer Aufklärungsziele zu erstellen.



5.3 Spionage aus Legalresidenturen

Nachrichtendienste haben die Möglichkeit, auf hauptamtliche Mitarbeiter zurückzugreifen, die an "Legalresidenturen" eingesetzt sind. Sie nutzen die diplomatischen und konsularischen Vertretungen ihres Landes sowie Presseagenturen ihrer Heimatländer in Deutschland als Stützpunkte für den getarnten Einsatz von Geheimdienstoffizieren. Das bedeutet, dass bei jedem privaten oder geschäftlichen Kontakt zu diesen Institutionen der Gesprächspartner ein Nachrichtendienstoffizier sein kann. Solche Tarndienstposten sind aber auch in staatlichen Handelsvertretungen und Firmenniederlassungen eingerichtet. Alle diese Institutionen bieten den Nachrichtendienstoffizieren einen gewissen Schutz vor strafrechtlicher Verfolgung, der unter diplomatischer Immunität natürlich am stärksten ist.

Diese Aufklärung aus "Legalresidenturen" wird von vielen Staaten betrieben.

5.4 Tarnung als Mitarbeiter wirtschaftlicher Unternehmen

Es muss davon ausgegangen werden, dass besonders russische Nachrichtendienste ihre Agenten - zu Hause wie im Ausland - zunehmend als Mitarbeiter privatwirtschaftlicher Unternehmen tarnen. Dafür spricht u.a., dass russische oder von russischem Kapital dominierte Firmen - auch sog. Jointventures - oft von ehemaligen Nachrichtendienstlern geführt werden. Dennoch ist der Nachweis der Spionage hier sehr schwer. Denn aktuelle Verbindungen zu den russischen Nachrichtendiensten sind kaum zu beweisen, weil das Verhalten dieser Unternehmen und ihrer Mitarbeiter nach außen eine normale Geschäftstätigkeit ist. Diese privatwirtschaftliche Legende der "nicht traditionellen Abdeckung" in Firmen ist als Methode zwar nicht neu, jedoch ist sie erst in Folge der politischen Veränderungen im heutigen Umfang möglich geworden; sie ist bei allen Sicherheitsüberlegungen und -konzepten mit einzubeziehen.

5.5 Gefährdung deutscher Unternehmen im Ausland

Im Rahmen der Globalisierung müssen sich deutsche Unternehmen mit Aktivitäten im Ausland darüber im Klaren sein, dass diese möglicherweise beobachtet werden und sie in Geschäftsbeziehungen verstrickt werden, die einen ungewollten Abfluss von Firmeninterna zur Folge haben können.

Insbesondere die speziellen Verhältnisse und die nachrichtendienstliche Tradition in der Gemeinschaft Unabhängiger Staaten (GUS) stellen Unternehmen, die dort tätig sind und investieren, vor erhebliche Probleme. So ist beispielsweise ein wichtiger Bestandteil des russischen Föderalen Sicherheitsdienstes FSB innerhalb des Departments "Spionageabwehr" die "Verwaltung für Spionageabwehr in der Wirtschaft". Angehörige dieser Sektion sollen in Russland verdeckt in verschiedenen Unternehmen, in Banken und Behörden tätig sein.

Wie zu Zeiten der Sowjetunion das KGB arbeitet der FSB mit russischen Behörden zusammen und erhält von ihnen Hinweise auf "Zielpersonen", die für eine Anwerbung in Frage kommen können. Behördenbedienstete, die Zugang zu geschützten Informationen haben, müssen ihre Kontakte zu Ausländern schriftlich dem FSB anzeigen, selbst wenn es sich nur um Zufallsbekanntschaften handelt. Zu melden sind dabei auch detailliert die Gesprächsinhalte. Der russische Inlandsdienst unterhält ein Netz von Informanten und geheimen Mitarbeitern unter der Zivilbevölkerung wie beispielsweise in den Hotels der großen Städte, in denen Geschäftsreisende und Touristen aus dem Westen logieren. Insgesamt haben die Überwachungsmaßnahmen gegen ausländische Geschäftsleute heute wieder einen Standard erreicht, wie er zu Zeiten des KGB üblich war.

Von der Überwachung des Internet und der gesamten elektronischen Kommunikation durch den FSB können sowohl Firmenniederlassungen als auch ausländische Besucher betroffen sein. Die dabei gewonnenen Erkenntnisse - etwa über Betriebsinterna oder persönliche Daten - können für operative nachrichtendienstliche Aktivitäten genutzt werden.

Ausländische Unternehmen, die in Russland geschäftlich tätig sind, Niederlassungen gründen oder investieren, sehen sich dort zudem mit einer Besonderheit konfrontiert, die es sonst nirgendwo gibt: Seit Beginn der 90er Jahre entstand in Russland eine Vielzahl von "privaten" Sicherheitsdiensten und Detekteien, deren Mitarbeiter und Leiter oftmals ehemalige, zum Teil hochrangige Nachrichtendienst-Mitarbeiter sind. Hinweisen zufolge soll häufig eine Verzahnung solcher

Unternehmen mit staatlichen Institutionen bestehen, die es den Nachrichtendiensten erlaubt, die Kenntnisse und Ressourcen der Sicherheitsdienste für ihre Zwecke zu nutzen. Ein bedeutendes Unternehmen dieser Art ist z.B. der "Russische nationale Dienst für Wirtschaftssicherheit"; er wurde 1992 gegründet. Leiter des Unternehmens ist ein ehemaliger Chef der Gegenspionage des KGB. Nach eigenen Aussagen beschäftigt er die Elite der ehemaligen Sowjetspionage. Sein Unternehmen, das zunächst wohl als "Auffangbecken" für ehemalige KGB-Mitarbeiter diente, bietet westlichen Geschäftsleuten seine Dienste als Auskunftei und Detektei sowie zur Vermittlung von Kontakten an.

5.6 Austauschwissenschaftler und Praktikanten

Im Zusammenhang mit dem Thema Wirtschaftsspionage ist auch auf eine verwandte Erscheinungsform illegaler – weil nachrichtendienstlich betriebener – Informations- und Materialbeschaffung hinzuweisen. Austauschwissenschaftler, Studenten und Journalisten werden eingesetzt bzw. abgeschöpft, um Informationen in offener oder auch verdeckter Weise zu beschaffen. Dies gilt auch für Staaten des Nahen, Mittleren und Fernen Ostens.

5.7 Proliferation

Klassische Wirtschaftsspionage vermischt sich oft mit dem beunruhigenden Thema "Proliferation", d.h. der Beschaffung von Materialien und Know-how zur Entwicklung und Herstellung von Massenvernichtungswaffen und der dazugehörigen Trägertechnologie, die ebenfalls häufig von Nachrichtendiensten gesteuert oder durchgeführt wird. Allerdings verfolgen Wirtschaftsspionage und Proliferation grundsätzlich unterschiedliche Ziele: Der Auftraggeber der Wirtschaftsspionage will seine Wirtschaftskraft verbessern. Ein Staat, der sich um Proliferation bemüht, bezweckt dadurch die Stärkung seines militärischen Potenzials.

Zum Thema Proliferation wird auf die Broschüre der Behörden für Verfassungsschutz "Proliferation - das geht uns an!" hingewiesen.



Proliferation – das geht uns an!

Probleme: wie werden
hergestellt?

Probleme: wie
erhalten sie Güter?

Wann Beschaffung
in Deutschland?

Wie werden
Massenvernichtungswaffen
beschafft?


Wann kann man Regeln
durchsetzen?

Welche Bedeutung hat
Wirtschaftsspionage für die
Proliferation?

Abrufbar im Internet unter
<http://www.verfassungsschutz.de>



6. Instrumente zur Bekämpfung von Wirtschaftsspionage und Konkurrenzausspähung



Die Abwehr von Wirtschaftsspionage ist schwieriger geworden, doch sie ist nicht aussichtslos. Voraussetzungen einer erfolgreichen Abwehr sind: Sensibilität gegenüber den Angriffsgefahren, Kenntnisse über die Methoden und Ziele der Nachrichtendienste, der Einsatz geeigneter Schutzmaßnahmen und die Einsicht in deren Notwendigkeit. Sie sind unverzichtbar, denn sie helfen, erhebliche wirtschaftliche Schäden zu vermeiden.

Die Verantwortung für den Schutz ihrer Betriebsgeheimnisse und ihres Know-hows liegt in erster Linie bei der Wirtschaft selbst. Der Staat versteht es als seine Pflicht, hierbei Hilfestellung zu leisten: So werden aus der Auswertung aufgeklärter Spionagefälle Hinweise und Strategien erarbeitet, die den Unternehmen bei der Vorbeugung gegen ähnliche Angriffe helfen können.

Nur gemeinsames Handeln kann letztlich den Erfolg bringen.

Diese notwendige Zusammenarbeit zwischen Staat und Wirtschaft muss kontinuierlich verbessert und intensiviert werden.

Damit der Wirtschaft aktuelle und umfassende Sicherheitskonzepte angeboten werden können, benötigen die zuständigen Behörden von der Wirtschaft Hinweise auf vermutete oder erkannte Ausforschungsversuche.

Hier besteht leider noch ein Defizit, welches sich an folgendem Beispiel aufzeigen lässt:

Bei der Umfrage einer Industrie- und Handelskammer zum Thema "Wirtschaftsspionage und Konkurrenzausspähung" bei etwa 2000 technologieorientierten Firmen antworteten nur 320 Firmen (16%).

Die konkrete Frage "Wurde Ihr Betrieb schon einmal - erkanntermaßen - abgeschöpft oder ausspioniert?" wurde von fast 10% der antwortenden Firmen bejaht. Dies sind immerhin 32 Firmen, denen möglicherweise ein Schaden entstanden ist. Doch keine dieser Firmen hatte jemals Kontakt zu einer Sicherheitsbehörde - Polizei oder Verfassungsschutz - aufgenommen.

Aus langjähriger Erfahrung mit Vertretern der Wirtschaft sowie im Umgang mit dem Problem Wirtschaftsspionage ist den Behörden für Verfassungsschutz bewusst, dass die Meldebereitschaft betroffener Firmen nicht sehr groß ist. Aus Sorge um das Firmenimage oder aus Sorge um wirtschaftliche Schäden wird häufig lieber versucht, die Probleme firmenintern zu lösen. Hierbei wird leider oftmals übersehen, dass die Verfassungsschutzbehörden ihnen zugeleitete Informationen vertraulich behandeln.

Die Hemmschwellen zwischen Wirtschaft und Verfassungsschutz müssen beseitigt werden und ein reger Informationsaustausch sollte entstehen.

Positive Ansätze stellen die neu entstandenen **Sicherheitspartnerschaften** zwischen Behörden, Verbänden und Wirtschaft dar. In Sicherheitsforen wird ebenso wie in Fachzeitschriften und über andere Medien über spezifische Themen der Wirtschaftsspionage und Konkurrenzausspähung informiert und diskutiert. An einigen Universitäten werden Konzepte zu einem Studiengang "Security Management" entwickelt.

Die Verbände für Sicherheit in der Wirtschaft bieten ebenso ihre Leistungen an wie eine große Anzahl von Wirtschafts- und Sicherheitsunternehmen, die sich mit Maßnahmen und technischen Lösungen zur Sicherheit beschäftigen.

Die Mitarbeiter der **Behörden für Verfassungsschutz** stehen den Unternehmen jederzeit für Gespräche, Beratung und Informationen bei der Prävention zur Verfügung. Sie bieten darüber hinaus aber auch Hilfestellung, Vermittlung zur Beratung durch Spezialisten⁶ und ggf. **vertrauliche Beratung** an, wenn ein Ausspähungsverdacht bereits besteht oder eingetreten ist.

Ziel dieser Broschüre ist es, zur Sensibilisierung und zur Schärfung des Problembewusstseins für das Thema Wirtschaftsspionage beizutragen.

⁶ z.B. zum Bundesamt für Sicherheit in der Informationstechnik, dessen Aufgaben nach § 3 BSI-Gesetz sind: Untersuchung von Sicherheitsrisiken bei Anwendung der IT, Entwicklung von Prüf- und Bewertungsverfahren, Zertifizierung im staatlichen Geheimschutz, Unterstützung und Beratung von Behörden, Herstellern, Vertreilern und Anwendern in Fragen der Sicherheit in der IT

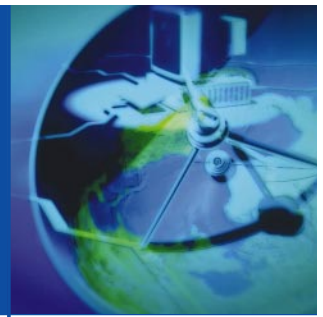
**Nehmen Sie das Angebot einer Beratung durch den
Verfassungsschutz an.**

**Lassen Sie sich bei der Lösung der vorgenannten
Sicherheitsprobleme in Ihrem Unternehmen helfen!**



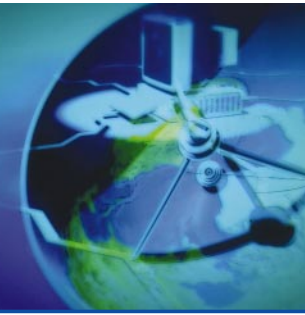
VEREINBAREN SIE EIN BERATUNGSGESPRÄCH!

7. Goldene Regeln der Prävention



Die nachfolgenden Merksätze fassen abschließend kurz und prägnant die wesentlichen Aspekte des Informationsschutzes zusammen. Bei Bedarf können sie durch unternehmensspezifische Gesichtspunkte ergänzt werden.

- Nicht warten bis der Spionagefall eingetreten ist!
- Aktuelle Informationen bei kompetenten Partnern einholen!
- Informationsschutz als wichtigen Bestandteil der Firmenphilosophie und Firmenstrategie verankern!
- Sicherheitsstandards regelmäßig analysieren!
- Ganzheitliches Sicherheitskonzept realisieren und permanent fortschreiben!
- Schutzmaßnahmen auf den Kernbestand zukunftssichernder Informationen konzentrieren!
- Einhaltung und Erfolg der Sicherheitsvorkehrungen kontrollieren, Sicherheitsverstöße sanktionieren!
- “Frühwarnsystem” zur Erkennung von Know-how-Verlusten installieren!
- Auffälligkeiten und konkrete Hinweise konsequent verfolgen, professionelle Hilfe in Anspruch nehmen!
- Informationsschutz ist ein strategischer Erfolgsfaktor!



8. Ihre Ansprechpartner:

Bundesamt für Verfassungsschutz
Merianstr. 100
50765 Köln
Tel: 0221-7920 • Fax: -798365
e-mail: bfvinfo@verfassungsschutz.de
<http://www.verfassungsschutz.de>

Landesamt für Verfassungsschutz Baden-Württemberg
Taubenheimstr. 85 a
70372 Stuttgart
Tel: 0711-954400 • Fax: -9544444
e-mail: lfv-bw@t-online.de • <http://www.baden-wuerttemberg.de/verfassungsschutz>

Bayerisches Landesamt für Verfassungsschutz
Knorrstr. 139
80937 München
Tel: 089-312010 • Fax: -31201380
e-mail: inform@lfv.bayern.de • <http://www.verfassungsschutz.bayern.de>

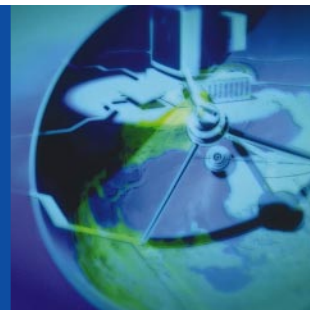
Senatsverwaltung für Inneres - Abteilung V -
Potsdamer Str. 186
10783 Berlin
Tel: 030-901290 • Fax: -90129844
e-mail: verfassungsschutz@berlin.de • <http://www.berlin.de/verfassungsschutz>

Ministerium des Innern des Landes Brandenburg
- Abteilung V -
Henning-von-Tresckow-Str. 9 - 13
14467 Potsdam
Tel: 0331-8662500 • Fax: -8662700230
e-mail: info@verfassungsschutz-brandenburg.de
<http://www.verfassungsschutz-brandenburg.de>

Landesamt für Verfassungsschutz Bremen
Flughafenallee 23
28199 Bremen
Tel: 0421-53770 • Fax: -5377195
e-mail: office@lfv.bremen.de

Freie und Hansestadt Hamburg
Behörde für Inneres
Landesamt für Verfassungsschutz
Johanniswall 4 III
20095 Hamburg
Tel: 040-244443 • Fax: -338360
<http://www.hamburg.de/behoerden/lfv/homepage.htm>

Landesamt für Verfassungsschutz Hessen
Behördenzentrum Wiesbaden
(ehemaliges US-Hospital, Gebäude 24)
Konrad-Adenauer-Ring 41-43
65187 Wiesbaden
Tel: 0611-720404 • Fax: -720179
<http://www.verfassungsschutz-hessen.de>



Innenministerium des Landes Mecklenburg-Vorpommern
- Abteilung II/5 -
Johannes-Stelling-Str. 21
19053 Schwerin
Tel: 0385-74200 • Fax: -714430
e-mail: vs-mv@t-online.de

Niedersächsisches Landesamt für Verfassungsschutz
Büttnerstr. 28
30165 Hannover
Tel: 0511-67090 • Fax: -6709393
e-mail: wirtschaftsschutz@nlv.niedersachsen.de

Innenministerium des Landes Nordrhein-Westfalen
- Abteilung VI -
Haroldstr. 5
40213 Düsseldorf
Tel: 0211-8712821 • Fax: -8712980
e-mail: info@mail.verfassungsschutz.nrw.de • <http://www.verfassungsschutz.nrw.de>

Ministerium des Innern und für Sport Rheinland-Pfalz
- Abteilung 6 -
Schillerplatz 3 - 5
55116 Mainz
Tel: 06131-163772 • Fax: -163688
e-mail: Abteilung6@ism.rlp.de • <http://www.verfassungsschutz.rlp.de>

Landesamt für Verfassungsschutz Saarland
Neugrabenweg 2 - 3. Etage
66123 Saarbrücken
Tel: 0681-30380 • Fax: -3038109
e-Mail: info@lfv.saarland.de • <http://www.innen.saarland.de/9144.html>

Landesamt für Verfassungsschutz Sachsen
Neuländer Straße 60
01129 Dresden
Tel: 0351-85850 • Fax: -8585500
e-mail: la.verfassungsschutz@sz-online.de • <http://www.sachsen.de/verfassungsschutz>

Ministerium des Innern des Landes Sachsen-Anhalt
- Abteilung 5 -
Zuckerbusch 15
39114 Magdeburg
Tel: 0391-5673900 • Fax: -5673999
e-mail: verfassungsschutz@abt5.mi.lsa-net.de • <http://www.mi.sachsen-anhalt.de/min/abt5/abt5.htm>

Innenministerium des Landes Schleswig-Holstein
- Abteilung IV / 7 -
Düsternbrooker Weg 92
24105 Kiel
Tel: 0431-9883500 • Fax: -9883503

Thüringer Landesamt für Verfassungsschutz
Haarbergstr. 61
99097 Erfurt
Tel: 0361-44060 • Fax: -4406251