

Wirtschaftsspionage in Baden-Württemberg und Bayern

D A T E N - F A K T E N - H I N T E R G R Ü N D E



Bayerisches
Landesamt für Verfassungsschutz



Baden-Württemberg
LANDESAMT FÜR VERFASSUNGSSCHUTZ

Wirtschaftsspionage in Baden-Württemberg und Bayern

DATEN - FAKTEN - HINTERGRÜNDE

Stand: Oktober 2006

IMPRESSUM:

Herausgeber:

Landesamt für Verfassungsschutz Baden-Württemberg
Taubenheimstraße 85A
70372 Stuttgart

Tel.: 0711 / 95 44 - 00
Fax: 0711 / 95 44 - 444
E-Mail: info@verfassungsschutz-bw.de

Bayerisches Landesamt für Verfassungsschutz
Knorrstraße 139
80937 München

Tel.: 089 / 3 12 01 - 0
Fax: 089 / 3 12 01 - 380
E-Mail: poststelle@lfv.bayern.de

Illustrationen, Grafiken & DTP:

Landesamt für Verfassungsschutz Baden-Württemberg

Druck:

E. Kurz & Co., Kernerstraße 5, 70182 Stuttgart

Vervielfältigung & Nachdruck:

unter Angabe der Herausgeber gestattet

Zitate:

Alle direkten Zitate sind in Kursivschrift gesetzt. Zitate aus Texten in alter Rechtschreibung wurden an die neue Rechtschreibung angeglichen.

INHALT	SEITE
1. Einführung	7
1.1 Allgemeiner Überblick	7
1.2 Begriffserläuterungen	8
1.2.1 Wirtschaftsspionage/Konkurrenzausspähung	9
1.2.2 Proliferation	10
2. Ursachen und Motive der Spionage	13
3. Hauptauftraggeber	15
3.1 Volksrepublik China	15
3.2 Russische Föderation und andere Länder der GUS	18
3.3 Proliferationsrelevante Länder	20
3.3.1 Islamische Republik Iran	21
3.3.2 Volksrepublik Nordkorea	22
3.4 Westliche Wirtschaftsnationen	23
4. Schwerpunkte der Spionage	24
4.1 Auswahl der Zielobjekte	24
4.2 Schwerpunkte der Ausforschung	26
4.2.1 Bevorzugte Zielbereiche	26
4.2.2 Besonders gefährdete Unternehmensbereiche	27
5. Methoden der Spionage	28
5.1 Auswertung offener Quellen	29
5.2 Gesprächsabschöpfung	30

INHALT	SEITE
5.3 Teilnahme am Wirtschaftsleben	30
5.4 Einsatz von Agenten	31
5.5 Einsatz technischer Mittel	31
5.5.1 Allgemeine Lagedarstellung	31
5.5.2 Täterbild und Fälle	34
5.5.3 Internet- und E-Mail-Überwachung	37
5.5.4 Spezifische Risiken	38
5.5.4.1 Lauschangriffe im Büro	38
5.5.4.2 Angriffe auf und über Telekommunikations- systeme/TK-Systeme	39
5.5.4.2.1 Digitale ISDN-TK-Anlagen	39
5.5.4.2.2 Mobiltelefone	40
5.5.5 Risiken drahtloser Kommunikationssysteme	40
5.5.5.1 Allgemeine Gefahren	40
5.5.5.2 Wireless LAN (WLAN)	41
5.5.5.3 Bluetooth	42
5.5.5.4 Spionagesoftware (Spyware)	42
5.5.5.5 Hacker und Hackertools	42
5.5.5.6 Laptop- und Hardware-Diebstahl	43
5.5.5.7 Unterlassene Löschung von Daten	44
5.5.5.8 Outsourcing	44
6. Schwachstellen des Informationsschutzes	45
7. Quantitative und qualitative Bewertung des Schadens	45
8. Schlussbetrachtung	47
9. Anhang	48
9.1 Literaturhinweise	48
9.2 Internetadressen	54

1. Einführung

1.1 Allgemeiner Überblick

Es ist unverkennbar, dass Wirtschaft und Wissenschaft in besonderem Maß von den Auswirkungen anhaltender Internationalisierungstendenzen in den politischen, wirtschaftlichen und wissenschaftlichen Beziehungen sicherheitsrelevant betroffen sind. Globale Kooperationen auf unterschiedlichsten Gebieten verlaufen parallel zu einer sich verschärfenden Wettbewerbssituation. Fremde Staaten suchen nach Möglichkeiten, wie sie ihre Positionierung im Weltgefüge durch ihr wirtschaftliches und nicht zuletzt militärisches Potenzial verbessern können. Die frühere Konfrontation mit politisch/ideologisch geprägten Wirtschaftssystemen ist hartem marktwirtschaftlichem Wettbewerb mit nicht minder komplexen Spionagerisiken gewichen. Dies kommt in zahlreicher werden den globalen Verflechtungen zum Ausdruck, bei denen sich Konkurrenz und Zusammenarbeit scheinbar nicht gegenseitig ausschließen.

Nachrichtendienstlich gesteuerte Spionage hat drei klassische Zielrichtungen: Wirtschaft/Wissenschaft, Politik und Militär. Diese Bereiche können jeweils „Einfallstore“ für legale und illegale Informationsbeschaffung darstellen. Bei der Planung, Realisierung und Kontrolle wehrtechnischer Produkte arbeiten Auftraggeber und Industrie naturgemäß sehr eng zusammen. Sensibler Informationsaustausch mit Geheimhaltungsbedarf ist dabei unumgänglich. Dies bietet wiederum Ansatzpunkte für illegalen Know-how-Transfer.

Das Ineinandergreifen wirtschaftlicher und militärischer Aspekte verdeutlicht folgender Spionagefall, der in Bayern und Niedersachsen aufgedeckt wurde:

- Wegen des Verdachts der Spionage für einen russischen Nachrichtendienst wurden zwei deutsche Staatsbürger festgenommen. Peter S., Vertriebs- und Projektleiter für Panzerabwehrwaffen bei der Tochterfirma eines in Baden-Württemberg ansässigen Unternehmens, hat Michael K., Inhaber einer Transport- und Handelsgesellschaft, mit rüstungstechnischem Know-how aus seinem Arbeitsbereich beliefert, das von K. an einen russischen Nachrichtendienst weitergeleitet wurde. S. bekleidete seit Mitte der 70er-Jahre verschiedene verantwortliche Positionen in wehrtechnischen Bereichen des Konzerns. Für den Verrat waren den Ermittlungen zufolge finanzielle Gründe ausschlaggebend.

Das Oberlandesgericht Celle verhängte gegen K. eine Freiheitsstrafe von drei Jahren und sechs Monaten sowie gegen S. eine Freiheitsstrafe

von drei Jahren und drei Monaten. Nach Auffassung des Gerichts liegt diese Tat an der Grenze zum besonders schweren Fall der Spionage.

Ein wesentliches Kriterium des Wettbewerbs ist das Streben nach Wissensvorsprung. Wettbewerbsvorteile sind für wirtschaftlichen Erfolg unverzichtbar. Sie können aber oft nur unter höchsten Anstrengungen beziehungsweise unter hohem Einsatz - meist knapper - finanzieller Mittel realisiert werden. Somit ist das Risiko des vergleichsweise „kostengünstigen“ illegalen Wissenstransfers in Forschung und Wirtschaft stets vorhanden und deshalb steht die Spionage im Ruf, als wirtschaftsstrategisches Instrument eingesetzt zu werden.

Vielfach wird verkannt, dass die Ausspähungsmöglichkeiten in einer zunehmend vernetzten Gesellschaft vielschichtiger geworden sind. Moderne Informations- und Kommunikationstechniken bringen spezifische Sicherheitsprobleme mit sich, indem sie vielfältige und teilweise leicht zu realisierende Ansatzpunkte für Spionage bieten oder als Hilfsmittel für nachrichtendienstliche Aktivitäten dienen können.

Die wirtschaftlich-wissenschaftlichen Infrastrukturen Baden-Württembergs und Bayerns weisen eine hohe Dichte an innovativen Firmen und wissenschaftlichen Einrichtungen der Hochschulen auf. Beide Bereiche sind hierzulande eng miteinander verknüpft und bieten auf internationaler Ebene Ansatzpunkte für Spionage. Es ist deshalb nicht überraschend, dass das nachrichtendienstliche Interesse fremder Staaten an diesen High-Tech-Ländern weiterhin unvermindert anhält.

1.2 Begriffserläuterungen

Die zielgerichtete Ausforschung des von Wirtschaftsunternehmen und wissenschaftlichen Einrichtungen oft mit hohem personellem und materiellem Aufwand erarbeiteten Know-hows wird mit unterschiedlichen Begriffen umschrieben. So werden landläufig die Bezeichnungen Betriebsspionage, Industriespionage, Wissenschaftsspionage, Konkurrenzspionage beziehungsweise Werksspionage für den gleichen Sachverhalt benutzt. Im Bereich des Verfassungsschutzes wird zwischen Wirtschaftsspionage und Konkurrenzausspähung unterschieden. Die Weiterverbreitung von Massenvernichtungswaffen beziehungsweise der zu ihrer Herstellung verwendeten Produkte einschließlich des dafür erforderlichen Know-hows sowie von entsprechenden Waffenträgersystemen (Proliferation) ist nach Auffassung der beiden Landesbehörden wegen der Zielrichtung Wirtschaft/Wissenschaft mit der Thematik Wirtschaftsspionage eng verknüpft. Auftraggeber von Wirtschaftsspionage wollen ihre Wirtschaftskraft verbessern. Staa-

ten, die sich um Proliferation bemühen, bezwecken dadurch die Stärkung ihres militärischen Potenzials.

1.2.1 Wirtschaftsspionage/Konkurrenzausspähung

Die staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben bezeichnet man als Wirtschaftsspionage. Die Bekämpfung solcher geheimdienstlichen Aktivitäten gehört zu den originären Aufgaben der Spionageabwehr der Verfassungsschutzbehörden.

Demgegenüber versteht man unter Konkurrenzausspähung die Ausforschung, die ein (konkurrierendes) Unternehmen gegen ein anderes betreibt. Obwohl die Beobachtung und Bekämpfung dieser Form des Wettbewerbs nicht zum gesetzlichen Auftrag des Verfassungsschutzes gehören, entfalten von der Spionageabwehr empfohlene Maßnahmen zum Schutz gegen Wirtschaftsspionage auch eine präventive Wirkung gegen Konkurrenzausspähung.

Bei der nachrichtendienstlich gesteuerten Wirtschaftsspionage steht ein Staat mit seinen gesamten finanziellen und infrastrukturellen Möglichkeiten im Hintergrund, während bei der Konkurrenzausspähung einzelne Unternehmen Auftraggeber sind. Weiter unterscheiden sich beide in Ziel und Dauer der Aktivitäten. In der Wirtschaftsspionage wird sehr viel langfristiger geplant und gehandelt, es wird unter nachrichtendienstlicher Absicherung gearbeitet. Bei der Konkurrenzspionage geht es dagegen oft impulsiv und kurzfristig zu. Es wird weniger auf Tarnung geachtet. Das Spionageziel muss zumeist innerhalb kürzester Zeit erreicht werden, insbesondere dann, wenn kurze Produktlebenszyklen den Innovationsrhythmus und somit den Wettbewerb beeinflussen. Methoden und Mittel der Konkurrenzausspähung sind mit denen der nachrichtendienstlich gesteuerten Spionage im Grundsatz vergleichbar. Weil das Entdeckungsrisiko geringer und die Gefahr zwischenstaatlicher Verwicklungen minimiert ist, muss immer wieder damit gerechnet werden, dass vermeintliche Konkurrenzspionage in Wirklichkeit von ausländischen staatlichen Stellen initiiert, gesteuert oder koordiniert wird.

Die Möglichkeiten der illegalen Informationsbeschaffung haben sich im Zuge der Einführung moderner Informations- und Kommunikationstechniken wesentlich erweitert. Somit steht ein Mix an Ausspähungsvarianten zur Verfügung, dessen konkrete Zusammensetzung sich an den jeweiligen Bedürfnissen und Möglichkeiten des Auftraggebers orientiert. Deshalb lassen sich in der Anfangsphase eines Verdachts exakte Zuordnungen auch kaum vornehmen.

1.2.2 Proliferation

Die Verfassungsschutzbehörden sind bereits seit langem damit befasst, Aktivitäten und Methoden der Proliferation zu erkennen und zu deren Verhinderung beizutragen. Da wegen komplexer Sachverhalte ein nachrichtendienstlicher Hintergrund oft nicht auf Anhieb zweifelsfrei erkennbar ist, genügt für das Tätigwerden des Verfassungsschutzes der Verdacht, dass der Warentransfer im Sinne des Außenwirtschafts- und Kriegswaffenkontrollgesetzes sowie der Außenwirtschaftsverordnung illegal ist, im Interesse eines fremden Staates erfolgt oder die beteiligten Beschaffungsorganisationen verdeckte Methoden anwenden, um den Endabnehmer oder den Verwendungszweck zu verschleiern. Ziel und Aufgabe der Verfassungsschutzbehörden ist es, verdächtige Personen und Unternehmen sowie die sich ständig wechselnden Beschaffungsbemühungen im Vorfeld zu beobachten, zur Verhinderung dieser illegalen Geschäfte im Zusammenwirken mit anderen Sicherheitsbehörden beizutragen und die gewerbliche Wirtschaft sowie wissenschaftliche Einrichtungen entsprechend zu sensibilisieren. Von besonderer Bedeutung sind hierbei Informationen über die Missbrauchsmöglichkeiten von Gütern, die scheinbar für zivile Anwendungen exportiert werden, aber tatsächlich für die Waffenherstellung Verwendung finden (Dual-use-Problematik).

Einige proliferationsrelevante Länder² stehen im Verdacht, mit unterschiedlicher Intensität Programme zur Entwicklung und Produktion von ABC-Waffen und dazugehöriger Trägersysteme voranzutreiben, um ihre militärische Position zu stärken. Mangels eigener Ressourcen sind diese Länder dabei meist auf das Wissen und die Technik westlicher Staaten angewiesen. Aufgrund der hier herrschenden restriktiven Exportkontrollen setzen einige proliferationsrelevante Staaten ihre Nachrichtendienste ein beziehungsweise nutzen nachrichtendienstliche Mittel, um die benötigten Güter und das erforderliche Know-how zu beschaffen. Zur Umgehung internationaler oder nationaler Embargobestimmungen bedienen sie sich zahlloser in- und ausländischer Tarnfirmen und diplomatischer Einrichtungen. Eine Reihe ausgeklügelter Methoden soll den eigentlichen Zweck der Warenlieferungen verschleiern und Abwehrmaßnahmen der Sicherheitsbehörden erschweren. Es zeichnet sich ab, dass diese Länder wegen der zunehmenden Verbesserung ihrer wissenschaftlichen und industriellen Infrastruktur nicht mehr auf die ausschließliche Beschaffung von Endprodukten angewiesen sind. Häufig reichen einzelne Komponenten aus, um ihre Rüstungsindustrie weiterzuentwickeln. Zudem ist zu erkennen, dass sich

² 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, Nordkorea, Indien, Pakistan, Syrien).

diese Staaten gegenseitig mit Know-how und Ausstattung zur Herstellung von Massenvernichtungswaffen und entsprechenden Trägersystemen unterstützen.

Die Brisanz von Kontakten zu proliferationsrelevanten Ländern veranschaulicht folgender Fall:

- Ein im süddeutschen Raum lebender Ingenieur wurde unter dem Verdacht der geheimdienstlichen Agententätigkeit festgenommen. Er war im Entwicklungsbereich eines bayerischen Luftfahrtunternehmens tätig und galt als zuverlässig. Der Ingenieur stand mit einem Nachrichtendienstoffizier seines arabischen Herkunftslandes in Verbindung, der an einer diplomatischen Vertretung in Berlin abgetarnt eingesetzt war. Als sich der Ingenieur mit firmeneigenen Dokumenten seines Arbeitgebers auf den Weg zu seinem Führungsoffizier machte, wurde er festgenommen. Das Strafverfahren führte zu einer Geldbuße in Höhe von rund 3.000 Euro.

Folgende Beispiele aus der Arbeit der Spionageabwehr zeigen Vorgehensweisen der Umwegbeschaffung auf:

- Ein baden-württembergisches Unternehmen, das bereits 1998 durch das Landesamt für Verfassungsschutz (LfV) umfassend mit dem Thema Proliferation vertraut gemacht worden war, hatte 2001 nach diversen Anfragen einschlägig bekannter iranischer Beschaffungsorganisationen mit der Abgabe von Angeboten reagiert. Die daraufhin eingeleiteten Ermittlungen und sonstigen Maßnahmen des LfV erbrachten neben diversen Kontakten und Verbindungen zu nachrichtendienstlich relevanten iranischen Stellen auch Erkenntnisse über konspiratives Verhalten und Abschottung des Unternehmens nach außen. Nachdem eine Ausfuhr genehmigungspflichtiger Güter bevorstand, wurde ein staatsanwalt-schaftliches Ermittlungsverfahren eingeleitet. Neben den festgestellten Straftatbeständen wurde eine erhebliche kriminelle Energie der Tatverdächtigen offenbar. Es bestand nie die Absicht, die geplanten Ausfuhr durch das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) genehmigen zu lassen. Auch in diesem Verfahren fiel auf, dass einige Unternehmen die ihnen bekannten rechtlichen Schranken schlichtweg ignorierten und zum unerlaubten Export ihrer Produkte bereit waren.

Hersteller und Exporteure unterliegen der Ausfuhrkontrolle. Sie soll verhindern, dass sensible Güter in den Besitz von proliferationsrelevanten Ländern gelangen können. Wie schwierig dies sein kann, zeigt folgender Fall:

- Ein bayerisches Unternehmen aus dem Bereich Anlagenbau erhielt eine Anfrage aus einem Nachbarstaat. Die ersuchende Firma konnte den Wunsch des aus dem Nahen Osten stammenden Kunden nicht selbst erfüllen. Bei der Bearbeitung der Anfrage fielen dem Exportverantwortlichen des Unternehmens einige Diskrepanzen auf. Da der Kaufmann durch ein Sensibilisierungsgespräch mit dem Bayerischen Landesamt für Verfassungsschutz über die Beschaffungsaktivitäten im Bereich der Proliferation aufgeklärt war, wandte er sich an die Behörde.

Die Ermittlungen ergaben, dass der Zielort des gewünschten Gutes die Hauptstadt eines proliferationsrelevanten Landes im Nahen Osten sein sollte. Als sehr unwahrscheinlich wurde der angegebene Verwendungszweck des gewünschten Produkts angesehen. Aufgrund der Spezifikation konnte vielmehr davon ausgegangen werden, dass dieses Dual-Use-Gut im militärischen Bereich Anwendung gefunden hätte. Zusätzlich konnte eine Widersprüchlichkeit bei den Angaben zum eigentlichen Endnutzer ermittelt werden. Wegen des Proliferationshintergrunds verzichtete das Unternehmen auf das möglicherweise lukrative Geschäft.

Eine Variante von wachsender Bedeutung ist die so genannte horizontale Proliferation. Sie bezeichnet den Austausch beziehungsweise die Weitergabe entsprechender Technologien bis hin zu fertigen Waffensystemen zwischen zwei oder mehreren proliferationsrelevanten Ländern - auch unter Mithilfe von westlichen Unternehmen. Sie kann z. B. durch die Weitergabe von Atomtechnologie in Form von Gasultrazentrifugen (GUZ), Know-how und Planunterlagen eine besondere Brisanz gewinnen, wie aus einem Lagebericht des Zollkriminalamts vom November 2004 zur horizontalen Proliferation mit Bezug zu Pakistan zu entnehmen ist:

„Dr. K. hatte im Zuge seiner wissenschaftlichen Tätigkeit in Europa in den 70er Jahren das Know-how zur Urananreicherung erworben und Pläne zum Bau von Gasultrazentrifugen an sich gebracht. Später machte er Karriere als Leiter der pakistanischen Urananreicherungsanlage K. RESEARCH LABORATORIES (KRL). Im Februar 2004 räumte er gegenüber dem pakistanischen Präsidenten Musharraf die Weitergabe von Atomtechnologie an Nordkorea, Iran und Libyen ein. Hierbei bediente sich K. seines Beschaffungsnetzwerks und einiger Vertrauter aus den KRL. In den drei Bestimmungsländern sollte die Atomtechnologie im militäri-

schen Nuklearprogramm zur Herstellung von hochangereichertem Uran für Atombomben verwendet werden.

Die GUZ-Produktion wurde aufgesplittet und von Pakistan in Länder verlegt, die keine Massenvernichtungswaffen herstellen (Malaysia, Türkei, Schweiz u. a.) und damit unverfänglich beliefert werden konnten. Zusätzlich wurden die Beschaffungen durch Falschdeklaration der Güter, Verschleierung von Endverwendern und Endbestimmungsort sowie Einschaltung von Zwischenhändlern verschleiert.“

Die horizontale Proliferation hat die Atomwaffenprogramme des Iran, Nordkoreas und Libyens wesentlich befördert. Anlässlich von Inspektionen der Internationalen Atomenergiebehörde (IAEA) im Jahr 2004 wurde festgestellt, dass Libyen hochangereichertes Uran, Zentrifugen und Konstruktionspläne besaß. Der von K. maßgeblich unterstützte Aufbau einer Urananreicherungsanlage befand sich noch in einem frühen Stadium und konnte nicht abgeschlossen werden, da die deutschen Behörden das Frachtschiff „BBC China“ mit einer Hauptlieferung für diese Anlage im Oktober 2003 gestoppt hatten. Im Gegensatz zu Libyen war der Iran eher an einer punktuellen Unterstützung aus dem Netzwerk des Wissenschaftlers interessiert; so wurden komplette Gasultrazentrifugen bezogen, um das entsprechende Handling zu erlernen. Nordkorea ist nach Angaben von K. ebenfalls mit GUZ-Technologie beliefert worden.

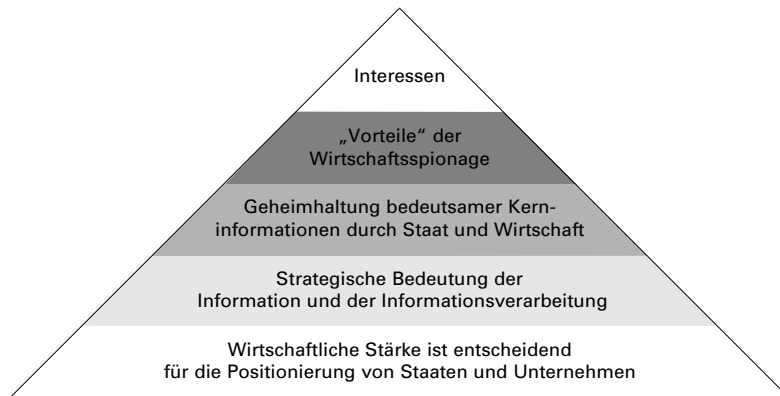
2. Ursachen und Motive der Spionage

Der Kampf der Wirtschaftsnationen um Weltmarktanteile, das Bemühen so genannter Schwellenländer³, der Wirtschaftskraft „klassischer“ Industrienationen nahe zu kommen, und nicht zuletzt die nach militärischer Macht strebenden proliferationsrelevanten Staaten können als ursächlich für die gegen Deutschland gerichteten Spionageaktivitäten angesehen werden.

Die Bedeutung der Wirtschaftsspionage kommt in der Verquickung von fünf ganz unterschiedlichen Einzelaspekten zum Ausdruck:

³ Gruppe relativ fortgeschrittener Entwicklungsländer, die aufgrund ihrer hohen wirtschaftlichen Eigendynamik beachtliche Industrialisierungsfortschritte erzielen konnten und in ihrem Entwicklungsstand gegenüber den Industrienationen deutlich aufgeholt haben.

Ursachen/Motive der Wirtschaftsspionage



- ❑ Wirtschaftliche Stärke ist der entscheidende Faktor für die Positionierung eines Staates oder eines Unternehmens:
Nach dem Ende des Kalten Krieges sind immer mehr Staaten dazu übergegangen, ökonomische Leistungsfähigkeit als Basis ihrer nationalen Stärke zu begreifen.
- ❑ Die strategische Bedeutung der Information und der Informationsverarbeitung:
Informationen sind in einer komplexen und sich immer schneller verändernden Welt, in der das Wissenspotenzial und die Verfügbarkeit wichtiger Daten zum richtigen Zeitpunkt die Handlungsfähigkeit und Leistungskraft von Staaten und einzelnen Unternehmen wesentlich bestimmen, zu einer bedeutenden Ressource von strategischem Wert geworden.
- ❑ Die Geheimhaltung bedeutsamer Informationen durch Staat und Wirtschaft:
Aus guten Gründen halten Staaten und Unternehmen strategisch beziehungsweise wirtschaftlich bedeutsame Kerninformationen geheim. Um sie auszuspähen, setzen fremde Nachrichtendienste das Instrument der Spionage ein.
- ❑ „Vorteile der Wirtschaftsspionage“:
Wirtschaftsspionage eröffnet Staaten und Unternehmen eine Reihe ganz unterschiedlicher Möglichkeiten. In der Gesamtschau führen diese Faktoren zu einer massiven Wettbewerbsverzerrung zugunsten solcher Volkswirtschaften, die Spionage betreiben.

- ❑ Wahrnehmung eigener Interessen:
Staaten und Unternehmen verfolgen eine Gesamtstrategie, die durch die Wahrnehmung eigener Interessen auf unterschiedlichsten Gebieten ihre konkrete Ausprägung erfährt. Sie ist letztlich der Spionage auslösende Faktor.

3. Hauptauftraggeber

Auf dem Sektor der nachrichtendienstlich gesteuerten Spionage sind China, die Russische Föderation und weitere Staaten der GUS sowie die proliferationsrelevanten Länder (vor allem Iran, Nordkorea) sehr aktiv. Sie wollen damit vorrangig ihr militärisches Potenzial beziehungsweise ihre Wirtschaftskraft stärken. Im Vergleich dazu spielen die Erkenntnisse über Aufklärungsaktivitäten westlicher Nachrichtendienste bislang eine untergeordnete Rolle.

3.1 Volksrepublik China

China strebt seit nahezu zwei Jahrzehnten mit ansteigender Vehemenz den wirtschaftlichen, wissenschaftlichen und rüstungstechnischen Gleichstand mit den führenden Industrienationen an.

Nachrichtendienste der Volksrepublik China mit Zielbereich Wirtschaft/Wissenschaft

	MSS Guojia Anaqaanbu (Ministry of State Security)	MID Zhong Chan Er Bu (Military Intelligence Department)	3 VBA Zhong Chan San Bu (Electronic Interception Department)
Aufgaben	Ziviler Inlands- und Auslands-Nachrichtendienst	Militärischer Inlands- und Auslands-Nachrichtendienst	Fernmeldeelektronische Aufklärung
Leiter	Minister Yongye XU	Generalmajor Yudong LUO	Generalmajor Quan SHI

Besonderes Augenmerk wird auf die Ausforschung der Schlüsseltechnologien und der Grundlagenforschung gelegt. Die Koordinierung der Beschaffungsaufträge, die mit Hilfe der mächtigen Nachrichtendienste MSS und MID umgesetzt werden, erfolgt über die Staatskommission für Wissenschaft und Technik. Chinesische Stellen üben aber auch wirtschaftlichen Druck durch das gegenseitige Ausspielen potenzieller Investoren aus, um an das gewünschte Know-how zu gelangen. In Verkennung dieser Zusammenhänge begeben sich häufig deutsche Wirtschaftsvertreter im Umgang mit chinesischen Geschäftspartnern in eine Situation, in der sie in Erwartung kurzfristiger wirtschaftlicher Erfolge leichtfertig ihren Wettbewerbsvorsprung aufs Spiel setzen.

In Deutschland fungieren Angehörige der Nachrichtendienste als Mitarbeiter der chinesischen Botschaft, in Handelsvertretungen und Presseagenturen. Nicht selten verzichten sie auf ihre Abtarnung. Ihre Aktivitäten werden durch die geheimdienstliche Anbindung hier lebender chinesischer Wissenschaftler und Studenten ergänzt.

Aber auch Handelsdelegationen stehen im Ruf, zielgerichtete Informationsbeschaffung in westlichen Unternehmen zu betreiben. Folgender Fall beweist das:

- Anlässlich des Besuchs einer chinesischen Handelsdelegation bei einem Unternehmen des Anlagenbaus hat ein Delegationsmitglied eine kurze Abwesenheit des von der betroffenen Firma zur Verfügung gestellten Betreuers genutzt, auf dem Tisch liegende Unterlagen beziehungsweise Pläne illegal in seinen Besitz zu bringen. Dieses Vorgehen wurde bei der vorzeitigen Rückkehr des Betreuers erkannt. Der Besuch dieses Delegationsmitglieds wurde daraufhin vom gastgebenden Unternehmen abrupt beendet.

Offizielle Stellen in China haben bereits ganz gezielt versucht, Wissenschaftler zum Zwecke der Informationsbeschaffung aus Industriebetrieben und wissenschaftlichen Einrichtungen der Bundesrepublik Deutschland anzusprechen beziehungsweise einzuschleusen.

- Der Inhaber eines baden-württembergischen Hightech-Unternehmens wurde aufgrund seiner wissenschaftlichen Qualifikation mehrfach als Referent zu Vorträgen nach China eingeladen. Dort wurden für ihn auch Begegnungen mit hochrangigen Funktionsträgern arrangiert. Überdies bot man ihm eine Professur an einer renommierten chinesischen Universität an. Im Verlauf der Kontakte stellte sich heraus, dass das eigentliche Interesse der Gastgeber auf eine seiner Entwicklungen im Bereich der Raketentechnik gerichtet war.

- An einem naturwissenschaftlichen Lehrstuhl einer bayerischen Universität konnte festgestellt werden, dass ein chinesischer Gastwissenschaftler geheimhaltungsbedürftiges Know-how aus dem Forschungsaufkommen per E-Mail an eine dem chinesischen Nachrichtendienst zuzurechnende Stelle gesandt hatte. Die Daten waren sowohl im Nuklearbereich als auch in der Raumfahrt genutzt worden. Der Chinese war bemerkenswerterweise laufend vom örtlichen chinesischen Konsulat betreut worden. Nach Bekanntwerden des Zwischenfalls musste er den Lehrstuhl verlassen und nach China zurückkehren.

Bei Jointventures mit China machen deutsche Unternehmen immer wieder die Erfahrung, dass ihre Partner die Produkte kopieren und unter eigenem Namen vertreiben. Chinesische Stellen versuchen aber auch, durch geschicktes Taktieren und durch gegenseitiges Ausspielen potenzieller Investoren an deutsche Hochtechnologie zu gelangen. Die Absicherung des eigenen Know-hows ist daher für die westliche Industrie eines der fundamentalen Probleme in der Zusammenarbeit mit chinesischen Geschäftspartnern.

Seit Jahren sind Anstrengungen der Volksrepublik China zu beobachten, ihre ehemaligen Auslandsstudenten mit Hilfe spezieller Förderprogramme in die Heimat zurück zu holen. Geschickt wird z.B. an den Patriotismus chinesischstämmiger Wissenschaftler und Manager im Ausland appelliert, um sie im Interesse ihres Heimatlandes zum Transfer von Wissen und Fertigkeiten zu bewegen. Es gibt Anzeichen dafür, dass auch chinesische Nachrichtendienste in entsprechende Aktivitäten eingebunden sind.

Als weitere Möglichkeit der Know-how-Beschaffung kann das zum 1. August 2003 in Kraft gesetzte Zertifizierungssystem „China Compulsory Certification (CCC)“ angesehen werden. Exporteure, die den chinesischen Markt bedienen wollen, müssen - entsprechend der jeweils geltenden Produktliste - ihre Waren zuerst einer Zertifizierung mit folgenden Schritten unterziehen:

- Antragstellung bei einer chinesischen Behörde,
- Typprüfung in einem akkreditierten Labor in China,
- Besichtigung der Fertigungsstätten durch chinesische Inspektoren sowie
- jährliche Folgeinspektionen.

Mit den geforderten Zertifizierungsschritten erhalten die Chinesen weitere strategisch bedeutsame Ansatzpunkte für umfangreiche Informationsbeschaffung.

gen. Das bereits hinlänglich bekannte und weiter zunehmende Problem von Plagiaten kann dadurch verschärft werden. Diese verursachen nicht nur wirtschaftliche Schäden durch Einbußen von Marktanteilen, sondern können zudem durch eklatante Qualitätsmängel zu Imageverlusten der Markeninhaber führen.

Nach Erkenntnissen des Verfassungsschutzes dienen Konferenzen und ähnliche Fachveranstaltungen der Abschöpfung von Wissenschaftlern und Ingenieuren. Dabei setzen die Nachrichtendienste auf das Bestreben von Experten, ihr Wissen mit anderen Kollegen auszutauschen. Dass solche Fachgespräche von den Partnern zur Abschöpfung genutzt werden, wird vielfach nicht wahrgenommen. So waren auch den Beteiligten des folgenden Falles sowohl der eigentliche Veranstalter als auch der wirkliche Hintergrund des Symposiums nicht bekannt.

- Ein chinesischer Dienst nahm Kontakt zu einem aus Asien stammenden Mitarbeiter eines bayerischen Hochtechnologie-Unternehmens auf. Dieser lieferte personenbezogene Daten über die bei seinem Arbeitgeber beschäftigten Landsleute. Durch die weitergegebenen Informationen gelang es dem Nachrichtendienst, die wegen ihres speziellen Aufgabenbereichs interessierenden Personen ins Visier zu nehmen. Diese Zielgruppe - meist Wissenschaftler - wurde dann unter Übernahme der Reisekosten zu Tagungen eingeladen. An der Konferenz im Heimatland nahmen chinesische Fachleute aus entsprechenden Fachrichtungen teil. Die erforderliche Zustimmung des Arbeitgebers zu diesen Vortragsreisen wurde nicht eingeholt. Die Mitarbeiter konnten deshalb auch nicht sensibilisiert werden.

Der beschriebene Modus deckt sich mit weiteren, bekannt gewordenen Fällen.

3.2 Russische Föderation und andere Länder der GUS

Seit dem 11. September 2001 treibt die Russische Föderation den Auf- und Ausbau ihrer bilateralen Verbindungen zu westlichen Nachrichten- und Sicherheitsdiensten vor allem zum Zwecke der Terrorismusbekämpfung voran.

Trotz der voranschreitenden Intensivierung der deutsch-russischen Beziehungen unternehmen die russischen Nachrichtendienste nach wie vor große Anstrengungen, um in Deutschland auf offenen und geheimen Wegen wichtige Informationen aus Politik, Militär, Wirtschaft und Wissenschaft zu beschaffen.

Mit Hilfe dieser Aktivitäten, die permanent den nationalen Interessen angepasst werden, können die Dienste weltweite politische und militärische Entwicklungen einschätzen und bei Bedarf darauf Einfluss nehmen. Auch die Leis-

tungsfähigkeit der russischen Wirtschaft profitiert enorm von diesen Ausspähungsergebnissen.

Nachrichtendienste der Russischen Föderation mit Zielbereich Wirtschaft/Wissenschaft

	SWR Slushba Wneschnej Raswedkij	GRU Glawnoje Raswedywatelnoje Uprawlenije	FSB Federalnaja Slushba Besopasnosti
Aufgaben	Zivile Auslandsaufklärung	Militärische Auslandsaufklärung	Ziviler & Militärischer Abwehrdienst mit ziviler Aufklärungs- komponente
Leiter	Generaloberst Sergej Nikolajewitsch LEBEDEW	Generaloberst Walentin Wladimirowitsch KORABELNIKOW	Minister Nikolaj Platonowitsch PATRUSCHEW

Als Reaktion auf innere Unruhen und aus Gründen der Effizienz wurden im Mai 2003 die russischen Nachrichtendienste umstrukturiert. Kompetenz und Einfluss des zivilen Auslandsnachrichtendienstes SWR⁴ und des „Föderalen Sicherheitsdienstes“ (FSB)⁵ wurden in den letzten beiden Jahren kontinuierlich und konsequent erweitert. Russische Medien berichteten allerdings, dass nach der 2003 aufgelösten „Föderalen Agentur für Regierungsfernmeldewesen und Information“ (FAPSI)⁶ mittlerweile sogar der SWR für eine Übernahme durch den FSB zur Disposition stehe. Fachkreise sehen darin eine Rückkehr zu einem neuen allmächtigen Geheimdienst mit einer Aufgabenfülle und Personalstärke, wie man sie zu Zeiten der Sowjetunion beim ehemaligen Inlands-KGB⁷ gewohnt war.

SWR und FSB sind seit März 2004 dem Präsidenten direkt unterstellt. Dem FSB-Direktor Nikolai PATRUSCHEW, einem ehemaligen KGB-Offizier, verlieh der russische Präsident Vladimir Putin den Status eines Ministers im Kabinettsrang mit erheblich erhöhtem Finanz- und Personalbudget und ausgeweiteten Vollmachten gegenüber staatlichen Organen.

⁴ „Slushba Wneschnej Raswedkij“; Ziviler Aufklärungsdienst.

⁵ „Federalnaja Slushba Besopasnosti“; Föderaler Sicherheitsdienst.

⁶ „Federalnoje Agenstwo Prawitelstvennoj Swjasi i Informazij“; Föderale Agentur für Regierungsfernmeldewesen und Information.

⁷ „Komitet Gosudarstvennoj Besopasnosti“; Komitee für Staatssicherheit.

Die russischen Nachrichtendienste sind seit jeher an Erkenntnissen aus allen Lebens- und Wissensbereichen interessiert. Ihre Palette umfasst sowohl klassische konspirative Beschaffungsmethoden als auch moderne, an den Möglichkeiten heutiger Technik ausgerichtete Vorgehensweisen. Über die weltweit gespannten Computer- und Datennetze lassen sich sowohl offene als auch - durch illegales gezieltes Eindringen in gesicherte Datenbanken - besonders geschützte Informationen erlangen.

Auch Angehörige diplomatischer oder konsularischer Vertretungen (Legalresidenturen⁸) nehmen bei der Informationsgewinnung nach wie vor eine besondere Rolle ein. Sie versuchen, durch Kontakte zu Vertretern von Politik, Militär, Wirtschaft, Wissenschaft und Forschung Wissenswertes in Erfahrung zu bringen. Dabei profitieren sie enorm von den Zugangsmöglichkeiten, die eine offene Gesellschaft und schwindende Ressentiments gegenüber dem ehemaligen Ostblock bieten.

Zugang zu periodisch erscheinenden Publikationen mit wissenschaftlichen Forschungsergebnissen, die geeignet sind, russische Forscher und Wissenschaftler zu unterstützen, erhalten Angehörige von Legalresidenturen der Russischen Föderation im Bundesgebiet über die Aufnahme in Adress- und Verteilerverzeichnisse verschiedener Forschungseinrichtungen.

Nachrichtendienstlich interessante Personen müssen auch heute noch davon ausgehen, während ihres Aufenthalts in Russland vom FSB permanent überwacht zu werden. Mehrere Mitarbeiter eines baden-württembergischen Unternehmens entdeckten während einer Geschäftsreise in ihrem Hotelzimmer eine optische (Kamera/Video) und akustische (Mikrofon) Raumüberwachungsanlage.

Von den anderen GUS-Staaten sind in Baden-Württemberg vor allem die Nachrichtendienste Kasachstans und der Ukraine aktiv.

3.3 Proliferationsrelevante Länder

Nach dem Sturz des irakischen Regimes stehen nun andere proliferationsrelevante Länder verstärkt im Brennpunkt. An vorderster Stelle sind der Iran und Nordkorea zu nennen.

⁸ Abgetarnter Stützpunkt eines fremden Nachrichtendienstes in einer offiziellen (z.B. Botschaft, Generalkonsulat) oder halböffentlichen (z.B. Presseagentur, Fluggesellschaft) Vertretung seines Landes im Gastland (= Operationsgebiet).

3.3.1 Islamische Republik Iran

Nachrichtendienste der Islamischen Republik Iran mit Zielbereich Wirtschaft/Wissenschaft

	MOIS/VEVAK Vezerat-e Ettela'at va Va Amniat-e Keshvar (Ministry of Intelligence and Security)	IRGC Pasdaran-i Inqilab-i Islami (Islamic Revolutionary Guard Corps) ND-Apparat der „Revolutionären Gardien“	J2 (Military Intelligence)
<i>Aufgaben</i>	Ziviler Inlands- und Auslands-Nachrichtendienst	Ziviler Inlands- und Auslands-Nachrichtendienst	Militärischer Inlands- und Auslands-Nachrichtendienst
<i>Leiter</i>	Minister Gholam Hossein MOHSENI-EDSCHEHEI	Yahya RAHIM-SAFARI	Hessam HASHEMI

Der Iran zählt gegenwärtig zu den weltweit aktivsten Einkäufern von Rüstungstechnologie. Nachrichtendienstlich gesteuerte Beschaffungsorganisationen bemühten sich in mehreren Fällen bei Firmen in Baden-Württemberg und Bayern um den Ankauf und die Lieferung militärisch verwendbarer Produkte - vorrangig Dual-Use-Güter. Welcher Aufwand zur Verschleierung des tatsächlichen Empfängers getrieben wird, zeigt folgender Fall:

- Als Versuch einer so genannten Umgehungslieferung ist die Absicht einer iranischen Beschaffungseinrichtung anzusehen, bei einer baden-württembergischen Firma Produkte zu beschaffen, die für das iranische Raketenprogramm hätten verwendet werden können. Da das Produkt wegen der Proliferationsrelevanz nicht in den Iran geliefert werden durfte, wurde der Export abgelehnt.

Im Jahr 2001 erteilte eine Firma in China, die als Beschaffungsfirma beziehungsweise Zwischenhändler für das iranische Raketenprogramm bekannt ist, einen vergleichbaren Auftrag. Sie nannte als Begründung dafür einen unverdächtigen zivilen Verwendungszweck sowie als tatsächlichen Empfänger des bestellten Produkts eine hier als proliferationsrelevant bekannte Einrichtung im Iran. Die Ausfuhr (über China in den Iran) wurde ebenfalls abgelehnt.

Eine ganze Reihe staatlicher und halbstaatlicher iranischer Einrichtungen im Bundesgebiet sowie zahlreiche ganz oder teilweise in iranischem Eigentum befindliche Firmen nach deutscher Rechtsform bieten den Nachrichtendiensten des Iran ideale Stützpunkte mitten im Operationsgebiet. Zudem bindet auch der Iran seine an westeuropäischen Forschungseinrichtungen in Ausbildung befindlichen Studenten und Austauschwissenschaftler systematisch in die nachrichtendienstliche Beschaffung ein („Wissenstransfer“).

3.3.2 Volksrepublik Nordkorea

Nordkorea betreibt ein ehrgeiziges atomares und konventionelles Rüstungsprogramm. Es ist bestrebt, westliche Technologien und Ausrüstungsgegenstände zu beschaffen. Zur Beschaffung von proliferationsrelevanten Techniken nutzen die nordkoreanischen Nachrichtendienste die diplomatischen Vertretungen ihres Landes oder bedienen sich des weit gespannten Netzes kleiner Beschaffungsfirmen. Güter, die Ausfuhrbeschränkungen unterliegen, werden zur Verschleierung des tatsächlichen Beschaffungszwecks mittels manipulierter Endverbrauchererklärungen beziehungsweise durch Umleitung über ein Drittland nach Nordkorea verbracht. Die Anstrengungen der politischen Führung, das Atomwaffenprogramm voranzutreiben, befähigen das Land - auch nach eigenen Angaben - zum eigenständigen Bau von Nuklearwaffen.

Gerade in den exportorientierten Ländern Baden-Württemberg und Bayern laufen Unternehmen schnell Gefahr, zu Verstößen gegen das Außenwirtschaftsgesetz (AWG) und das Kriegswaffenkontrollgesetz (KWKG) verleitet zu werden oder gar mit dem Strafrecht in Konflikt zu geraten. Davon betroffen sind vor allem Firmen, die entsprechende Genehmigungsvoraussetzungen für Exporte in Krisengebiete beachten müssen.

- Im Mai 2004 wurde der Geschäftsführer einer Firma in **Königsbronn/Krs. Heidenheim** vor dem Landgericht Stuttgart wegen des Verstoßes gegen das Außenwirtschaftsgesetz (AWG) und das Kriegswaffenkontrollgesetz (KWKG) zu einer Freiheitsstrafe von vier Jahren verurteilt. Hintergrund des Urteils war sein Versuch, 214 Aluminiumrohre mit einem Gesamtgewicht von rund 22 Tonnen mit Hilfe einer Hamburger Firma ohne die erforderliche Genehmigung aus dem Europäischen Gemeinschaftsgebiet über China nach Nordkorea auszuführen. Die Spezifikationen und Abmessungen der Rohre sind für die Herstellung von Gasultrazentrifugen zur Produktion von waffenfähigem Uran für Kernwaffen oder sonstige Kernsprengkörper geeignet. Die Liefere-

rung konnte noch auf dem Seeweg gestoppt werden. Der Geschäftsführer des beteiligten Hamburger Transportunternehmens, der in die verbotene Ausfuhr eingebunden war, wurde zu einer Freiheitsstrafe von einem Jahr und drei Monaten auf Bewährung verurteilt.

Zuwiderhandlungen gegen Ausfuhrverbote und Embargobestimmungen werden zunehmend mit dem Verdacht der geheimdienstlichen Agententätigkeit in Zusammenhang gebracht, weil eine Steuerung durch den jeweiligen Nachrichtendienst vermutet beziehungsweise nicht ausgeschlossen werden kann.

3.4 Westliche Wirtschaftsnationen

Auch westliche Industrienationen bedienen sich angesichts eines verschärften internationalen Wettbewerbs ihrer Nachrichtendienste um Wettbewerbsvorteile für die einheimische Wirtschaft zu erlangen. Eine systematische Wirtschaftsspionage gegen die Bundesrepublik Deutschland konnte aber bislang nicht festgestellt werden.

Die Ansatzmöglichkeiten für illegale Informationsbeschaffungen sind zahlreich. Es muss davon ausgegangen werden, dass Nachrichtendienste interessierende Projekte in Forschung und Entwicklung fremder Staaten aufmerksam mit geeigneten Maßnahmen der Informationsbeschaffung begleiten, um gewonnene Erkenntnisse der Wirtschaft ihres Landes zugute kommen zu lassen.

Der Vorteil westlicher Staaten besteht in den besseren technischen Aufklärungsmöglichkeiten mit Hilfe der Satelliten-, Kommunikations- und Nachrichtentechnik. Ein gegenüber Angehörigen dieser Staaten vorhandener Vertrauensvorsprung eröffnet auch bessere Zugangschancen beim Einsatz menschlicher Quellen zur Nachrichtengewinnung. Die als „Human Intelligence“ bezeichnete Informationsgewinnung ist der letztlich doch nur punktuell einsetzbaren technischen Aufklärung immer noch überlegen und wird deshalb weiterhin genutzt. Die hierzu eingeschleusten oder „eingekauften“ Firmenmitarbeiter verfügen über dauerhafte Zugänge und können ihr Wissen sowie sensibles Material den Auftraggebern kontinuierlich zukommen lassen.

Die durch die Globalisierung bedingte Beteiligung ausländischer Firmen an deutschen Unternehmen eröffnet weitere Möglichkeiten der Ausspähung. Staaten oder Konkurrenzfirmen können sich als Venture-Capital-Geber, Firmenaufkäufer oder im Rahmen eines Jointventure Zugang zu vertraulichen Firmendaten verschaffen.

4. Schwerpunkte der Spionage

Illegale Informationsbeschaffung vollzieht sich nicht nach weltweit einheitlichem Muster. Jeder Staat betreibt sie in Abhängigkeit von seinen spezifischen Bedürfnissen und unter Berücksichtigung der ihm zur Verfügung stehenden operativen Möglichkeiten. Bei der Ausspähung selbst kommt es immer auf einen sachgerechten Kompromiss zwischen Dringlichkeit und Vollständigkeit der Information an.

4.1 Auswahl der Zielobjekte

Zur Beurteilung der Frage, ob ein bestimmtes Unternehmen als Zielobjekt in Betracht kommt, hat sich das Instrument der Zielobjektanalyse bewährt. Dabei wird eine Reihe unternehmensspezifischer Gesichtspunkte - wie Struktur, Zugangsmöglichkeiten, Personalaufbau und Sicherheitseinrichtungen - unter die Lupe genommen.

Zielobjektanalyse

- ❖ Unternehmensgeschichte
- ❖ Unternehmenspolitik
- ❖ Unternehmensstruktur
 - ♦ Eigentumsverhältnisse, Verzahnung mit anderen Unternehmen, Leistungskapazität, Produkte
- ❖ Lage, bauliche Besonderheiten, Verbindungswege zu wichtigen Produktionsstätten
- ❖ Zugangsmöglichkeiten, Maßnahmen des Objektschutzes
- ❖ Personalaufbau, Auflistung aller Geheimnisträger
- ❖ Handelsbeziehungen, Reisen von Firmenangehörigen

Ergebnis der Zielobjektanalyse

Detaillierte Aussage über

- ❖ lohnenswerte Ausspähungsbereiche
- ❖ operative Ansatzpunkte in Bezug auf die unterschiedlichen Wissensträger (Personen/DV-Datenträger/Akten)
- ❖ den potenziellen Ertrag
- ❖ das Aufdeckungs- und Sanktionsrisiko

Eine solche Analyse erlaubt eine detaillierte Aussage über lohnenswerte Ausspähungsbereiche, operative Ansatzpunkte in Bezug auf die unterschiedlichen Wissensträger (Personen, DV-Datenträger, Akten), den potenziellen Ertrag sowie das Aufdeckungs- und Sanktionsrisiko.

Das Interesse richtet sich in erster Linie auf die Branchenführer beziehungsweise auf forschungsintensive Unternehmen mit herausragendem Know-how. Die Betriebsgröße allein ist kein entscheidender Faktor. Auch innovative Klein- und Mittelbetriebe sind lohnenswerte Ausspähungsziele, zumal zahlreiche Mittelständler mit ihren Produkten sogar Weltmarktführer sind.

Dass auch neu gegründete Unternehmen interessante Ausspähungsziele sein können, zeigt folgendes Beispiel. Über eine bestehende Sicherheitsverbindung wurde das Bayerische Landesamt für Verfassungsschutz auf folgenden Sachverhalt aufmerksam gemacht:

- Ein Start-up-Unternehmen im Hightech-Bereich aus dem Raum **München** stellte sich mit einem weltweit einmalig entwickelten Gerät für Navigationstechnik auf dem Markt vor. Es suchte Geldgeber für diese Geschäftsidee. Es bot sich mit dieser innovativen Produktentwicklung unter anderem bei internationalen Investment-Foren beziehungsweise Kapitalbörsen an. Da solche Informationen gezielt durch fremde Nachrichtendienste ausgewertet werden, erweckte das Auftreten der Firma auch das Interesse der Geheimdienste. Unter den Interessenten befanden sich deshalb auch Unternehmen, die dem Bayerischen Landesamt für Verfassungsschutz als Tarnorganisationen der Nachrichtendienste ihrer Länder bekannt sind. Die vermeintlichen Kunden erkundigten sich sehr genau über die Weiterentwicklungen und Möglichkeiten des Produkts.

Im Laufe der Gespräche wurden auch Scheinofferten abgegeben, die für die Firmenleitung nicht als solche erkennbar waren. Der Jungunternehmer ging deshalb auf das lukrativste Angebot ein. Unter dem Vorwand, das Geschäft dort endgültig abzuschließen, wurde er in das Heimatland des vermeintlichen Geschäftspartners eingeladen. Die Übernahme der gesamten Auslagen dieser Geschäftsreise durch den Einladenden nahmen dem Firmenchef die letzten Zweifel an der Aufrichtigkeit des Angebots.

Wieder zurück in Bayern, musste der Unternehmer feststellen, dass die finanziellen Zusagen nicht eingehalten wurden und sein Besuch offensichtlich missbräuchlich genutzt wurde. Es muss davon ausgegangen werden, dass die Gespräche lediglich der Aufklärung der Einsatzfähigkeit des Geräts und der möglichen Konkurrenzsituation auf dem Markt dienten. Das Unternehmen musste daraufhin Insolvenz anmelden.

4.2 Schwerpunkte der Ausforschung

4.2.1 Bevorzugte Zielbereiche

Die Interessen fremder Nachrichtendienste haben in den letzten Jahren keine wesentlichen Änderungen erfahren. Sie sind weiterhin außerordentlich breit gefächert und können - je nach Bedarf des Auftraggebers - sowohl die Aufklärung des Wirtschaftspotenzials, der Wirtschaftspolitik und wirtschaftlicher Strategien als auch die Ausspähung der industriellen Forschung und Produktion, des Handels und der wirtschaftlichen Organisation umfassen.

Hochindustrialisierte Länder sind in erster Linie an wirtschaftlichen oder wirtschaftspolitischen Strategien interessiert, während es Staaten mit Technologierückstand eher auf Ergebnisse der Grundlagenforschung und konkrete Produkte abgesehen haben. Am Beispiel der Schwellenländer wird die Problematik besonders deutlich. Sie verfügen meist über umfangreiche Ressourcen an (teilweise hochqualifizierten) Arbeitskräften im Niedriglohnbereich, große Grundflächen und Rohstoffvorkommen. Mit dem erforderlichen Know-how auf den Gebieten der Hochtechnologie können sie dann zu ernsthaften Konkurrenten für die etablierten Industrienationen heranwachsen.

Schwerpunkte der Informationsbeschaffung in den Unternehmen selbst sind zukunftsichernde und strategisch bedeutsame Hoch- und Querschnittstechnologien und zwar nicht nur solche mit direktem militärischem Bezug. Zu den wichtigsten Technologiebereichen gehören:

- Informationsverarbeitung/Kommunikationstechnik/Elektronik,
- Hochleistungsrechner,
- Luft- und Raumfahrt/Verkehrstechnik,
- Werkstoffe,
- Produktionstechnik,
- Biotechnik und Medizin,
- Nanotechnologie sowie
- Energie- und Umwelttechnik.

In Baden-Württemberg und Bayern haben sich die Ausspähungsbemühungen in den letzten Jahren auf die hier traditionell besonders stark vertretenen Branchen Maschinen-/Fahrzeug- und Motorenbau sowie Elektronik/Mess- und Steuerungstechnik konzentriert.

4.2.2 Besonders gefährdete Unternehmensbereiche

Das Ausforschungsinteresse beschränkt sich keineswegs auf die Beschaffung fertiger Endprodukte, sondern gilt - von der Idee über die Forschung, Entwicklung, Herstellung und Vermarktung - grundsätzlich dem gesamten Entstehungs- und Vermarktungszyklus eines Wirtschaftsguts. Solche Informationen, die von Nachrichtendiensten nach der Art eines Puzzles zusammengefügt werden, können - von der Unternehmensleitung über die Forschung und Entwicklung bis hin zur EDV - auf jeder Ebene und in allen Bereichen eines Unternehmens anfallen.

Ausspähungsgefährdete Unternehmensbereiche

Organisationseinheiten	Ausspähungsinhalte	Gefährdete Funktionsträger/ Bereiche
Aufsichtsorgane	strategische/taktische Entscheidungen	Gesellschafter, Beirat, Aufsichtsrat
Unternehmensleitung	strategische/taktische Entscheidungen	Geschäftsführer, Vorstand, Sekretariat, Controller, Revisoren
Verwaltung Personalabteilung Betriebsrat	Personenbezogene Daten, strategische Entscheidungen	Telefonzentrale, Arbeitnehmervertretung/ Wirtschaftsausschuss
Forschung Entwicklung	Produktideen/-strategien Designstudien	Projektleiter, Laborant
Produktion	Produktideen Konstruktionsunterlagen Herstellungsverfahren Qualitätsprüfungsdaten Steuerungssysteme	Verfahrenstechniker, Qualitätsprüfer, Monteure, Werkstoffprüfer
Einkauf Verkauf	Lieferantendaten Kundendaten Marketingstudien Marketingstrategien	Einkaufsleiter, Vertriebsleiter
Finanzwesen	Kalkulationsunterlagen Budgetplanung Investitionsvorhaben	Sachbearbeiter
Datenverarbeitung	Zentraler Zugriff auf alle Datenbestände	Operator, Programmierer, Wartungstechniker, Systemadministrator

5. Methoden der Spionage

Fremde Nachrichtendienste versuchen mit immer neuen Methoden ihre Vorgehensweise zu verschleiern. Dennoch sind bestimmte Grundmuster deutlich zu erkennen, die bei der Suche nach speziellen Informationen durchaus auch gebündelt eingesetzt werden. Neben klassischen nachrichtendienstlichen (konspirativen) Spionagemethoden nutzen ausländische Staaten auch legale Beschaffungsmöglichkeiten. Diese können eine Vorstufe für illegale Aufklärungsaktivitäten bilden und ebenfalls eine schädigende Wirkung mit gravierenden Folgen für das betroffene Unternehmen entfalten. Und wenn es gar nicht anders geht, wird auch zu kriminellen Methoden wie Diebstahl, Unterschlagung, Urkundenfälschung, Betrug und Erpressung gegriffen.

Oft geübte Praxis ist der Diebstahl oder die zeitweise Entwendung von Notebooks auf Dienstreisen. Zum Beispiel wurden Angehörigen von Forschungs- und Entwicklungsabteilungen baden-württembergischer und bayerischer Unternehmen während Grenzkontrollen bei der Einreise in mehrere Länder die mitgeführten Rechner für einen längeren Zeitraum entzogen. Es ist davon auszugehen, dass die darauf gespeicherten Daten kopiert und dortigen Bedarfsträgern zur illegalen Weiterverwendung zugänglich gemacht wurden.

Aber auch bei Hotelaufenthalten im Ausland oder bei der Nutzung öffentlicher Verkehrsmittel können mitgeführte Computer das Ziel konspirativer Zugriffe sein. Speicherinhalte wie technische Dokumentationen, Strategiepapiere oder Kalkulationsunterlagen sind leicht zu kopieren und missbräuchlich weiter zu verwenden. Der Schaden durch den Verlust der Daten kann dabei den Schaden, der durch Diebstahl der Hardware entsteht, erheblich übersteigen.

Dem Bayerischen Landesamt für Verfassungsschutz sind mehrere Fälle abhanden gekommener Informations- und Kommunikationsgeräte bekannt geworden. Die Umstände und die Motivlage für das Verschwinden solcher Geräte können meist nicht sofort verifiziert werden.

Der Geschäftsführer einer bayerischen Firma wandte sich an die Spionageabwehr des Landesamts für Verfassungsschutz in München. Das Gespräch bezog sich auf den erneuten unerklärlichen Verlust eines firmeneigenen Notebooks - bereits vor Jahresfrist musste das Unternehmen den Verlust eines Notebooks feststellen.

Nach Beurteilung dieses Falles durch das Bayerische Landesamt für Verfassungsschutz besteht der Verdacht, dass es sich bei beiden Fällen um Wirtschaftsspionage beziehungsweise Konkurrenzspionage handeln könnte. So

waren auf den Festplatten der Computer überwiegend schutzbedürftige Informationen gespeichert. Außerdem waren im direkten Umfeld des Standorts der Rechner höherwertige Computer gestanden, die offenbar nicht das Interesse der Diebe erweckten. Es kann daraus der Schluss gezogen werden, dass nicht die Hardware, sondern die gespeicherten Informationen Ziel des Diebstahls waren.

Im Einzelnen kommen folgende Methoden der Wirtschaftsspionage in Betracht:

Methoden der Wirtschaftsspionage



5.1 Auswertung offener Quellen

Nachrichtendienstlich interessante Informationen werden zu einem großen Teil durch die Auswertung frei zugänglicher Quellen beschafft. Dies trifft besonders auf wissenschaftliche Ausarbeitungen wie Forschungsberichte und Diplomarbeiten zu. Aber auch Werkszeitungen, Handbücher, Dokumentationen im Zusammenhang mit Qualitätszertifizierungen oder Beschreibungen zu versichernden Risiken, Patent-/Lizenzunterlagen und nicht zuletzt Firmenpräsentationen im Internet sowie Werbe- und Informationsunterlagen können interes-

sante Einblicke mit dem Risiko der missbräuchlichen Verwendung der entsprechenden Daten gewähren.

Die Bereitschaft der Unternehmen zu kundenfreundlicher Transparenz bietet fremden Nachrichtendiensten ideale Ansatzpunkte für diese Form der Informationsbeschaffung. Die systematische Auswertung offener Quellen lässt nicht nur wertvolle Rückschlüsse auf aktuelles Know-how und zukünftige Projekte zu, sondern liefert auch detaillierte Persönlichkeitsbilder. Entscheidungsträger und Mitarbeiter im Forschungsbereich können mit diesem Hintergrundwissen gezielt nachrichtendienstlich angegangen werden.

5.2 Gesprächsabschöpfung

Die offene Gewinnung von Informationen bei gutgläubigen Gesprächspartnern gehört ebenfalls zum Handwerkszeug von Nachrichtendiensten: Vor allem bei Messen, Kongressen und Werksbesichtigungen sind im Verlauf von Verkaufsverhandlungen oder Fachgesprächen Betriebsgeheimnisse schnell offenbart. Aber auch abends an der Bar oder bei gesellschaftlichen Anlässen kommt es immer wieder vor, dass Unternehmensvertreter in Fachdiskussionen verwickelt und ihnen bei dieser Gelegenheit wertvolle Informationen entlockt werden. Und wer hat nicht schon bei einer Zugfahrt oder Flugreise interessante Firmeninterna erfahren?

5.3 Teilnahme am Wirtschaftsleben

Wettbewerb und Kooperation liegen oft eng beieinander. Wettbewerber fusionieren auf bestimmten Geschäftsfeldern oder gründen Gemeinschaftsunternehmen. Solche Transaktionen erlauben dem Partner den Zugriff auf Firmengeheimnisse. Bei Unternehmenskooperationen treffen häufig unterschiedliche Sicherheitsphilosophien aufeinander, was den Abfluss von Know-how begünstigen kann. Für fremde Nachrichtendienste bieten „gemischte“ Firmen und Jointventures geeignete Ansatzpunkte, nachrichtendienstlich tätige Personen abzutarnen und zu legendieren. Aber auch die Akquisitionsphase bietet einem potenziellen Kunden viele Möglichkeiten der kostenlosen Know-how-Beschaffung, z.B. über die Anforderung detaillierter Produkt- und Leistungsbeschreibungen im Rahmen von Angeboten und/oder sogar die Entsendung von Personal zur Begutachtung der Firma des Lieferanten.

Eine - wenn auch marktwirtschaftliche - Variante des ungewollten internationalen Know-how-Abflusses ist die Firmenübernahme durch Mehrheitsbeteiligung oder kompletten Unternehmensaufkauf. Beispielhaft hierfür ist die wachsende Zahl ausländischer Unternehmensbeteiligungen an deutschen Firmen der

Wehrtechnikbranche. Aber auch Unternehmen der Konsum- und Investitionsgüterindustrie mit zukunftsweisendem Firmen-Know-how befinden sich im Visier aufstrebender Direktinvestoren aus dem Ausland. Bei solchen Transaktionen geraten nicht nur das spezielle Wissen der zu übernehmenden Firma in fremde Hände, sondern auch die möglicherweise sensiblen Beziehungen zu Zulieferern und Kunden etc.

5.4 Einsatz von Agenten

Gerade im Bereich der nachrichtendienstlich gesteuerten Wirtschaftsspionage erweisen sich offenbar trotz aller technischen Möglichkeiten menschliche Quellen auch weiterhin als unverzichtbar. Ihr besonderer Wert besteht darin, dass sie nicht nur kontinuierlich aus einem Zielobjekt agieren, sondern zugleich auch z.B. beschaffte Informationen fachlich bewerten können.

Eingeschleuste (Leiharbeitskräfte, Studenten, Praktikanten) oder angeworbene Innentäter stellen aufgrund ihrer Zugangsmöglichkeiten und der Kenntnis innerbetrieblicher Schwachstellen die größte Gefahr für die Sicherheitsinteressen eines Unternehmens dar. Aber auch Außentäter können großen Schaden anrichten. Nicht nur Großunternehmen sind heute auf externe Spezialisten angewiesen. Aus Kostengründen erfolgt auch bei mittleren und kleinen Unternehmen ein Outsourcen von betrieblichen Funktionsbereichen mit hohem Erkenntniswert. Ein Risiko ist regelmäßig dann vorhanden, wenn den Dienstleistern wesentliche Betriebsinterna zur Erfüllung ihrer Aufgaben zugänglich gemacht werden müssen.

5.5 Einsatz technischer Mittel

5.5.1 Allgemeine Lagedarstellung

Nicht erst seit dem 11. September 2001 warnen Experten vor Angriffen auf Informationsinfrastrukturen. Die Diskussionen um die Abhängigkeit moderner Informationsgesellschaften von der Verfügbarkeit, Vertraulichkeit und Integrität der Daten und Systeme einerseits und die Verletzlichkeit der Technologien andererseits sind nicht neu - verändert haben sich seither „nur“ die Dimensionen möglicher Bedrohungen und Schäden und die damit verbundene öffentliche Wahrnehmung potenzieller Gefahren. Apokalyptisch anmutende Szenarien des „Information Warfare“ oder des „Cyber-Terrorismus“ haben ihren Ursprung in bereits bekannten, latenten Schwachstellen der Systeme und ihres Umfelds. Informations- und Telekommunikationssysteme (ITS) eignen sich generell sowohl als Ziel als auch als Mittel zum Zweck. Dabei spielen die technischen Rahmenbedingungen eines weltweiten IT-Einsatzes sowie konkrete Sicher-

heitslücken eine beachtliche Rolle. Sie bieten Ansatzmöglichkeiten für Angreifer, die Know-how-Diebstahl zum Ziel haben. Der finanzielle und technische Aufwand für Erfolg versprechende Angriffe ist oftmals im Vergleich zum potenziellen Schaden gering. Geografische, zeitliche und sprachliche Barrieren spielen in diesem Zusammenhang ebenso wenig eine Rolle wie das technische Know-how des Angreifers. Diesem stehen leistungsfähige und weltweit frei verfügbare „Einbruchswerkzeuge“ zur Verfügung. Präventive technische Sicherheitsmaßnahmen halten mit den originären Entwicklungs- und Innovationszyklen längst nicht mehr Schritt. Das Risiko der Entdeckung ist gering.

Die missbräuchliche Nutzung beziehungsweise die allgemeine Bedrohung der Informationstechnik lassen sich ganz grob in drei Kategorien unterteilen. Sie sind zunächst unabhängig von der jeweiligen Angriffsmotivation zu sehen. Angriffe können sowohl von innen als auch von außen erfolgen:

- Datenspionage:** Dieser Angriff umfasst jede Form des unerlaubten Versuchs, sich Zugang zu Daten zu verschaffen, um sie zu kopieren, zu kontrollieren, zu beeinflussen oder missbräuchlich zu nutzen.
- System- und Datensabotage:** Ziel eines Angreifers ist es, Systeme und/oder Daten nachhaltig zu stören, zu manipulieren, zu blockieren, zur falschen Zeit oder am falschen Ort wieder einzuspielen, zu filtern oder zu zerstören.
- Information Warfare:** Dieser Begriff umschreibt eine Fülle gezielter Angriffe auf Informationsinfrastrukturen und davon abhängige Einrichtungen des Staates und der Wirtschaft. Letztlich ist Ziel solcher Attacken, eigene Informationsüberlegenheit zu schaffen und zu bewahren, um militärische, politische, weltanschauliche, ethnische oder ökonomische Interessen gegenüber Dritten durchzusetzen.

Die „Schwachstelle Mensch“ ist in komplexen Informationsinfrastrukturen einer der Hauptgründe für erfolgreich verlaufende technische Angriffe. Nach der 2004 erschienenen aktuellen <kes> Microsoft-Sicherheitsstudie⁹ schätzen die Befragten nach wie vor „*Irrtum und Nachlässigkeit eigener Mitarbeiter*“, aber auch „*unbeabsichtigte Fehler von Externen*“ als größtes Sicherheitsrisiko ein.

⁹ <kes> - Die Zeitschrift für Informations-Sicherheit: „Lagebericht zur Informations-Sicherheit“, Jahrgang 2004, Hefte 4, 5 und 6.

Neben den bisher dargestellten allgemeinen Bedrohungen gibt es eine Reihe typischer Risiken und Schwachstellen beim Einsatz von ITS, die unbeabsichtigte Informationsverluste nach sich ziehen und Angreifern illegales Erlangen sensibler Informationen erleichtern können:

- Missbräuchliche Nutzung frei verfügbarer, offener und sensibler Informationen in Netzen (Internet),
- Angriffe durch Innentäter am (unternehmens-/behörden-) eigenen Computer,
- sorgloser Umgang mit Passwörtern und Nutzeridentifikationen,
- mangelhafte Installation und Konfiguration von IT-Systemen,
- Hacking-, Abhör- und Lauschangriffe auf Räume, Netze, (mobile) IT-Systeme und Telekommunikationseinrichtungen,
- unbefugte Zugriffe auf logische wie physikalische Datenfernübertragungskanäle, interne (vor Ort) und externe (Remote-Access) Fernwartungs- und Administrationskomponenten,
- Einschleusung von Viren, Würmern, Trojanern und anderen ausführbaren Programmen mit Schadfunktion,
- Manipulation von System- und Anwendungssoftware sowie Diebstahl von Hardware/-komponenten (PCs, Laptops, Notebooks, mobile beziehungsweise kabellose IT- und TK-Systeme, Datenträger und sonstige Speichermedien).

Die meisten der für unser Gemeinwesen zum Teil überlebensnotwendigen Infrastrukturen (Verkehr, Energieversorgung, Gesundheitsvorsorge, Rettungsdienste, Banken, Rechenzentren, Kommunikationsnetze etc.) befinden sich in Händen der Privatwirtschaft. In sicherheitsmäßiger Hinsicht sind sie keine Inseln, sondern sind vielmehr in internationale Strukturen von Informations- und Kommunikationssystemen eingebunden und tangieren insofern fast alle Bereiche des Gemeinwesens.

Der Schutz kritischer Infrastrukturen muss dabei aus der Perspektive der Terrorismusabwehr sowie der Perspektive der Naturkatastrophe oder größerer Unglücksfälle betrachtet werden. Die Verfassungsschutzbehörden des Bundes und der Länder sowie das Bundesamt für Sicherheit in der Informationstechnik

(BSI) arbeiten deshalb gemeinsam mit anderen staatlichen und privaten Sicherheitsorganisationen intensiv an Lagebildern sowie an personellen, materiellen und organisatorischen Schutzkonzepten. Zahlreiche Angriffe auf öffentliche und private - nationale Grenzen überschreitende - IT-Infrastrukturen legen nahe, sich dem Thema der IT-Sicherheit aus repressiver und präventiver Sicht anzunehmen.

5.5.2 Täterbild und Fälle

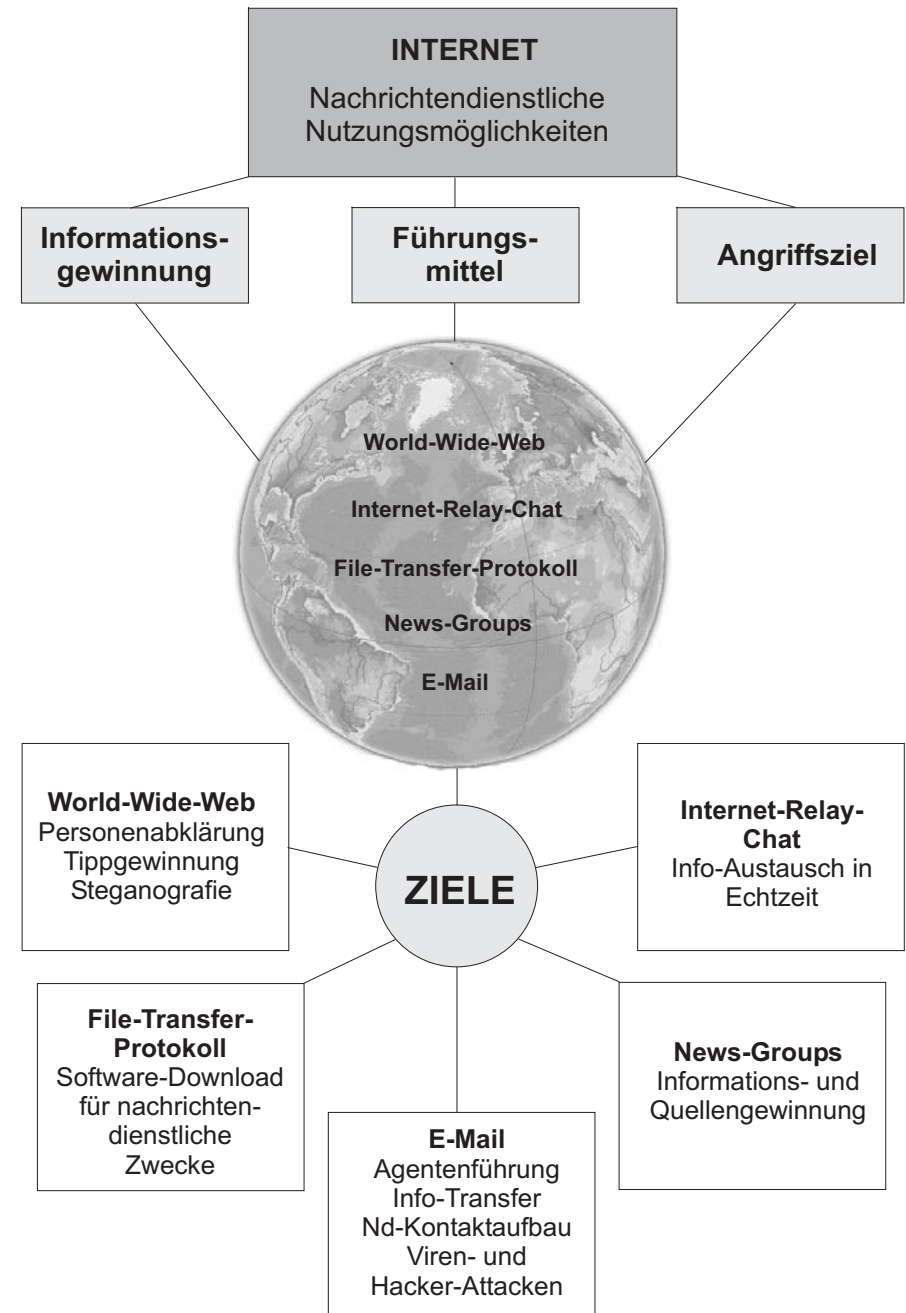
Eine Analyse erkannter Fälle führte zu Täterbildern, die vom illoyalen Mitarbeiter über politisch motivierte Hacker oder Einzeltäter, Tätergruppen der Organisierten Kriminalität, extremistische/terroristische Gruppierungen bis hin zu Nachrichtendiensten fremder Staaten reichten. Es zeigte sich, dass klassische Außentäter versuchen, möglichst unentdeckt und langfristig über legale wie illegale Zugänge Informationen aus angegriffenen IT- oder Telekommunikationssystemen zu beschaffen oder gar die Kontrolle über die „gehackten“ Systeme zu übernehmen.

Annähernd 70 bis 80 Prozent der IT-Angriffe sind Innentätern¹⁰ zuzuschreiben, d. h. sie erfolgen durch illoyale aktive Beschäftigte und ehemalige Mitarbeiter. Ihre Kenntnisse über innerbetriebliche Schwachstellen sowie über die vielfach ungehinderten und unkontrollierten Zugangs- und Zugriffsmöglichkeiten machen sie zur größten Gefahr für die Sicherheitsinteressen von Unternehmen.

Nachrichtendienste sind heutzutage auch auf vielfältige Weise im Internet präsent: z.B. in eigener Sache mit teilweise sehr aufwändig gestalteten Homepages, aber auch im Hinblick auf ihre Beschaffungsaufträge. Sie nutzen das Internet nicht nur als Mittel zur Steuerung und Führung von Agenten, sondern aufgrund seiner anonymen Struktur auch als attraktives Mittel nachrichtendienstlicher Informationsgewinnung.

Online lassen sich beispielsweise über das WorldWideWeb (WWW) aktuelle und nachrichtendienstlich hochwertige Informationen aus weltweit verteilten Quellen zusammentragen. Die Abklärung interessanter Einzelpersonen (Lebenslauf mit Bild, Adresse, Telefonnummern, Aufgabenspektrum, wissenschaftliche Veröffentlichungen, Hobbies etc.) oder die Erhebung neuester Forschungsberichte via Internet können bis zu einem gewissen Grad riskante Agentenoperationen ersetzen und erfordern zudem einen wesentlich geringe-

¹⁰ Prof. Dr. Heinz Thielmann (Fraunhofer Institut SIT Darmstadt), Vortrag anlässlich der Tagung des Münchner Kreises „Sicherheit und Schutz in der Informationsgesellschaft“ am 18. September 2003 in München, URL: www.muenchner-kreis.de.



ren finanziellen und zeitlichen Aufwand. Die Ergebnisse lassen sich verschlüsselt oder mit Hilfe steganografischer Verfahren¹¹ der Führungsstelle übermitteln. Effektivität und Erfolg der nachrichtendienstlichen Verbindung zwischen Agenten und ihren Führungsoffizieren hängen maßgeblich davon ab, wie sicher der Informationsaustausch funktioniert. Seit dem fast schon legendären KGB-Hacker-Fall im Jahr 1989¹² sind in der Bundesrepublik Deutschland keine Computerspionagefälle mehr bekannt geworden, die so eindeutig und beweisbar der nachrichtendienstlichen Szene zugeordnet werden können. Andererseits kommt der Nichtständige Ausschuss des Europäischen Parlaments über das Abhörssystem ECHELON¹³ in seinem Abschlussbericht¹⁴ zu folgendem Fazit:

„Das Risiko- und Sicherheitsbewusstsein bei kleineren und mittleren Unternehmen ist bedauerlicherweise oft unzureichend und die Gefahren der Wirtschaftsspionage und des Abhörens von Kommunikation werden oft nicht erkannt. Da auch bei europäischen Institutionen (...) das Sicherheitsbewusstsein nicht immer sehr ausgeprägt ist, besteht unmittelbarer Handlungsbedarf.“

Diese Aussage deckt sich mit den praktischen Erfahrungen der beiden Landesämter für Verfassungsschutz.

In den letzten Jahren wurden sowohl im UNO-Hauptquartier in New York als auch in einem Gebäude des EU-Ministerrats - u. a. in den Büros und Besprechungsräumen Deutschlands, Frankreichs, Großbritanniens und anderer Staaten - professionelle Abhöranlagen entdeckt. Der Lauschangriff in Brüssel wurde von der EU offiziell bestätigt. Die laufenden Ermittlungen haben jedoch bis heute keinen Hinweis auf den Urheber erbracht. In beiden Fällen wird besonders von der Presse ein nachrichtendienstlicher Hintergrund vermutet, dieser konnte aber bis heute nicht nachgewiesen werden.

¹¹ Hierbei werden Informationen in Bildern oder Musikdateien versteckt, die zum Beispiel per Mail verschickt oder gänzlich offen über eine Website in das Internet eingestellt werden können. Da diese Veränderungen der Ausgangsdatei weder sicht- noch hörbar sind, ist ihre Entdeckung praktisch nicht möglich.

¹² Vgl. ausführliche Falldarstellung in „Computerspionage - Risiken und Prävention“, Bundesministerium für Wirtschaft / BMWI, Bonn, Publikation Nr. 444, Stand Juli 1998, URL: www.genial-media.biz/Downloads/BSI-Computerspionage.pdf.

¹³ ECHELON ist ein von den USA, Großbritannien, Kanada, Australien und Neuseeland betriebenes elektronisches Aufklärungssystem. Weitere Informationen zum Thema ECHELON können im Internet u.a. unter www.heise.de/tp (Heise-Verlag, Telepolis, Echelon-Spezial) und www.fas.org (Federation of American Scientists) abgerufen werden.

¹⁴ Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON), 2001/2098 (INI) vom 11. Juli 2001, RR\445698DE.doc, PE 305.391/, URL: http://www.europarl.eu.int/tempcom/echelon/pdf/rapport_echelon_de.pdf.

Entsprechende Tools und die notwendige Elektronik zur Durchführung von Lauschangriffen sind über das Internet oder in „Spionläden“ relativ einfach zu beschaffen. Mit Geräten, die oft nur wenig kosten, können teure Entwicklungen und Wettbewerbsvorteile entwertet oder gar wirtschaftliche Existenzen in Frage gestellt werden. Immer leistungsfähigere, global vernetzte Informations- und Kommunikationssysteme erleichtern den Zugriff auf das weltweit verfügbare unverschlüsselte Wissen. Außerdem hinterlassen elektronische Angriffe auch weniger Spuren als Agenten oder andere Formen traditioneller Spionage.

5.5.3 Internet- und E-Mail-Überwachung

Neben ECHELON gibt es eine Reihe anderer Überwachungssysteme und -programme, die eine strategische und flächendeckende Internet- und E-Mail-Überwachung gewährleisten. Nachrichtendienste, Polizeibehörden und Sicherheitsorganisationen fremder Länder setzen solche Systeme im staatlichen Auftrag ein, teilweise auf Basis entsprechender Gesetze, die den „Betreibern“ weit reichende Befugnisse einräumen.¹⁵

Seit 1998 überwacht der russische Inlandsgeheimdienst FSB mit dem Überwachungsprogramm SORM II¹⁶ offiziell den gesamten E-Mail- und Internet-Verkehr, der über russische Internet-Service-Provider (ISP) abgewickelt wird. Auf der Grundlage des gleichnamigen Gesetzes müssen die ISP auf eigene Kosten eine Überwachungsschnittstelle einrichten. Die abgehörten Daten werden dann online via Glasfaserkabel in Echtzeit direkt zum Rechenzentrum des FSB übermittelt.

Nach vergleichbaren Standards und Prinzipien arbeitet das vom US-amerikanischen Nachrichtendienst FBI¹⁷ entwickelte Überwachungsprogramm DSC1000, besser bekannt unter dem ursprünglichen Namen „Carnivore“ („Fleischfresser“). Nach Einschätzung von Experten sind die USA mit DSC1000 führend in der Überwachung des E-Mail-Verkehrs.

In Großbritannien sorgt das RIP-Gesetz¹⁸ seit seinem Inkrafttreten im Jahr 2000 für öffentliche Diskussionen. Die britischen ISP sind demnach verpflichtet, ohne richterlichen Beschluss dem britischen Inlandsnachrichtendienst MI5 und der Polizei den gesamten Internet-Datenverkehr zugänglich zu machen.

¹⁵ Bundeszentrale für politische Bildung, Schriftenreihe (Bd. 386), Die Politik der Infosphäre, Teil V Globale Sicherheit, Ziffer 5.1 Überwachung.

¹⁶ „Sistema Operativno-Rozysknykh Meropriyatij“ (System operativ-aufklärerischer Maßnahmen, SORM II).

¹⁷ Federal Bureau of Investigation (FBI), US-Bundespolizei mit Zuständigkeit für die Spionageabwehr.

¹⁸ Regulation of Investigatory Powers Act, URL://www.parliament.the-stationary-office.co.uk/pa/cm199900/cmbills/064/2000064.htm.

Die Übergänge von gesetzlich legitimierten Überwachungsmaßnahmen von Polizei und Nachrichtendiensten zu Zwecken der Strafverfolgung, der Gefahren- und der Terrorismusabwehr hin zu Grauzonenbereichen ohne Regelung der Art und des Überwachungsumfangs sind fließend. In über 60 Ländern werden derzeit entsprechende Einschränkungen, Kontroll- und Überwachungsmaßnahmen vor allem in Bezug auf die freie Internetnutzung praktiziert¹⁹. Simon Davies²⁰ stellt sehr zutreffend fest:

*„Die Überwachung ist zu einer festen Mehrwertkomponente der Architektur von Informations- und Kommunikationstechnologien geworden. Alle Kommunikationssysteme und Netzwerke beinhalten heute irgendeine Form von fester Überwachungskomponente“.*²¹

Neben den bereits dargestellten Möglichkeiten fremder Nachrichtendienste, mittels strategischer Überwachungs- und Abhörsysteme den weltweiten E-Mail-Verkehr zu überwachen, sind heute eine Fülle von Überwachungsprogrammen am freien Markt verfügbar. Sie können durch Unbefugte heimlich installiert und missbräuchlich eingesetzt werden. Diese Programme kontrollieren und protokollieren den gesamten eingehenden wie ausgehenden elektronischen Briefwechsel von einem und an einen PC oder in ein und aus einem Netzwerk. Zusätzlich sind sie in der Lage, sämtliche Nutzeraktivitäten (besuchte Internetseiten, gestartete Anwendungen, Tastaturanschläge, PC-Starts, Chat-Unterhaltungen, Telegramme [ICQ, Yahoo etc.], Peer-to-peer-Aktivitäten, Tauschbörsen, User Logon/Logoff ...) und/oder Netzwerkaktivitäten (grafische Auswertung von Proxies, Routern, Firewalls) zu protokollieren und diese Protokolle verdeckt per E-Mail an die Adresse des Auftraggebers weiterzuleiten.

5.5.4 Spezifische Risiken

5.5.4.1 Lauschangriffe im Büro

Informationsschutzkonzepte für gefährdete Bereiche von Staat und Wirtschaft konzentrieren sich häufig auf digitale Daten in Informations- und Kommunikationssystemen. Oftmals werden aber höchst sensible Vorgänge bei Besprechungen und in Konferenzen sowie vor allem im täglichen Arbeitsablauf erörtert,

ohne dass der „Verletzlichkeit“ des gesprochenen Worts größere Bedeutung beigemessen wird. Nicht zuletzt die vertraute Umgebung des eigenen Büros oder der Geschäftsräume vermittelt ein subjektives Sicherheitsgefühl bei den Besprechungsteilnehmern.

Lauschangriffe klassischer Art auf Büros stellen nach wie vor ein Sicherheitsrisiko dar. Fachleute sprechen gar von einer „Renaissance der Wanzen“²². Folgt man den Darstellungen in der Fachpresse, so befinden sich nach Schätzung von Herstellern inzwischen 500.000 bis 1.000.000 Abhörgeräte im Besitz von Privatpersonen. Außer „Wanzen“ sind auch akustische (Richt- und Körperschallmikrofone, als Mikrofone manipulierte Lautsprecher) sowie optische Lauschmittel (Laser-Abhörsysteme, Infrarotsender und -empfänger) als „Angriffswaffen“ verfügbar.

Als weitere Angriffsvariante gilt die unbefugte und missbräuchliche Nutzung der so genannten kompromittierenden Abstrahlung. Elektronische Geräte (PCs, Monitore, Tastaturen, Drucker, Fax-Geräte, Modems etc.) erzeugen eine hochfrequente elektromagnetische Strahlung. Bei informationsverarbeitenden Geräten führt diese Strahlung auch die gerade bearbeitete Information, den so genannten Klartextanteil, mit sich. Dieser kann mit entsprechendem technischen Aufwand auch noch in einiger Entfernung empfangen, herausgefiltert, aufgezeichnet oder sichtbar gemacht und so die Information „offline“ rekonstruiert und ausgewertet werden.

5.5.4.2 Angriffe auf und über Telekommunikationssysteme/TK-Systeme

5.5.4.2.1 Digitale ISDN-TK-Anlagen

ISDN-TK-Anlagen enthalten eine Fülle nützlicher und sinnvoller Funktionen, die zum Teil jedoch von externen Angreifern missbräuchlich verwendet werden können. Nur in seltenen Fällen sind diese Angriffe oder Manipulationen durch die Nutzer der Anlagen selbst festzustellen. Hinzu kommt, dass die Anwender digitaler TK-Anlagen ihre Systeme größtenteils weder selbst konfigurieren noch administrieren. Ein genauer Überblick über aktuelle Einstellungen oder gar ein nachvollziehbares Protokoll der Anlagenkonfiguration fehlen deshalb. Erschwerend wirkt hierbei auch, dass die TK-Systeme zunehmend komplexer und dadurch „undurchschaubarer“ werden.

Das Spektrum möglicher Gefahren und Bedrohungen umfasst unter anderem die Manipulation oder gar Zerstörung von IT-Geräten oder Zubehör, den Ver-

¹⁹ Reporter ohne Grenzen: Internet Under Surveillance 2004, URL: http://www.rs.org/rubrique.php?id_rubrique=433.

²⁰ Direktor der britischen Cyberrechte-Initiative Privacy International.

²¹ Bundeszentrale für politische Bildung, Schriftenreihe (Bd. 386), Die Politik der Infosphäre, Teil V Globale Sicherheit, Ziffer 5.1 Überwachung.

²² Ansgar Huth, <kes> - Zeitschrift für Informations-Sicherheit „Renaissance der Wanzen“, Heft 2002/4, S. 6ff.

traulichkeitsverlust von in TK-Anlagen gespeicherten Daten, das Abhören von Telefongesprächen, Datenübertragungen und Räumen, Gebührenbetrug sowie den Missbrauch von Remote-Zugängen (interne und/oder externe Fernwartungsschnittstellen). Nicht selten ist festzustellen, dass TK-Anlagen über längere Zeiträume aus Unkenntnis oder Bequemlichkeit der Nutzer noch mit der Standard-Passworteinstellung der Hersteller betrieben werden. Diese werkseitig voreingestellten Passwörter fast aller Anlagentypen sind in einschlägigen Hackerforen im Internet bereits veröffentlicht. Darüber hinaus können alle angeschlossenen Endgeräte (Telefone, Faxgeräte und Anrufbeantworter) mit den heute zur Verfügung stehenden Angriffswerkzeugen nahezu problemlos logisch wie physikalisch abgehört werden.

5.5.4.2.2 Mobiltelefone

Mit Einführung der mobilen Telefone hat sich die Spionageabwehr zunächst mit der Möglichkeit des Abhörens von Mobilfunkkommunikation beschäftigt. Technische Beschreibungen, Funktionsweise, Gefährdungspotenziale und vor allem Schutzmaßnahmen für Mobiltelefone nach dem GSM-Standard (Groupe Spéciale Mobile beziehungsweise Global System for Mobile Communication) sind umfassend in der BSI-Broschüre „Mobiltelefone - Gefährdungen und Sicherheitsmaßnahmen“²³ dargestellt.

Das technische Abhören der Telefonate selbst kann über die unbefugte Nutzung der technischen Einrichtungen der Netzbetreiber oder mit entsprechendem Aufwand auf den unverschlüsselten Übertragungswegen der Richtfunkstrecken erfolgen. Mit handelsüblichen oder manipulierten Mobiltelefonen lassen sich unbemerkt Raumgespräche aufzeichnen oder abhören.

5.5.5 Risiken drahtloser Kommunikationssysteme

5.5.5.1 Allgemeine Gefahren

Drahtlos heißt, Informationen (Sprache, Daten, Bilder, ...) mit Hilfe elektromagnetischer Wellen (Funk) oder per Infrarot-Licht - ohne physikalische Verbindung (Kupferkabel, Lichtwellenleiter) zwischen den beteiligten Kommunikationssystemen - zu übertragen. Die wesentlichen Systeme, die hier heute zum Einsatz kommen, sind Funk-LANs (Wireless LANs/WLANs), Bluetooth-Module, DECT-Sprach- und Datenkommunikationssysteme (Digital Enhanced Cord-

²³ URL: <http://www.bsi.de/literat/doc/gsm/index.htm>.

less Telecommunications), Infrarot-Systeme (Infrared Data Association/IrDA), drahtlose Tastaturen und Mäuse sowie GSM-Mobiltelefone. Drahtlos heißt aber auch, dass die Kommunikationsströme zwischen Sender und Empfänger von unbefugten Dritten mit entsprechend leistungsfähiger Technik (Richtantennen, Empfängermodulen) - teilweise weit über die normale Nutzreichweite der Funksysteme hinaus - empfangen, abgehört, aufgezeichnet oder manipuliert werden können.

„Mehr als die Hälfte der drahtlosen Netze bei deutschen Unternehmen ist nicht ausreichend gegen Mithörer geschützt“, so das alarmierende Ergebnis einer Studie der Wirtschaftsprüfungsgesellschaft Ernst & Young bereits aus dem Jahr 2003.²⁴ Das Eindringen in und die missbräuchliche und unbefugte Nutzung von drahtlosen lokalen Kommunikationssystemen hat sich zwischenzeitlich zu einem regelrechten Sport in Hackerkreisen entwickelt. Die Funkanbindung stationärer und vor allem mobiler Endgeräte an Kommunikationsnetze sowie kabellose Eingabegeräte bieten nicht nur Nutzern, sondern auch Hackern, Konkurrenten oder fremden Nachrichtendiensten völlig neue „kostenlose Freiheiten“ bei der Nutzung von Netzen, angeschlossenen IT-Systemen sowie des Internets und seinen Diensten.

5.5.5.2 Wireless LAN (WLAN)

Die Wireless LAN-Technologie erlebt derzeit einen ungeheuren und nahezu ungebremsten Boom. Diese relativ junge Technik zeichnet sich insbesondere dadurch aus, dass sie preisgünstig, komfortabel, flexibel und mobil einsetzbar ist. Jede der aktuellen Studien und Untersuchungen²⁵ zu Wireless LANs beklagt jedoch sehr deutlich die systeminhärente Unsicherheit der angebotenen Produkte und technischen Standards. Der amerikanische Anbieter für Sicherheitssoftware RSA zieht als Fazit einer entsprechenden Studie:

„Das Ausmaß von unsachgemäß konfigurierten Netzwerken in Europa ist immer noch erschreckend und hat zur Folge, dass Hunderte von Unternehmen anfällig für Angriffe sind.“

²⁴ Wireless LAN - Ein Paradies für Hacker? Studie zur Sicherheit von drahtlosen Netzwerken in deutschen Unternehmen, 9. April 2003, URL: [http://www.ey.com/global/download.nsf/Germany/WLAN_Studie/\\$file/WLAN.pdf](http://www.ey.com/global/download.nsf/Germany/WLAN_Studie/$file/WLAN.pdf).

²⁵ u. v. a.: RSA Security Studie: WLANs sind auch an Börsenplätzen unsicher, Heise online news vom 25. Juni 2004, URL: <http://www.heise.de/newsticker/meldung/48593>.
Per Anhalter durchs Internet, c't 13/2004, S. 92: Offene Funknetze: Schwarz-Surfen vom 10. Juni 2004, URL: <http://www.heise.de/ct/04/13/092/>.

5.5.5.3 Bluetooth

Bei Bluetooth handelt es sich aus technischer Sicht um einen offenen Industriestandard (IEEE 802.15²⁶) zur drahtlosen Sprach- und Datenkommunikation. Viele Hersteller mobiler Kommunikationsgeräte haben diesen Standard bereits in ihre Produkte (Mobiltelefone, Headsets, Smartphones, Persönliche Digitale Assistenten/PDAs, Laptops, Digitalkameras, Diktiergeräte, u.a.) integriert.

Das BSI hat in seinen Broschüren²⁷ zu den Sicherheitsaspekten drahtloser Kommunikationssysteme eine Reihe schwerwiegender Schwachstellen und Sicherheitslücken beschrieben. Selbst wenn die vom BSI empfohlenen Schutzmaßnahmen implementiert und umgesetzt werden, verbleibt immer noch eine Reihe von Restrisiken.

5.5.5.4 Spionagesoftware (Spyware)

Spyware installiert sich für den Nutzer unbemerkt im Hintergrund schon alleine beim normalen Surfen im Internet. Die verdeckte Installation sendet dann jedes Mal, wenn der Nutzer online geht, sensible Nutzer- und Firmendaten ins Internet beziehungsweise an vorgegebene Empfängeradressen. Die Gefährlichkeit von Spyware besteht im Gegensatz zu Computerviren auch darin, dass durch die heimliche Installation die Rechnerleistung nicht beeinträchtigt und insofern der potenzielle Schaden nicht oder erst viel zu spät entdeckt wird.

5.5.5.5 Hacker und Hackertools

Aus Sicht des Verfassungsschutzes bedienen sich Datenspione und Datensaboteure auch der Mittel und Methoden des Hackings. Das nicht eindeutig zu definierende Täterprofil des Hackers beschreibt - in Abhängigkeit der jeweiligen Motivlage - Personen, die sich mit erheblichem und umfassendem Sachverstand legale wie illegale Zugänge zu IT-Systemen verschaffen. Hacker mit hoher krimineller Energie beziehungsweise im Auftrag fremder Nachrichtendienste, die illegal in fremde Netze beziehungsweise Rechner eindringen, um dort Daten und Programme auszuspionieren, zu beschädigen oder zu manipulieren, werden heute eher als Cracker bezeichnet.

²⁶ IEEE (Institute of Electrical and Electronics Engineers) ist ein weltweiter Berufsverband von Ingenieuren aus den Bereichen Elektrotechnik und Informatik, der Gremien für die Standardisierung von Technologien, Hardware und Software bildet.

²⁷ BSI, Drahtlose lokale Kommunikationssysteme und ihre Sicherheitsaspekte, URL: <http://www.bsi.de/literat/doc/drahtloskom/index.htm>.

5.5.5.6 Laptop- und Hardware-Diebstahl

Datendiebstahl und Datenspionage müssen nicht immer auf elektronischem Weg stattfinden. In vielen Fällen ist es weitaus einfacher, Datenträger (z.B. Festplatten, Disketten, CD-ROM) oder ganze Rechner (PC, Workstation, Server) besonders aus ungesicherten und physikalisch ungeschützten Bereichen eines Unternehmens zu entwenden.

Am 7. Juli 2004 sind aus dem Los Alamos National Laboratory, einem der wichtigsten Waffenlabors der USA, zwei Datenträger verschwunden, die nach Einschätzung von Experten hochbrisante Daten enthielten. In der Folge wurden vorübergehend alle geheim eingestuft Projekte eingestellt. Zu Beginn des Jahres 2004 wurden in Sachsen komplette Rechner sowohl aus einer wissenschaftlichen Einrichtung als auch aus einem Forschungslabor entwendet. Diese Liste ließe sich beliebig fortsetzen und auch die Landesbehörden für Verfassungsschutz in Bayern und Baden-Württemberg werden in ihrer täglichen Arbeit immer wieder mit Fällen von Hardware-Diebstahl konfrontiert. In der Zwischenzeit stellt sich hier für Polizei wie Verfassungsschutz konkret die Frage, ob die Täter „nur“ an der Hardware oder vielmehr an den darauf gespeicherten Informationen interessiert sind. Seitens der Betroffenen unterbleibt in den allermeisten Fällen eine methodische Analyse sämtlicher vergleichbarer Vorfälle. Die jeweiligen Einzelfälle werden als ärgerlicher, aber tragbarer Hardwareverlust „verbucht“, auf eine Einschaltung der Sicherheitsbehörden wird verzichtet.

Noch einfacher ist der Diebstahl mobiler Endgeräte (Laptop, Notebook, PDA, Handy etc.). Gerade in diesem Bereich haben die Verlustrisiken als Folge der stetig wachsenden Mobilität und Erreichbarkeit drastisch zugenommen. Vielfach sind auf diesen Geräten jedoch äußerst sensible und vertrauliche Daten gespeichert, deren unbefugte Nutzung im Verlustfall große Schäden nach sich ziehen können. Die Dimension solcher gezielter Diebstähle zeigt einer der spektakulärsten Fälle der Vergangenheit auf: Irwin Jacobs²⁸ musste nach einer Präsentation vor Journalisten im Hyatt Regency Hotel/Kalifornien den Verlust seines Laptops vermelden. Auf die Frage, was alles auf seinem Notebook gespeichert sei, antwortete er schlicht: „Alles“.

Die FBI/CSI²⁹-Studie 2005 weist hier einen Gesamtschaden von 4.107.300 US-Dollar aus (2004: 6.734.500 US-Dollar) und immerhin ca. 50 Prozent der

²⁸ Gründer und Vorstandsvorsitzender des amerikanischen Telekommunikationsausrüsters Qualcomm.

²⁹ Computer Security Institute (CSI), Studie „Computer Crime and Security Survey“, Tenth Annual 2005, URL: <http://www.gocsi.com>.

befragten Unternehmen waren von solchen Diebstählen betroffen. Eine Zusammenfassung der Firma zTrace Technologies³⁰ gibt sehr anschaulich einen Überblick über das geschilderte Problem.

5.5.5.7 Unterlassene Löschung von Daten

Datenspione können jedoch auch auf andere Weise fündig werden. Eine unüberschaubare Anzahl ausgemusterter Geräte (PCs, Digitalkameras, Kopierer, Fax-Geräte, Multifunktionsgeräte, Laptops, Handys, PDAs etc.) und Datenträger werden, ohne vorher die darauf gespeicherten Daten zuverlässig und sicher zu löschen, über Internet-Auktionshäuser oder einfach auf Flohmärkten zum Wiederverkauf angeboten³¹. In einem aktuellen Fall³² wurde ein Datenträger mit streng vertraulichen Polizeidaten über das Internet-Auktionshaus Ebay versteigert. Der gebrauchte Datenträger mit 20 Gigabyte Speicher enthielt interne Alarmpläne für „besondere Lagen“ wie Geiselnahmen oder Entführungen, Namenslisten für die Besetzung von Krisenstäben, Einsatzbefehle und -analysen.

5.5.5.8 Outsourcing

Unter dem allgemeinen Kostensenkungsdruck konzentrieren sich immer mehr Unternehmen auf ihre Kernkompetenzen und lagern bislang selbst erbrachte Leistungen aus. Insbesondere im IT-Bereich kann dies erhebliche Risiken mit sich bringen, die bei entsprechenden Entscheidungen unbedingt berücksichtigt werden sollten:

- Schaltung neuer externer (un-/gesicherter) Kommunikationsverbindungen nach innen und nach außen,
- Bindung an die (Sicherheits-) Technologie des Outsourcing-Partners,
- Verlust eigener Kompetenz bei IT-Betrieb und IT-Sicherheit,
- Verlust der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität eigener Daten beim Outsourcing-Partner im Rahmen der Kommunikation.

³⁰ URL: <http://www.ztrace.com/de/FactsPage.asp>.

³¹ Computerwoche vom 26. August 2003: E-Bay-Kunde ersteigert PDA mit vertraulichen Daten von Morgan Stanley (Finanz- und Unternehmensberatungsfirma), URL: <http://www.computerwoche.de/index.cfm?pageid=254&artid=52500>.

³² SPIEGEL ONLINE vom 2. April 2005: Polizei-Daten bei Ebay versteigert, URL: <http://spiegel.de/netzwelt/politik/0,1518,349274,00.html>.

Sofern diese Aspekte nicht Bestandteil einer Outsourcing-Strategie sind, besteht ein hohes Risiko, dass firmenvertrauliche Daten nicht nur beim auftraggebenden Unternehmen selbst, sondern vor allem auch beim Outsourcing-Dienstleister ausspioniert oder (technische) Einfallstore für externe Angreifer oder Schadsoftware (Viren, Spyware etc.) geschaffen werden.

6. Schwachstellen des Informationsschutzes

Die geschilderten Methoden wären bei weitem nicht so erfolgreich, gäbe es nicht eine Reihe typischer Schwachstellen des Informationsschutzes - quasi die „Einfallstore“ für Spionage. Herausragende Schwachstellen sind:

- menschliche Schwächen („Schwachstelle Mensch“: falsches Verhalten in kritischen Situationen aus Vorsatz, Fahrlässigkeit oder Überforderung); Der „allgemeine Wertewandel“ oder das „schwindende Unrechtsbewusstsein“ sind nur sehr pauschale Erklärungen für das Phänomen, dass sich Mitarbeiter zunehmend illoyal gegenüber ihrem Arbeitgeber verhalten. Tatsächlich spielen nicht selten die private Situation und persönliche Konflikte eine ausschlaggebende Rolle. Geltungssucht, Überschuldung, Partnerkonflikte sowie berufliche Enttäuschung können zu kriminellen Handlungen führen.
- fehlende oder konzeptionslose Prävention;
- fehlende Berücksichtigung von Sicherheitsbelangen in den Unternehmenszielen;
- fehlende Vorstellungen über Existenz und Wert eigener Betriebsgeheimnisse und ihrer strategischen Bedeutung für das Unternehmen;
- keine oder unzureichende Regeln für den Umgang mit Betriebsgeheimnissen.

7. Quantitative und qualitative Bewertung des Schadens

Eine wissenschaftlich fundierte Quantifizierung des Schadens durch Wirtschaftsspionage für die baden-württembergische Wirtschaft liegt seit 2004 vor.

Vom Sicherheitsforum Baden-Württemberg³³ wurde beim Institut für Betriebswirtschaftslehre der Universität Lüneburg eine empirische Studie in Auftrag gegeben. Sie kam zu dem Ergebnis, dass der Wert des Wettbewerbsvorsprungs der befragten Unternehmen in Baden-Württemberg 700 Millionen Euro beträgt. Bezogen auf Baden-Württemberg beträgt das Gefährdungspotenzial hochgerechnet 7 Milliarden Euro pro Jahr. Der verursachte Schaden durch Spionage belief sich bei den befragten Unternehmen auf 52 Millionen Euro. Die auf dieser Basis für Baden-Württemberg hochgerechneten Schäden betragen ca. eine Milliarde Euro. Obwohl es für die bayerische Wirtschaft keine vergleichbare Studie gibt, lassen sich die für Baden-Württemberg festgestellten Ergebnisse aufgrund der Vergleichbarkeit der Wirtschaftsstandorte auf Bayern im Grundsatz übertragen.

Ein Wissensabfluss unter Beteiligung fremder staatlicher Organe wurde nur von großen Unternehmen erkannt. Nach Einschätzung des LfV Baden-Württemberg könnte dies auf unzureichende interne Sicherheitsstrukturen in kleinen und mittleren Firmen zurückzuführen sein. Außerdem unterscheiden sich in bestimmten Situationen die Vorgehensweisen fremder Nachrichtendienste nicht wesentlich von denjenigen der Konkurrenz. Die erkannten nachrichtendienstlichen Aktivitäten stellen wahrscheinlich nur die „Spitze des Eisbergs“ dar.

Auch in qualitativer Hinsicht fällt die Bewertung angesichts der dynamischen Entwicklung technischer Möglichkeiten eindeutig aus. Immer leistungsfähigere, aber in der Mehrzahl der Fälle nur unzureichend gesicherte Computer und weltumspannende Datennetze eröffnen völlig neue und mit relativ wenig Aufwand verbundene Möglichkeiten der Informationsbeschaffung. Die rapide Zunahme des multimedialen und multinationalen Informationsaustausches in Forschung, Entwicklung und Produktion macht es Wirtschaftsspionen heutzutage relativ leicht, in die Informations- und Kommunikationstechnik (IuK) eines Unternehmens einzudringen und sich „auf Knopfdruck“ fertig aufbereitetes Know-how zu beschaffen. Eine mutmaßlich hohe Anzahl unerkannter Angriffe sowie Schwierigkeiten bei der Verifikation entsprechender Fälle lassen eine erhebliche Dunkelziffer in dieser Schadenskategorie vermuten.

³³ Das Sicherheitsforum Baden-Württemberg ist ein Zusammenschluss von Unternehmen, Verbänden, Kammern, Forschungseinrichtungen und Behörden des Landes, die es sich unter anderem zur Aufgabe gemacht haben, den Technologievorsprung der baden-württembergischen Wirtschaft und Forschung vor Spionage zu schützen.

8. Schlussbetrachtung

Der härter werdende Konkurrenzkampf zwischen Staaten und Unternehmen einerseits sowie die strategische Bedeutung und die permanent steigende Verletzlichkeit des Rohstoffs „Information“ andererseits haben zur Folge, dass auf dem Sektor Wirtschaftsspionage keine Entwarnung gegeben werden kann. Informationen werden in Zukunft in noch stärkerem Maße als heute über Firmen- oder Landesgrenzen hinweg ausgetauscht. Vor diesem Hintergrund gibt es neue rechtliche Problemstellungen bezüglich des Eigentums an global vagabundierenden Informationen.

In fremden Ländern sind Informationen häufig völlig anderen Gefahren ausgesetzt als im Ursprungsland, weil Daten- und Informationsschutz unter Umständen einen anderen Stellenwert haben. Hinzu kommt, dass im Zeitalter der Globalisierung multinational strukturierte Unternehmen weltweite strategische Allianzen eingehen und damit Kooperationspartner und Konkurrent zugleich sein können - ein Umstand, der es ebenfalls schwer macht, Wissen zu schützen, ohne sich kontraproduktiv abzuschotten. Know-how-Schutz ist also eine Herausforderung mit globaler Dimension und strategischer Erfolgsfaktor zugleich.

Grundvoraussetzung für eine wirkungsvolle Bekämpfung der Wirtschaftsspionage ist, dass sich jeder einzelne Mitarbeiter eines Unternehmens - vom Konzernchef bis zum Lehrling - des Ausspähungsrisikos und seiner ganz persönlichen Verantwortung bewusst ist.

9. Anhang

9.1 Literaturhinweise

- Ackermann, Ralf; Görtz, Manuel
Voice over IP Security
Sicherheitsrelevante Herausforderungen bei VoIP - eine kritische Bestandsaufnahme
<kes> 2005#5, S. 36ff .
- Amelunxen, Clemens
Spionage und Sabotage im Betrieb
Kriminalistik Verlag, Heidelberg, 1997
- BDI (Hrsg.)
Wirtschafts- und Betriebsspionage
BDI-Drucksache Nr. 274
Köln, 1994
- Bedeković, Benjamin
Risiko Wissen
IT-gestütztes Wissensmanagement braucht spezifisches Sicherheitsmanagement
<kes> 2005#3, S. 52ff.
- Beer, Daniel; Hohl, Peter; Jung, Astrid; Sabitzer, Werner (Hrsg.)
Sicherheits-Jahrbuch 2005/2006
Secu Media-Bücher, Zürich-Ingelheim, 2004
- Bramford, James
NSA: Die Anatomie des mächtigsten Geheimdienstes der Welt
Bertelsmann Verlag, München, 2001
- BSI (Hrsg.)
VoIPSEC Studie zur Sicherheit von Voice over Internet Protocol
BSI
- BSI (Hrsg.); Schulze, Tillmann
Aktueller Lagebericht
Wie sicher ist die IT in Deutschland
<kes> 2005#4, S. 21ff.
- Bundesamt für Verfassungsschutz (Hrsg.)
Proliferation - das geht uns an!
Köln, 2004
- Bundesamt für Verfassungsschutz (Hrsg.)
Ihre Verantwortung - unsere Sicherheit. Über den Umgang mit vertraulichen Informationen
Köln, 2004
- Bundesamt für Verfassungsschutz (Hrsg.)
Wirtschaftsspionage: Information und Prävention
Köln, 2003
- Dreger, Wolfgang
Counter Intelligence: Betriebliche Spionageabwehr. So schützen Sie Ihr Firmen-Know-how gegen Ausspähung durch die Konkurrenz
Expert Verlag, Renningen-Malmsheim, 1998
- Dreger, Wolfgang
Konkurrenz-Analyse und Beobachtung. Mit System zum Erfolg im Wettbewerb
Expert Verlag, Ehningen bei Böblingen, 1992
- Eckert, Claudia
IT-Sicherheit - Konzepte, Verfahren, Protokolle
Wissenschaftsverlag Oldenbourg, München, 2001
- Fink, Manfred
Lauschziel Wirtschaft: Abhörgefahren und -techniken, Vorbeugung und Abwehr
Richard Boorberg-Verlag, Stuttgart, 1996
- Finster, Eberhard
Information Warfare - der Krieg der Zukunft
WIK 00/4, S. 63ff., 2000
- Finster, Eberhard
Mehr Sicherheitsverantwortliche erforderlich
WIK 05/3, S. 19ff., 2005
- Förster, Andreas
Maulwürfe in Nadelstreifen,
Wirtschaftsspionage – der neue Job der Geheimdienste
Henschel-Verlag, Berlin, 1997
- Fuchs, Hans Joachim (Hrsg.); Kammerer, Jörg; Ma, Xiaoli; Rehn, Ina Melanie;
Piraten, Fälscher und Kopierer - Strategien und Instrumente zum Schutz geistigen Eigentums in der Volksrepublik China
Gabler Verlag, Wiesbaden, 2006

- Gaulke, Markus **Digitale Abgründe: Was die Computerbranche ihren Kunden verschweigt.**
Risiken ausschließen -Investitionen sichern- Systeme optimieren
Verlag Moderne Industrie, Landsberg, 1996
- Glitza, Klaus-Henning **Handy-Gespräche: Wer hört mit?** IMSI-Catcher nutzt Behörden und Spionen
WIK 03/11, S. 13ff.
- Glitza, Klaus-Henning **Sicherheitslücken bei WLAN und Blue Tooth**
WIK 04/10, S. 24ff.
- Glitza, Klaus-Henning **Spionagegefahr durch Mobil-Funk:** So stoppen Sie unerwünschte Handy-Nutzung
WIK 04/4, S. 25ff.
- Glitza, Klaus-Henning **Wirtschaftsspionage auf chinesische Art?**
Zertifizierung mit bedenklichen Hintertüren
WIK 04/1, S. 10ff.
- Hartwig, Stefan, Dr. **Nutzung offener Quellen verlangt kritische Bewertung**
WIK 05/3, S. 31ff.
- Hartwig, Stefan, Dr. **Wie Mitarbeiter Informationen weitergeben**
WIK 04/6, S. 10ff.
- Hummelt, Roman **Wirtschaftsspione auf dem Datenhighway**
Strategische Risiken und Spionageabwehr
Carl Hanser Verlag, München, Wien, 1997
- Jakob, Bernd **Geheime Nachrichtendienste und Globalisierung**
(Europäische Hochschulschriften: Reihe 31, Politikwissenschaft, Band 380)
Peter Lang Verlag, Frankfurt, 1999
- <kes> Die Zeitschrift für Informations-Sicherheit (Hrsg.)
<kes> **Microsoft-Sicherheitsstudie 2004**
Lagebericht zur Informations-Sicherheit
<kes> 2004#4, S. 6ff., <kes> 2004#5, S. 6ff.,
<kes> 2004#6, S. 6ff.
- <kes> Die Zeitschrift für Informations-Sicherheit (Hrsg.)
Konsequenzen der Pass-Biometrie
<kes> 2005#2, S. 6ff.
- Koch, Egmont R.; Sperber, Jochen
Die Datenmafia, Computerspionage und neue Informationskartelle
Rowohlt TB-Verlag, Reinsbeck bei Hamburg, 1996
- Könning, Ulrich **Betriebsspionage im Mittelstand?**
WIK 98/6, S. 23
- Landesamt für Verfassungsschutz Baden-Württemberg (Hrsg.)
Know-how-Schutz - Handlungsempfehlungen für die gewerbliche Wirtschaft
Stuttgart, 2004
- Liman, Burkhard **Bewertung des irregulären Verlustes von Know-how**
Wirtschaftsverlag Bachem, Köln, 1999
- Lux, Christian; Peske, Thorsten
Competitive Intelligence und Wirtschaftsspionage
Gabler Verlag, Wiesbaden, 2002
- Mangstl, Herbert **Lauschangriffe und kompromittierende Abstrahlung**
KES 00/2, S. 6ff.
- Nathusius, Ingo **Wirtschaftsspionage, Gefahren, Strukturen und Bekämpfung**
Kriminalistik Verlag, Heidelberg, 2001
- Odenthal, Roger **Die Vertuschung als „hohe Kunst“ der Mitarbeiterkriminalität**
WIK 05/6, S. 12ff.
- Pfaff, Dietmar; Altensen, Astrid
Immer noch der Geruch von Industriespionage
WIK 03/11, S. 23ff.
- Roth, Jürgen **Russen-Mafia in deutschen Chef-Etagen?** Die Gangster aus dem Osten
Europa-Verlag, Hamburg, 2003

Schumacher, Manfred **Feind hört mit!**
Mangelndes Sicherheitsbewusstsein bei Video-Konferenzen
<kes> 2005#2, S. 60ff.

Siemens, Olaf **Viren in Werkzeugmaschinen?**
WIK 05/6, S. 55ff.

Sicherheitsforum Baden-Württemberg
Fall- und Schadensanalyse bezüglich Know-how-/Informationsverlusten in Baden-Württemberg ab 1995
Stuttgart, 2004

Sitt, Axel **Erfolgsfaktor Sicherheit** – Schützen Sie Ihr Unternehmens-Know-how vor dem Zugriff der Konkurrenz
ECON-Verlag, Düsseldorf, 1998

Stoffel, Matthias **Phishing: Wer haftet für den Schaden?**
WIK 05/3, S. 37ff.

Ulfkotte, Udo **Marktplatz der Diebe:** Wirtschaftsspionage in Deutschland
Bertelsmann Verlag, München, 1999

Ulfkotte, Udo **Wirtschaftsspionage: wie deutsche Unternehmen von ausländischen Geheimdiensten ausgeplündert und ruiniert werden** (aktualisierte Taschenbuchausgabe)
Goldmann Verlag, München, 2001

von Calum, Macleod **Hallo Partner...., Gedanken angesichts Trojanischer Pferde zur Industriespionage**
<kes> 2005#3, S. 6ff.

Weise, Horst **Private Nachrichtendienste versprechen Hilfe**
WIK 05/2, S. 13ff.

WIK (Hrsg.) **Faktor Mensch für Finanzinstitute größtes IT-Risiko**
WIK 05/4, S. 23ff.

WIK (Hrsg.) **WIK-Sicherheits-Enquête 2004/2005**
WIK 05/1, S. 7ff., WIK 05/2, S. 17ff.,
WIK 05/3, S. 59ff.

Wittmann, Jürgen **Die Wege der Hacker in die Firmenrechner**
WIK 99/5, S. 69ff.

Zumwinkel, Andreas **„Risikofaktor“ Mitarbeiter?**
W&S 98/10, S. 44ff.

9.2 Internetadressen

Homepage von	Fundstelle
Arbeitsgemeinschaft Sicherheit in der Wirtschaft e. V. (ASW)	www.asw-online.de
Bundesamt für Sicherheit in der Informationstechnik (BSI)	www.bsi.de
Bundesamt für Verfassungsschutz (BfV)	www.verfassungsschutz.de
Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA)	www.bafa.de
Bundeskriminalamt (BKA)	www.bka.de
Landesamt für Verfassungsschutz Baden-Württemberg	www.verfassungsschutz-bw.de
Landesamt für Verfassungsschutz Bayern	www.verfassungsschutz.bayern.de
Sicherheit im Internet (Mittelstand sicher im Internet)	www.sicherheit-im-internet.de
Sicherheitsforum Baden-Württemberg	www.sicherheitsforum-bw.de
Bundesverband der Deutschen Industrie e.V. (BDI)	www.bdi-online.de
Europol	www.europol.eu.int
heise online	www.heise.de
Telepolis ECHELON	www.heise.de/tp/r4/spezial/ech.html
Telepolis-infowar	www.heise.de/tp/r4/

Homepage von Fundstelle

Sicherheits-Fachverlage

<kes> online	www.kes.info
WIK, Zeitschrift für Sicherheit in der Wirtschaft	www.wik.info
W+S Sicherheitsmagazin für Trends, Technik und Dienstleistung	www.ws-huethig.de

Fremdsprachliche Adressen:

American Society for Industrial Security (ASIS)	www.asisonline.org
Critical Infrastructure Assurance Office (CIAO)	www.doc.gov
National Counterintelligence Center (NACIC)	www.nacic.gov
National Security Agency (NSA)	www.nsa.gov
Canadian Society for Industrial Security	www.csis-scsi.org
Ecole de Guerre Economique	www.ege.eslsca.fr
Federation of American Scientists	www.fas.org/main/home.jsp

VERTEILERHINWEIS

Diese Informationsschrift wird vom Landesamt für Verfassungsschutz Baden-Württemberg und dem Bayerischen Landesamt für Verfassungsschutz im Rahmen ihrer gesetzlichen Verpflichtung zur Unterrichtung der Öffentlichkeit herausgegeben. Sie darf weder von Parteien noch von deren Kandidaten oder Helfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für alle Wahlen.

Missbräuchlich ist insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel.

Untersagt ist auch die Weitergabe an Dritte zum Zwecke der Wahlwerbung.

Auch ohne zeitlichen Bezug zu einer Wahl darf die vorliegende Druckschrift nicht so verwendet werden, dass dies als Parteinahme des Herausgebers zugunsten einzelner politischer Gruppen verstanden werden könnte. Diese Beschränkungen gelten unabhängig vom Vertriebsweg, also unabhängig davon, auf welchem Wege und in welcher Anzahl diese Informationsschrift dem Empfänger zugegangen ist.

Erlaubt ist jedoch den Parteien, die Informationsschrift zur Unterrichtung ihrer Mitglieder zu verwenden.

**SONSTIGE PUBLIKATIONEN DES
LANDESAMTS FÜR VERFASSUNGSSCHUTZ BADEN-WÜRTTEMBERG**

Öffentlichkeitsarbeit, Taubenheimstraße 85 A, 70372 Stuttgart
Tel.: 0711/9544-181/182, Fax: 0711/9544-444

Verfassungsschutz Baden-Württemberg - Februar 2005

Rechtsextremismus - März 2006

Linksextremismus in der Bundesrepublik Deutschland - Allgemeine Entwicklung - Februar 2003

Islamistischer Extremismus und Terrorismus - April 2006

Erscheinungsformen des Ausländerextremismus - März 2001

Die „Scientology-Organisation“ (SO) - Juli 2003

Know-how-Schutz - Handlungsempfehlungen für die gewerbliche Wirtschaft - Juli 2004

Diese und weitere Publikationen des Landesamts für Verfassungsschutz Baden-Württemberg können auf der Internetseite www.verfassungsschutz-bw.de eingesehen und heruntergeladen werden.

**SONSTIGE PUBLIKATIONEN DES
BAYERISCHEN STAATSMINISTERIUMS DES INNERN UND DES
BAYERISCHEN LANDESAMTS FÜR VERFASSUNGSSCHUTZ**

Presse- und Öffentlichkeitsarbeit, Knorrstraße 139, 80937 München
Tel.: 089/31201-0, Fax: 089/31201-380

Demokratie braucht unseren Schutz - Juni 2000

Faltblattserie „SCHÜTZ UNSERE DEMOKRATIE“ - Januar 2002
mit folgenden Themen: Verfassungsschutz, Terror und Gewalt, Rechtsextreme Parteien,
Revisionismus, Neonazismus, Kommonismus, Islamischer Extremismus,
Scientology-Organisation, Organisierte Kriminalität, Spionage.

Neonazismus und rechtsextreme Gewalt - November 2005

**10 Jahre Beobachtung der Organisierten Kriminalität
durch das Bayerische Landesamt für Verfassungsschutz** - Juli 2004

Das System Scientology: Wie Scientology funktioniert - 25 Fragen mit Antworten - Juli 2004

Aktuelle Publikationen sind auf den Internetseiten des Bayerischen Staatsministeriums des Innern (www.stmi.bayern.de) und des Bayerischen Landesamtes für Verfassungsschutz (www.verfassungsschutz.bayern.de) abrufbar.

