

## E. SPIONAGEABWEHR, GEHEIM- UND SABOTAGESCHUTZ

### 1. Aktuelle Entwicklungen und Tendenzen

Die Verbreitung von Massenvernichtungswaffen oder von Mitteln zu ihrer Herstellung hat sich zu einem globalen sicherheitspolitischen Problem entwickelt. Nicht nur Staaten streben den Besitz solcher Waffen an, auch Terroristen haben schon ihre Absicht bekundet, sich ABC-Waffen oder atomwaffenfähiges Material beschaffen zu wollen.

Durch den Besitz von Massenvernichtungswaffen kann der militärische und der politische Handlungsspielraum von Staaten spürbar erweitert werden. Es eröffnen sich neue Möglichkeiten der Einschüchterung und der reinen Abschreckung; die militärische Schlagkraft wird deutlich verbessert. Zudem wird das politische Gewicht eines Landes, das über solche Waffen verfügt, erheblich erhöht.

Immer mehr Staaten sind technisch in der Lage, Waffen mit einem ungeheuren Vernichtungspotenzial zu produzieren. Vor allem die Atomprogramme einiger Länder und der damit verbundene „nukleare Schwarzmarkt“ stellen ein bedeutendes globales Bedrohungspotenzial dar. Anfang des Jahres 2005 hat Nordkorea den Besitz von Kernwaffen eingestanden, und der Iran steht trotz gegenteiliger Beteuerungen im Verdacht, auf dem Umweg über die zivile Nutzung der Kernkraft die Fähigkeit zur Herstellung von Atomwaffen erlangen zu wollen.

Die Bekämpfung der Proliferation<sup>443</sup> ist daher eine wichtige sicherheitspolitische Aufgabe, zu der auch die Verfassungsschutzbehörden ihren Beitrag leisten. Dieser Komplex hat - wie schon in den Vorjahren - auch 2005 die Arbeit der Spionageabwehr des Landesamts für Verfassungsschutz (LfV) dominiert. Die Spionageabwehr trägt durch die Verfolgung und Aufklärung entsprechender Aktivitäten nicht nur dazu bei, die Urheber solcher Beschaffungsaktivitäten identifizieren und bestrafen zu können, sondern leistet gleichzeitig offensive Aufklärungsarbeit, um zu verhindern, dass baden-württembergische Unternehmen oder Geschäftsleute aus Unkenntnis oder Fahrlässigkeit in riskante Proliferationsgeschäfte verwickelt werden.

<sup>443</sup> Proliferation: Weiterverbreitung von Massenvernichtungswaffen beziehungsweise der zu ihrer Herstellung verwendbaren Produkte einschließlich des dafür erforderlichen Know-hows sowie von entsprechenden Waffenträgersystemen.

Die Problematik der Wirtschaftsspionage ist zwar in den Medien etwas in den Hintergrund getreten, beschäftigt die Spionageabwehr aber nach wie vor. Speziell die Erfahrungen deutscher Firmen und ihrer Repräsentanten in China belegen, dass dieser Staat auf den verschiedensten Ebenen eine konsequente und gut durchdachte Strategie verfolgt, um möglichst zum „Nulltarif“ modernstes Know-how zu erlangen. Quer durch Deutschland klagen in Bezug auf China immer mehr Unternehmen darüber, dass man ihnen ihre Technologie „gestohlen“ hätte. Ein weiterer Schwerpunkt sind die Aktivitäten der Russischen Föderation, die bei aller Annäherung an den Westen offenbar nicht auf die Möglichkeiten nachrichtendienstlicher Informationsbeschaffung verzichten will.

Weltumspannende Informations- und Kommunikationssysteme neuester Generation eröffnen der Spionage völlig neue Dimensionen. Fast täglich lassen Besorgnis erregende Meldungen über die Verwundbarkeit moderner Technik mit enormen finanziellen Auswirkungen aufhorchen: Wirtschaftsspionage mit „Trojanischen Pferden“<sup>444</sup>, die enorme Zunahme erkannter Schwachstellen in komplexen Softwaresystemen, globale Computerviren-Epidemien, gravierende Sicherheitslücken bei häufig ungenügend abgesicherten Wireless Local Area Networks (WLAN) und bei Internettelefonaten, die Ausspähung von Passwörtern und PINs<sup>445</sup> mit gefälschten E-Mails<sup>446</sup>, durch Keylogger-Systeme<sup>447</sup> oder durch Spionagesoftware<sup>448</sup>, die Generierung von Abhörmöglichkeiten durch manipulierte Mobiltelefone und Telekommunikationsanlagen oder die Rekonstruktion eines Textes anhand von Tippgeräuschen der Computertastatur. Diese Liste aktueller Beispiele ließe sich beliebig verlängern. Wirtschaft und Gesellschaft sind jedoch auf eine sichere Informationstechnik angewiesen. Der baden-württembergische Verfassungsschutz engagiert sich deshalb stark auf dem Feld der Prävention.

Die Unternehmen sind für den Schutz ihrer Betriebsgeheimnisse selbst verantwortlich. Viele wiegen sich nach den bisherigen Erfahrungen in trügeri-

*„In vielen Nationen müssen Sie zudem davon ausgehen, dass nachrichtendienstliche Zugänge zum Vorteil der nationalen Wirtschaft genutzt werden.“*  
(Frank Lesiak, Sicherheitsexperte des BND auf der 9. Deutschen Mobile Computing Konferenz 2005 am Spitzingsee)

**Risiken der  
Kommunikations-  
technik**

<sup>444</sup> Als „Trojanisches Pferd“ bezeichnet man in der Computersprache Programme, die sich als nützliche Programme tarnen, aber in Wirklichkeit Malware (Schad-Software) einschleusen und im Verborgenen unerwünschte Aktionen ausführen.

<sup>445</sup> Persönliche Identifikationsnummer (PIN-Code oder Geheimzahl).

<sup>446</sup> Phishing: Durch gefälschte E-Mails versuchen Betrüger Nutzerdaten auszuspähen und an Passwörter, Daten für das Onlinebanking und Kreditkartennummern der Kunden zu gelangen.

<sup>447</sup> Softwareprogramme oder Hardwarebausteine, die heimlich alle Tastatureingaben eines PC-Anwenders aufzeichnen.

<sup>448</sup> Programme (Spyware und Adware), die ohne Wissen des PC-Anwenders Daten sammeln und verdeckt weitergeben.

scher Sicherheit. Die bereits in den letzten Jahren praktizierte Unterstützung der baden-württembergischen Wirtschaft in Sicherheitsfragen durch das Sicherheitsforum Baden-Württemberg<sup>449</sup> wird deshalb fortgesetzt.

Die LfV-Broschüre zum Thema „Know-how-Schutz“ hat auch im Jahr 2005 ein beachtliches Echo gefunden, ein sichtbarer Hinweis auf die nach wie vor bestehende Aktualität des Themas.

## 2. Daten, Fakten, Hintergründe

### 2.1 Proliferation

Die erheblichen Aufrüstungsbemühungen von Staaten wie Iran, Nordkorea, Pakistan und Syrien bei ABC-Waffen und bei Trägertechnologien stellen eine weltweite Bedrohung dar. Wegen der strengen Embargobestimmungen wird in der Regel nicht auf den Erwerb von Endprodukten abgezielt, sondern auf die Beschaffung von Einzelkomponenten. Bevorzugtes Interesse besteht an „Dual-Use-Gütern“, die sowohl zivil wie auch militärisch einsetzbar sind. Fließdruckmaschinen können beispielsweise sowohl zur Herstellung von Masten für Straßenbeleuchtungen als auch zur Fertigung von Gehäusen für Raketen oder Rotoren für Gas-Ultrazentrifugen<sup>450</sup> eingesetzt werden.

Da die proliferationsrelevanten Staaten aus den Fehlern der Vergangenheit gelernt haben, wird es zunehmend schwieriger, ihre teilweise unter Beteiligung von Geheimdienstmitarbeitern konspirativ arbeitenden Beschaffungsnetze zu enttarnen. Besondere Aufmerksamkeit ist jedenfalls dann geboten, wenn folgendes Szenario festgestellt werden kann:

- Ständige Einrichtung im staatlichen Bereich (Forschungseinrichtung, Staatshandelsfirma oder private Firma im staatlichen Auftrag), die insbesondere für die politische Führung (Rüstungsministerien, Militär)
- Nachrichten (dazu gehören auch Gegenstände mit Informationswert) und/oder Güter systematisch (nach einem vom Staat vorgegebenen Plan)

<sup>449</sup> Vgl. Kapitel 3.3.

<sup>450</sup> Diese werden für die Anreicherung von zivilem zu waffenfähigem Nuklearmaterial benötigt.

- unter Anwendung konspirativer Mittel (Tarnfirma)

sammelt, um vor allem das militärische Potenzial des beschaffenden Staates zu stärken.

Für die Beschaffung von Proliferationsgütern werden kleine und mittelständische Firmen bevorzugt. Häufig werden die Waren über deutsche Strohleute geordert und auf Umwegen über Osteuropa oder fernöstliche Länder an ihren Bestimmungsort transportiert. Nachfolgend geschilderter Fall zeigt, wie Exportbestimmungen umgangen werden:

- Ein pakistanischer Geschäftsmann mit zahlreichen sehr guten Kontakten zur Regierung seines Heimatlandes versuchte, mit dem deutschen Geschäftsführer eines mittelständischen Unternehmens in Baden-Württemberg ein bundesweites Netz für Beschaffungen im Bereich atomarer Analysetechnik aufzubauen. Die Lieferungen sollten über einen osteuropäischen Zwischenhändler an die pakistanische Atomindustrie gelangen. Die Sicherheitsbehörden wurden auf die illegalen Beschaffungsmaßnahmen aufmerksam, als das Netzwerk auf weitere, an Deutschland angrenzende Länder ausgedehnt werden sollte.

Nach Erkenntnissen der international eng zusammenarbeitenden Sicherheitsbehörden werden solche Lieferungen auch über die Vereinigten Arabischen Emirate abgewickelt. Eine herausragende Rolle spielt dabei die „Jebel Ali Freezone“ in Dubai. Dort sind hunderte Firmen ansässig, die an sie gelieferte Bestellungen auch aus dem Bereich „Dual-Use-Güter“ weiterleiten. Manche Länder nutzen für die Beschaffung der so genannten sensitiven Waren auch ihre amtlichen und halbamtlichen Vertretungen in Deutschland. Solche Stützpunkte bieten eine perfekte Tarnung, indem sie neben ihrer offiziellen Funktion - etwa der Förderung von Handelsbeziehungen - auch Möglichkeiten zur Vermittlung und zum Abschluss illegaler Geschäfte eröffnen.

Einige proliferationsrelevante Staaten treten mittlerweile selbst weltweit als Exporteure von Komponenten und Herstellungstechnologien für Massenvernichtungswaffen auf. Diese „horizontale Proliferation“ unterläuft zunehmend die bisherige Nichtverbreitungspolitik mit Hilfe von Exportkontrollen in westlichen Industriestaaten.

### 2.1.1 Islamische Republik Iran

Der Iran ist in allen Bereichen der konventionellen Rüstung, der Nuklear- und Trägertechnologie sowie auf dem Sektor Entwicklung und Herstellung biologischer und chemischer Kampfstoffe aktiv. Nach bisherigem Kenntnisstand wurden überwiegend Teile und Ersatzteile für Maschinen, Fahrzeuge und halbfertige Erzeugnisse aus Stahl und Aluminium sowie Dual-Use-Güter gekauft. Offen und verdeckt durchgeführte Beschaffungsmaßnahmen betrafen in der Vergangenheit vornehmlich Spezialwerkzeugmaschinen, Windkanalaustrüstungen, Kreiseltechnologien, Antriebs- und Steuerungssysteme, Testanlagen, Messgeräte und Festtreibstoffkomponenten. Die dadurch eingetretene Abhängigkeit von Ersatzteil- und Komponentenerlieferungen kann selbst wiederum zur Entdeckung konspirativ beschaffter, den Exportbeschränkungen unterliegenden Güter führen.

Der Iran arbeitet seit langem zielstrebig und ausdauernd an einem Atomprogramm. In Baden-Württemberg konnte eine iranische Delegation beobachtet werden, die zu verschiedenen Unternehmen im Bundesgebiet - in der Mehrzahl Zulieferer für die Atomindustrie - Kontakt suchte. Die Delegation vertrat hierbei eine bereits seit Jahren dem Landesamt für Verfassungsschutz als nachrichtendienstlich gesteuerte Beschaffungsorganisation bekannte Firma mit Sitz in Teheran.



### 2.1.2 Demokratische Volksrepublik Korea

Nordkorea hat sich 2002 aus dem Atomwaffensperrvertrag zurückgezogen und im Februar 2005 erstmals erklärt, Atomwaffen zu besitzen. Hauptstreitpunkte in den nachfolgenden internationalen Verhandlungen waren Nordkoreas Forderungen nach einem Programm zur zivilen Nutzung der Atomenergie und Sicherheitsgarantien.

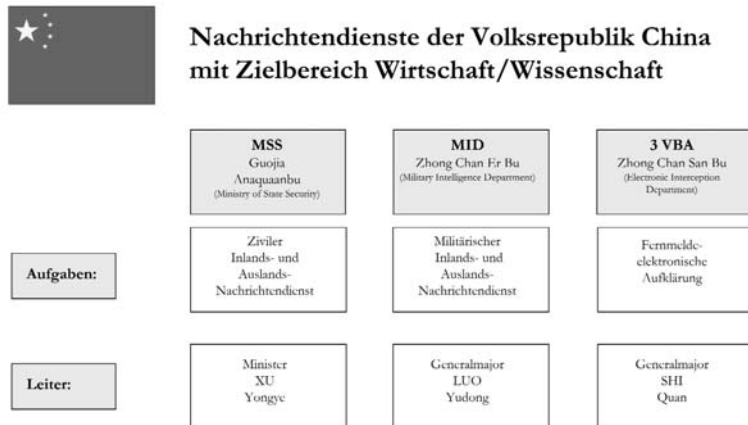
Bei seiner technologischen Weiterentwicklung ist Nordkorea auf Know-how und Dual-Use-Güter aus den westlichen Industrieländern angewiesen. Die Nachrichtendienste unterstützen diese „Aufholjagd“ mit Nachdruck. Sie nutzen bei ihren Aktivitäten primär Botschaften beziehungsweise Handelsvertretungen sowie - als „Rückgrat“ der Beschaffung - bestimmte Außenhandelsgesellschaften des Landes. In den letzten Jahren wurde dieses Netz durch kleinere Unternehmen im Ausland mit nordkoreanischer Beteiligung ergänzt, bei denen die Beschaffung von Dual-Use-Gütern unter dem Deckmantel der Vermittlung beziehungsweise Abwicklung umfangreicher und legal erscheinender Import-/Exportgeschäfte erfolgen kann. Die gewünschte Ware wird zum Beispiel in der Bestellung einer Vielzahl unkritischer Produkte mit nachprüfbarem Endverbraucher „versteckt“.

## 2.2 Wirtschaftsspionage

### 2.2.1 Volksrepublik China

China unternimmt größte Anstrengungen, um an die Leistungsfähigkeit hoch entwickelter Staaten anzuknüpfen. Die Konjunkturdaten der letzten Jahre zeigen, dass der Wirtschaftsboom unvermindert anhält. Fortschritte, die im Westen jeweils mehrere Generationen beansprucht haben, werden hier in knapp einer Generation erzielt. Dabei profitiert das Land enorm vom Know-how seiner ausländischen Partner. Die „China-Euphorie“ ist auch in Baden-Württemberg deutlich zu spüren. Eine gegenüber den Vorjahren weiter angestiegene Zahl einheimischer Unternehmen hat sich im Reich der Mitte engagiert. Firmen aus fast allen Technologiebereichen und Dienstleister vereinbaren Kooperationen mit chinesischen Partnern oder verlagern ihre Produktionsstätten, zuweilen gar einen Teil ihrer Forschung und Entwicklung, nach China und gehen damit zum Teil unübersehbare Sicherheitsrisiken ein. Volkswirtschaftliche Brisanz ist dann gegeben, wenn illegal und zum „Nulltarif“ Know-how abfließt, ganz besonders, wenn es mit

staatlicher Unterstützung zur Stärkung der Zukunftsfähigkeit der einheimischen Wirtschaft entwickelt worden ist. Die Absicherung des eigenen Know-hows ist daher für unsere Industrie eines der fundamentalen strategischen Probleme in der Zusammenarbeit mit chinesischen Partnern.



Als zuverlässiger Garant für die Modernisierung der chinesischen Wirtschaft und das Überleben des politischen Systems setzen die chinesischen Nachrichtendienste vielseitige Methoden ein, um auf den klassischen Aufklärungsfeldern Politik, Wirtschaft, Militär, Wissenschaft und Forschung den globalen Überblick zu gewinnen und technologischen Anschluss an die USA und Europa zu erlangen. Die intensivsten Auslandsaufklärungsaktivitäten entfalten das Ministerium für Staatssicherheit (MSS) als ziviler Dienst und die 2. Hauptverwaltung für Nachrichtenwesen des Generalstabs der Volksbefreiungsarmee als militärischer Nachrichtendienst (MID). Für die Fernmelde- und elektronische Aufklärung aus dem militärischen, diplomatischen und zivilen Bereich ist die 3. Abteilung des Generalstabs der Volksbefreiungsarmee (3VBA) zuständig. Koordiniert und geleitet werden alle bedeutenden nachrichtendienstlichen Operationen von einer zentralen Beschaffungsstelle.

Für die offene und verdeckte Informationsgewinnung in Deutschland werden vor allem abgetarnte Stützpunkte an den diplomatischen Vertretungen, Niederlassungen chinesischer Firmen, akkreditierte Journalisten, Praktikanten, Studenten sowie Wissenschaftler eingesetzt. Das Landesamt für Verfassungsschutz erhielt von zahlreichen Vorkommnissen Kenntnis, bei denen in deutschen Unternehmen tätige chinesische Praktikanten und Hospitanten

unberechtigt umfangreiches Datenmaterial aus Firmennetzen auf ihre Laptops oder USB-Sticks kopierten und über das Internet nach China transferierten.

- In einem Fall lagerten 170 CDs mit sensiblen Entwicklungsdaten einer Rüstungsfirma in der Wohnung einer Chinesin. Sie zeigte bei ihrer Befragung keinerlei Unrechtsbewusstsein und konnte auch keinen Grund für ihren Datenmissbrauch benennen. Nach ihrer „Enttarnung“ bewarb sie sich bei einem anderen baden-württembergischen Unternehmen, um dort möglicherweise auf dieselbe Art und Weise an Informationen zu gelangen.

Der Einsatz von Studenten, Praktikanten und Wissenschaftlern als Informanten erschwert die Aufdeckung entsprechender staatlich gesteuerter Aktivitäten. Die Zahl einreisender Chinesen ist wegen der Lockerung der Reisebeschränkungen in den letzten Jahren um ein Vielfaches gestiegen. China kann deshalb eine große Anzahl unverdächtig auftretender Quellen einsetzen, um an eine Fülle von Einzelinformationen zu gelangen, die dann im Heimatland zusammengeführt werden. Die im Ausland agierenden Chinesen unterliegen einem ausgeklügelten Überwachungssystem und können auch durch die Anwendung von Druckmitteln - Probleme bei der Passverlängerung oder Repressalien gegen Familienangehörige in China - zur Spionagetätigkeit animiert oder genötigt werden.

- Investieren in den chinesischen Markt bedeutet nicht unbedingt garantierten Profit. Diese Erfahrung machte auch ein mittelständisches Unternehmen in Baden-Württemberg, das bisher seine Produkte auf dem Weltmarkt nahezu konkurrenzlos anbot. Bevor es auch in China aktiv werden konnte, musste es die Voraussetzungen der seit 1. August 2003 gültigen Pflichtzertifizierung „China Compulsory Certification“ (CCC) erfüllen. Es legte den chinesischen Behörden interne Akten und Mustergeräte zur Prüfung der in den Dokumenten verlangten Spezifikationen vor. Nach einem ständigen Wechsel der Ansprechpartner und einer Bearbeitungszeit von über einem halben Jahr wurde die Zertifizierung abgeschlossen. Das Unternehmen begann daraufhin, seine Waren in die Volksrepublik zu exportieren. Kurze Zeit später tauchte bereits die perfekte Kopie eines seiner Produkte auf einer Messe auf.

Es verstärkt sich der Verdacht, dass über das Zertifizierungssystem von staatlicher Seite gezielt der Versuch unternommen wird, an fremdes Know-how

**Einsatz von Auslandschinesen ohne ND-Hintergrund**

**problematische Zertifizierung**

**Methoden der Informationsgewinnung**

zu gelangen. Den meisten Unternehmen, die sich einem solchen Verfahren unterziehen, dürfte überhaupt nicht bewusst sein, welche Folgen für sie daraus erwachsen können.

Eine häufig eingesetzte und wirksame Methode der nachrichtendienstlichen Informationsbeschaffung ist die gezielte Verbindungsaufnahme zu anderen Tagungsteilnehmern und Messebesuchern. Aus zunächst fachbezogenen und deshalb unverfänglich wirkenden Gesprächen können tiefere, vertrauensvolle Beziehungen entstehen. Nicht selten kommt es daraufhin zu Einladungen nach China. Dort gestalten die Geheimdienste ihren „Gästen“ den Aufenthalt möglichst angenehm und versuchen, sie abzuschöpfen und für eine Mitarbeit zu gewinnen, ohne dass ihr Ziel sofort erkennbar wird. Besonderes Interesse zeigen sie an Informations-, Luft- und Raumfahrttechnologien und an allen rüstungsrelevanten Industriebereichen.

Es muss auch nach wie vor damit gerechnet werden, dass Gepäckstücke und Hotelzimmer durchsucht, Telekommunikationsanlagen abgehört, E-Mails mitgelesen und Besprechungen mitgeschnitten werden.

Die kommunistische Regierungspartei duldet weiterhin keine Bestrebungen, die ihre Machtposition gefährden könnten. Die Überwachung der in Deutschland ansässigen Landsleute, die dem politischen System ihres Heimatlandes kritisch gegenüberstehen und einer Oppositionsgruppe angehören, zählt ebenfalls zu den Aufgaben der chinesischen Nachrichtendienste. In Baden-Württemberg lebende Anhänger der in China seit 1999 verbotenen Falun-Gong-Bewegung unterrichteten das LfV von Störaktionen gegen ihre Aktivitäten durch massiven Telefonterror.

### 2.2.2 Russische Föderation

Um den Nachrichtendiensten wirksame Grundlagen für ein erfolgreicheres Arbeiten zu verschaffen, wurden im Jahr 2003 tief greifende - und in der Zwischenzeit wohl abgeschlossene - Restrukturierungsmaßnahmen angeordnet, die Kompetenzen erweitert sowie ihr im Jahr 2004 bereits deutlich angehobener Etat im Jahr 2005 nochmals um 25 Prozent erhöht.

Trotz der guten zwischenstaatlichen Beziehungen mit Russland sind die russischen Dienste auch in Deutschland unverändert aktiv. Sie haben den Auftrag, wichtige Informationen aus Politik, Militär, Wirtschaft und Wissenschaft zu beschaffen. Vor allem der industrielle Sektor soll durch solche Maßnahmen unterstützt werden.



Primär zuständig für die zivile operative Auslandsaufklärung ist der Auslandsnachrichtendienst SWR<sup>451</sup>. Er verfügt über mehr als 13.000 Mitarbeiter. Um an besonders sensible Informationen zu gelangen, wirbt er weltweit Agenten an - auch in Deutschland.

Der militärische Auslandsnachrichtendienst GRU<sup>452</sup> wurde nach dem Zusammenbruch der Sowjetunion im Jahr 1992 von der Russischen Föderation übernommen und unverändert erhalten. Mit seinen ca. 12.000 Mitarbeitern untersteht der nach eigenen Angaben „*geheimste Dienst Russlands*“ dem Verteidigungsministerium. Sein vorrangiger Aufklärungsauftrag in Deutschland ist die Informationsbeschaffung aus den Bereichen Bundeswehr und Rüstungstechnik. Operationen können sowohl vom russischen Territorium als auch von den Legalresidenturen<sup>453</sup> in den diplomatischen und konsularischen Vertretungen in Deutschland ausgehen. Bei der Anwerbung neuer Agenten erkunden die in Gesprächsführung bestens geschulten Operativoffiziere die Lebensumstände, Zugangsmöglichkeiten und die Eignung ihrer Zielpersonen, die sie dann auch selbst führen, für eine spätere Zusammenarbeit. Ziel ist es, die Quelle durch ein sehr enges persönliches, fast freundschaftliches Verhältnis an ihren Führungsoffizier zu binden.

Die Legalresidenturen sind eine wesentliche Stütze der russischen Spionage im Bundesgebiet. Ihre vielfältigen Kontakte zu Politik, Militär, Wirtschaft, Wissenschaft und Forschung nutzen sie zur nachrichtendienstlichen Informationsgewinnung. Die Führungsoffiziere - Angehörige von SWR und

<sup>451</sup> „Slushba Wneschnoj Raswedkij“.

<sup>452</sup> „Glawnoje Raswedwatelnoje Uprawlenije“.

<sup>453</sup> Abgetarnte Stützpunkte fremder Nachrichtendienste in den offiziellen Vertretungen (insbesondere Botschaften, Konsulate, Handelsvertretungen) des Auftraggebers im Operationsgebiet.

„Spionage ist für uns kein abstraktes Risiko, sondern eine tatsächliche Bedrohung, gegen die wir uns schützen müssen. Und auch bei materiell motivierten Diebstählen dürfen die Informationen nicht zugänglich sein.“

(Peter Warnicke, Oberstleutnant, IT-Sicherheitsbeauftragter der Bundeswehr, Pressemitteilung der Utimaco Safeware AG zur Ausrüstung von 20.000 Bundeswehr-Notebooks mit der Sicherheitssoftware SafeGuard Easy)

GRU - nehmen zum Beispiel auf Messen und Fachkongressen Kontakt zu Vertretern deutscher Unternehmen auf und beschaffen offen zugängliches Material. Besonderes Interesse finden die Informationstechnik, elektronische Systeme, Steuerungssysteme und die Forschung.

Die Einbindung der Legalresidenturen in die Nachrichtenbeschaffung veranschaulicht folgender Vorgang:

- Wie internationale Medien erst geraume Zeit nach der Entdeckung und der diplomatischen Lösung des Falles im April 2005 berichteten, führte Alexander K., russischer Konsul in Hamburg, ca. 20 geheime Treffen mit einem Bundeswehrangehörigen in Süddeutschland durch. Für vertrauliche Unterlagen über deutsche Waffensysteme und moderne Fernmeldetechnik bezahlte er seinem Informanten insgesamt ca. 10.000 Euro. Nach Intervention des Bundesamtes für Verfassungsschutz bei der russischen Regierung wurde der Diplomat am 5. Dezember 2004 aus Deutschland abberufen.

**Aufwertung des FSB**

Der Föderale Sicherheitsdienst FSB<sup>454</sup> hat in seiner Eigenschaft als tragendes Element der staatlichen Sicherheitsstruktur eine weitere Festigung erfahren. Er verfügt über ca. 350.000 Mitarbeiter und ist zuständig für die zivile und militärische Spionageabwehr, die Beobachtung des politischen Extremismus sowie die Bekämpfung von Terrorismus und die Aufklärung der Organisierten Kriminalität. Unter dem Deckmantel „Spionageabwehr“ wirbt er ausländische Staatsangehörige an, die sich in Russland aufhalten, und betreibt auf diese Weise ebenfalls Auslandsaufklärung.

Russischen Medienberichten zufolge erging Ende August 2005 eine Weisung der Regierung an die Telefongesellschaften des Landes, dem FSB und dem Innenministerium uneingeschränkt Zugriffsrecht auf ihre Datenbanken mit Informationen über Ferngespräche, Rechnungen, angebotene Dienstleistungen und Kundendaten zu gewähren. Damit erhält der FSB eine optimale Ergänzung zu den Monitoring-Systemen SORM 1 und 2, die es dem Geheimdienst gestatten, jederzeit Telefongespräche mitzuhören und Internetaktivitäten zu überwachen. Durch diese zusätzlichen Informationen kann der FSB, auch rückwirkend, auf sämtliche Personen- und Anschlussdaten sowie Gesprächsinhalte zugreifen und sie für nachrichtendienstliche Zwecke nutzen. Deutsche Firmen und Privatpersonen müssen

<sup>454</sup> „Federalnaja Slushba Besopasnosti“.

„85% des geistigen Eigentums einer Firma kann aus E-Mails ausgelesen werden und die Leute behandeln E-Mails immer noch wie ein Stiefkind.“  
(John Dolan, Manager bei Oracle, Quelle: silicon.de, „Schlamperei ist schlimmer als mobile Viren“)

damit rechnen, in Russland bei der Nutzung von Telefon und Internet in das Blickfeld des FSB zu geraten und gezielt überwacht zu werden.

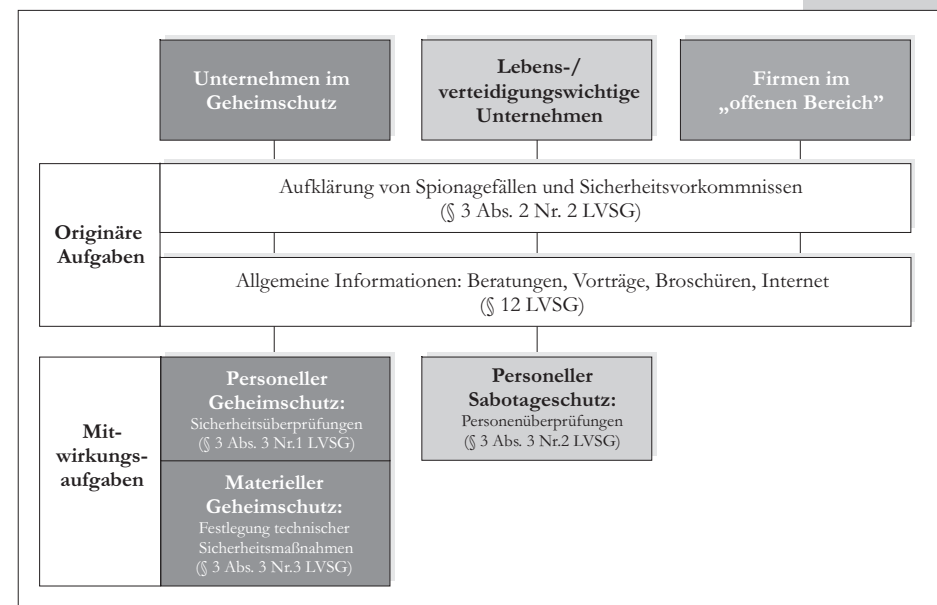
**3. Prävention**

Unter dem Begriff Prävention versteht man die Gesamtheit aller vorbeugenden Maßnahmen, die der Verfassungsschutz entweder aufgrund gesetzlichen Auftrags zu erfüllen hat oder aus Opportunitätsgründen heraus ergreifen kann, um sensitives Wissen oder die Integrität sicherheitsempfindlicher Einrichtungen zu schützen.

Mitarbeiter der Spionageabwehr haben auch 2005 in zahlreichen Vorträgen bei Firmen, Verbänden und Behörden die aktuelle Risikolage hinsichtlich Spionage und Sabotage aufgezeigt und zielgruppengerechte Empfehlungen zur Verhinderung von Schäden sowie zur richtigen Verhaltensweise im Konfliktfall gegeben.

Beratungsangebot

**Leistungsangebot des Landesamts für Verfassungsschutz Baden-Württemberg für die Wirtschaft**



### 3.1 Geheim- und Sabotageschutz

Ein wesentliches Element der Prävention bildet der förmliche Geheim- und Sabotageschutz, der wiederum Teil der gesetzlich vorgeschriebenen so genannten Mitwirkungsaufgaben<sup>455</sup> ist. Diese umfassen u.a. Sicherheitsüberprüfungen von Personen, technische und organisatorische Maßnahmen sowie die Beratung von Behörden und Wirtschaftsunternehmen.

Während der Geheimschutz in erster Linie als Vorbeugungsmaßnahme gegen Ausspähungsbemühungen fremder Nachrichtendienste anzusehen ist, soll der Sabotageschutz den Bestand lebens- und verteidigungswichtiger Einrichtungen sichern. Beide Aufgabenstellungen erfordern komplexe Sicherheitslösungen mit umfassenden Schutzmaßnahmen auf personellem, organisatorischem und technischem Gebiet, die nur im Wege des intensiven Zusammenwirkens von Staat und Wirtschaft erfolgreich zu bewältigen sind.

In Baden-Württemberg sind derzeit über 200 Unternehmen in das amtliche Geheimschutzverfahren einbezogen und rund 25 Unternehmen als lebens- und verteidigungswichtig eingestuft. Sie werden vom Landesamt für Verfassungsschutz regelmäßig über sicherheitsgefährdende Bestrebungen beziehungsweise Aktivitäten fremder Nachrichtendienste aufgeklärt und entsprechend beraten. Ziel ist es, den hiesigen Unternehmen bei der Aufarbeitung von Sicherheitsvorkommnissen kompetent zur Seite zu stehen und sie durch ein ausgefeiltes Präventionsprogramm in die Lage zu versetzen, Gefahren frühzeitig zu erkennen und darauf auch angemessen reagieren zu können.

### 3.2 Objektschutz als integraler Bestandteil der IT-Sicherheit

Der Beratungsschwerpunkt liegt dabei seit Jahren auf dem Gebiet der IT-Sicherheit. Immer mehr Behörden und Unternehmen sind bereit, den Schutz ihrer Informations- und Kommunikationssysteme (IuK) zu verbessern und entsprechend zu investieren. Der baden-württembergische Verfassungsschutz legt bei diesen Beratungen besonderes Augenmerk auf die Schnittstelle zwischen der IT-Sicherheit und der konventionellen Gebäudesicherheit. Nur wenn die jeweiligen Sicherheitskonzepte im Sinne eines ganzheitlichen Informationsschutzes aufeinander abgestimmt sind und ein-

<sup>455</sup> Neben den originären Aufgaben gem. § 3 Abs. 2 LVSG nimmt das Landesamt für Verfassungsschutz gem. § 3 Abs. 3 LVSG auch Mitwirkungsaufgaben wahr, die regelmäßig den Antrag (zum Beispiel auf Durchführung einer Sicherheitsüberprüfung) einer externen Stelle voraussetzen.

heitliche Bedrohungsszenarien beziehungsweise Schutzzieldefinitionen berücksichtigen, erreichen sie die gewünschte Wirkung.

Konkrete Bedrohungen treten vor allem dann auf, wenn es unbefugten Dritten gelingt, sich ungehindert oder ohne größere Barrieren überwinden zu müssen, Zugang zu Betriebsgeländen und Gebäuden zu verschaffen oder gar in sensible Bereiche von Behörden oder Wirtschaftsunternehmen vorzudringen. Das folgende Beispiel aus der Beratungspraxis des Landesamts für Verfassungsschutz verdeutlicht, welche Risiken entstehen können, wenn unzureichende Objektschutzmaßnahmen getroffen oder bestehende Vorkehrungen außer Kraft gesetzt werden:

- Ein überregional tätiges, strategisch besonders bedeutsames Rechenzentrum ist durch stetigen Personal- und Aufgabenzuwachs permanent inhomogen gewachsen. Sicherheitsmaßnahmen konzentrierten sich auf die immer komplexer werdenden IT-Systeme und Netze. Doch weder die Gebäude- noch die vorhandene materielle Sicherheitsinfrastruktur konnten mit dieser Entwicklung Schritt halten. Vielmehr wurden unter anhaltendem finanziellem Druck Sicherheitsmaßnahmen (unter anderem personelle Bewachung, ständige Pfortenbesetzung, technische Überwachung) reduziert oder gänzlich aufgegeben. Bei der nachfolgenden Auslagerung von Organisationseinheiten und IT-technischen Einrichtungen in zusätzlich angemietete Gebäude wurde auf die Realisierung an sich gebotener Schutzmaßnahmen weitgehend verzichtet. Unbefugte konnten sich somit fast ungehindert Zugang zu den Objekten und den sensiblen IT-Einrichtungen verschaffen.

Grundlegende Basis für die Beratungspraxis des LfV auf dem Sektor der materiellen Sicherheit sind neben dem eigenen Erfahrungswissen und den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) die am 20. Dezember 2004 erlassene Neufassung der Verschlusssachenanweisung (VSA) des Landes Baden-Württemberg und deren zeitgleich veröffentlichte ergänzenden Richtlinien, insbesondere die VS-IT-Richtlinie.<sup>456</sup>

*„Statt aufwendig ins Firmennetz einzudringen, reicht es, den Laptop zu stehlen, während der Besitzer beim Geschäftsessen ist, und heimlich die Festplatte zu spiegeln.“*

*(Frank Lesiak, Sicherheitsexperte des BND auf der 9. Deutschen Mobile Computing Konferenz 2005 am Spitzingsee)*

**Problem:**  
**Gebäudesicherheit**

<sup>456</sup> URL: [http://www.verfassungsschutz-bw.de/spio/files/spio\\_praev\\_2005-02\\_2.html](http://www.verfassungsschutz-bw.de/spio/files/spio_praev_2005-02_2.html).

### 3.3 Sicherheitsforum Baden-Württemberg

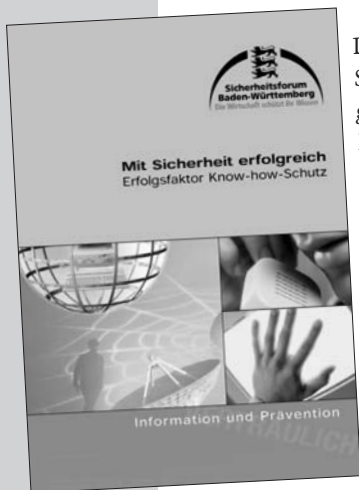
Das Landesamt für Verfassungsschutz war 1999 neben namhaften Repräsentanten aus Wirtschaft, Forschung und Verwaltung Gründungsmitglied des Sicherheitsforums Baden-Württemberg. Dieses Gremium hat es sich zum Ziel gesetzt, Hilfe zur Selbsthilfe bei der Sicherung des Technologievorsprungs der heimischen Wirtschaft und Forschung zu leisten. Darüber hinaus soll auch die Sensibilität für andere Gefährdungspotenziale wie Extremismus, Terrorismus, Sabotage und allgemeine Wirtschaftskriminalität gefördert werden.

Die Mitglieder verstehen sich als Bindeglied zwischen Wirtschaft und Politik und haben ihren Handlungsrahmen entsprechend festgelegt. Als Tätigkeitsschwerpunkte gelten folgende Aufgaben:

- Sensibilisierung besonders von kleinen und mittelständischen Unternehmen für Gefahren durch Angriffe, die insbesondere zum Verlust von Know-how führen können, von innen und außen,
- Hilfestellung bei der Entwicklung von Instrumenten für den unternehmensspezifischen Informationsschutz,
- Entwicklung von Ansätzen für ganzheitliche Sicherheitsbetrachtungen und
- Reaktion auf aktuelle Sicherheitslagen.

Die Ende 2004 veröffentlichten Ergebnisse der vom Sicherheitsforum bei der Universität Lüneburg in Auftrag gegebenen Fall- und Schadensanalyse hatten eine beachtliche Wirkung in der Öffentlichkeit. Die Studie hat bereits bestehende Befürchtungen bestätigt, dass bei kleinen und mittelständischen Unternehmen selbst die grundlegendsten Vorkehrungen gegen Spionage beziehungsweise illegalen Informationsabfluss vielfach unbekannt, nicht vorhanden oder unzureichend sind. Das Landesamt für Verfassungsschutz hat im Jahr 2005 die Ergebnisse der Studie - insbesondere die Empfehlungen zur Prävention - aufbereitet und daraus entsprechende Empfehlungen abgeleitet. Es misst beispielsweise der

#### Aufgaben



Schaffung innerbetrieblicher Sicherheitsstrukturen eine hohe Priorität zu. An ihrer Spitze müssen qualifizierte haupt- oder nebenamtliche Sicherheitsverantwortliche mit weit reichenden Kompetenzen stehen.

Neu verfügbar ist die von allen Mitgliedern des Sicherheitsforums gemeinsam erarbeitete Broschüre „Mit Sicherheit erfolgreich - Erfolgsfaktor Know-how-Schutz“. Sie beschreibt exemplarische Fälle aus der Praxis und gibt konkrete Empfehlungen zur Verbesserung des Informationsschutzes. Weitere Hinweise gibt es auf der Internetseite [www.sicherheitsforum-bw.de](http://www.sicherheitsforum-bw.de).

*„Das erfolgreichste Konzept für IT-Sicherheit liegt in der Fähigkeit der Unternehmen, die richtige Mischung aus Know-how, Strategie und Technologie zu implementieren.“*

*(Dr. Kurt Glasner, Experte für den Bereich Information Technology und Partner bei der Wirtschaftsprüfungs- und Beratungsgesellschaft PricewaterhouseCoopers AG, Pressemitteilung der PwC vom 17. Oktober 2005)*

### 4. Erreichbarkeit der Spionageabwehr

Wenn Sie Hinweise oder Anregungen geben wollen beziehungsweise weitere Informationen wünschen, so können Sie die Spionageabwehr wie folgt erreichen:

Landesamt für Verfassungsschutz Baden-Württemberg  
- Abteilung 4 -  
Taubenheimstraße 85 A  
70372 Stuttgart

Telefon 0711 - 95 44 301  
Telefax 0711 - 95 44 444

Über ein **Vertrauliches Telefon** können Sie der Spionageabwehr unter

**0711 - 9 54 76 26** (Telefon) und  
**0711 - 9 54 76 27** (Telefax)

rund um die Uhr Informationen - auch anonym - übermitteln. Selbstverständlich werden Ihre Hinweise auf Wunsch vertraulich behandelt.