

## E. SPIONAGEABWEHR, GEHEIM- UND SABOTAGESCHUTZ

### 1. Aktuelle Entwicklungen und Tendenzen

Die weltpolitische Lage war in den letzten Jahren drastischen Veränderungen unterworfen. Im Mittelpunkt deutscher Sicherheitsinteressen steht inzwischen nicht mehr die klassische Landesverteidigung. Heutzutage stellen - neben dem internationalen Terrorismus und gewaltsam ausgetragenen nationalistisch und ethnisch motivierten regionalen Konflikten - die ABC<sup>345</sup>-Waffen-Fähigkeit von Krisenländern<sup>346</sup> sowie die immer zahlreicher werdenden Angriffe auf unsere Informations- und Kommunikationssysteme die hauptsächlichliche Bedrohung dar.

*„Wir haben heute die Fähigkeit, unsere Raketen bis zu 2000 Kilometer weit zu schicken.“*

(Akbar Haschemi Rafsandschani, Iranischer Ex-Präsident, www.orf.at. vom 6. Oktober 2004, Meldung über ein Interview Rafsandschani mit der staatlichen iranischen Nachrichtenagentur IRNA in Teheran am 5. Oktober 2004)

Der anhaltende Nuklearpoker Nordkoreas und die Besorgnis, der Iran könnte neben dem Aufbau eines zivilen Atomprogramms auch die Entwicklung von Kernwaffen erfolgreich vorantreiben, haben die Welt 2004 wiederholt in Unruhe versetzt. Die Politik beider Länder lässt eine Entwicklung mit möglicherweise weit reichenden Konsequenzen erahnen: die Verbreitung militärisch nutzbarer Kerntechnik könnte weitere Staaten animieren,

selbst nach Atomwaffen zu greifen und damit bedeutsame Verschiebungen der strategischen und militärischen Kräfteverhältnisse nach sich ziehen. Auch terroristische Fanatiker könnten den Besitz von Nuklearsprengstoff anstreben. Die westliche Außen- und Sicherheitspolitik ist daher darauf ausgerichtet, die Weiterverbreitung von Massenvernichtungswaffen und Trägersystemen zu verhindern und bereits die Weitergabe des einschlägigen Know-hows und der notwendigen technischen Bausteine zu unterbinden. Die Spionageabwehr des Landesamts für Verfassungsschutz Baden-Württemberg (LfV) hat sich deshalb auch 2004 mit Nachdruck der Aufklärung solcher Aktivitäten im Interesse fremder Staaten angenommen, bei denen Anhaltspunkte dafür vorliegen, dass sie als illegal im Sinne des Außenwirtschafts- oder Kriegswaffenkontrollgesetzes anzusehen sind und die beteiligten Beschaffungsorganisationen dabei geheimdienstliche oder geheimdienstähnliche Methoden anwenden.

Die klassischen Felder der Spionage - Politik, Militär und Wirtschaft/Wissenschaft - traten daneben etwas in den Hintergrund, ohne allerdings ihre

<sup>345</sup> Atomare, biologische und chemische Waffen.

<sup>346</sup> 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), vgl. Kapitel 2.1.

Aktualität zu verlieren. 2004 waren aus Sicht der Spionageabwehr in diesem Zusammenhang die tief greifenden Veränderungen des politischen Systems in Russland sowie die wirtschaftliche Entwicklung in der Volksrepublik China und der dort praktizierte Umgang mit dem geistigen Eigentum Dritter besonders bedeutsam. Die aktuellen Erfahrungen deutscher Firmen und ihrer Repräsentanten im Ausland belegen, dass auch weiterhin mit Versuchen gerechnet werden muss, hierzulande erarbeitetes Know-how zum Nulltarif abzuschöpfen.

Einen wichtigen Beitrag zur Aufhellung der Gefahren, die der einheimischen Industrie durch Wirtschaftsspionage und durch die vom LfV mangels Zuständigkeit nicht zu bearbeitende Konkurrenzausspähung drohen, leistet die von der Universität Lüneburg im Auftrag des Sicherheitsforums Baden-Württemberg durchgeführte Fall- und Schadensanalyse auf dem Sektor Know-how-/Informationsverluste. Durch Interviews und Fragebogenauswertung konnten die Erfahrungen und Einschätzungen von 400 Unternehmen aus Baden-Württemberg zusammengeführt werden. Demnach beträgt das Gefährdungspotenzial für Produktideen und Produktions-Know-how mehrere Milliarden Euro pro Jahr, immense Schäden sind bereits eingetreten. Auch zeigt sich, dass erhebliche Defizite im präventiven Bereich und bei der Aufarbeitung festgestellter Sicherheitsvorkommnisse bestehen.

Die Spionageabwehr hat 2004 erneut an der Bekämpfung des Islamismus mitgewirkt. Speziell ihre über Jahrzehnte hinweg gesammelten Erfahrungen bei der Beobachtung fremder Nachrichtendienste und aktuelle Erkenntnisse in Bezug auf Vertreter einschlägig aktiver Geheimdienste und andere verdächtige Akteure waren wichtige Mosaiksteine für die Einschätzung der Gesamtsituation.

Im Rahmen der präventiven Spionageabwehr wurde der bisherige Kurs konsequent fortgesetzt. Der Mix aus allgemeiner Öffentlichkeitsarbeit in den Medien, unternehmens- oder themenbezogenen Vorträgen und Beratungen sowie der Beteiligung an Sicherheitspartnerschaften hat verstärkt Beachtung gefunden und eine rege Nachfrage speziell aus der Wirtschaft hervorgerufen. Im Vordergrund stand das Bemühen der Unternehmen, ihre Mitarbeiter bei Auslandseinsätzen möglichst optimal auf potenzielle Gefahren vorzubereiten und damit drohenden Informationsverlusten frühzeitig vorzubeugen. Besonderes Interesse bestand auch an der Einschätzung technischer Entwicklungen unter Sicherheitsaspekten. Aufgeschreckt durch



### Prävention

Medienberichte über Schwachstellen bei drahtlosen Kommunikationssystemen hat eine Reihe von Sicherheitsverantwortlichen auf die Kompetenz des LfV zurückgegriffen. Solche Kontakte waren auch immer wieder Anlass, ganz generell vor den neuen Dimensionen und der gesteigerten Qualität der Angriffe auf Informations- und Kommunikationssysteme zu warnen. Besondere Probleme ergeben sich hier durch die Anonymität der Akteure, die weltumspannenden Möglichkeiten des Zugriffs auf die gesamte Infrastruktur einer modernen Informationsgesellschaft sowie durch die Tatsache, dass Auswirkungen oft nur schwer und zu spät erkannt werden.

## 2. Daten, Fakten, Hintergründe

### 2.1 Krisenländer

Die Verbreitung nuklearer, biologischer und chemischer Massenvernichtungswaffen stellt eines der größten Bedrohungspotenziale dar. Unbeirrbar halten die so genannten Krisenländer an ihrem Ziel fest, in den Besitz solcher Waffen und der zu ihrem Einsatz benötigten Trägertechnologie zu gelangen. Staaten wie Iran, Nordkorea, Indien, Pakistan oder Syrien sehen darin ein notwendiges Mittel, um äußere Bedrohungen abzuwehren oder politische Forderungen gegenüber benachbarten Ländern oder der internationalen Staatengemeinschaft besser durchsetzen zu können. Mit der zunehmenden Zahl der Krisenherde wächst auch die Bedeutung der Aufdeckung proliferationsrelevanter Sachverhalte. Länder, deren Nachrichtendienste sich um Waffentechnologien beziehungsweise Dual-Use-Güter<sup>347</sup> bemühen, nutzen teilweise die Möglichkeit, über Tarnorganisationen Kontakte zu hier ansässigen Firmen herzustellen. Gerade im exportorientierten Baden-Württemberg 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 aus **Königsbronn/Krs. Heidenheim** vom Landgericht Stuttgart wegen Verstoßes gegen das AWG und das KWKG zu einer Freiheitsstrafe von vier Jahren verurteilt. Hintergrund des Urteils war sein Versuch, 214 Aluminiumrohre mit einem Gesamtgewicht von rund 22 Tonnen

<sup>347</sup> Als „Güter mit doppeltem Verwendungszweck“ werden Güter einschließlich Datenverarbeitungsprogrammen und Technologien bezeichnet, die sowohl für zivile als auch militärische Zwecke verwendet werden können.

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 Lieferung konnte auf dem Seeweg gestoppt werden. Der Geschäftsführer des beteiligten Hamburger Transportunternehmens, der sich an der verbotenen Ausfuhr beteiligte, wurde zu einer Freiheitsstrafe von einem Jahr und drei Monaten auf Bewährung verurteilt.

Zuwiderhandlungen gegen Ausfuhrverbote und Embargobestimmungen wurden 2004 immer häufiger mit dem Verdacht der geheimdienstlichen Agententätigkeit in Zusammenhang gebracht, weil eine Steuerung durch den jeweiligen Nachrichtendienst vermutet beziehungsweise nicht ausgeschlossen werden konnte.

Nicht selten basieren Proliferationsgeschäfte<sup>348</sup> auf skrupelloser Gewinnsucht unter grober Missachtung der Bedrohung, die mittlerweile von den Krisenländern ausgeht:

- So zeigte sich der Geschäftsführer eines Unternehmens, das unter anderem mit Maschinen für die Pharmaindustrie handelt, die auch zur Herstellung chemischer Kampfstoffe geeignet sind, uneinsichtig. Nachdem das LfV ihn auf die Gefahren aufmerksam gemacht hatte, kündigte er an, seine Geschäfte in Zukunft vom benachbarten Ausland aus abwickeln zu wollen.

Proliferation wird auch durch illegalen Wissenstransfer begünstigt. Ingenieuren und Wissenschaftlern aus Krisenländern bieten sich vielfältige Möglichkeiten, im westlichen Ausland gezielt einschlägiges Know-how zu erlangen.

Maßnahmen des LfV zur Verhinderung von Proliferationslieferungen führten in einem weiteren Fall zu Erkenntnissen über einen deutschen Unternehmer, der versucht hatte, bei einem Auslandsaufenthalt illegale Beschaffungsbemühungen mit seinem Wissen zu unterstützen:

- Ein Ingenieur aus Baden-Württemberg stand mit Rat und Tat einer iranischen Beschaffungsdelegation, zu der auch iranische Wissen-

<sup>348</sup> Proliferation: Weiterverbreitung von Massenvernichtungswaffen beziehungsweise der zu ihrer Herstellung verwendbaren Produkte einschließlich des dafür erforderlichen Know-hows sowie von entsprechenden Waffenträgersystemen.

schaftler gehörten, bei dem Versuch zur Seite, im benachbarten Ausland 24 Telemanipulatoren<sup>349</sup> zur Bearbeitung von Plutonium zu erwerben. Sie sollten von dort als Bestandteil eines militärischen Nuklearprogramms an den ausländischen Empfängerstaat für die Handhabung abgebrannter Kernbrennstäbe sowie zur Trennung von Plutonium geliefert werden. Das LfV konnte zur Eröffnung des Ermittlungsverfahrens wegen Verstoßes gegen das KWKG und geheimdienstlicher Agententätigkeit gemäß § 99 Strafgesetzbuch Hintergrundinformationen beitragen.

Nach den Erfahrungen der Verfassungsschutzbehörden gibt es folgende Anhaltspunkte für illegale Beschaffungsaktivitäten durch Krisenländer:

### Illegale Beschaffungsmethoden - Proliferation

**WORAN KANN MAN ILLEGALE GESCHÄFTE ERKENNEN?**

Nach Erfahrungen der Verfassungsschutzbehörden aus Bund und Ländern können folgende Anhaltspunkte auf ein proliferationsrelevantes Geschäft hindeuten:

- Der tatsächliche Endverbleib der Güter ist unklar und kann nicht plausibel erklärt werden.
- Der Kunde kann nicht erklären, wofür das Produkt gebraucht wird beziehungsweise der beabsichtigte Verwendungszweck weicht erheblich von der vom Hersteller vorgegebenen Produktbestimmung ab.
- Der Kunde handelt üblicherweise mit militärischen Gütern.
- Der auftretende Käufer verfügt nicht über das erforderliche Fachwissen.
- Die tatsächliche Identität eines Neukunden ist nicht bekannt.
- Es werden ohne erkennbaren Grund Zwischenhändler eingeschaltet.
- Der Kunde wünscht eine außergewöhnliche Etikettierung oder Kennzeichnung/Beschriftung, um die Güter zu neutralisieren.
- Angebotene Zahlungsbedingungen sind besonders günstig, wie zum Beispiel Barzahlung, hohe Vorauszahlungen oder ungewöhnliche Provisionen.
- Der Käufer verzichtet auf das Einweisen in die Handhabung, auf Serviceleistungen oder auf Garantie.
- Firmenangehörige werden zu Ausbildungszwecken zur Herstellerfirma nach Deutschland geschickt, obwohl eine Einweisung vor Ort praktischer und sinnvoller wäre.
- Mitglieder von Besucherdelegationen werden namentlich nicht vorgestellt.
- Zu weiteren Geschäftskontakten nach Deutschland wird geschwiegen.

Quelle: Broschüre „Proliferation - das geht uns an“.

<sup>349</sup> Industrieroboter, der von einer Bedienkonsole aus gesteuert wird, um Arbeiten in gefährlicher oder unzugänglicher Umgebung zu ermöglichen; findet beispielsweise auch in der minimal-invasiven Chirurgie Verwendung.

Die Verfassungsschutzbehörden des Bundes und der Länder haben gemeinsam eine aktualisierte Broschüre<sup>350</sup> zum Thema Proliferation herausgegeben, die weiterführende Informationen und nützliche Kontaktadressen enthält.

### 2.2 Volksrepublik China

Seit Beginn der Reformpolitik Ende der 70er-Jahre hat die wirtschaftliche Entwicklung Chinas einen atemberaubenden Aufschwung erfahren. Auf dem Land und seiner Wirtschaft ruhen große Erwartungen. Kaum ein renommiertes Unternehmen kann es sich noch leisten, auf dem wachstumsstarken chinesischen Markt nicht vertreten zu sein. Die Zahl von Produktionsstätten und Repräsentanzen deutscher Firmen hat sich gegenüber dem Vorjahr mit weit über 2.000 - darunter allein circa 450 aus Baden-Württemberg - deutlich erhöht. Der Druck, im „Reich der Mitte“ zu investieren, ist größer als die begründete Sorge, sich auf diese Weise gleichzeitig die eigene Konkurrenz „heranzuzüchten“. Speziell Unternehmen, die sogar ihre Forschungsbereiche dorthin verlagern, laufen Gefahr, ungewollt kostenlose „Entwicklungshilfe“ zu leisten.

Zwar ist China zwischenzeitlich allen internationalen Konventionen zum Schutz geistigen Eigentums beigetreten. Gleichwohl beklagt die deutsche Wirtschaft, dass die Umsetzung der Gesetze vielerorts noch sehr zu wünschen übrig lasse und es so gut wie nichts gebe, was dort nicht kopiert werde. Die Aussage eines Insiders, „*was Sie an Know-how und Technologie nach China bringen, ist weg*“, unterstreicht diese Befürchtungen.

In einem metallverarbeitenden Betrieb in Baden-Württemberg ist ein chinesischer Praktikant durch die massive Missachtung von Sicherheitsvorschriften aufgefallen, indem er verbotswidrig seinen privaten Laptop in das Unternehmen einschleuste und aus dem firmeninternen Computernetz die gesamten Daten eines kurz vor Beendigung stehenden Projekts auf seine Festplatte lud. Außerdem bemühte er sich in aufdringlicher Weise, Gespräche von Kollegen mitzuhören und hielt sich bevorzugt auch außerhalb der üblichen Arbeitszeiten im Unternehmen auf.

<sup>350</sup> Die Broschüre „Proliferation - das geht uns an!“ kann über die Verfassungsschutzbehörden des Bundes und der Länder bezogen werden; sie ist unter anderem auf der Homepage des Landesamts für Verfassungsschutz Baden-Württemberg eingestellt.



Gefahren

Beispiel

„Die Angst vor Technologieklaue ist für fast alle deutschen Zulieferer, die derzeit in China tätig sind, ein besonders wichtiges Thema.“

(Wirtschaftsprüfungsgesellschaft Ernst & Young AG, Studie „Automobilstandort Deutschland in Gefahr?“, September 2004)

## nachrichtendienstliche Aktivitäten

Sofern eine offene Erkenntnisgewinnung nicht möglich ist, setzt die Volksrepublik China nach wie vor auf ihre personenstarken Nachrichtendienste. Diese betreiben auch in Baden-Württemberg eine intensive Aufklärung im wirtschaftlichen und wissenschaft-

lichen Bereich. Hier ist weiterhin eine hohe Anzahl chinesischer Wissenschaftler und Doktoranden zu beobachten. Sie verfügen nicht nur über fundiertes Wissen, sondern haben häufig auch noch unbeschränkten Zugang zu sensiblen Arbeitsbereichen. Dadurch eröffnen sich diesem Personenkreis ideale Möglichkeiten zur Ausspähung wertvoller Informationen. In Einzelfällen konnten Kontakte zu Nachrichtendienstangehörigen an der Chinesischen Botschaft in Berlin festgestellt werden. Das LfV nahm dies zum Anlass, Wissenschafts- und Forschungseinrichtungen sowie Wirtschaftsunternehmen zu sensibilisieren und auf die besondere Problematik hinzuweisen. Insbesondere wurde der Umgang mit chinesischen Delegationen thematisiert und auf die Risiken des Abhandenkommens von Unterlagen beziehungsweise Laptops und des unbefugten Fotografierens aufmerksam gemacht.

Auffällig sind ferner Verbindungen von Angehörigen chinesischer Legalresidenzen<sup>351</sup> zu landsmannschaftlichen Verbänden und Vereinen. Die Vorsitzenden solcher Vereine werden von chinesischen Nachrichtendiensten teilweise ganz gezielt eingesetzt, um sie in ihrem Sinne zu steuern. Besonders verdiente Funktionäre erhalten Einladungen zu Staatsempfängen. Die Vereine bekommen, sofern sie eine staats-treue Linie verfolgen, finanzielle Unterstützung. Funktionäre chinesischer Studentenvereinigungen beobachten zum Beispiel ihre studierenden Landsleute, um frühzeitig oppositionelle Bestrebungen erkennen zu können. Angehörige der seit 1999 in China verbotenen Falun-Gong-Bewegung sind - ungeachtet ihrer Nationalität - weiterhin auch im Ausland einer repressiven Überwachung durch chinesische Nachrichtendienste ausgesetzt.

### 2.3 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 stringent voran. Trotz der wachsenden Intensivierung der deutsch-russischen Beziehungen unternehmen die russischen Nach-

richtendienste jedoch 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 Leistungsfähigkeit der eigenen Wirtschaft profitiert enorm von diesen Ausspähungsergebnissen.

Der Präsident der Russischen Föderation, Wladimir Putin, hat als Reaktion auf innere Unruhen und aus Gründen der Effizienz im Mai 2003 die Sicherheitsdienste umstrukturiert. Macht und Einfluss des zivilen Auslandsnachrichtendienstes SWR<sup>352</sup> und des „Föderalen Sicherheitsdienstes“ (FSB)<sup>353</sup> 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)<sup>354</sup> 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 des Kalten Krieges beim ehemaligen „Komitee für Staatssicherheit“ (KGB)<sup>355</sup> gewohnt war.

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

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. Langjährig geführte Agenten mit Zugang zu besonderen Zielobjekten sind nicht nur in der Lage, kontinuierlich Wissen zu beschaffen, sondern können dieses zugleich auch noch unter fachlichen Gesichtspunkten bewerten. Über

„Wichtiger als Beziehungen sind die realen Vollmachten des FSB und seine Kontrolle über andere Dienststellen.“  
(Wladimir Pryblowskij, Politologe, Frankfurter Rundschau vom 15. Juli 2004, „Kreml baut Macht des Geheimdienstes aus“)

## große Anstrengungen

## Stärkung der Nachrichtendienste

## Methoden

## Russische Föderation

<sup>351</sup> Abgetarnte Stützpunkte fremder Nachrichtendienste in den offiziellen Vertretungen (insbesondere Botschaften, Konsulate, Handelsvertretungen) des Auftraggebers im Operationsgebiet.

<sup>352</sup> „Slushba Wneschnej Raswedkij“.

<sup>353</sup> „Federalnaja Slushba Besopasnosti“.

<sup>354</sup> „Federalnoje Agenstwo Prawitelstvennoj Swjasi i Informazij“.

<sup>355</sup> „Komitet Gosudarstvennoj Besopasnosti“.

die weltweit gespannten Computer- und Datennetze lassen sich sowohl offene als auch - durch illegales gezieltes Eindringen in gesicherte Datenbanken - besonders geschützte Informationen erlangen. Um zu verhindern, dass für die Existenz und den wirtschaftlichen Erfolg von Unternehmen bedeutsames Know-how in falsche Hände gerät, sollte beispielsweise der Internetauftritt regelmäßig unter Sicherheitsaspekten „gecheckt“ werden.

Auch die diplomatischen oder konsularischen Vertretungen (Legalresidenturen) nehmen bei der Informationsgewinnung nach wie vor eine besondere Rolle ein. Ihre Mitarbeiter 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.

#### Beispiel

- Angehörige von Legalresidenturen der Russischen Föderation im Bundesgebiet erhalten über die Aufnahme in Adress- und Verteilerverzeichnisse verschiedener Forschungseinrichtungen periodisch erscheinende Publikationen mit wissenschaftlichen Forschungsergebnissen, mit denen sie russische Forscher und Wissenschaftler unterstützen.

Nachrichtendienstlich interessante Personen müssen auch heute noch davon ausgehen, während ihres Aufenthalts in Russland vom FSB permanent überwacht zu werden.

#### Beispiel

- Mehrere Mitarbeiter eines baden-württembergischen Unternehmens entdeckten während einer Geschäftsreise in ihrem Hotelzimmer eine optische (Kamera/Video) und akustische (Mikrofon) Raumüberwachungsanlage.

#### andere GU-Staaten

Von den anderen GU-Staaten sind in Baden-Württemberg vor allem die Nachrichtendienste Kasachstans, Georgiens und der Ukraine aktiv. Der ukrainische Auslandsnachrichtendienst wurde aus dem Inlandsnachrichtendienst SBU<sup>356</sup> herausgelöst. Die neu geschaffene Behörde SWRU<sup>357</sup> hat die Aufgabe, Aufklärung unter anderem in den Bereichen Politik, Militär, Wirtschaft, Wissenschaft und Technologie zu betreiben.

<sup>356</sup> „Slushba Bezapasnost Ukrainy“, Sicherheitsdienst der Ukraine.

<sup>357</sup> „Slushba Wneschnej Raswedki Ukrainy“, Auslandsnachrichtendienst der Ukraine.

### 3. Prävention

Dem Landesamt für Verfassungsschutz obliegt die gesetzlich definierte Aufgabe, beim Schutz gegen Ausforschung von Staatsgeheimnissen und zur Sicherheit strategischer Einrichtungen, dem so genannten Geheim- und Sabotageschutz, mitzuwirken. Dies bedeutet personelle Maßnahmen wie Sicherheitsüberprüfungen und materielle Vorkehrungen sowohl auf amtlicher als auch auf wirtschaftlicher Seite und umfasst zudem die laufende Beratung und Betreuung. Ein effektiver Geheimschutz erfordert umfassendes Hintergrundwissen zu Schwerpunkten und Vorgehensweisen fremder Nachrichtendienste und ist ein wesentlicher Bestandteil der präventiven Spionageabwehr. Am Beispiel der gewerblichen Wirtschaft stellt sich der Geheim- und Sabotageschutz als ein komplexer Aufgabenbereich für das LfV dar.

#### 3.1 Geheimschutz in der Wirtschaft

Ziel des Geheimschutzes in der Wirtschaft ist der Schutz von im öffentlichen Interesse geheim zu haltenden Tatsachen, Gegenständen oder Erkenntnissen - der so genannten Verschlusssachen -, die einem Unternehmen zur Durchführung eines staatlichen Auftrags (zum Beispiel im Verteidigungsbereich) überlassen werden.

Die Aufnahme eines Unternehmens in die amtliche Geheimschutzbetreuung wird in der Regel damit eingeleitet, dass der öffentliche Auftraggeber bei der zuständigen Stelle einen Antrag stellt. Bei Aufträgen von Bundesbehörden, zum Beispiel des Bundesamts für Wehrtechnik und Beschaffung, ist grundsätzlich das Bundesministerium für Wirtschaft und Arbeit (BMWA) zuständig. Fungiert dagegen eine Landesbehörde als öffentlicher Auftraggeber, so tritt die jeweils zuständige oberste Landesbehörde an die Stelle des BMWA. Als Antragsberechtigte kommen auch Unternehmen in Betracht, die sich ihrerseits bereits selbst in der amtlichen Geheimschutzbetreuung befinden und beabsichtigen, einer anderen Firma einen geheimschutzbedürftigen Unterauftrag zu erteilen. Grundlegende Voraussetzung für das Verfahren ist die rechtsverbindliche Anerkennung der Bestimmungen des „Handbuchs für den Geheimschutz in der Wirtschaft“ (GHB)<sup>358</sup> durch Abschluss eines öffentlich-rechtlichen Vertrags zwischen zuständiger Behörde und Unternehmen.

<sup>358</sup> Weitere Informationen sowie der Text des am 15. November 2004 in überarbeiteter Version herausgegebenen GHB können unter [www.bmwa-sicherheitsforum.de](http://www.bmwa-sicherheitsforum.de) abgerufen werden.

*personelle  
und materielle  
Maßnahmen*

*Ziel*

*Verfahren*

„Wir waren schon sehr überrascht, wie sorglos selbst kommerzielle Nutzer des Internets mit sensiblen Daten umgehen.“

(Ulrich Greveler, Lehrstuhl für Netz- und Datensicherheit der Ruhr-Universität Bochum, Pressemitteilung der Ruhr-Universität Bochum vom 29. November 2004, „RUB-Forscher decken Sicherheitslücken auf: Sensible Daten in Internetverbindungen via Satellit“)

Weitere Schritte sind die Einsetzung eines zentralen Sicherheitsorgans im Unternehmen, des so genannten Sicherheitsbevollmächtigten, und die Sicherheitsüberprüfung des betroffenen Personals, die unter Mitwirkung der jeweils zuständigen Verfassungsschutzbehörde durchgeführt wird. Im Bedarfsfall sind zusätzlich materielle Sicherheitsvorkehrungen zu treffen, bei deren Festlegung neben dem

Bundesamt für die Sicherheit in der Informationstechnik (BSI) auch das Landesamt für Verfassungsschutz beteiligt ist.

In Baden-Württemberg sind derzeit weit über 200 Firmen in das Geheimschutzverfahren (Bund oder Land) einbezogen. Sie werden vom LfV betreut und regelmäßig über sicherheitsgefährdende Bestrebungen beziehungsweise geheimdienstliche Aktivitäten fremder Nachrichtendienste aufgeklärt und beraten.

### 3.2 Beratungspraxis des Landesamts für Verfassungsschutz

Sicherheit in der amtlich betreuten Wirtschaft und insbesondere auch in Unternehmen, die nicht in die Geheimschutzbetreuung aufgenommen sind, ist ein wichtiger Standortfaktor. Das Spektrum der Bedrohung reicht von Spionage und Terrorismus bis hin zu Korruption und Organisierter Kriminalität.

Bezogen auf Fälle des Know-how-Diebstahls geht von illoyalen Mitarbeitern das größte Risiko aus. Weitere Schwachpunkte der Informationssicherheit stellen beispielsweise Geschäftsbeziehungen mit Fremdfirmen und der Missbrauch moderner Kommunikationsnetze dar.

Deshalb ist eine angepasste Präventionsstrategie notwendig. Das Landesamt für Verfassungsschutz hat es sich zum Ziel gesetzt, den Informationsschutz in der gewerblichen Wirtschaft durch Aufklärung und Beratung weiter zu stärken, um damit Ausspähungsversuchen fremder Nachrichtendienste und der Bedrohung durch terroristische und extremistische Bestrebungen vorzubeugen. Die empfohlenen personellen, technischen und organisatorischen Schutzvorkehrungen wirken sowohl gegen Spionageangriffe fremder Nachrichtendienste als auch gegen Ausspähungsbemühungen konkurrierender Unternehmen.

- Eine mittelständische Firma aus Baden-Württemberg befürchtete illegalen Know-how-Abfluss und wandte sich daher an die Spionageabwehr des LfV. Auslöser war die Manipulation an einem Rechner im Forschungs- und Entwicklungsbereich während der Abwesenheit des zuständigen Mitarbeiters. Sehr schnell wurden gravierende Sicherheitsmängel offenbar: Von der Zutrittskontrolle über das Schlüsselmanagement bis hin zur Absicherung der EDV-Anlage und der Zugriffsberechtigung auf sensible Daten lagen die Schutzmechanismen im Argen. Durch Aufzeigen eines Bedrohungsszenarios konnte die Geschäftsleitung davon überzeugt werden, Sicherheit zum festen Bestandteil des Qualitätsmanagements zu machen. Als ersten Schritt bestimmte das Unternehmen einen Sicherheitsverantwortlichen, der anhand der Empfehlungen des LfV ein Sicherheitskonzept entwickelte, das auf die speziellen Bedürfnisse des Unternehmens zugeschnitten ist. Dabei wurde dem überragenden Grundsatz aus dem amtlichen Geheimschutz „Kenntnis nur, wenn nötig“ in besonderer Weise Rechnung getragen.

Die öffentlichkeitswirksamen Maßnahmen des Landesamts für Verfassungsschutz einerseits und verschiedene sicherheitsrelevante Vorfälle andererseits haben eine zunehmende Sensibilität bei den Unternehmen bewirkt. Dies lässt sich auch aus der deutlichen Zunahme von Beratungersuchen aus der Wirtschaft ablesen. Dabei kam immer wieder ein großes Interesse an der Sensibilisierung von Mitarbeitern zum Ausdruck, die in Länder mit besonderen Sicherheitsrisiken entsandt werden. Diesem Anliegen konnte durch entsprechende Reise- und Verhaltensempfehlungen weitgehend entsprochen werden. Für Trainings- und Schulungsprogramme sind die Wirtschaftsunternehmen allerdings selbst verantwortlich. Unternehmen, die sich unter Missachtung der notwendigen Sicherheitsvorkehrungen im Ausland betätigen, riskieren erhebliche Nachteile.

### 3.3 Presse- und Öffentlichkeitsarbeit der Spionageabwehr

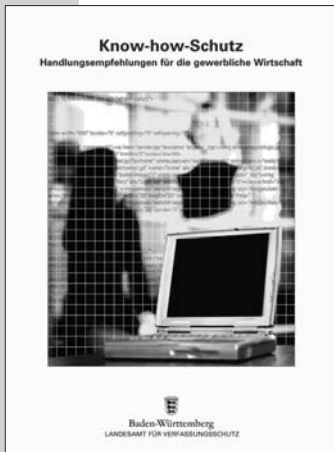
Das Landesverfassungsschutzgesetz sieht in § 12 ausdrücklich vor, dass das Innenministerium und das Landesamt für Verfassungsschutz die Öffentlichkeit periodisch oder aus gegebenem Anlass unter anderem über sicherheitsgefährdende oder geheimdienstliche Tätigkeiten unterrichten. Mitarbeiter der Spionageabwehr erstellen regelmäßig Informationsmaterial, hal-

*Beispiel*

*Zunahme von  
Beratungs-  
ersuchen*

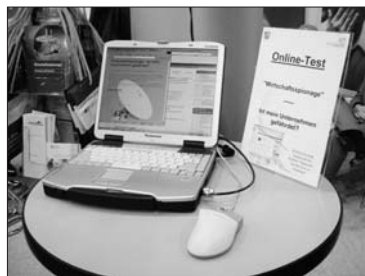
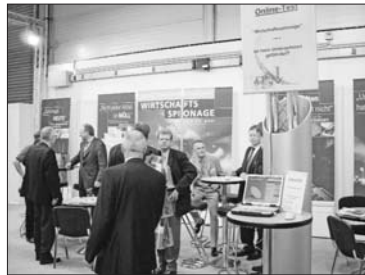
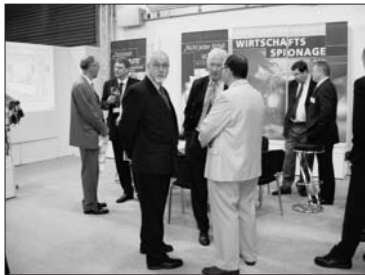
## Aktivitäten 2004

ten Fachvorträge, führen Beratungsgespräche und unterstützen Firmen bei der Erarbeitung von Schutzkonzeptionen.



Im November 2004 wurde die Broschüre „Know-how-Schutz - Handlungsempfehlungen für die gewerbliche Wirtschaft“ veröffentlicht. Sie bietet eine praxisorientierte Grundlage für firmenspezifische Know-how-Schutzkonzepte und kann auch auf der Homepage des Landesamts für Verfassungsschutz<sup>359</sup> abgerufen werden.

Mit dem Thema Wirtschaftsspionage beteiligte sich die Spionageabwehr des LfV an einem gemeinsamen Messestand der Verfassungsschutzbehörden des Bundes und der Länder wiederum erfolgreich an der Essener Sicherheitsmesse SECURITY 2004.



Essener Sicherheitsmesse SECURITY 2004

Im Jahr 2004 wurden von Angehörigen der Spionageabwehr rund 20 Vorträge gehalten, über 90 Behörden- und Firmenberatungen durchgeführt und 15 Medienkontakte wahrgenommen.

### 3.4 Sicherheitsforum Baden-Württemberg - Die Wirtschaft schützt ihr Wissen

Das Sicherheitsforum Baden-Württemberg wurde 1999 initiiert. Vertreter aus Wirtschaft, Wissenschaft, Verbänden, Kammern und Behörden haben es sich unter anderem zur Aufgabe gemacht, die Sicherheitspartnerschaft im Bereich von Wirtschaft und Politik unter besonderer Berücksichtigung der Belange kleiner und mittelständischer Unternehmen in Baden-Württemberg weiter zu entwickeln. Die Aktivitäten des Gremiums sind darauf ausgerichtet, in Grundsatzfragen der Informationssicherheit eine Scharnierfunktion zwischen Wirtschaft und Wissenschaft einerseits sowie der Politik andererseits zu erfüllen.

Die Quantifizierung von Wissensverlusten der Wirtschaft durch Spionage war bislang weitgehend auf Schätzwerte gestützt. Daher gab das Gremium bei der Universität Lüneburg eine wissenschaftliche Studie mit dem Ziel in Auftrag, die Höhe des Schadens zu ermitteln, welcher der baden-württembergischen Wirtschaft durch ungewollten Know-how-Verlust entsteht. Das Ergebnis der auf empirischer Basis durchgeführten Untersuchung wurde am 13. Oktober 2004 vorgestellt.



v. links: Wirtschaftsminister Ernst Pfister MdL, Innenminister Heribert Rech MdL, Prof. Dr. Egbert Kahle (Universität Lüneburg), Dr. Hans-Jürgen Reichardt (IHK Region Stuttgart).

wissenschaftliche  
Studie zum  
Schaden durch  
Know-how-  
Verlust

Vorstellung der  
Fall- und  
Schadensanalyse

<sup>359</sup> URL: <http://www.verfassungsschutz-bw.de>.

„Ich würde schätzen, dass etwa 15 Prozent der Unternehmen, die solche Netze [drahtlose Computernetze] betreiben, ungeschützt sind.“

(Clements Cap, Professor für Informations- und Kommunikationsdienste an der Universität Rostock, SPIEGEL ONLINE vom 25. September 2004, „Jedes vierte WLAN ist völlig ohne Schutz“)

Der Studie zufolge sind landesweit jährlich materielle und geistige Werte in Höhe von etwa sieben Milliarden Euro von Informationsverlusten bedroht. Mehr als zwei Drittel der beteiligten Unternehmen waren nach eigener Kenntnis bereits Opfer eines „unfreundlichen Informationsabflusses“. Es entstand ein Schaden von

rund 52 Millionen Euro. Die auf dieser Basis hochgerechneten Schäden für Baden-Württemberg betragen circa eine Milliarde Euro. In Relation dazu wurde der Mitteleinsatz der Unternehmen zum Zwecke der Prävention als zu gering angesehen.

Einer der herausragenden Gesichtspunkte der vom Sicherheitsforum speziell für die mittelständischen Unternehmen erarbeiteten Empfehlungen ist die Schaffung einer betrieblichen Sicherheitsinfrastruktur, die zumindest einen haupt- oder nebenamtlichen Sicherheitsverantwortlichen vorsehen sollte. Er muss beispielsweise in der Lage sein, das komplexe Thema des Informationsschutzes unter besonderer Berücksichtigung der IT-Sicherheit verantwortlich zu bearbeiten und sowohl intern als auch extern als kompetenter Ansprechpartner zur Verfügung zu stehen. Das allgemeine Sicherheitsbewusstsein der Firmenangehörigen und Geschäftspartner bedarf im Rahmen eines umfassenden Sicherheitskonzepts überdies einer permanenten Pflege.

Das LfV sieht sich durch die Ergebnisse der Studie in seiner bisherigen Einschätzung zum Stand des Informationsschutzes im Land bestätigt. Es unterstützt die Forderung, präventive Maßnahmen im Rahmen eines ganzheitlichen Sicherheitskonzepts unter Berücksichtigung personeller, materieller, organisatorischer und rechtlicher Aspekte zu realisieren.

Die Studie mit den speziellen Präventionsempfehlungen des Sicherheitsforums kann neben zahlreichen weiteren Beiträgen zum Thema Unternehmenssicherheit auf der Website des Sicherheitsforums<sup>360</sup> eingesehen werden.

#### 4. Erreichbarkeit der Spionageabwehr

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

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. Alle Mitbürger, die aus ihrem beruflichen und privaten Umfeld Hinweise auf Spionagesachverhalte geben, leisten einen wesentlichen Beitrag für den Erhalt der inneren und äußeren Sicherheit.



<sup>360</sup> URL: <http://www.sicherheitsforum-bw.de>.