

## E. SPIONAGEABWEHR, GEHEIM- UND SABOTAGESCHUTZ

### 1. Aktuelle Entwicklungen und Tendenzen

Die Verhinderung der Weiterverbreitung von Massenvernichtungswaffen und Trägersystemen ist ein Schwerpunkt der westlichen Außen- und Sicherheitspolitik. Belege für die globale Bedeutung dieser Thematik sind der unter anderem mit der Existenz von Massenvernichtungswaffen begründete Irak-Krieg, die Befürchtungen in Bezug auf ein Atomwaffenprogramm des Iran und die Entwicklung von Kernwaffen durch Nordkorea. Darüber hinaus muss damit gerechnet werden, dass sich Terroristen in den Besitz solcher Waffen bringen wollen. Weltweit wurden politische, wirtschaftliche und

*Proliferation*

„Gesetzlose Regime, die atomare, chemische und biologische Waffen besitzen oder nach ihrem Besitz streben, sind heute die größte Gefahr für Amerika und die Welt“

(George W. Bush, Präsident der Vereinigten Staaten von Amerika, DER SPIEGEL Nr. 10/2003 vom 1. März 2003)

und militärische Schritte zur Unterbindung der Proliferation<sup>393</sup> unternommen. Ganz aktuell beteiligt sich Deutschland im Rahmen der Proliferation Security Initiative (PSI) an der Bekämpfung des Handels mit konventionellen Raketen und Massenvernichtungswaffen.

Das Landesamt für Verfassungsschutz Baden-Württemberg hat sich auf dem Feld der Spionageabwehr auch im Jahr 2003 überwiegend mit proliferationsrelevanten Sachverhalten beschäftigt. Länderspezifische Beschaffungsmethoden konnten dabei nicht festgestellt werden. Die industrielle

und wirtschaftliche Infrastruktur einer Reihe so genannter Krisenländer<sup>394</sup> ist mittlerweile so leistungsfähig, dass sie in der Lage sind, sich gegenseitig mit Know-how zu unterstützen und Beschaffungsaktivitäten immer mehr auf ganz spezielle, nur in Hochtechnologieländern erhältliche Komponenten zu konzentrieren. Nordkorea ist - ebenso wie der Iran und einige andere Länder - ein ausgewiesener Waffenexporteur und erschließt sich mit diesem florierenden Geschäft erhebliche Geldquellen. Die momentan noch weit gehend

<sup>393</sup> Weiterverbreitung von Massenvernichtungswaffen beziehungsweise der zu ihrer Herstellung verwendbaren Produkte einschließlich des dafür erforderlichen Know-hows sowie von entsprechenden Waffenträgersystemen.

<sup>394</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: Indien, Iran, Syrien, Nordkorea, Pakistan, Libyen).

offenen Fragen, ob etwa die alten Beschaffungsnetze des Irak durch andere Staaten oder Organisationen genutzt werden und welche Konsequenzen sich durch die veränderten politischen Bedingungen für den Themenkomplex Proliferation insgesamt ergeben, werden in Zukunft die Spionageabwehr intensiv beschäftigen.

Die klassische Spionage hat durchaus weiterhin ihre Bedeutung, auch wenn Verratsfälle nur sporadisch an die Öffentlichkeit gelangen und Verurteilungen überführter Agenten relativ selten geworden sind.

„klassische“  
Spionage

Gerade in Zeiten weltumspannender Krisen und immer wieder neu aufflammender brisanter lokaler Konflikte sind fremde Staaten daran interessiert, möglichst frühzeitig über vielfach geheim gehaltene politische, militärische und wirtschaftliche Entwicklungen informiert zu sein. In Baden-Württemberg spielt die Wirtschafts- und Wissenschaftsspionage als Ausfluss der herausragenden technologischen Leistungsfähigkeit der hier ansässigen Unternehmen

„Spionage findet immer statt. Daran hat sich auch durch die politische Entspannung nichts geändert.“

(Fritz Stepper, Sprecher des Bundesamts für Verfassungsschutz, Computerwoche vom 26. September 2003)

und Forschungseinrichtungen traditionell eine wichtige Rolle. Dabei konnten immer wieder Überschneidungen zwischen nachrichtendienstlicher Spionage, Konkurrenzausspähung und legitimer Marktbeobachtung festgestellt werden.

Aktivitäten gingen vor allem von den oben erwähnten Krisenländern, der Volksrepublik China und der Russischen Föderation aus:

Besondere Aufmerksamkeit verdient die mit Effektivitätsgesichtspunkten begründete Umorganisation der russischen Geheimdienste. Mit der Auflösung der „Föderalen Agentur für Regierungsfremmeldewesen und Information“ (FAPSI)<sup>395</sup> und der damit verbundenen Stärkung des Inlandsnachrichtendienstes FSB<sup>396</sup> sind - damals bewusst vorgenommene - Dezentralisierungsmaßnahmen der nachkommunistischen Ära wieder rückgängig gemacht worden. Damit ist ein Apparat entstanden, der hinsichtlich seiner Aufgabenfülle und Personalstärke durchaus mit dem ehemaligen Inlands-KGB<sup>397</sup> verglichen werden kann. Über die Auswirkungen dieser organisatori-

Umorganisation russischer Geheimdienste

<sup>395</sup> „Federalnoje Agenstwo Prawitelstvennoj Swjazi i Informazij“.

<sup>396</sup> „Federalnaja Slushba Besopasnosti“, Föderaler Sicherheitsdienst.

<sup>397</sup> „Komitet Gosudarstvennoj Besopasnosti“, Komitee für Staatssicherheit.

schen Maßnahmen auf Spionageaktivitäten kann zum gegenwärtigen Zeitpunkt nur spekuliert werden.

China setzt bei seinem wirtschaftlichen Höhenflug auch weiterhin auf die Unterstützung seiner Nachrichtendienste, die außerordentlich geschickt alle sich bietenden Möglichkeiten nutzen. Sie sind vor allem deshalb erfolgreich, weil die Sicherung des eigenen Know-hows bei vielen der in China engagierten deutschen Firmen keine entscheidende Rolle spielt. Das ab 1. August 2003 für den Import bestimmter Waren nach China verbindlich eingeführte Zertifizierungssystem („China Compulsory Certification“/CCC)<sup>398</sup> birgt zusätzliche Sicherheitsrisiken.

Die Krisenländer bedienen sich neben den Mitteln der klassischen Spionage auch nachrichtendienstlich gesteuerter staatlicher Firmen und konspirativ arbeitender Organisationen, um die strengen Gesetze und Exportkontrollen in Deutschland leichter umgehen zu können.

Über Spionageaktivitäten politisch befreundeter Staaten liegen derzeit keine konkreten Erkenntnisse vor.

Bei den Ausspähungsmethoden ist die Technik weiter im Vormarsch. Die meisten der vielfach im Internet oder in speziellen „Spionläden“ erhältlichen Gerätschaften wie Minikameras, Keylogger<sup>399</sup>, Wanzen oder Richtmikrofone sind nicht nur außerordentlich leistungsfähig, sondern auch sehr einfach zu installieren und zu nutzen. Foto-Handys entwickeln sich immer mehr zu einem Sicherheitsproblem für Firmen und Behörden. Die neue Dimension dieser Gefährdung liegt in der Möglichkeit, in sensiblen Bereichen unbemerkt zu fotografieren und Bilder in Sekundenschnelle über das Telefonnetz als Multimediale Nachricht (MMS) zu verschicken.

Im vergangenen Jahr ist die Spionageabwehr noch einmal mit den Hinterlassenschaften der ehemaligen DDR konfrontiert worden. Die Freigabe der so genannten „Rosenholz“-Dateien<sup>400</sup> hat dreizehn Jahre nach der deutschen Einheit erneut den Blick darauf gelenkt, wie ver-

lockend für manchen Bundesbürger die Zusammenarbeit mit dem Regime in Ostberlin gewesen ist. Zudem hat sie eine öffentliche Diskussion darüber ausgelöst, inwieweit Personen in politisch verantwortlichen oder sicherheitsempfindlichen Positionen einer Überprüfung unterzogen werden sollen.

Spionage findet noch immer tagtäglich statt. Dieser Lageeinschätzung muss neben der Bearbeitung konkreter Fälle vor allem durch konsequente präventive Maßnahmen Rechnung getragen werden. Nach einer umfassenden Neuausrichtung der vorbeugenden Spionageabwehr in den vergangenen Jahren hat das Landesamt für Verfassungsschutz im Jahr 2003 besonderes Augenmerk auf die zielgerichtete Aufarbeitung bestimmter Problemfelder in Zusammenarbeit mit potenziell Betroffenen gelegt. So wurden beispielsweise in einer aufwändigen Aktion gezielt Firmen mit Geschäftsverbindungen nach China auf ihre Erfahrungen vor Ort angesprochen und gleichzeitig auf die dort drohenden Gefahren aufmerksam gemacht. Für den Bereich der Technik gilt es darauf hinzuweisen, dass viele angebotene IT-Sicherheitsprodukte selbst nicht genügend Sicherheit bieten oder geeignete Systeme oft unprofessionell eingesetzt werden.

Die konkreten Erfolge der Spionageabwehr im Jahr 2003 können aus Geheimhaltungsgründen nur in Einzelfällen publik gemacht werden. Es lässt sich hier aber feststellen, dass die Zahl der Erkenntnisfälle<sup>401</sup> und der qualifizierten Verdachtshinweise wieder zugenommen hat. Firmen zeigen ein gesteigertes Interesse an Sensibilisierungsgesprächen und fallbezogenen Beratungen.

## 2. Daten, Fakten, Hintergründe

### 2.1 Krisenländer

#### 2.1.1 Allgemeines

So genannte Krisenländer wie Iran, Syrien, Libyen und Nordkorea sind bestrebt, in den Besitz von atomaren, biologischen und chemischen Vernichtungswaffen (ABC-Waffen) zu gelangen, um vor allem

<sup>398</sup> Vgl. S. 281f.

<sup>399</sup> Keylogger gibt es sowohl als Hardware- (Geräte) als auch als Software-Version (beispielsweise integriert in Computerviren). Sie protokollieren - unbemerkt vom Anwender - alle Tastatureingaben.

<sup>400</sup> CD-ROM-Kopien der in den USA befindlichen mikroverfilmten Karteien der Hauptverwaltung Aufklärung des ehemaligen Ministeriums für Staatssicherheit (MfS) der früheren DDR.

<sup>401</sup> Ein durch Ermittlungen der Sicherheitsbehörden oder durch die Offenbarung einer Person bestätigter Sachverhalt, in dem die nachrichtendienstliche Beziehung der Person zu Mitarbeitern oder Institutionen eines fremden Nachrichtendienstes nachgewiesen ist.

### Problem: „Dual-Use- Güter“

ihre politischen Ziele besser durchsetzen zu können. Deshalb wird mit allen Mitteln versucht, sich das notwendige Wissen, die Ausgangsprodukte und Waren illegal zu beschaffen. Ein besonderes Problem stellen dabei Dual-Use-Güter<sup>402</sup> dar. So werden oft nicht genehmigungspflichtige Einzelteile von zivilen Anlagen, Geräten oder Technologien exportiert, die auch zur Herstellung von Waffen geeignet sind. Zahlreiche Ermittlungsverfahren belegen, dass der Irak bis kurz vor Kriegsbeginn im Frühjahr 2003 gegen das 1991 verhängte UN-Embargo wiederholt verstoßen hat.

### Proliferation - Vorgehens- weise

Proliferationsbemühungen werden weiterhin nach klassischem Muster betrieben. Neben der Abwicklung von Aufträgen über Drittländer und deren Finanzierung über Koordinierungsstellen verschleiern die Auftraggeber den tatsächlichen Endverbraucher und verbergen illegale Warenlieferungen unter unverdächtigen Massenerzeugnissen, so dass der Proliferationscharakter für deutsche Händler nicht erkennbar ist. Dass auch im Ausland agierende Zwischenhändler vor der Strafverfolgung durch die deutsche Justiz nicht sicher sein können, macht folgender Fall deutlich:

- Ein in Jordanien ansässiger Geschäftsmann irakischer Herkunft und der Inhaber einer **Mannheimer** Firma sollen gemeinschaftlich mit einem Diplom-Ingenieur aus **Pforzheim** in den Jahren 1999 und 2000 in mehreren Fällen unter anderem an der Lieferung von Tiefbohrwerkzeugen in den Irak mitgewirkt haben. Die Werkzeuge waren für die Herstellung von ABC-Waffen-fähigen Geschützrohren geeignet. Dabei soll das **Mannheimer** Unternehmen zur Vortäuschung eines Inlandsgeschäfts als angeblicher Abnehmer der Ware genutzt worden sein. In diesem Zusammenhang wurde der **Pforzheimer** Ingenieur bereits zu fünf Jahren und drei Monaten Freiheitsstrafe verurteilt.<sup>403</sup> Aufgrund eines Haftbefehls der deutschen Justiz verhafteten bulgarische Behörden den irakischen Geschäftsmann im November 2002 auf dem Flughafen Sofia und lieferten ihn drei Monate später zur Strafverfolgung an Deutschland aus. Das Landesamt für Verfassungsschutz war an der Aufdeckung dieser Kooperation beteiligt und hatte den Sachverhalt zur strafrechtlichen Verfolgung und Verhinderung

<sup>402</sup> Als „Güter mit doppeltem Verwendungszweck“ werden Güter einschließlich Datenverarbeitungsprogrammen und Technologien bezeichnet, die sowohl für zivile als auch militärische Zwecke verwendet werden können.

<sup>403</sup> Landgericht Mannheim, Az.: 626 Js 26390/02.

weiterer illegaler Ausfuhren dem Zollfahndungsdienst übergeben.

Der nachfolgend aufgeführte Fall belegt, dass auch von weiteren Krisenländern entsprechende Aktivitäten in Baden-Württemberg ausgehen:

- Das Landgericht Mannheim verurteilte im September 2003 einen kanadischen Staatsangehörigen russischer Herkunft wegen illegalen Waffenhandels im Auftrag einer jordanischen Beschaffungsorganisation und pakistanischer Stellen zu einer Freiheitsstrafe von zwei Jahren und zehn Monaten.<sup>404</sup> Der in Kanada, in der Schweiz und in Deutschland niedergelassene Geschäftsmann handelte mit Rüstungsgegenständen und koordinierte dabei seine weltweiten Aktivitäten per Telefon lange Zeit unauffällig von seiner Wohnung in Baden-Württemberg aus.

### 2.1.2 Iran

An den staatlich gesteuerten Maßnahmen des Iran zur Erlangung von Rüstungsgütern sowie von Dual-Use-Technologien und -Waren ist eine Vielzahl von Einrichtungen beteiligt. Als aktivste Beschaffungsorganisation ist die für alle Proliferationsbereiche zuständige „**Defence Industries Organization**“ (**DIO**) in Erscheinung getreten. Bei der Entwicklung des Nuklearprogramms nimmt die „**Atomic Energy Organization of Iran**“ (**AEOI**), die mehrere Kernforschungszentren betreibt, eine zentrale Rolle ein. Inspektoren der Internationalen Atomenergiebehörde (IAEO) stellten in einer Gasultrazentrifugen-Anlage in Natanz im Zentraliran sowie in einer weiteren Einrichtung nahe Teheran Spuren von hochangereichertem Uran fest. Belege für den Verdacht, der Iran arbeite an der Entwicklung von Atomwaffen, konnten allerdings nicht gefunden werden.

Auf dem Gebiet der Waffenträgertechnologie verfolgt der Iran ebenfalls ein eigenständiges Programm. So konnte im Juli 2003 die Entwicklung einer Trägerrakete (SHAHAB-3) mit einer Reichweite von 1.500 km abgeschlossen und das System den iranischen Streitkräften übergeben werden. An der Entwicklung von Raketen mit noch grö-

<sup>404</sup> Landgericht Mannheim, Az.: 626 Js 16404/03.

*iranische  
Beschaffungs-  
organisationen*

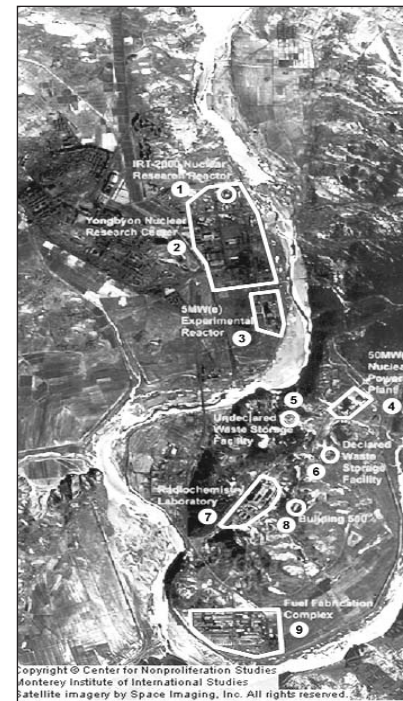
ßerem Aktionsradius wird gearbeitet. Dies verdeutlicht die Gefahr, die nicht nur den Regionen in unmittelbarer Nachbarschaft, sondern langfristig auch Deutschland und anderen NATO-Mitgliedsstaaten droht. Vor diesem Hintergrund bearbeitet das Landesamt für Verfassungsschutz mehrere Fälle, bei denen Anhaltspunkte darauf hindeuten, dass der Iran mit dem Mittel der Verschleierung proliferationsrelevante Technologien für militärische Zwecke beschafft. Zwei Beispiele sollen dies verdeutlichen:

- Ein iranischer Geschäftsmann bereist regelmäßig das Bundesgebiet und unterhält Geschäftsbeziehungen zu mehreren Maschinenbau-Unternehmen in Baden-Württemberg, die sich unter anderem mit der Produktion von Prüfgeräten beschäftigen. Ferner bestehen Kontakte zu einer bereits zuvor auffällig gewordenen, iranisch kontrollierten Firma in Norddeutschland und einem ausländischen Unternehmen, das seine Dienste für den Betrieb von Briefkastenfirmen anbietet. Diese und weitere Verdachtsmomente deuten auf ein Beschaffungsnetz zur Verschleierung des Endverbrauchers im Iran hin.
- Ein iranisches Unternehmen verfügt über enge Kontakte zu mehreren in Baden-Württemberg ansässigen Firmen sowie zu einer Privatperson. Die Vorgehensweise bei der Lieferung von Präzisionswerkzeugen an einen branchenfremden Betrieb und der persönliche Hintergrund der Gesellschafter des iranischen Unternehmens in Verbindung mit ihren jüngsten geschäftlichen Aktivitäten in unserem Bundesland lassen auf eine Verschleierung proliferationsrelevanter Geschäfte schließen. Dieser Verdacht gründet sich nicht zuletzt darauf, dass bereits früher ein Mitarbeiter dieser Firma in Proliferationsverdacht geraten war.

**2.1.3 Koreanische Demokratische Volksrepublik (Nordkorea)**

Für sein ehrgeiziges atomares und konventionelles Rüstungsprogramm ist Nordkorea bestrebt, westliche Technologien und Ausrüstungsgegenstände zu beschaffen. Es waren Bemühungen feststellbar, Güter, die Ausfuhrbeschränkungen unterliegen, durch manipulierte Endverbrauchererklärungen beziehungsweise durch die Ausfuhr über

ein Drittland nach Nordkorea zu verbringen. Nordkorea ist zum eigenständigen Bau von Nuklearwaffen fähig und hat die Entwicklung einer Atombombe eingeräumt. Offiziell begründet wird dies mit der Notwendigkeit finanzieller Einsparungen bei der konventionellen Rüstung sowie der Bedrohung durch die USA und Südkorea.



Nordkoreanisches Atomforschungszentrum

1. IRT 2000 Atomforschungsreaktor
2. Yongbyon Atomforschungszentrum
3. 5 Megawatt Experimentalreaktor
4. 50 Megawatt Atomkraftwerk
5. Atommülllager (vermutet)
6. Atommülllager (geklärt)
7. Radiochemisches Labor (Forschung und Entwicklung, Herstellung von Treibstoff und Wiederaufarbeitung)
8. Gebäude 500 (Lagerstätte für flüssigen und festen Atommüll)
9. Treibstoffproduktion

Copyright © Center for Nonproliferation Studies  
 Monterey Institute of International Studies  
 Satellite Imagery by Space Imaging, Inc.  
 All rights reserved  
 Homepage: <http://cns.mii.edu>



Chemische Institute in Nordkorea

1. Chemisches Institut, Filiale Kanggye
2. Chemisches Institut, Filiale Shin'uiju
3. Chemisches Institut, Filiale Hamhung
4. Hamhung Universität der Chemie
5. Forschungsinstitut Nr. 398 (Forschung und Entwicklung von Gegengiften und Dekontaminierungsmethoden)
6. Chemische Forschung an der 2. naturwissenschaftlichen Akademie
7. Zentrales analytisches Labor
8. Büro für atomare und chemische Verteidigung
9. Abteilung 32 (Forschung und Entwicklung chemischer Waffen)

*Beispiel*

- Im Oktober 2003 begann vor dem Landgericht Stuttgart der Prozess gegen den Geschäftsführer einer Firma in **Königsbronn/Krs. Heidenheim**. Er steht im Verdacht, unter Beteiligung einer Hamburger Firma bei der Lieferung von Aluminiumröhren über die Volksrepublik China nach Nordkorea mitgewirkt zu haben. Zuvor sensibilisierte das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) die Firma und verweigerte die notwendige Ausfuhrgenehmigung. Die Teile wären zum Einbau in Gasultrazentrifugen geeignet gewesen, die zur Produktion von waffenfähigem Uran benötigt werden.

## 2.2 Volksrepublik China

Schon seit nahezu zwei Jahrzehnten versucht die Volksrepublik (VR) China zu den hoch entwickelten Staaten im Westen aufzuschließen und in Verfolgung dieses Ziels ihre eigenen außenpolitischen und wirtschaftlichen Einwirkungsmöglichkeiten stetig zu verbessern. Der Zuwachs des Bruttoinlandsprodukts Chinas lag im Jahr 2003 bei über 9 Prozent. Das innerhalb der letzten sieben Jahre um insgesamt 46 Prozent angestiegene Engagement deutscher Firmen in der Volksrepublik verdeutlicht die Perspektiven der deutsch-chinesischen Wirtschaftsbeziehungen. Aktuell sind in der VR China mehr als 1.500 deutsche Unternehmen mit Repräsentanzen oder Kapitalbeteiligungen vertreten, davon rund 350 aus Baden-Württemberg. Daraus resultieren vielfältige Kooperationen im Hochschul- und Forschungsbereich sowie zahlreiche Studien- und Schulaufenthalte chinesischer Staatsbürger im Bundesgebiet. China stellt mittlerweile mit über 19.000 (Stand: Wintersemester 2002/03) die größte Gruppe ausländischer Studenten.

Parallel dazu ist ein gezieltes Aufklärungsverhalten chinesischer Nachrichtendienste bis hin zum Einsatz menschlicher Quellen zu beobachten. Hauptträger der nachrichtendienstlichen Aktivitäten im Ausland sind das „**Ministerium für Staatssicherheit**“ (MSS) und der „**Militärische Informationsdienst**“ (MID). Beide sind mit der Beschaffung von Informationen aus den klassischen Aufklärungsfeldern Politik, Militär, Wirtschaft, Wissenschaft und Forschung betraut. Charakteristisch ist der lange Zeitraum, über den Kontakte aufgebaut und gepflegt werden, bis der nachrichtendienstliche Hintergrund offenkundig wird.

*verstärkte  
Aktivitäten  
chinesischer  
Nachrichtendienste*

Die chinesische Botschaft unterhält über zahlreiche Vereine in allen Universitätsstädten Baden-Württembergs enge Verbindungen zu Studenten und Wissenschaftlern. Die Mitglieder dieser Vereine werden bei „Kulturveranstaltungen“ der Botschaft in regelmäßigen Abständen ideologisch „auf Linie“ gebracht. Der wissenschaftliche Nachwuchs im Ausland ist zudem angehalten, in gewissen Zeitabständen Berichte über seine Studien- und Forschungstätigkeiten abzugeben.

Zusätzlich wird angestrebt, das Wissen der Auslandsstudenten durch Rückholprogramme verstärkt zu nutzen. Bisher kehrte nur etwa ein Viertel nach Abschluss des Studiums in die VR China zurück. Finanzielle Unterstützungsmaßnahmen zu Firmengründungen in China sollen dem bisherigen Trend entgegenwirken. Die gezielte Nutzung des Know-hows und der Kontakte von im Ausland lebenden Chinesen ist besonders anschaulich an den Absichten der ostchinesischen Provinz Shandong zu erkennen. Sie will zur Anwerbung neuer Investitionen 100 Auslandschinesen als Vermittler einsetzen, die über entsprechenden wirtschaftlichen Einfluss verfügen und den Aufbau eines weltweiten Netzwerks vorantreiben sollen. Um für potenzielle Auslandsinvestitionen einen besseren Service anbieten zu können, wurde eine Datenbank errichtet, die 160 Schlüsselprojekte der Provinz enthält. Das Vorhaben, diese Datenbank um auslandschinesische Vereinigungen und Namen bedeutender Auslandschinesen zu erweitern, eröffnet auch den chinesischen Nachrichtendiensten hervorragende Perspektiven für die gezielte Anwerbung von Personen mit vielversprechenden Zugangsmöglichkeiten.

Ein weiterer Weg zur Informationsbeschaffung durch Angehörige von Geheimdiensten oder durch die chinesische Botschaft in Deutschland ist der Aufbau von Beziehungen zu Wirtschaftsvertretern und zu wissenschaftlichen Einrichtungen in Baden-Württemberg.

China hat seit dem 1. August 2003 ein neues Zertifizierungssystem („China Compulsory Certification“/CCC) für den Import bestimmter Waren in Kraft gesetzt. Dabei sind neben diversen Konsumgütern vor allem elektronische und elektrotechnische Geräte sowie deren Komponenten

„Wir müssen schneller etwas Neues bringen, als die Chinesen kopieren können“  
(Gerhard Sturm, geschäftsführender Gesellschafter der EBM Elektrobau Mulfingen GmbH & Co., Stuttgarter Zeitung Nr. 114 vom 19. Mai 2003)

*ideologische  
„Betreuung“  
der Auslandschinesen*

*Nutzung von  
Datenbanken*

**Zertifizierungs-  
system**

betroffen. Aufgrund der Vorschriften werden ausländische Anbieter gezwungen, vollständige technische Dokumentationen in chinesischer Sprache auszuhändigen und in ein Prüfverfahren des Produkts durch ein chinesisches Labor einzuwilligen. Überdies verpflichten sie sich, den chinesischen Inspektoren regelmäßig umfassende Einblicke in die Fertigungsstätten zu geben.

Die kommunistische Regierungspartei duldet weiterhin keine Bestrebungen, die ihre Machtposition gefährden könnten. Zu den Ausspähungszielen der Nachrichtendienste gehören daher auch in Deutschland lebende chinesische Oppositionelle, die in zahlreichen Vereinen organisiert sind. Besondere Aufmerksamkeit gilt der in China seit Juli 1999 verbotenen Falun-Gong-Bewegung, die auch hierzulande über Anhänger verfügt. Ihre Mitglieder werden inzwischen ohne Rücksicht auf ihre Nationalität von den chinesischen Diensten weltweit beobachtet und teilweise Repressalien ausgesetzt.

**2.3 Russische Föderation und andere Länder der GUS**

Die Geheimdienste der Russischen Föderation versuchen unverändert, mit hohem Engagement und großem Personalaufwand auf konspirativen Wegen interessante Informationen aus Politik, Wirtschaft, Wissenschaft und Militär zu beschaffen.

Unter anderem werden Mitarbeiter der Geheimdienste für ihren Einsatz mit einer Legende ausgestattet, die sie als Mitglieder des diplomatischen Corps oder als Journalisten ausweist. Sie sind in staatlichen Auslandsvertretungen oder Presseagenturen russischer Medien in Deutschland auf so genannten Tarndienstposten untergebracht und können so auf unverdächtige Weise mit Zielpersonen Kontakt aufnehmen.

Sehr offensiv wurden auch auf eigenem Territorium Aktivitäten mit der Zielrichtung entfaltet, Informationen aus Deutschland zu erlangen. Geschäftsreisende, Firmenrepräsentanten, Wissenschaftler, aber auch Touristen, die etwa aus Baden-Württemberg nach Russland reisen, müssen sich der Gefahr bewusst sein, auf unterschiedliche Art und Weise zur Mitarbeit und Verratstätigkeit verführt zu werden.

**Ausspähung  
Oppositio-  
neller****Arbeit unter  
Legende****Aktivitäten  
gegen Deut-  
sche in Russ-  
land**

Eine weitere Vorgehensweise russischer Nachrichtendienste besteht darin, ehemalige hauptamtliche Mitarbeiter als Privat- oder Geschäftsreisende getarnt ins Bundesgebiet einzuschleusen. Das nach Auflösung der Sowjetunion Ende 1991 geschaffene Visa-Kontrollverfahren hat jedoch dazu geführt, dass eine hohe Zahl solcher Einreiseversuche erkannt und zurückgewiesen werden konnte.

Die Regierung der Russischen Föderation hat die Struktur ihres Sicherheitsapparats im Jahr 2003 durch einschneidende Maßnahmen, die der russische Präsident per Dekret vom 11. März 2003 bekannt gab, radikal verändert. Kernaufgaben und ein Großteil der Organisationseinheiten von FAPSI sowie die vollständige Kontrolle über den Grenzschutz wurden dem Inlandsnachrichtendienst FSB zugeschlagen. Er erhielt erweiterte Kompetenzen, mehr Personal, ein höheres Budget und nimmt inzwischen eine Aufgabenfülle wahr, die der des einstigen Inlands-KGB nahezu gleichkommt. Der verbliebene Teil von FAPSI soll dem militärischen Nachrichtendienst GRU<sup>405</sup> angegliedert werden. Russische Medien berichteten, dass die Umorganisation seit August 2003 abgeschlossen sei.

Konkrete Auswirkungen dieser Umstrukturierung auf die Arbeit der russischen Dienste konnten bisher noch nicht festgestellt werden. Das Landesamt für Verfassungsschutz geht jedoch davon aus, dass mit der Zusammenfassung mehrerer Behörden zu einem mächtigen Dienst die Freisetzung von Synergieeffekten und eine wesentlich effizientere Arbeit im In- und Ausland angestrebt werden. Geht es hier nur um eine Anpassung der diversen russischen Sicherheitsdienste an die neuen Bedrohungen in der Welt, so wie auch die USA ein zentrales neues Heimatschutzministerium mit umfassenden Zuständigkeiten eingerichtet haben? Oder soll hier ein machtvoller Nachrichtendienst wie der im Oktober 1991 aufgelöste sowjetische KGB wieder erstehen? Vieles spricht für die zweite These, nicht zuletzt die Tatsache, dass Präsident Putin zwischenzeitlich die Schlüsselpositionen des russischen Regierungsapparats mit Personen besetzt hat, die - wie er selbst - zuvor eine herausgehobene Geheimdienstfunktion innehatten.

**Umorganisa-  
tion**

<sup>405</sup> „Glawnoje Raswedywatelnoje Uprawlenije“; Militärische Aufklärung.

Von den anderen Nachfolgestaaten der ehemaligen Sowjetunion sind in Baden-Württemberg vor allem die Nachrichtendienste Kasachstans, der Ukraine und Georgiens aktiv.

### 3. Prävention

Die wirksame Bekämpfung nachrichtendienstlicher Aktivitäten erfordert einen ganzheitlichen Ansatz. Dementsprechend ist die repressive Spionageabwehr eng mit präventiven Schutzmechanismen verzahnt. Je komplexer sich die Gefährdungslage darstellt, umso größer wird die Bedeutung vorbeugender Maßnahmen. Im Wesentlichen zielt die vorbeugende Spionageabwehr darauf ab, die Verrats-tätigkeit in allen relevanten Bereichen zu erschweren, den vom Angreifer zu betreibenden Aufwand nachhaltig zu steigern und das Risiko der Entdeckung unkalkulierbar zu machen.

Klassische Elemente der Prävention sind personelle und materielle Schutzmaßnahmen. Die meisten und schwerwiegendsten Sicherheitsverletzungen sind auf menschliches Fehlverhalten der „Geheim-nisträger“ in Behörden und Unternehmen zurückzuführen, da gerade sie die Abläufe und Schwachstellen an ihrem Arbeitsplatz am besten kennen. Soweit dieser Personenkreis Zugang zu staatlichen Ver-schluss-sachen (VS) des Geheimhaltungsgrades VS-VERTRAULICH und höher erhalten soll, wird er zuvor einer Sicherheitsüberprüfung unter Mitwirkung der Verfassungsschutzbehörden unterzogen. Die personellen Maßnahmen werden durch materielle Sicherheitsvorkehrungen ergänzt. Hier berät das Landesamt für Verfassungsschutz Unternehmen und Behörden über bauliche, mechanische, elektronische und organisatorische Schutzmaßnahmen. In der Regel geht es um die Absicherung besonders schutzbedürftiger Bereiche durch den Einsatz moderner Sicherheits- und Gefahrenmeldetechnik.

#### 3.1 Informations- und Telekommunikationssysteme (ITS)

Nicht erst seit dem 11. September 2001 warnen Experten - zum Teil vergeblich - 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 und Risiken. Apokalyptisch anmutende Szenarien des „Information Warfare“<sup>406</sup> oder des „Cyber-Terrorismus“ haben ihren Ursprung in bereits bekannten, latenten Schwachstellen der Systeme und ihres Umfelds. ITS eignen sich generell sowohl als Ziel als auch als Mittel zum Zweck. Dabei spielen die Rahmenbedingungen des weltweiten IT-Einsatzes sowie konkrete Sicherheitslücken eine entscheidende Rolle und sorgen insgesamt für ein „angreiferfreundliches“ Klima und in der Folge für ungewollte Abflüsse von Know-how.

#### 3.1.1 Rahmenbedingungen

Wirtschaft und Politik fordern eine weltweite und mobile Kommunikation, Interoperabilität der Systeme, permanente Verfügbarkeit von Wissen in verteilten, virtuellen Strukturen und Erreichbarkeit des Personals zu jeder Zeit an jedem Ort. Folgen dieser Forderungen sind Standardisierung von Software, Fernwartung und zentrale Administration von ITS, eine zunehmende Monopolisierung im Hard- und Softwarebereich sowie eine enorme Zunahme der Komplexität der Systeme, aber auch der inhärenten Schwachstellen und Sicherheits-lücken<sup>407</sup>. Der finanzielle und technische Aufwand zur erfolgreichen Durchführung von Angriffen ist daher oftmals gering im Vergleich zum potenziellen Schaden. 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 Werkzeuge zur Verfügung. Präventive technische Sicherheitsmaßnahmen halten mit den originä-

„Die Informations- und Kommunikationsnetze eines Landes sind Nervenstränge unserer Informationsgesellschaft. Daher ist die Sicherung IT-abhängiger Infrastrukturen für uns eine zentrale Aufgabe.“

(Dr. Göttrik Wewer, Staatssekretär im Bundesinnenministerium, Pressemitteilung des Bundesministeriums für Wirtschaft und Arbeit vom 15. Mai 2003 (BITKOM und Bundesregierung gründen ein IT-Notfallzentrum für den Mittelstand))

Sicherheits-lücken

<sup>406</sup> Vgl. Kap. 3.1.2, S. 286f.

<sup>407</sup> Programmierfehler (bugs), Installations-, Konfigurations- und Administrationsmängel, versteckte Funktionalitäten von Systemen und Programmen (easter eggs), illegale Hintertüren (trap doors).

personelle  
und materielle  
Maßnahmen

Gefährdung  
von Informa-tionsinfra-  
strukturen

**Täterbild**

ren Entwicklungs- und Innovationszyklen längst nicht mehr Schritt. Das Täterbild reicht vom illoyalen Mitarbeiter über den politisch motivierten Hacker oder Einzeltäter, Tätergruppen der Organisierten Kriminalität, extremistische/terroristische Gruppierungen bis hin zu Nachrichtendiensten fremder Staaten. Das Risiko der Entdeckung ist gering. Dazu kommt, dass auch kriminelle Erscheinungsformen des täglichen Lebens unmittelbar im Internet ihr Pendant gefunden haben. Dazu gehören unter anderem virtuelle Sitzblockaden („Sit-In-tools“, verteilte Denial-of-service-Attacken), Protestschreiben (Mailbombing), Vandalismus (Web-Page-Defacement), Demonstrationen (Hacktivism), Cyberkriminalität, -terrorismus und -krieg. Gemeinsame Aufgabe der Sicherheitsbehörden und der Betroffenen in Staat und Wirtschaft muss es deshalb sein, das bestehende gravierende Ungleichgewicht zwischen Angriffsmethoden und Abwehrmöglichkeiten deutlich zu verringern.

**3.1.2 Risiken und Bedrohungen**

Die missbräuchliche Nutzung beziehungsweise die allgemeine Bedrohung der Informationstechnik lassen sich ganz grob in drei Merkmalskategorien unterteilen. Diese Bedrohungen umfassen dabei physische wie logische (elektronische) Gefährdungen. 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.
- ❑ **Daten- und Systemsabotage:** Ziel eines Angreifers ist es, Daten und/oder Systeme 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.

**drei Gefährdungskategorien**

Letztlich ist Ziel solcher Attacken, eigene Informationsüberlegenheit zu schaffen und zu bewahren, um militärische, politische, weltanschauliche, ethnische oder ökonomische Interessen gegenüber Dritten durchzusetzen.

Abgesehen von Gefahren, die durch Einwirkung höherer Gewalt (Naturkatastrophen, Feuer, Wasser etc.) entstehen können, basieren die wesentlichsten Gefährdungspotenziale auf menschlichem Versagen oder Fehlverhalten in kritischen Situationen, grundlegenden organisatorischen Mängeln, technischem Versagen von Systemen oder Komponenten und vorsätzlichen, schädigenden Handlungen von Personen. Gerade die „Schwachstelle Mensch“ ist in komplexen Informationsinfrastrukturen Hauptursache für erfolgreich verlaufende technische Angriffe. Fehlen dann noch entsprechende Konzepte, Richtlinien und Handlungsanweisungen, werden die Folgen und Schäden für die Betroffenen schnell unüberschaubar. Außerdem beklagt nahezu jede aktuelle Broschüre oder Studie<sup>408</sup> zum Thema IT-Sicherheit, dass Staat und Wirtschaft unter dem Druck leerer Kassen immer weniger geneigt sind, in IT-Sicherheitsmaßnahmen zu investieren. Andererseits wird weiter vehement am Ausbau Internet- und Web-basierender Anwendungen gearbeitet, mit dem Ergebnis, dass dadurch die angeschlossenen Systeme unter Umständen noch verletzlicher werden.

Neben den bisher dargestellten allgemeinen Bedrohungen und Gefahren gibt es eine Reihe typischer Risiken und Schwachstellen beim Einsatz von ITS, die unbeabsichtigte Informationsverluste oder (irreparable) Schäden nach sich ziehen können:

- ❑ **Missbräuchliche Nutzung frei verfügbarer, offener und sensibler Informationen in Netzen (Internet),**

**„Schwachstelle Mensch“**

„Es wäre grundsätzlich falsch, notwendige Sicherheitsmaßnahmen aus Kostenersparnis zu unterlassen.“

(Bundesinnenminister Otto Schily, Interview mit dem Handelsblatt vom 6. Oktober 2003)

**Risiken**

<sup>408</sup> Unter anderem BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.), Sicherheit für Systeme und Netze in Unternehmen, 2. überarbeitete Auflage, Einführung in die IT-Sicherheit und Leitfaden für erste Maßnahmen vom 15. Oktober 2003 (<http://www.bitkom.org>).

**Risiken**

- 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 Datenfernübertragungskonäle, 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).

**3.1.3 Schutzmaßnahmen**

Um bewusster mit potenziellen Risiken und Bedrohungen umgehen zu können, sind folgende Basisschutzmaßnahmen heutzutage für das Funktionieren von ITS unabdingbar:

- Ausbildung und Sensibilisierung der Mitarbeiter,
- baulicher/technischer Zugangs- und Zutrittsschutz,
- Abhörschutz,
- Sicherheitsanweisungen und -empfehlungen,

**Schutzmaßnahmen**

- Regelung von Verfahrensabläufen,
- Regelung von Zuständigkeiten/Verantwortungsbereichen/Zugriffsrechten,
- Datensicherung,
- sicherer Internetzugang,
- Virenschutz,
- Sicherheitskontrollen.

**3.1.4 Sicherheitskritische Infrastrukturen**

Die meisten der für unser Gemeinwesen zum Teil überlebensnotwendigen Infrastrukturen (Verkehr, Energieversorgung, Gesundheitsvorsorge, Rettungsdienste, Banken, Rechenzentren, Kommunikationsnetze etc.) befinden sich in Händen der Privatwirtschaft. Die bereits dargestellten Risiken und Bedrohungen, denen diese IT-Systeme heute ausgesetzt sind, erfordern zum Teil völlig neue Ansätze, um das Funktionieren dieser Infrastrukturen sicherzustellen. Das Landesamt für Verfassungsschutz arbeitet deshalb gemeinsam mit staatlichen und privaten Sicherheitsorganisationen intensiv an personellen, materiellen und organisatorischen Konzepten.

**3.2 Presse- und Öffentlichkeitsarbeit der Spionageabwehr**

Spionagerisiken werden zunehmend differenzierter und komplexer. Im Alltagsgeschäft geraten sie leicht aus dem Blickfeld und müssen daher immer wieder neu ins Bewusstsein gerufen werden. Die Spionageabwehr des Landesamts für Verfassungsschutz nutzt im Rahmen ihrer repressiven und präventiven Arbeit vielfältige Möglichkeiten, auf die sich verändernden Gefahren und die Auswirkungen des illegalen Abflusses von Know-how hinzuweisen und geeignete Gegenmaßnahmen zu empfehlen.

**Erarbeitung von Konzepten**

So wurden im Jahr 2003 über 150 Behörden- und Firmenberatungen durchgeführt. Darüber hinaus konnten Fragen der Spionageabwehr in Beiträgen für Funk und Fernsehen sowie Tageszeitungen und Fachzeitschriften thematisiert werden. In Betrieben, Behörden und Verbänden sowie im Hochschulbereich wurden mehr als 30 Fachvorträge gehalten, die oft zu einer Beratung vor Ort führten. Ergänzt wird die Presse- und Öffentlichkeitsarbeit durch Informationsangebote auf der Homepage des Landesamts für Verfassungsschutz.

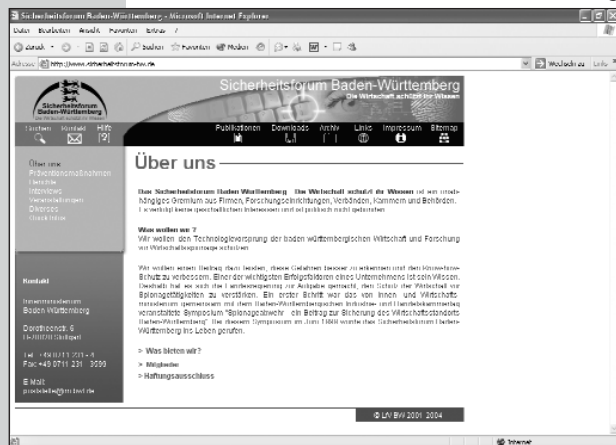
### 3.3 „Sicherheitsforum Baden-Württemberg - Die Wirtschaft schützt ihr Wissen“

Das Sicherheitsforum Baden-Württemberg setzt sich aus Mitgliedern der Wirtschaft, Wissenschaft, Verbände, Kammern und Behörden zusammen. Seine Hauptaufgabe besteht darin, speziell kleineren und mittelständischen Firmen den Themenkomplex Unternehmensschutz

näher zu bringen und Hilfestellung bei der Planung und Realisierung konzeptioneller Maßnahmen der betrieblichen Sicherheit zu leisten. Das Landesamt für Verfassungsschutz trägt als Mitglied mit dem Wissen und den Erfahrungen aus der Spionageabwehr zu weiterführenden Überlegungen

des Forums in Angelegenheiten des Informationsschutzes und der Unternehmenssicherheit bei.

Weitere Informationen über die Aktivitäten des Sicherheitsforums Baden-Württemberg sind im Internet unter [www.sicherheitsforum-bw.de](http://www.sicherheitsforum-bw.de) zu bekommen.



## 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.