

G. SPIONAGEABWEHR, GEHEIM- UND SABOTAGESCHUTZ

1. Aktuelle Entwicklungen und Tendenzen

Vom zivilen Nuklearprogramm zur militärischen Nutzung ist es mitunter nur ein kleiner Schritt. Nachdem das kommunistische Nordkorea unter seinem diktatorisch regierenden Führer Kim Jong-il bereits im Februar 2005 offiziell bekannt gegeben hatte, im Besitz von Kernwaffen zu sein, hat der erfolgreiche Atombombentest vom 9. Oktober 2006 die Welt aufgeschreckt.

Ein weiterer permanent schwelender Krisenherd ist der Iran. Die Vermutung, dass dort unter dem Deckmantel eines zielstrebig verfolgten zivilen Atomprogramms heimlich an der Entwicklung von Nuklearwaffen gearbeitet wird, umfangreiche Raketentests sowie der in den Medien immer wieder erhobene Vorwurf, Kurz- und Mittelstreckenraketen an die „Hizb Allah“ geliefert zu haben, rückten den Iran in den Mittelpunkt der weltweiten Anti-Proliferationsbemühungen⁴⁰⁷.

Das Landesamt für Verfassungsschutz Baden-Württemberg (LfV) ist eng in die gesamtstaatlichen Anstrengungen zur Proliferationsbekämpfung eingebunden und trägt durch die Verfolgung solcher Aktivitäten dazu bei, deren Urheber identifizieren und bestrafen zu können. Gleichzeitig leistet das LfV offensive Aufklärungsarbeit, um zu verhindern, dass baden-württembergische Unternehmen oder Geschäftsleute in riskante Geschäfte verwickelt werden. Dabei werden auch Überschneidungen der Themenfelder „Proliferation“ und „islamistischer Terrorismus“ beobachtet.

Nach wie vor muss in Deutschland von ernst zu nehmenden Spionageaktivitäten fremder Nachrichtendienste ausgegangen werden. Speziell China und Russland messen der Auslandsaufklärung einen hohen Stellenwert bei. In Baden-Württemberg, der Region mit der höchsten Innovationskraft innerhalb der Europäischen Union, liegt der Schwerpunkt eindeutig im Bereich der Wirtschafts- und Wissenschaftsspionage. Trotz leistungsfähiger technischer Spionagemöglichkeiten wird auf die Gewinnung menschlicher Quellen nach wie vor nicht verzichtet, da sie eine kontinuierliche Informationsgewinnung aus dem Zielobjekt und eine unmittelbare fachliche Bewertung der beschafften Informationen gewährleisten.

Der Nachholbedarf der Volksrepublik China gegenüber den hoch entwickelten Staaten des Westens wird auf den verschiedensten Ebenen durch

⁴⁰⁷ Proliferation: Weiterverbreitung von Massenvernichtungswaffen beziehungsweise der zu ihrer Herstellung verwendbaren Produkte einschließlich des dafür erforderlichen Know-hows sowie von entsprechenden Waffenträgersystemen.

eine konsequente und gut durchdachte Strategie zur Beschaffung ausländischer Know-hows unterstützt, wie sie gegenwärtig von anderen Staaten nicht bekannt ist. Die in diesen Prozess eingebundenen chinesischen Nachrichtendienste treten in Deutschland eher zurückhaltend, in China selbst aber durchaus aggressiv auf.

Trotz der guten zwischenstaatlichen Beziehungen auf Regierungsebene sind die russischen Geheimdienste in der Bundesrepublik Deutschland weiterhin sehr aktiv und beschaffen Informationen aus Politik, Militär, Wirtschaft und Wissenschaft.

Die Wirtschaft ist ein Hauptfaktor für Stabilität und Leistungskraft unseres Staates. Als Sicherheitsbehörde hat der Verfassungsschutz die Aufgabe, geheimdienstliche Angriffe fremder Staaten auf die Wirtschaft rechtzeitig zu erkennen und die Abwehr der von ihnen ausgehenden Gefahren zu ermöglichen. Ziel ist, auf einschlägige Risiken aufmerksam zu machen und Sorge dafür zu tragen, dass die in Baden-Württemberg ansässigen Unternehmen bei strategischen oder sicherheitsmäßig relevanten Entscheidungen über alle notwendigen Informationen verfügen.

2. Daten, Fakten, Hintergründe

2.1 Proliferation

Die Machthaber von Staaten wie Iran, Syrien, Pakistan oder Nordkorea sehen im Besitz von Massenvernichtungswaffen ein geeignetes Mittel, um sich machtpolitisch zu positionieren, symbolisch ihre Herrschaft zu legitimieren und vermeintliche externe Bedrohungen abzuwehren. Außerdem dient er als Druckmittel in bilateralen oder internationalen Verhandlungen.

Zum Teil sind diese Länder bereits in der Lage, den Bedarf an einschlägigen Waren und Know-how im eigenen Land zu decken oder sie beliefern sich gegenseitig damit (horizontale Proliferation). So werden nicht nur Maschinen und Ausrüstungsgegenstände, sondern bereits vollständige und einsatzfähige Raketensysteme oder das Wissen um deren Herstellung gehandelt.

Trotzdem sind diese Staaten auch weiterhin auf hochwertige Güter oder Spezialwissen aus High-Tech-Ländern angewiesen. Wie schon in den vergangenen Jahren gestalteten sich 2006 die Beschaffungsaktivitäten der um Proliferation bemühten Länder äußerst konspirativ. Dadurch sollen Exportgenehmigungs- und Kontrollmechanismen, zu deren Einhaltung sich die

„geheimdienstliche Angriffe auf die Wirtschaft“

Massenvernichtungswaffen als Mittel der Machtpolitik

Krisenherd
Iran

Spionageaktivitäten fremder Nachrichtendienste

Bundesrepublik Deutschland als Mitglied der internationalen Staatengemeinschaft verpflichtet hat, unterlaufen werden. Nur durch die effektive Zusammenarbeit von Bundesamt für Wirtschaft und Ausfuhrkontrolle, Bundeskriminalamt, Bundesnachrichtendienst, Zollkriminalamt und Verfassungsschutzbehörden kann diesen internationalen Übereinkommen wirksam Geltung verschafft werden.

2.1.1 Iran

Der Iran besitzt mittlerweile modernste Kurz- und Mittelstreckenraketen sowie Marschflugkörper. Nach erfolgreichem Testflug der Shahab 3 mit einer Reichweite von 1.500 Kilometern wird momentan mit Hochdruck an der Entwicklung von Flugkörpern jenseits des 2.000-Kilometer-Radius gearbeitet. Zu diesem Zweck bemühte sich das Land auch bei Unternehmen in Baden-Württemberg um die Beschaffung von Spezialwerkzeugen, Windkanal-ausrüstungen, Antriebs- und Steuersystemen, Testanlagen, Messgeräten, Festtreibstoffkomponenten mit Mixern und Informationen zur Kreiseltechnologie:

- Ein mittelständisches High-Tech-Unternehmen teilte dem LfV mit, dass aus dem Iran regelmäßig Anfragen zu seinen für die Herstellung von Raketentreibstoff notwendigen Produkten eingehen. Obwohl definitiv noch nie geliefert worden sei, habe es zwischenzeitlich auch Anfragen zu Ersatzteillieferungen gegeben. Nach Recherchen des LfV wurden gebrauchte Maschinen des Unternehmens im Internet und auf Gebrauchtgütermessen weltweit angeboten und dürften auf diesem Weg in den Iran gelangt sein. Der Fall belegt exemplarisch, mit welcher Vehemenz sich der Iran um dringend benötigte Embargogüter bemüht, und dass er nicht immer in der Lage ist, erforderliche Ersatzteile selbst herzustellen.

Die aktuelle Fallbearbeitung lässt erkennen, dass die in Baden-Württemberg nachgefragten Waren zumeist Dual-Use-Güter⁴⁰⁸ sind, welche in ihren Parametern häufig nur geringfügig von solchen Produkten abweichen, die der Exportkontrolle unterliegen:

- Die der Spionageabwehr einschlägig bekannte iranische Firma A aus Teheran erkundigte sich bei einem baden-württembergischen Unternehmen nach Spezialwerkzeugen, die üblicherweise in der Fahrzeugindustrie Verwendung finden. Als Besteller trat dann

⁴⁰⁸ Als „Güter mit doppeltem Verwendungszweck“ werden Güter einschließlich Datenverarbeitungsprogrammen und Technologien bezeichnet, die sowohl für zivile als auch für militärische Zwecke verwendet werden können.

jedoch nicht die Firma A, sondern die ebenfalls im Iran ansässige Firma B in Erscheinung. Erst im Nachhinein wurde offenkundig, dass sich die Firma A lediglich in B umbenannt hatte und nach wie vor unter der alten Adresse residierte. Beide Firmen sind dem iranischen Beschaffungsverbund für Trägertechnologie zuzurechnen, und es ist zu befürchten, dass die an sich harmlose Lieferung nunmehr bei der Herstellung von Raketen-Start-Ausrüstungen Verwendung findet. Dieses Beispiel zeigt auf, wie schwierig es mitunter sein kann, Proliferationshandlungen im Dual-Use-Bereich zu erkennen. Andererseits wäre das Geschäft sehr leicht zu verhindern gewesen, wenn den Begleitumständen des Auftrags mehr Beachtung geschenkt worden wäre.

Eine weitere beliebte Methode, um an sensible Güter zu gelangen, ist die Bildung von schwer durchschaubaren Beschaffungsketten. Durch die Einschaltung mehrerer in- und ausländischer Zwischenhändler soll die Identität des wahren Auftraggebers verborgen bleiben:

- Iranische Einkäufer versuchten, bei einer hiesigen Firma High-Tech-Geräte für die Luftfahrtindustrie zu beschaffen. Nachdem das Bundesamt für Wirtschaft und Ausfuhrkontrolle auf den kritischen Empfänger hingewiesen hatte, wurde von dem Geschäft zunächst Abstand genommen. Kurz darauf kaufte jedoch ein in Deutschland lebender iranischer Geschäftsmann die Geräte und deklarierte den Vorgang als Inlandsgeschäft. Die Lieferung erfolgte dann aber unter Einschaltung eines Zwischenhändlers im europäischen Ausland in den Iran. Dort wurden die Geräte nachweislich in militärische Fluggeräte eingebaut. Im Februar 2006 wurden vier in diese Transaktion verwickelte Personen - darunter auch der Geschäftsführer der baden-württembergischen Firma - festgenommen.

Nach wie vor ist im Zusammenhang mit iranischen Proliferationsbemühungen auch das Phänomen „illegaler Wissenstransfer“ von Bedeutung. Dabei geht es in erster Linie um die Aus- und Fortbildung von Postgraduierten, Studenten und Wissenschaftlern aus sicherheitskritischen Ländern, die unter dem Deckmantel des freien Austauschs technologisch-wissenschaftlicher Informationen an sensiblen Forschungsprojekten im westlichen Ausland mitwirken und sich auf diesem Wege das Know-how zur Entwicklung von Massenvernichtungswaffen und Raketen verschaffen:

- Eine wissenschaftliche Einrichtung in Baden-Württemberg, die sich auch mit Oberflächenbeschichtung und Nanotechnologie befasst,

wurde von einem iranischen Forschungsinstitut um Unterstützung gebeten. Wissenschaftler und Studenten aus dem Iran sollten umfassende Einblicke in die Technologien erhalten, um mit dem erworbenen Wissen anschließend die Fahrzeugindustrie ihres Heimatlandes voranbringen zu können. Da dieses Know-how jedoch sehr viel mehr für die Reichweitensteigerung von Raketen von Bedeutung ist als für die Kfz-Branche, wurde das Ersuchen abschlägig beschieden.

2.1.2 Demokratische Volksrepublik Korea (Nordkorea)

Zur Stützung seines diktatorischen Regimes unterhält das vom übrigen Weltgeschehen auch heute noch weitgehend abgeschottete kleine Land mit mehr als 1,1 Millionen aktiven Soldaten und rund 4,7 Millionen Reservisten eine der weltweit größten Armeen. Weitere wichtige Garanten des herrschenden Systems sind die sechs Nachrichten- und Sicherheitsdienste, die allesamt dem Staats- und Parteichef Kim Jong-il direkt unterstellt sind. Dabei ist an erster Stelle das für die politische Inlands- und Auslandsaufklärung zuständige „Ministerium für Staatssicherheit“ zu nennen. In seiner Machtfülle ist es allenfalls mit dem ehemaligen sowjetischen KGB⁴⁰⁹ zu vergleichen.

Es leben nur wenige nordkoreanische Staatsbürger in Deutschland und das Handelsvolumen zwischen beiden Ländern belief sich 2005 auf lediglich 75 Millionen Euro. Angesichts dieser Rahmenbedingungen ist es nicht einfach, proliferationsrelevante Geschäfte zu kaschieren. Gleichwohl ist Nordkorea sehr stark an westlicher Technologie interessiert, um damit sein gewaltiges Arsenal an Massenvernichtungswaffen weiter aufzurüsten. Beschaffungsaktivitäten - die sich gelegentlich auch auf Baden-Württemberg erstrecken - gehen zumeist von den Legalresidenturen⁴¹⁰ der nordkoreanischen Geheimdienste an der Berliner Botschaft aus. Die Abwicklung entsprechender Geschäfte vollzieht sich regelmäßig über Drittländer wie zum Beispiel China oder Singapur. Dort ansässige nordkoreanische Tarnfirmen fungieren als angebliche Endverbraucher.

Die Entwicklung in Nordkorea ist darüber hinaus unter dem Aspekt der horizontalen Proliferation von höchster Brisanz. Als regelmäßige Abnehmer nordkoreanischer Rüstungstechnologie sind bisher Länder wie Jemen, Iran, Libyen, Pakistan und Syrien aufgefallen. Letztlich erscheint auch die Weiter-

gabe proliferationsrelevanten Materials oder Know-hows an Terrororganisationen nicht völlig ausgeschlossen.

2.2 Wirtschafts-/Wissenschaftsspionage

Angesichts eines knallharten globalen Konkurrenzkampfes - manche Experten sprechen sogar von einem „Wirtschaftskrieg“ - werden von einigen Staaten Informationen aus Wirtschaft und Wissenschaft auch unter Einsatz ihrer Nachrichtendienste beschafft. Damit sind ganz unterschiedliche „Vorteile“ verbunden wie:

- ❑ Stärkung der nationalen Volkswirtschaft und Verbesserung der eigenen Forschungspotenziale durch Zeit- und Kostenersparnis sowie Vermeidung von Fehlentwicklungen,
- ❑ Analyse des Standes der Technik (Schlüsseltechnologien, rüstungsrelevante Bereiche),
- ❑ Benchmarking hinsichtlich Wirtschaftskraft, Zielen und Strategien sowie
- ❑ Beeinflussung von Marktchancen und -risiken.

In der Gesamtschau können diese Faktoren eine massive Wettbewerbsverzerrung bewirken.

Die Ausspähungsbemühungen fremder Staaten konzentrierten sich in den letzten Jahren auf die Bereiche Informations- und Kommunikationstechnik, Elektronik, Luft- und Raumfahrt, Verkehrstechnik, Werk- und Verbundstoffe, Produktionstechnik, Biotechnik, Nanotechnologie, Energie- und Umwelttechnik sowie auf den Maschinen- und Fahrzeugbau. Betroffen sind nicht nur große Firmen, sondern in beträchtlichem Ausmaß besonders innovative kleine und mittlere Unternehmen, die oft nicht über geeignete Sicherheitsvorkehrungen verfügen, um sich gegen den Diebstahl ihres Know-hows erfolgreich zur Wehr setzen zu können.

Die Wissenschaftsspionage ist seit jeher eine beliebte Methode, um in einem möglichst frühen Entwicklungsstadium an Informationen und Know-how zu gelangen. Bei der Ausspähung wird nicht selten die grundgesetzlich garantierte Freiheit der Wissenschaft bewusst missbraucht. Mehrere aktuelle Vorfälle in wissenschaftlichen Einrichtungen unterstreichen die Aussage. Das LfV weist immer wieder auf diese Gefahren hin, weil darunter langfristig nicht nur die Kompetenz der betroffenen wissenschaftlichen Einrichtung leiden könnte, sondern durch das Ausbleiben von Rückflüssen aus der wirtschaftlichen Umsetzung der häufig von staatlicher Seite finanzierten Forschungsergebnisse auch volkswirtschaftliche Nachteile zu befürchten sind.

„Vorteile“ der Informationsgewinnung durch Nachrichtendienste

Gefahren der Wirtschaftsspionage

⁴⁰⁹ „Komitet Gosudarstvennoj Besopasnosti“ („Komitee für Staatssicherheit“).

⁴¹⁰ Abgetarnte Stützpunkte fremder Nachrichtendienste in den offiziellen Vertretungen (insbesondere Botschaften, Konsulate, Handelsvertretungen) des Auftraggebers im Operationsgebiet.

2.2.1 Volksrepublik China

China hat - auf dem Weg vom Schwellenland zur globalen Wirtschaftsmacht - ein immenses Interesse daran, gleichzeitig seinen Technologierückstand zu verringern und sich auf dem Weltmarkt optimal zu positionieren. Weil die Entwicklung wirtschaftlicher und wissenschaftlicher Potenziale aus eigener Kraft viel Geld kostet, gut ausgebildete Fachleute erfordert und zudem relativ lange dauert, hat das Land eine umfassende, durchdachte Strategie zur schnelleren und kostengünstigeren Modernisierung seiner Volkswirtschaft entwickelt, die auf den verschiedensten Ebenen konsequent umgesetzt wird und auch den Einsatz von Nachrichtendiensten einschließt. Chinesische Aktivitäten nehmen momentan einen Großteil der Kapazitäten der Spionageabwehr in Anspruch.

Chinas Strategie zur Modernisierung seiner Volkswirtschaft

„Die westlichen Industrienationen haben ihr Know-how zum großen Teil an China weitergegeben und damit ihre Aufgabe erfüllt. Sie werden bald nicht mehr gebraucht. Ein Angriff aus China ist nur eine Frage der Zeit.“

(Philipp Vorndran, Chefstrategie der Credit Suisse, Quelle: SPIEGEL 37/2006, S. 68)

Trotz fortschreitender Entwicklung der Privatwirtschaft ist prinzipiell dann von staatlich gelenkter Spionage auszugehen, wenn wirtschaftspolitische und militärische Interessen im Vordergrund stehen. Projekte in strategisch bedeutsamen Entwicklungsbranchen unterliegen einem besonders hohen Risiko der nachrichtendienstlichen Unterwanderung.

Mitarbeiter der chinesischen Nachrichtendienste tarnen sich z.B. als Diplomaten

In Deutschland nutzen Mitarbeiter der chinesischen Nachrichtendienste ihre Tarnung als Diplomaten in den amtlichen chinesischen Vertretungen oder als Angehörige von Medienagenturen ihres Heimatlandes zur verdeckten Gewinnung von Informationen. Sie knüpfen Kontakte zu wissenschaftlichen und politischen Einrichtungen, zu Wirtschaftsunternehmen, Stiftungen und zu staatlichen Stellen. Die Teilnahme an Messen oder anderen öffentlichen Veranstaltungen dient dem Kennenlernen interessanter Personen.

Während früher eher „Amateurspione“ die Szene prägten und nach dem „Staubsaugerprinzip“ wahllos alle verfügbaren Informationen zusammengetragen haben, wird mittlerweile verstärkt auf gut ausgebildete „Kundschafter“ gesetzt. Der zielorientierte Einsatz von bestimmten Studenten (im Wintersemester 2005/2006 waren an deutschen Hochschulen mehr als 27.000 chinesische Studenten immatrikuliert), Praktikanten, Doktoranden, Wissenschaftlern und Forschern an ausländischen Universitäten und Forschungseinrichtungen zum Zwecke der Informationsgewinnung wird schon seit Jahren erfolgreich praktiziert. Dieser Personenkreis reist häufig bereits mit einem fundierten Fachwissen nach Deutschland ein und wird innerhalb seines Fachbereichs bald als Kapazität anerkannt und respektiert. Bereits

Schüler mit hervorragenden Zeugnissen werden vom Nachrichtendienst auf ihre künftige Einsatzfähigkeit im Ausland überprüft und bei Eignung bis zu ihrer Rückkehr begleitet und gefördert.

Deutsche Unternehmen, die in China investieren, setzen oft - wie von der chinesischen Seite gefordert - den neuesten Stand der Technik ein und wecken dadurch Begehrlichkeiten. Es zeigt sich immer wieder, dass geistiges Eigentum westlicher Unternehmen in der Volksrepublik China nur schwer zu verteidigen ist.

„Geschäfte in China machen heißt: hundert Prozent Technologietransfer.“
(Lutz Kahlbau, Leiter der Sparte Energieerzeugung von Siemens in China, Quelle: Die Welt, 17. Februar 2006, Flucht nach vorn)

Geschäftsreisende und Firmenrepräsentanten müssen stets damit rechnen, dass ihre Büros und Hotelzimmer observiert und durchsucht sowie Telefon- und Internetverbindungen überwacht werden. Unternehmen machen immer wieder die Erfahrung, dass intern geführte Gespräche mit raffiniert angebrachten hochwertigen Abhöranlagen belauscht werden.

Zudem besteht in China die Gefahr, nachrichtendienstlich angesprochen zu werden. Einen willkommenen Anlass dazu bieten immer wieder tatsächliche oder provozierte Gesetzesverstöße. Auch Spionage unter einem „offiziellen“ Vorwand kann nicht ausgeschlossen werden:



Handy-gesteuerte „Abhörwanze“
(aufgefunden im Büro einer deutschen Firma in China)

Gefahr nachrichtendienstlicher Ansprachen

- Die Niederlassung einer deutschen Firma in Shenzhen wurde von der örtlichen Polizeibehörde aufgefordert, eine Software auf ihrem Rechner zu installieren, die sämtliche Netzwerkaktivitäten (Internet, FTP) registriert und aufzeichnet. Diese Protokollierungen sollen als Beweismittel dienen, falls Angestellte der Firma verdächtigt werden sollten, rechtswidrige Internet-Aktivitäten zu entfalten. Es wurde eine Software empfohlen, die zu diesem Zweck von der chinesischen Sicherheitsbehörde zertifiziert wurde. Nach Aussage des Niederlassungsleiters handelt es sich um eine Art Feldversuch, der im Frühjahr 2006 in Shenzhen gestartet wurde und früher oder später auf ganz China ausgeweitet werden soll. Es wird befürchtet, dass entge-

gen entsprechenden Erklärungen der chinesischen Seite die Software mehr sensible Daten abgreifen könnte als offiziell beschrieben.

Anfragen von Wirtschaftsvertretern an die Spionageabwehr mit Bezug zu China nahmen im Jahr 2006 deutlich zu. Bei Beratungsgesprächen wurde regelmäßig der Verlust von Know-how beklagt:

- Bei einem baden-württembergischen Entwickler für Halbleiterlösungen in der Kfz-Elektronik fiel ein chinesischer Mitarbeiter auf, weil er in einem persönlichen Ordner seines Arbeitsplatz-PCs firmeninterne Daten aus zukunftssträchtigen Bereichen abgelegt hatte, für die er keine Zugriffsberechtigung besaß. Die Überprüfung seiner Bewerbungsunterlagen ergab, dass er die Darstellung seines Werdegangs perfekt an das Anforderungsprofil des Unternehmens angepasst hatte. Weiterhin konnte festgestellt werden, dass er bei der Bewerbung um seinen vorherigen Arbeitsplatz auf exakt die gleiche Art und Weise vorgegangen war, nur waren seinerzeit ganz andere Eigenschaften gefordert worden. Die Gesamtumstände dieses Falles sowie die weiteren Ermittlungsergebnisse lassen auf eine gezielte Steuerung durch chinesische Nachrichtendienste schließen.
- Ein chinesischer Wissenschaftler wirkte an einem Forschungsvorhaben im kerntechnischen Bereich mit. Kurz vor Abschluss des Projekts mussten seine Arbeitskollegen feststellen, dass die wissenschaftlichen Ergebnisse in China bereits veröffentlicht worden waren.
- Ein wissenschaftliches Institut für Informationstechnik stellte einen chinesischen Studenten als Praktikanten ein. Trotz Verbots der Nutzung eigener IT-Geräte wurde bei einer Kontrolle des institutsinternen Netzes festgestellt, dass er vertrauliche Daten auf seinen privaten Laptop überspielt hatte. Bemerkenswert war die Reaktion der Forschungseinrichtung, die den Täter lediglich zur Einhaltung der internen Vorschriften anhielt und das regelwidrige Verhalten nicht weiter ahndete.
- Ein chinesischer Wissenschaftler bewarb sich um Mitarbeit im Forschungsbereich einer staatlichen Hochschule. Nach seiner Anstellung stellte sich heraus, dass er den wissenschaftlichen Vorlauf, den er bei seiner Bewerbung vorgegeben hatte, nicht besaß. Außerdem fiel er dadurch auf, dass er im Institut unberechtigt fotografierte und versuchte, an für ihn gesperrte Daten zu gelangen. Der Verdacht eines nachrichtendienstlichen Auftrags liegt nahe, da sein Aufent-

halt von chinesischen diplomatischen Einrichtungen im Bundesgebiet finanziert und eng begleitet wurde.

Aufgabe der Spionageabwehr ist es, solchen Fällen nachzugehen, um betroffenen beziehungsweise gefährdeten Unternehmen und wissenschaftlichen Einrichtungen Gefahren und Risiken aufzuzeigen, sie bei internen Entscheidungsprozessen zu beraten und letztlich den Nachweis einer nachrichtendienstlichen Steuerung zu führen.

2.2.2 Russische Föderation

Die Russische Föderation und die Bundesrepublik Deutschland unterhalten seit Jahren stabile wirtschaftliche und politische Beziehungen. Ungeachtet dessen entwickeln die Nachrichtendienste Russlands nach wie vor umfangreiche Aktivitäten gegen Deutschland.

Der Präsident der Russischen Föderation hat die russischen Sicherheitsdienste erneut gestärkt. Nach Medienberichten sieht ein Konzept zur Haushalts- und Steuerpolitik 2007 vor, die Ausgaben für die nationale Sicherheit um 23,1 Prozent gegenüber 2006 zu steigern. Der Militäretat soll um 24,6 Prozent erhöht werden. Wie schon in den vergangenen Jahren profitieren davon auch die Nachrichtendienste.

Der zivile Auslandsnachrichtendienst SWR⁴¹¹ ist für die Auslandsaufklärung in den Bereichen Politik, Wirtschaft und Wissenschaft zuständig und wird von Armeegeneral Sergej LEBEDEW geleitet.

Die Aufgaben des von Armeegeneral Walentin KORABELNIKOW geführten militärischen Auslandsnachrichtendienstes GRU⁴¹² sind heutzutage weitaus breiter gefächert als zu Zeiten der UdSSR. Neben klassischer Militärspionage erstrecken sich die Aktivitäten des GRU mittlerweile auch auf alle militärrelevanten zivilen Bereiche. Dies gilt vor allem für wissenschaftlich-technologische Informationen, die für militärische Zwecke nutzbar sind.

Der zivile Inlandsnachrichtendienst FSB⁴¹³ unter der Leitung von Armeegeneral Nikolaj PATRUSCHEW ist für die Spionageabwehr, die Beobachtung des politischen Extremismus sowie die Bekämpfung von Organisierter Kri-

⁴¹¹ „Slushba Wneschnej Raswedkij“ („Dienst für Ermittlungen im Ausland“).

⁴¹² „Glawnoje Raswedwatelnoje Uprawlenije“ („Hauptverwaltung für Aufklärung“ beim Generalstab der Streitkräfte).

⁴¹³ „Federalnaja Slushba Besopasnosti“ („Föderaler Dienst für Sicherheit“).

minalität und Terrorismus zuständig. Unter dem Vorwand der Spionagebekämpfung versucht der FSB auch, Angehörige deutscher Firmen und Privatpersonen bei Aufenthalten in Russland nachrichtendienstlich anzubahnen und somit in anderen Zielbereichen Auslandsaufklärung zu betreiben. Bei seinen Abwehraktivitäten betreibt er eine intensive Kontrolle des Datenverkehrs, der in Russland über das Internet abgewickelt wird. Daher müssen auch deutsche Staatsangehörige bei Aufenthalten in Russland damit rechnen, bei der Nutzung des Internets oder des Telefons vom FSB überwacht zu werden.

Die größte Gefahr ging 2006 wiederum von den Legalresidenturen⁴⁴⁴ aus. Die verhältnismäßig hohe Präsenz der dort tätigen erkannten Geheimdienstangehörigen unterstreicht den besonderen Stellenwert, der Deutschland als Aufklärungsziel immer noch beigemessen wird. Anlässlich der Novellierung des Gesetzes „Über die Auslandsaufklärung“ bestätigte ein Mitglied der Staatsduma und ehemaliger Angehöriger der Auslandsspionage, dass viele russische Nachrichtendienstmitarbeiter unter gesetzlicher Abtarnung als Diplomaten, Journalisten oder Geschäftsleute arbeiten und teilweise sogar formell andere Staatsangehörigkeiten annehmen würden. Geschützt durch die diplomatische Immunität ist es für russische Agenten ein Leichtes, mit interessant erscheinenden Zielpersonen unverfänglich in Kontakt zu treten, um von ihnen wichtige Informationen zu erlangen.

- Auf diese Weise wurde beispielsweise dem Mitarbeiter einer baden-württembergischen High-Tech-Firma durch den Angehörigen eines russischen Nachrichtendienstes der Auftrag zur Beschaffung eines der Ausfuhrkontrolle unterliegenden Rüstungsgegenstandes erteilt.
- In einem weiteren Fall wurde der Mitarbeiter einer im süddeutschen Raum ansässigen Rüstungsfirma nach einem Messebesuch von einem Russen aufgesucht und für die Beschaffung entsprechender Firmeninterna gewonnen. Darunter befanden sich Skizzen und Beschreibungen von lasergesteuerten Waffen.

Solche Fälle belegen, dass die Wirtschaftsspionage für die Staatsführung der Russischen Föderation nach wie vor hohe Priorität besitzt. Dabei geht es vorrangig um die Beschaffung von Informationen zu richtungweisenden Neuerungen im wissenschaftlich-technischen Bereich.

⁴⁴⁴ Abgetarnte Stützpunkte fremder Nachrichtendienste in den offiziellen Vertretungen (insbesondere Botschaften, Konsulate, Handelsvertretungen) des Auftraggebers im Operationsgebiet.

3. Prävention

Unter dem Begriff „Prävention“ ist die Gesamtheit aller vorbeugenden Maßnahmen zu verstehen, die der Verfassungsschutz entweder aufgrund gesetzlichen Auftrags zu erfüllen hat oder aus Opportunitätsgründen heraus ergreifen kann, um Behörden, Wirtschaft und Wissenschaft vor Gefährdungen und illegalem Wissensabfluss zu schützen. Präventionsmaßnahmen werden in zunehmendem Maße von der Wirtschaft eingefordert, und es wird ihnen ein immer größerer Stellenwert beigemessen.

3.1 Geheim- und Sabotageschutz

Der förmliche Geheim- und Sabotageschutz ist ein wesentlicher Bestandteil der Prävention zum Schutz gegen die Ausforschung von Staatsgeheimnissen und zur Sicherheit lebens- und verteidigungswichtiger Einrichtungen. Diese den Mitwirkungsaufgaben des Verfassungsschutzes zuzurechnenden Vorbeugungsmaßnahmen umfassen Sicherheitsüberprüfungen von Personen, die an sicherheitsempfindlichen Stellen tätig sind, technische und organisatorische Maßnahmen sowie die ständige Beratung und Betreuung behördlicher und wirtschaftlicher Einrichtungen.

In Baden-Württemberg sind derzeit über 200 Firmen in das amtliche Geheimschutzverfahren einbezogen und rund 20 als lebens- und verteidigungswichtig eingestuft. Sie werden vom LfV regelmäßig über Ausspähungsversuche fremder Nachrichtendienste und die Bedrohung durch sicherheitsgefährdende Bestrebungen unterrichtet und entsprechend beraten.

3.2 Beratung und Aufklärung von Wirtschaft und Wissenschaft

Einen breiten Raum der präventiven Maßnahmen nimmt die Unterstützung der Forschungseinrichtungen und der nicht in das behördliche Geheimchutzverfahren einbezogenen baden-württembergischen Unternehmen bei der Erhaltung ihres technologischen Vorsprungs ein. Eine umfassende Palette praxisgerechter Maßnahmen - beispielsweise die Herausgabe von Informationsmaterial, Informations- und Beratungsgespräche sowie Unterstützung bei der Erstellung von Schutzkonzeptionen - bietet „Hilfe zur Selbsthilfe“. Im Jahr 2006 ist die Nachfrage nach Beratungsleistungen und Vortragsveranstaltungen durch Mitarbeiter des Wirtschaftsschutzes signifikant gestiegen.

Ziel des LfV ist es, mit seinen Beratungs- und Serviceangeboten speziell die in Baden-Württemberg vorherrschenden kleinen und mittleren Betriebe zu

„Das Know-how unserer Unternehmen ist eines der wertvollsten Güter und muss daher besonders geschützt werden“

(Innenminister Dr. Ingo Wolf, Nordrhein-Westfalen, am 11. Mai 2006 auf der Tagung „Wirtschaftsschutz in NRW - 2006“ in Düsseldorf, Quelle: WIK 06/3, S. 26)

erreichen. Sie sind oftmals Vorreiter bei der Einführung neuer Technologien und verfügen vielfach nicht über ausreichende Sicherheitsstrukturen zum Schutz ihres Know-hows. Zu diesem Zweck wurden Unternehmen direkt kontaktiert oder über Wirtschafts- und Sicherheitsverbände sensibilisiert. In der Folge gingen beim LfV vermehrt Hinweise ein, die eine anhaltende Gefährdung durch Spionage belegen.

Auf der Mobility & Business, der Messe für Geschäftsreisen, Fuhrpark und mobile Kommunikation im Mai 2006 in Stuttgart, informierte das LfV schwerpunktmäßig über die Sicherheit bei Geschäftsreisen ins Ausland. Dabei standen sowohl der Schutz der Reisenden selbst vor Ansprachen und Anwerbungsversuchen fremder Nachrichtendienste als auch die sichere Informations- und Datenübertragung im Mittelpunkt. Daneben wurden in einer messebegleitenden Seminarreihe die Themen Spionage und Wirtschaftsschutz eingehend beleuchtet.



Die Spionageabwehr beteiligte sich auch an einem gemeinsamen Stand der Verfassungsschutzbehörden des Bundes und der Länder bei der Essener Sicherheitsmesse SECURITY 2006 zum Themenkomplex Wirtschaftsspionage. In vielen Gesprächen wurden Fragen zur IT-Sicherheit und zum Informationsschutz erörtert und mehrere Verdachtshinweise entgegengenommen.

3.3 Sicherheitsdefizite bei mobilen Geräten und Anwendungen

Ein Schwerpunkt der IT-Sicherheit liegt auf der Sicherung mobiler Geräte⁴¹⁵ und Anwendungen, weil sowohl die Zahl mobiler Mitarbeiter in Wirtschaftsunternehmen als auch die Absatzzahlen der Hersteller solcher Geräte kontinuierlich steigen. Mitarbeiter sollen weltweit und permanent erreichbar sowie Unternehmensdaten unmittelbar verfügbar sein. Fast alle mobilen Endgeräte zeichnen sich dadurch aus, dass so genannte PIM-Daten⁴¹⁶ ortsunabhängig nutzbar sind, Anwendungen mit stationären Endgeräten synchronisiert und aktualisiert und fast generell via Funk oder Mobilfunk⁴¹⁷ Telekommunikationsdienstleistungen abgerufen und genutzt

⁴¹⁵ Beispielsweise Laptops, Notebooks, Sub-Notebooks, Mobiltelefone, Smartphones, Personal Digital Assistants (PDAs), Palmtops, Handhelds, E-Mail-Messaging-Geräte, USB-Sticks, MP3-Player und Digitalkameras.

⁴¹⁶ Personal Information Manager: Software, die persönliche Daten wie Kontakte, Aufgaben, Terminplanung, Notizen, ToDo-Listen und Dokumente (Briefe, Faxe, E-Mails) verwaltet und speichert.

⁴¹⁷ Beispielsweise Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), Universal Mobile Telecommunications System (UMTS), Enhanced Data Rates for GSM Evolution (EDGE), Wireless Local Area Network (WLAN), Wireless Fidelity (WiFi) und Bluetooth.

werden können oder den direkten Zugriff auf das Unternehmensnetzwerk erlauben. Nach aktuellen Studienergebnissen des Marktforschungsunternehmens Forrester⁴¹⁸ geben europäische Firmen 32 Prozent ihres Telekommunikations- und Vernetzungsbudgets für mobile Lösungen aus.

Der mittlerweile starken Verbreitung und Nutzung mobiler Systeme steht ein hohes Risiko des Verlusts der Verfügbarkeit und der Vertraulichkeit der dort gespeicherten Daten gegenüber. Die <kes>/Microsoft-Sicherheitsstudie 2006⁴¹⁹ kommt hier zusammenfassend zum Ergebnis, dass die Sicherheit mobiler Systeme als gering und deren Gefährdung als sehr hoch einzuschätzen sei. Allein 27 Prozent der befragten Unternehmen gaben an, sicher zu sein, dass Unbefugte durch Verlust oder Diebstahl der Geräte Zugang zu schutzwürdigen Daten erhalten könnten. Fast die Hälfte der Befragten attestierte ihren mobilen Anwendungen allenfalls ein eben noch ausreichendes Sicherheitsniveau. Die in Unternehmensnetzwerken und -systemen heute gebräuchlichsten Sicherheitsmaßnahmen - wie zum Beispiel Virenschutz, Verschlüsselung und Firewalls - werden nur in sehr begrenztem Umfang zum Schutz mobiler Geräte genutzt, obwohl nach Expertenmeinung mehr als die Hälfte der unternehmenskritischen und sensiblen Daten (auch) auf Mobilgeräten gespeichert sind.⁴²⁰ Regelmäßige Sicherungen der mobilen Datenbestände sind dabei eher die Ausnahme. Inzwischen setzen Unternehmen zwar fast standardmäßig Passwort-/ PIN-Verfahren⁴²¹ zum Schutz der gespeicherten Daten ein, allerdings unterbleiben sowohl die Integration der mobilen Endgeräte in umfassende strategische Konzepte als auch die Absicherung drahtloser Datenübertragungsverfahren.⁴²² Gleichzeitig steigt die Zahl der Schadprogramme, die von Hackern gezielt für Angriffe auf Mobilsysteme genutzt werden können, rapide an.⁴²³

Nach den Erfahrungen des LfV steht das Verhalten mobiler Mitarbeiter teilweise in krassem Widerspruch zu ihrem Wissen. Wie eine aktuelle Studie des Netzwerkausrüsters Cisco Systems⁴²⁴ belegt, kennen diese Mitarbeiter

⁴¹⁸ Forrester „The State of European Enterprise Mobility in 2006“, 13. Oktober 2006, URL: <http://www.forrester.com/Research/Document/Excerpt/0,7211,39877,00.html>.

⁴¹⁹ Lagebericht zur Informationssicherheit: Teil 1 in <kes> 2006#4, S. 24ff.; Teil 2 in <kes> 2006#5, S. 40ff.; Teil 3 in <kes> 2006#6, S. 48ff.

⁴²⁰ Portal All About Security: „Mobile Endgeräte bedrohen die IT-Sicherheit“, 31. Oktober 2006, URL: <http://www.all-about-security.de/artikel+M5aed5627f9f.html>.

⁴²¹ Studie Coleman Parkers Research/Avanade: „Mobile technology in the enterprise: the mobile world at work“, 30. Mai 2006, URL: Symantec-Studie zur mobilen Sicherheit, April 2006, URL: http://www.avanade.com/uk/_uploaded/pdf/wpaperthemobileworldatworkresearch515273.pdf.

⁴²² Symantec-Studie zur mobilen Sicherheit, April 2006, URL: http://www.symantec.com/content/en/us/about/media/mobile-security_Full-Report.pdf.

⁴²³ Symantec Internet Security Threat Reports, URL: http://www.symantec.com/region/de/PressCenter/Threat_Reports.html.

⁴²⁴ Cisco Systems-Studie zum Thema „Mobile Mitarbeiter“, November 2006, URL: http://www.cisco.com/global/DE/presse/meld_2006/11_08_2006-it-security-mobile-mitarbeiter.shtml.

ständige Erreichbarkeit versus Vertraulichkeit gespeicherter Daten

starke Zunahme mobiler Lösungen

„In vier von fünf Unternehmen wurde bereits ein mobiles Gerät als verloren gemeldet und dies erschreckend häufig direkt in der Firma“, sagt Frank Bunn, Senior Solution Marketing Manager bei Symantec. „Aber so ärgerlich der Verlust der Geräte an und für sich ist, weit schwerer wiegt die Tatsache, dass die darauf befindlichen geschäftskritischen Daten ebenfalls für immer verschwunden sind und womöglich von Dritten missbraucht werden.“ Die befragten Unternehmen gaben an, dass sich neben den Firmendaten schätzungsweise im Schnitt 21 Prozent externe, also Kundendaten, auf den Geräten befinden.

(Frank Bunn, Senior Solution Marketing Manager bei Symantec, Quelle: Compliance Magazin)

sehr wohl die Risiken und sind auch über entsprechende Sicherheitsanforderungen informiert, setzen aber dennoch mobiles Firmen-Equipment privat ein, stellen es Dritten (Freunde, Bekannte, Kollegen, Familienangehörige) für den Privatgebrauch zur Verfügung, öffnen E-Mails unbekannter Absender und nutzen ungesicherte, drahtlose Verbindungen von Nachbarn oder installieren selbst ungeprüfte Software.

Die wesentlichsten Gefährdungen und Risiken beim Einsatz mobiler Endgeräte sind:

- „Risikofaktor Mensch“: Geräte- und/oder Datenverluste durch Irrtum, Fahrlässigkeit, Nachlässigkeit, mangelndes Sicherheitsbewusstsein und Vorsatz
- Manipulation des Betriebssystems durch Viren, Würmer und Trojaner
- Hardware-/Datenverlust durch Diebstahl oder Nachlässigkeit
- Mangelhafte Authentisierung der Nutzer der Endgeräte (Verzicht auf Passwort-/PIN-Verfahren, keine Aktivierung vorhandener Sicherheitsfunktionalitäten)
- Fehlende Rechteverwaltung auf den Endgeräten
- Keine Verschlüsselung der Daten
- Abhörriisiko bei Nutzung ungeschützter drahtloser Übertragungsverfahren
- Hacking-Angriffe über ungeschützte drahtlose Übertragungsverfahren
- Fehlendes „Patchmanagement“⁴⁴⁵, um erkannte Software-Schwachstellen zu schließen
- Datenverluste durch unterbliebene oder mangelhafte Datensicherung
- Gefährdung des Firmennetzwerks durch Anschluss „verseuchter“ Mobilgeräte.

Aus Sicht des LfV sind deshalb organisatorische und technische Schutzmaßnahmen beim Einsatz mobiler Systeme unabdingbar. Ein Verzicht auf entsprechende Sicherheitsvorkehrungen führt im Zweifel nicht nur zum Verlust der Geräte und Daten selbst, sondern auch zu einer erheblichen

⁴⁴⁵ Patchmanagement ist das strukturierte, schnelle und weitestgehend automatische Schließen erkannter Schwachstellen in Betriebssystemen und Anwendungssoftware auf Rechnern (PC, Server etc.) in komplexen und heterogenen IT-Systemlandschaften durch Administratoren oder Sicherheitsverantwortliche.

Gefährdung der Firmennetzwerke und der dort gespeicherten Informationen. Dass dabei in der Folge auch beträchtliche finanzielle Schäden entstehen können, veranschaulicht eine Studie der amerikanischen Beratungs- und Forschungseinrichtung Ponemon Institute.⁴²⁶ Danach bergen mobile Geräte das größte Risiko für Datenverluste und damit verbundene finanzielle Einbußen in sich. In 45 Prozent der untersuchten Fälle seien gestohlene oder verlorene Mobilgeräte und mobile Datenträger für den entstandenen Schaden direkt verantwortlich. Um solche Schäden erst gar nicht entstehen zu lassen, beziehungsweise, um das eventuelle Schadensausmaß drastisch zu reduzieren, empfiehlt das LfV die nachfolgenden Schutzvorkehrungen:

- Schulung und Sensibilisierung der mobilen Mitarbeiter beziehungsweise der Nutzer mobiler Endgeräte
- Erarbeitung entsprechender Richtlinien und Anweisungen sowie Integration in bestehende betriebliche Sicherheitskonzepte
- Verbot der privaten Nutzung der Firmengeräte/Verbot des Einsatzes privater Mobilgeräte zu dienstlichen Zwecken
- Aktivierung und Nutzung angebotener Sicherheitsfunktionalitäten der Geräte
- Einsatz von (mobilen) Virenscannern und Personal Firewalls
- Verschlüsselung der Speicher und/oder der Speicherinhalte
- Einsatz leistungsfähiger Authentifizierungsmechanismen (Zusatzsoftware)
- Verwendung „starker“⁴²⁷ Passwörter/PIN und deren regelmäßige Änderung
- Absicherung/Verschlüsselung der Übertragungsverfahren
- Einführung eines regelmäßigen „Patchmanagements“ für sicherheitsrelevante Updates
- Erarbeitung eines Datensicherungskonzepts für mobile Anwendungen
- Regelmäßige Prüfung der Sicherheitskonfiguration
- Schutz der Firmennetzwerke vor unautorisiertem Zugriff mobiler Endgeräte zum Beispiel durch Firewalls oder VPNs (Virtual Private Networks).

Unabdingbare Voraussetzung für eine risikolose Nutzung mobiler Anwendungen und Geräte ist die Integration in ein ganzheitliches Informations-

⁴²⁶ Ponemon Institute: „2006 Annual Study: Cost of a Data Breach“, Oktober 2006, URL u. a.: <http://www.vontu.com/offers/costofbreach.asp>.

⁴²⁷ Starke Passwörter/PIN sind mindestens acht Zeichen lang, in zufälliger Reihenfolge alpha-numerisch aufgebaut, verwenden Groß- und Kleinbuchstaben sowie Sonderzeichen.

schutzkonzept, das die Vertraulichkeit, Integrität und Verfügbarkeit der Daten und Systeme gewährleistet. Ergänzend ist bei der Aussonderung oder dem Verkauf mobiler Geräte darauf zu achten, dass sensible Daten aus dem Speicher entfernt werden, damit sie nicht in die Hände Unbefugter gelangen können.

3.4 Sicherheitsforum Baden-Württemberg - die Wirtschaft schützt ihr Wissen

Das 1999 unter Beteiligung des Landesamts für Verfassungsschutz gegründete Sicherheitsforum Baden-Württemberg hat sich zu einem wichtigen Sicherheitsinstrument vor allem für die mittelständische Wirtschaft entwickelt. Es soll dazu beitragen, dass die Unternehmen neben den Gefahren des Terrorismus alltäglichere Geschäftsrisiken wie den Verlust des eigenen Know-hows oder die Computerkriminalität nicht vernachlässigen.

Die Mitglieder des Forums legen bei regelmäßigen Sitzungen die zukünftigen Aktivitäten mit der Zielsetzung fest, die Scharnierfunktion zwischen Politik und Wirtschaft weiter auszubauen und vor allem die kleinen und mittleren Unternehmen mit aktuellen Sicherheitsfragen vertraut zu machen. So wurde im Oktober 2006 in **Mannheim** eine Vortragsreihe zu Aspekten der Unternehmenssicherheit gestartet, die zukünftig auf alle Regionen Baden-Württembergs ausgedehnt werden soll. Für 2007 ist die Vergabe eines Sicherheitspreises geplant.

Die Internetseite des Sicherheitsforums⁴²⁸ informiert über eine breite Palette von Sicherheitsthemen und ermöglicht den Zugriff auf eine Auswahl aktueller Informationen aus unterschiedlichen Quellen („Quick Infos“).

4. Erreichbarkeit der Spionageabwehr/Weitere Informationen

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

⁴²⁸ URL: <http://www.sicherheitsforum-bw.de>.

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

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

0711 - 954 76 26 (Telefon) und
0711 - 954 76 27 (Telefax)

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

Aktuelle Informationen zum Thema Spionageabwehr erhalten Sie auch im Internet:



Hier finden Sie auch die Ende 2006 gemeinsam mit dem Bayerischen Landesamt für Verfassungsschutz erstellte Broschüre „Wirtschaftsspionage in Baden-Württemberg und Bayern - Daten - Fakten - Hintergründe“ zum Herunterladen. Sie wurde im Januar 2007 herausgegeben. Darüber hinaus wird noch die Broschüre „Know-how-Schutz - Handlungsempfehlungen für die gewerbliche Wirtschaft“ (2004) angeboten. Beide Broschüren können beim LfV auch kostenlos bestellt werden.