Bundesamt für
Verfassungsschutz

Bedrohung der Wirtschaft im Zeitalter der Globalisierung

Bedrohungen der Wirtschaft im Zeitalter der Globalisierung

Publikation der Vorträge des 6. Symposiums des Bundesamtes für Verfassungsschutz am 3. Dezember 2007

Impressum:

Herausgeber: Bundesamt für Verfassungsschutz
Merianstr. 100
50765 Köln
Tel.: 0 18 88 - 7 92 / 0
Fax: 0 18 88 - 79 83 65
e-Mail: info@verfassungsschutz.de
Internet: http://www.verfassungsschutz.de

Layout und Druck: Bundesamt für Verfassungsschutz
IT 21.2 PrintCenter

Inhaltsverzeichnis **Seite**

Heinz Fromm, Präsident des Bundesamtes für Verfassungsschutz

Begrüßung

Meine sehr geehrten Damen und Herren,

ich heiße Sie herzlich willkommen zum 6. Symposium des Bundesamtes für Verfassungsschutz.

Ich begrüße besonders den für die Koordination der Nachrichtendienste des Bundes zuständigen Abteilungsleiter im Bundeskanzleramt, Herrn MinDir Klaus-Dieter Fritsche, der auch als früherer Vizepräsident des BfV mit dem Thema vertraut ist. Sehr herzlich begrüße ich auch die anwesenden Kolleginnen und Kollegen aus dem Bundesministerium des Innern.

Meine Damen und Herren, eine effiziente Zusammenarbeit und ein vertrauensvolles Verhältnis der Sicherheitsbehörden des Bundes und der Länder gehört heute zu den wichtigsten Voraussetzungen für eine erfolgreiche Aufgabenerfüllung. Ein Zeichen hierfür ist auch, dass ich den Präsidenten und den Vizepräsidenten des Bundesnachrichtendienstes, Herrn Uhrlau und Herrn von Brandis, hier begrüßen kann, ebenso wie Herrn Alff, den Präsidenten des Militärischen Abschirmdienstes, und den Abteilungspräsidenten des Bundeskriminalamtes, Herrn Wittling.

Wie ernst der Verfassungsschutz die heute hier debattierte Problematik nimmt, zeigt auch die große Zahl meiner anwesenden Kollegen aus den Landesbehörden. Stellvertretend begrüße ich Frau Claudia Schmid, die Leiterin der Berliner Verfassungsschutzbehörde. Herzlich willkommen, liebe Kolleginnen, liebe Kollegen.

Der Schutz der Wirtschaft erfordert eine intensive Zusammenarbeit der Sicherheitsbehörden auf internationaler Ebene. Es ist ein positives Zeichen, dass viele Verbindungsbeamte ausländischer Nachrichtendienste anwesend sind, darunter auch solche, mit denen wir nicht in allen Fragen übereinstimmen.

Es ist uns ein besonderes Anliegen, Sicherheitsfragen mit Vertretern der Wirtschaft zu erörtern. Konstruktive Kontakte sind eine unabdingbare Voraussetzung für eine erfolgreiche Gefahrenabwehr. Deshalb ist es mir ein große Freude, in großer Zahl Verantwortliche aus den Sicherheitsbereichen wichtiger Unternehmen und Organisationen zu begrüßen. Wir freuen uns sehr, dass Sie gekommen sind.

Schließlich möchte ich die zahlreichen Vertreter der Medien herzlich will-

kommen heißen.

Es ist das dritte Mal, dass unser Symposium in den Räumen der Bundesakademie für Sicherheitspolitik stattfindet. Dass wir uns hier wohl fühlen, ist somit keine Frage. Ein herzliches Dankeschön gilt Ihnen, Herr Dr. Adam, für die Gastfreundschaft und die freundlichen Worte zur Eröffnung, selbstverständlich auch für die Unterstützung durch Sie und Ihre Mitarbeiter. Ebenso herzlich danke ich meinen Mitarbeitern für die inhaltliche und organisatorische Vorbereitung des heutigen Symposiums.

Mein besonderer Dank gilt den Referentinnen und Referenten. Wir freuen uns auf den Beitrag von Herrn Juillet aus Paris, Manager und Geheimagent, wie die Frankfurter Allgemeine Zeitung schreibt. Ebenso gespannt dürfen wir auf den Beitrag von Frau Professorin Merkel und Herrn Professor Kahle von der Universität Lüneburg sein. Mein Dank gilt auch dem Vorsitzenden der Arbeitsgemeinschaft der Wirtschaft, Herrn Dr. Menk, der über die im Zeichen der Globalisierung signifikant zunehmenden Sicherheitsgefährdungen für die Wirtschaft sprechen wird. Ebenso danke ich Herrn Dr. Maurer aus dem Bundesministerium für Wirtschaft und Technologie für seinen Beitrag über die Bedeutung des Geheimschutzes.

Meinen Mitarbeitern, Herrn Sassenscheidt-Grote und Herrn Kurek, die nachher referieren werden, danke ich ebenfalls sehr herzlich. Und, last but not least, gilt mein Dank den Dolmetschern für ihre Unterstützung.

Meine sehr verehrten Damen und Herren,
wie in jedem Jahr haben wir für unser Symposium ein Thema gewählt, das gesellschaftliche Relevanz und Aktualität verbindet. Die „Bedrohung der Wirtschaft im Zeitalter der Globalisierung“ ist eine Thematik, die uns alle angeht. Wir müssen die vorhandenen Ressourcen bündeln und eine gemeinsame Abwehrstrategie von Staat und Wirtschaft entwickeln, um die einzelnen Unternehmen, aber auch die Volkswirtschaft insgesamt zu schützen.

Wir müssen sie auch schützen gegen militante, politisch motivierte Angriffe, wie wir sie zuletzt im Zusammenhang mit dem G8-Gipfel in Heiligendamm erlebt haben. Die Taterklärungen zeigen, dass es den Akteuren - es handelt sich ausschließlich um Linksextremisten - über eine Verunsicherung und Einschüchterung der Unternehmen und ihrer Beschäftigten hinaus, letztlich darum geht, die Grundstrukturen der freiheitlichen Ordnung zu treffen.

Im Vordergrund unseres diesjährigen Symposiums aber steht die Abwehr der Wirtschaftsspionage.

Seit jeher gehört die Wirtschaft neben der Politik und dem Militär zu den „klassischen“ Aufklärungszielen der Nachrichtendienste. Nicht zuletzt auch deshalb, weil eine funktionierende Ökonomie eine der Grundvoraussetzungen für die innere Stabilität von Staaten ist. Gerade im Zeitalter der Globalisierung und einer verschärften Konkurrenz auf dem Weltmarkt ist Wirtschaftsspionage und ihre Abwehr noch wichtiger geworden. Dies gilt in besonderem Maße für ein Land wie Deutschland, das seinen Reichtum nicht in erster Linie Rohstoffen verdankt, sondern den innovativen Fähigkeiten seiner Menschen und Unternehmen.

Das Interesse von Konkurrenten und Nachrichtendiensten gilt insbesondere Fertigungstechniken, Patenten sowie strategischen Planungen. Über den materiellen Schaden der durch einen so genannten „unfreundlichen Informationabfluss“, durch Know-how-Verlust entsteht, werden wir von Frau Professorin Merkel und Herrn Professor Kahle interessante empirische Daten erfahren.

Der Staat hat ein elementares Interesse daran, einen illegalen Wissenstransfer zu verhindern, technologisches und unternehmerisches Know-how zu schützen. Selbstverständlich kann der Staat einen umfassenden Schutz nicht gewährleisten. Wie andere Staaten die Gefahrenabwehr organisieren, werden wir von Herrn Juillet erfahren, dem „Beauftragten für ökonomische Intelligenz“ in Frankreich.

Im Rahmen der staatlichen Maßnahmen zum Schutz der Wirtschaft kommt der Spionageabwehr eine große Bedeutung zu. Sie gehört zu den Kernkompetenzen des Verfassungsschutzes. Die hier vorhandenen Erkenntnisse und Analysen politischer und militärischer Spionage - insbesondere bezüglich der modi operandi, der Vorgehensweise des Gegners - sind auch für die Abwehr der Wirtschaftsspionage von hohem Wert.

Wenngleich verfeinerte Methoden der Gegenseite die Abwehr illegaler Ausforschung im Wirtschaftsbereich erschweren, ist diese gleichwohl nicht aussichtslos. Das Internet spielt dabei eine herausgehobene Rolle. Und zwar nicht nur bei der Gewinnung offen verfügbarer Informationen, sondern auch im Zusammenhang mit neuartigen Angriffs- und Ausspähungstechniken. Ein wirkungsvoller Schutz gegen derartige Angriffe ist aufwendig. An Stelle eines wenig effizienten punktuellen Vorgehens gilt es auf der Basis methodischen Wissens ein ganzheitliches Schutzkonzept zu entwickeln, eine Kombination sorgfältig abgestufter und abgestimmter Entscheidungen personeller und materieller Art. Das Bundesamt für Verfassungsschutz steht dabei als koordinierende Zentralstelle für die Lagedarstellung und den gezielten Informationsrückfluss zur Verfügung.

Es sind mehrere Voraussetzungen, die für eine erfolgreiche Abwehr erfüllt sein müssen: Zum einen die Sensibilität gegenüber den Angriffsgefahren, des Weiteren Kenntnisse über Methoden und Ziele der Nachrichtendienste. Und schließlich gilt es, geeignete Schutzmaßnahmen zu entwickeln und umzusetzen.

Meine Damen und Herren, freuen Sie sich mit mir auf interessante Beiträge. Ich danke herzlich Herrn Werner Sonne, dass er als Moderator für das diesjährige Symposium des BfV zur Verfügung steht.

Prof. Dr. Wilma Merkel / Prof. Dr. Egbert Kahle, Leuphana Universität Lüneburg

Wettbewerb um Know-how – Schaden durch Know-how – Verlust

Dem Thema Schutz vor Know-how-Verlust, meistens als Business Intelligence (Synonyma: Corporate Intelligence und Competitive Intelligence) bezeichnet, ist angesichts zunehmender internationaler Konkurrenz[1] und datentechnischer Vernetzung[2] eine immer stärkere Bedeutung zuzuordnen. Die Konkurrenzanalyse (Competitive Intelligence) wird bereits seit PORTER als eine zentrale Aufgabe der strategischen Planung angesehen[3]. Die Gewinnung und der Schutz von Daten werden für eine erfolgreiche Unternehmenspolitik immer wichtiger, da die Wissensbasierung der Produkte und Prozesse mehr und mehr zum entscheidenden Wettbewerbsfaktor wird[4] (Rode 2001, Kahle 2001).

Die Kenntnis über die eigenen Wissensbestände und deren Gefährdungspotential (personal, organisatorisch, technisch) sowie die Gestaltung geeigneter Schutzmaßnahmen lässt sich auch als Strategisches Sicherheitsmanagement (Strategic Security Management) bezeichnen, wenn man die defensive Sichtweise des Problems betonen will; dabei ist auf die unterschiedliche inhaltliche Interpretation von Sicherheit (certainty, security, validity) hinzuweisen[5].

Bei der Frage des Wettbewerbs um Know-how oder um Wissen und wissensbasierte Produkte und Verfahren geht es um die Schaffung und Erhaltung von strategischen Wettbewerbsvorteilen; dabei ist der Begriff des Know-How weit zu interpretieren und umfasst auch das Know-What, Know-Who (Wissen, wer was weiß) und Know-Why. Unter den sich verschärfenden Marktbedingungen und der zunehmenden Geschwindigkeit technologischen Wandels sowohl in der Erstellung von Produkten und Dienstleistungen als auch in den Möglichkeiten ihrer Dokumentation werden nachhaltige strategische Wettbewerbsvorteile immer bedeutsamer. Strategische Wettbewerbsvorteile sind durch drei Kriterien zu beschreiben[6]:

1 Calori , R – Atamer, T. – Nunes, P., The dynamics of international competition – from practice to theory, London - Thousand Oaks – New Delhi 2000

2 Mocker, H. – Mocker, U., Intranet – Internet im betrieblichen Einsatz: Grundlagen, Umsetzung, Praxisbeispiele, Frechen-Königsdorf 1998; Schneier, B., Secrets and lies: digital security in a networked world, New York 2000

3 Porter M.E., Competitive Strategy – Techniques for Analyzing Industries and Competitors, New York 1980; Porter, M.E., Competitive Advantage Creating and sustaining competitive Advantage, New York 1985; Oster, S., Modern Competitive Analysis, 2.ed. York –Oxford 1994

4 Kahle, E., Betriebliche Entscheidungen, 6. Auflage München 2001; Rode, N., Wissensmarketing, Wiesbaden 2001

5 Kahle, E. Merkel, W., Fall- und Schadensanalyse bezüglich Know-How-/Informationsverlusten in Baden-Württemberg ab 1995, Lüneburg 2004, S, 3f.

6 Simon, H., Management strategischer Wettbewerbsvorteile, in: ZfB 58. Jg., 1988, S. 465

1. Sie müssen ein für den Kunden wichtiges Leistungsmerkmal betreffen
2. Der Vorteil muss vom Kunden tatsächlich wahrgenommen werden
3. Der Vorteil darf von der Konkurrenz nicht schnell einholbar sein, d.h. er muss eine gewisse Dauerhaftigkeit aufweisen

Die gleichzeitige Erfüllung der drei Kriterien „wichtig", „wahrgenommen" und „dauerhaft" bildet eine hohe Messlatte. Zur Einschätzung des eigenen Vorteils ist die Konkurrenzanalyse bedeutsam, in der eine Reihe von Faktoren oder Merkmale zu betrachten sind[7]:

- Gesamtstrategie
- Produktqualität
- Preise und Konditionen
- Vertrieb, Außendienst
- Segment, Positionierung, Image
- F & E Strategie
- Kostensituation
- Produkttechnologie
- Personen im Management
- Prozesstechnologie
- Finanzkraft

Diese Faktoren, die als Quellen von Wettbewerbsvorteilen und damit als Erfolgsfaktoren[8] angesehen werden können und die sich auf verschiedene Glieder der Wertschöpfungskette[9] beziehen können, sind vielfältig und werden auf unterschiedliche Weise beschrieben und abgegrenzt. Ebenso sind bezüglich der Formen der Entstehung von Wettbewerbsvorteilen im Rahmen der Wettbewerbsstrategie und der daran Beteiligten erhebliche Unterschiede zu erkennen[10], die wenigstens teilweise unternehmensgrößenspezifisch sind, d.h. bei KMU anders aussehen als bei großen Unternehmen. Wettbewerbsvorteile basieren auf Wissen, das über die weiteren

7 ders. a.a.O., S.467

8 vgl. Welge, M. K. , - AL-Laham, A., Strategisches Management, 4. Auflage, Wiesbaden 2003, S. 127, 231, 238, 536 ff.; etwas anders: Haake, K., Strategisches Verhalten in europäischen Klein- und Mittelunternehmen, Berlin – München – St. Gallen 1987, S. 188f.

9 vgl. Porter, M.E., Wettbewerbsvorteile: Spitzenleistungen erreichen und behaupten, 2. Auflage, Frankfurt/M. – New York 1989, S. 59 ff.

10 vgl. Welter, F., Strategie, KMU und Umfeld, Handlungsmuster und Strategiegenese in kleinen und mittleren Unternehmen, Berlin 2003, 89 ff., 159, 209;

Stufen „Können", „Handeln" und „Kompetenz"[11] zur Wettbewerbsfähigkeit führt[12] und auf organisatorischer Ebene auch auf Vertrauen[13], was gegebenenfalls noch näher zu erläutern ist.

Einmal gewonnene Wettbewerbsvorteile können auf verschiedene Weise gehalten werden oder verloren gehen; letzteres kann unbeabsichtigt oder durch andere beabsichtigt geschehen[14]: Wenn durch das Handeln anderer Wissen oder Informationen verloren gehen, wird das im Nachfolgenden umfassend als unfreundlicher Informationsabfluss bezeichnet[15].

Im Zuge einer Untersuchung[16] zu den Wegen und Folgen unfreundlichen Informationsabflusses und den Möglichkeiten seiner Eindämmung durch verschiedene Sicherheitsmaßnahmen wurde eine empirische Erhebung in Baden-Württemberg durchgeführt, bei der etwas mehr als 2000 zufällig ausgewählte Industrieunternehmen mit einem umfangreichen Fragebogen befragt wurden, der auf einer vorangegangenen Fall- und Schadensanalyse ausgewählter Fälle konkreten unfreundlichen Informationsabflusses entwickelt wurde. Es gab 431 Antworten, die als eine hinreichende empirische Grundlage für eine gesicherte Hochrechnung des Schadenspotentials angesehen werden können. Es ergab sich ein Gesamtumsatzvolumen der befragten Unternehmen von knapp 30 Mrd. €, was etwa 10 % des Bruttoinlandsprodukts des Landes Baden-Württemberg entspricht; mit dem Multiplikator 10 kann man die Befunde auf dieses Land hochrechnen und mit dem weiteren Multiplikator 7 von dort auf die Bundesrepublik Deutschland. Der Umfang der gefährdeten Wettbewerbsvorteile belief sich für die befragten Unternehmen auf etwa 700 Mio. €, damit für Baden-Württemberg auf 7 Mrd. € und für die Bundesrepublik auf rund 50 Mrd. €. Die aufgetretenen Schäden – bei insgesamt 190 der 400 befragten Firmen – beliefen sich auf 52 Mio. €; hochgerechnet auf die 400 sind das 110 Mio. €. Die tatsächlichen Schäden betragen demnach für Baden-Württemberg ca. 1 Mrd. € und für die Bundesrepublik ca. 7 bis 8 Mrd. €. Demgegenüber wird für Schutzmaßnahmen nur etwa ein Drittel der Schadenssumme ausgegeben; bezogen auf die Gefährdungssumme ist das weniger als 5 %. Eine aktuelle Erhebung zur Wirtschaftskriminalität[17] beziffert den Schaden pro Fall Industriespionage einschließlich Produktpiraterie auf etwa 240.000 €.

Für die Einschätzung der Schadensproblematik war es auch bedeutsam, wie der Wettbewerbsvorteil entstanden war, ob und wie er gefährdet war und

11 zu organisationalen Kompetenzen und insbesonders zu organisationalen Metakompetenzen vgl. Bouncken, R.B., Organisationale Metakompetenzen, Wiesbaden 2003
12 vgl. Die Wissenstreppe von North, K., Wissensorientierte Unternehmensführung, 4. Aufl. Wiesbaden 2002, S. 39
13 vgl. Staehle, W.H., Management, 8. Auflage, München 1999, S. 409
14 vgl. Kahle, E., Security-Management unter HR- und Organisationsaspekten, in: Personalführung 5/2002, S. 29
15 Kahle, E. – Merkel, W., Fall- und Schadensanalyse bezüglich Know-how-/ Informationsverlusten in Baden-Württemberg ab 1995, uv. Manuskript, Lüneburg 2004, S.25
16 dies. a.a.O.
17 Bussmann, K.D. – Nestler C. – Salvenmoser, St., Wirtschaftskriminalität 2007, Frankfurt/Main – Halle/Saale 2007, S. 18

welche Sicherungsmaßnahmen getroffen wurden. Hierzu wurden auch die relative Marktstellung (Monopol, Oligopol, Polypol) (lokal, regional, überregional) und die Unternehmensgröße erhoben, wobei die Mehrzahl der Angaben auf Einzel- und Kleinserienfertigung in oligopolistischen oder polypolistischen Märkten hinweist und eine nationale oder internationale Marktstellung innehat. Die Unternehmensgröße wurde über den Jahresumsatz differenziert (unter 2 Mio €, 2 –10 Mio €, 10 – 50 Mio €, 50- 200 Mio €, 200 – 500 Mio € und über 500 Mio €). Die Auswertung der Befunde ergab – entgegen den bisherigen üblichen Größenabgrenzungen[18] – einen deutlichen Unterschied bei vielen Aspekten an der 50 Mio € Grenze. Dies wäre ein erster Ansatz zu einer Neudefinition der Größengrenzen für KMU, die bei Industrieunternehmen herkömmlich bei 20 Mio DM, d.h. 10 Mio €[19] angesetzt wurde und die nun auf das Fünffache anzuheben wäre. Das entspräche dann auch eher dem EU-Standard, der die Grenze bei 40 Mio € zieht[20]. Als Ursache sind dabei einerseits inflationäre Wirkungen im Verlauf der letzten 30 Jahre und andererseits Produktivitätssteigerungen in diesem Zeitraum anzusehen.

Welche ungefähren Aufwendungen haben Sie für die Erstellung bzw. Erarbeitung des Wettbewerbsvorteils/-vorsprungs gehabt?

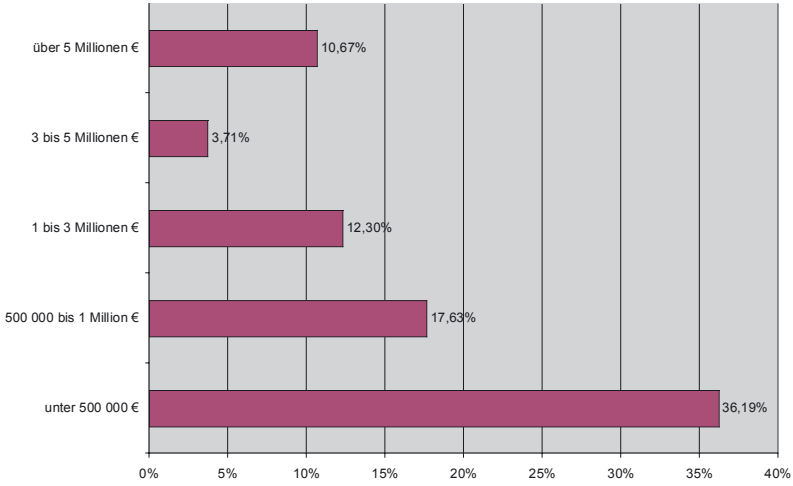


Abbildung: Verteilung der Aufwendungen für Wettbewerbsvorteile nach Umsatz der Firmen

18 vgl. Haake, K., Strategisches ..., a.a.O., S. 14; Kahle,E., Organisation der Mittelständischen Unternehmung, in: Frese, E. (Hrsg.) Handwörterbuch der Organisation, 1992, Sp 1409

19 Mugler, J., Betriebswirtschaftslehre der Klein- und Mittelbetriebe, 2. Auflage, Wien – New York 1995, S. 30

20 Pichler, J.H.- Pleitner, H.J. – Schmidt, K.H., Management in KMU, 3. Auflage, Bern – Stuttgart – Wien 2000, S. 13

Bei der Art des Wettbewerbsvorteils wurde eine größere Zahl von Möglichkeiten abgefragt, deren Auswahl und Beschreibung sich aus einer Vorstudie von acht Fällen ergab. In dieser Vorstudie wurden ausführliche Interviews mit Leitungspersonen in Unternehmen durchgeführt, die von unfreundlichem Informationsabfluss betroffen waren und die in freier Form über den Gesamtkomplex der Gefährdung von Wettbewerbsvorteilen einschließlich ihrer Entstehung erzählen sollten und erzählt haben. Es ergaben sich folgende Wettbewerbsvorteile mit

Mehrfachnennungen:

- Überlegene Produkte
- Neue Produkte
- Beherrschung spezifischer Produktionsprozesse/Arbeitsmethoden
- Maschinenausstattung
- Mitarbeiterstamm
- Kundenstamm/Kundenbeziehung
- Lieferantenbeziehungen
- Vertriebssystem
- Kooperationen/Netzwerke
- Forschungspotenzial/-ergebnisse
- Organisatorische Vorteile
- Unternehmenskultur/Betriebsklima
- Strategie

Eine größenabhängige Korrelationsrechnung zeigte, dass überlegene Produkte, neue Produkte, die Beherrschung spezifischer Produktionsprozesse oder Arbeitsmethoden, besondere Vertriebsvorteile, Forschungspotenzial und Strategie bei den großen Unternehmen stärker vertreten sind, während Mitarbeiterstamm, Kooperationen und Netzwerke sowie Unternehmenskultur und Betriebsklima ebenso deutlich den kleineren Unternehmen zuzurechnen sind. Die Analysen zeigten aber auch deutlich, dass Vertriebsformen und Forschungspotenzial insgesamt weniger bedeutend für den Wettbewerbsvorteil sind als Mitarbeiterstamm (Platz 1), die Be-

herrschung spezifischer Verfahren (Platz 2) und überlegene und neue Produkte (fast gleichauf auf Platz 3).

In einem weiteren Schritt wurde erhoben, wie die Wettbewerbsvorteile entstanden waren. Hier hatten sich folgende Möglichkeiten in der Vorerhebung ergeben:

- Idee einer Person
- Gemeinsame Idee mehrerer Personen in der Unternehmung (Team)
- Gemeinsame Idee mit Kunden/Kooperation mit Kunden
- Entwurf/Projektbearbeitung einer oder mehrerer Abteilungen
- Gewachsen aus dauerhafter Zusammenarbeit
- Gewachsen durch strategische Investition in innovative Geschäftsfelder
- Fremdforschung/Fremdentwicklung
- Marktbeobachtung

Insgesamt zeigte sich ein deutliches Vorherrschen der Entstehung von Wettbewerbsvorteilen durch die gemeinsame Arbeit mehrerer Personen und durch dauerhafte Zusammenarbeit mit Kunden oder Kooperationspartnern; in der Größensicht sind die größeren Unternehmen stärker in der gemeinsamen Ideenfindung im Unternehmen, während die kleineren stärker von der Zusammenarbeit profitieren. Bei diesen ist auch die Ideenfindung durch einen Einzelnen stärker, wenn auch nicht so stark ausgeprägt. Strategische Investitionen und Marktbeobachtung werden deutlich mehr von größeren Unternehmen genutzt, ebenfalls die Projektarbeit, die in den kleineren Unternehmen fast unbedeutend ist.

Da viele Wettbewerbsvorteile aus Kooperationsbeziehungen entstehen und es andererseits das Problem des Opportunismus in solchen Beziehungen gibt, das in „Learning Races“ [21] gipfeln kann, war es bedeutsam, die Kooperationsbeziehungen näher zu betrachten. Hier hatten sich in der Vorerhebung Hinweise auf unterschiedliche Absicherungsmöglichkeiten in Kooperationsbeziehungen ergeben:

21 vgl. Bouncken, R.B., Determinanten, Möglichkeiten und Konsequenzen für Lernprozesse in Netzwerken kleinerer und mittlerer New Media Unternehmen, in: Jahrbuch für KMU-Forschung, S. 11; Gulati, R. – Nohiria, N. – Zaheer, A., Strategic Networks, in : Strategic Management Journal, 21. Jg. Nr. 3, 2000, S. 203 – 215, hier S. 211

- Kooperationsvertrag
- Wechselseitige Kapitalbeteiligung
- Klare Absprachen über Informations- und Verwertungsrechte
- Überprüfung der jeweiligen Leistungsbeiträge
- Regelmäßige Abstimmungen über Arbeitsfortschritte und eventuelle Probleme
- Den Partnern werden eigene Sicherheitsstandards vorgegeben
- Durchführung von Sicherheitsaudits

Von diesen war nur die regelmäßige Überprüfung der jeweiligen Leistungsbeiträge nicht größenerheblich; für alle anderen Maßnahmen gab es größenabhängige Unterschiede, allerdings auf sehr unterschiedlichen absoluten Niveau.

Während Kooperationsverträge bei fast zwei Drittel aller Befragten vorlagen, gab es eigene Sicherheitsvorgaben oder Sicherheitsaudits nur bei 3 bzw. 1 Prozent. Für den allgemeinen Schutz von Wettbewerbsvorteilen waren in der Vorerhebung eine Reihe von Faktoren genannt worden, die von der fehlenden Notwendigkeit eines Schutzes bis zu verschiedenen konkreten Maßnahmen reichten. Es wurden genannt:

- Wettbewerbsvorteil ist nicht imitierbar und erodiert nicht
- ...ist imitierbar (muss stets durch Innovationen verteidigt werden)
- ...ist rekonstruierbar (leicht nachahmbar)
- Geschützt durch nationales Patent
- Geschützt durch internationales Patent
- Geschützt durch Umgehungspatente
- Geschützt durch Gebrauchsmuster
- Nicht geschützt
- Nachahmung setzt erhebliche spezifische Investitionen voraus
- Nachahmung nützt nicht, da keine weiteren Kunden vorhanden

- Vorteil liegt in der Unternehmensorganisation (Arbeitsteilung, Struktur)
- Vorteil liegt in der Unternehmenskultur (Werte, Identifikation, Betriebsklima)
- Es gibt spezielle Sicherheitsmaßnahmen

Von diesen Einflussgrößen waren drei, nämlich „Nützt nichts, da keine weiteren Kunden", „der Vorteil liegt in der Organisation" und „es gibt spezielle Sicherheitsmaßnahmen", nicht größenabhängig.

Es wurde sichtbar, dass ausschließlich kleine und mittlere Unternehmen – wenn auch nur in geringer Zahl – Wettbewerbsvorteile besitzen, die überhaupt nicht imitierbar sind und dass sie in vielen Fällen rekonstruierbare Vorteile haben, deutlich mehr als die großen Unternehmen; bei diesen überwiegen stattdessen die imitierbaren Vorteile, die immer wieder durch Innovationen neu gewonnen werden müssen, d.h. man versucht und muss versuchen, dem Wettbewerb immer einen Schritt voraus zu sein. Patentschutz ist bei den kleinen Unternehmen deutlich weniger zu finden als bei den großen; die Patentanmeldung ist nach Aussagen aus der Vorerhebung vielen zu teuer. Umgehungspatente, d.h. die Absicherung von anderen Lösungswegen als dem eigentlich eingesetzten, um die eigene Lösung vor Alternativen zu schützen, sind in KMU überhaupt nicht im Einsatz und eventuell sogar unbekannt. Entsprechend diesen Befunden sind auch Gebrauchsmuster als die einfachere und billigere Form des Schutzes bei KMU weniger eingesetzt und dementsprechend ist dann das Fehlen von solchen Sicherungsmaßnahmen deutlich stärker verbreitet. Der Schutz vor Nachahmung dadurch, dass spezifische Investitionen für die Fertigung getätigt werden müssen, ist auch bei großen Unternehmen stärker ausgeprägt als bei kleinen, aber nicht so stark wie die anderen Einflussgrößen. Dafür ist der Schutz der Wettbewerbsvorteile durch eine starke Unternehmenskultur bei KMUs größer.

Bezüglich der Schadensbearbeitung und der Kooperation mit den Sicherheitsbehörden haben sich ebenfalls erhebliche Schwächen und Defizite gezeigt. In knapp der Hälfte aller Fälle erfolgte überhaupt keine inhaltliche Bearbeitung des Schadensfalls und nur in 8 % der Fälle wurden externe Sicherheitsberater oder Sicherheitsbehörden hinzugezogen. Die Einschätzung der Arbeit der Sicherheitsbehörden und die Kooperation mit ihnen zeigt deutlichen Handlungsbedarf:

Knapp der Hälfte der Befragten ist die Arbeit der Sicherheitsbehörden nicht

bekannt und sie hält sie für unnötig. 13 % kennen diese Arbeit nicht, würden sie aber ihrer Auffassung nach benötigen; nur in knapp 10 % der Fälle sind die richtigen Ansprechpartner bei den Sicherheitsbehörden bekannt, in weniger als der Hälfte davon bestehen regelmäßige Arbeitskontakte. Ganze 2 % der Befragten haben ein umfassendes, mit den Sicherheitsbehörden abgestimmtes Sicherheitskonzept. Weitere Schwächen werden in der Wirksamkeit der Sicherheitsbehörden (3 %) und in unklaren Zuständigkeitsregelungen (2%) gesehen; der wettbewerbsrechtliche und arbeitsrechtliche Schutz wird als zu schwach angesehen. Alle diese Schwächen sind bei KMU stärker ausgeprägt als bei großen Unternehmen.

Zusammenfassend lassen sich diese Befunde wie folgt einordnen und interpretieren:

- Kleine und mittlere Unternehmen leiten ihre Wettbewerbsvorteile aus „soft skills“ ab; für sie sind Mitarbeiterstamm, Kooperationen in Netzwerkform und Unternehmenskultur besonders wichtig. Letztlich sind das alles Faktoren, in denen Vertrauen [22] eine besondere Rolle spielt.
- Die Entstehung von Wettbewerbsvorteilen ist bei KMU’s eher personenbezogen. KMU’s sehen die Schutzbedürftigkeit ihrer Wettbewerbsvorteile weniger deutlich und tun weniger zu deren Schutz bzw. können nicht so viel tun.
- KMU’s haben größeren Informationsbedarf zu den Schutzmöglichkeiten allgemeiner Art und durch die Sicherheitsbehörden.

Literatur:

Bouncken, R.B., Determinanten, Möglichkeiten und Konsequenzen für Lernprozesse in Netzwerken kleinerer und mittlerer New Media Unternehmen, in: Meyer, A. (Hrsg.), New Economy im Kontext kleinerer und mittlerer Unternehmen, Jahrbuch für KMU-Forschung, 2002, S. 1-21

Bouncken, R. B., Organisationale Metakompetenzen – Theorie, Wirkungszusammenhänge, Ausprägungsformen und Identifikation, Wiesbaden 2003

Bouncken, R.B., (Hrsg.), Management von KMU und Gründungsunternehmen, Wiesbaden 2003

22 vgl. Kahle, E., Vertrauensbasierte Netzwerke als Chancen für kleine und mittlere Unternehmen, in: Pleitner, H.J. (ed.), Beiträge zu den Rencontres 1998, St. Gallen 1998, S. 535-544; Kahle, E.,Voraussetzungen und Möglichkeiten organisationalen Lernens aus kognitionswissenschaftlicher Sicht, in: Schwaninger, M: (Hrsg.), Intelligente Organisationen - Konzepte für turbulente Zeiten auf der Grundlage von Systemtheorie und Kybernetik, Berlin 1999, S. 103 –118; Kahle, E., Vertrauen als Voraussetzung für bestimmte Formen des Wandels, in: Brauchlin, E. – Pichler, J.H. (hrsg.),Unternehmer und Unternehmensperspektiven für Klein- und Mittelunternehmen, Berlin – St. Gallen 2000, S. 535 – 546; Welter, F. – Höhmann, H.H. et al., Vertrauensbeziehungen in KMU, RWI Materialien Heft 10, Essen 2004

Bussmann, K.D. – Nestler C. – Salvenmoser, St., Wirtschaftskriminalität 2007, Frankfurt/Main – Halle/Saale 2007

Calori, R – Atamer, T. – Nunes, P., The dynamics of international competition – from practice to theory, London - Thousand Oaks – New Delhi 2000

Gulati, R. – Nohiria, N. – Zaheer, A., Strategic Networks, in : Strategic Management Journal, 21. Jg. Nr. 3, 2000, S. 203 – 215

Haake, K., Strategisches Verhalten in europäischen Klein- und Mittelunternehmen, Berlin – München – St. Gallen, 1987

Kahle, Organisation der Mittelständischen Unternehmung, in: Frese, E. (Hrsg.) Handwörterbuch der Organisation, 1992, Sp. 1408 – 1419

Kahle, E., Vertrauensbasierte Netzwerke als Chancen für kleine und mittlere Unternehmen, in: Pleitner, H.J. (ed.), Beiträge zu den Rencontres 1998, St. Gallen 1998, S. 535-544

Kahle, E.,Voraussetzungen und Möglichkeiten organisationalen Lernens aus kognitionswissenschaftlicher Sicht, in: Schwaninger, M: (Hrsg.), Intelligente Organisationen - Konzepte für turbulente Zeiten auf der Grundlage von Systemtheorie und Kybernetik, Berlin 1999, S. 103 –118

Kahle, E., Vertrauen als Voraussetzung für bestimmte Formen des Wandels, in: Brauchlin, E. – Pichler, J.H. (hrsg.), Unternehmer und Unternehmensperspektiven für Klein- und Mittelunternehmen, Berlin – St. Gallen 2000, S. 535 – 546

Kahle, E., Betriebliche Entscheidungen, 6. Auflage München 2001

Kahle, E., Security-Management unter HR- und Organisationsaspekten, in: Personalführung 5/2002, S. 22 – 31

Kahle, E. – Merkel, W., Fall- und Schadensanalyse bezüglich Know- How/Informationsverlusten in Baden-Württemberg ab 1995, Lüneburg 2004

Kahle, E. Unterschiede in der Entstehung und Sicherung von Wettbewerbsvorteilen bei KMU und großen Unternehmen, in: Füglistaller, U. – Volery, Th. – Weber, W. (Hrsg.), Value Creation in Entrepreneurship and SMEs – Wertgenerierung durch Unternehmertum und KMU, Rencontres de St. Gall, St. Gallen 2004

Mocker, H. – Mocker, U., Intranet – Internet im betrieblichen Einsatz: Grundlagen, Umsetzung, Praxisbeispiele, Frechen-Königsdorf 1998

Mugler, J., Betriebswirtschaftslehre der Klein- und Mittelbetriebe, 2. Auflage, Wien – New York,1995

North, K., Wissensorientierte Unternehmensführung, 4. Aufl. Wiesbaden 2002

Oster, S., Modern Competitive Analysis, 2.ed. York –Oxford 1994

Pichler, J.H. – Pleitner, H.J. – Schmidt, K.H., Management in KMU, Die Führung von Klein- und Mittelunternehmen, 3. Auflage, Bern – Stuttgart – Wien 2000

Porter, M.E., Competitive Strategy – Techniques for Analyzing Industries and Competitors, New York 1980

Porter, M.E., Competitive Advantage: Creating and sustaining competitive Advantage, New York 1985

Porter, M.E., Wettbewerbsvorteile: Spitzenleistungen erreichen und behaupten, 2. Auflage, Frankfurt/M. – New York 1989

Rode, N., Wissensmarketing, Wiesbaden 2001

Schneier, B., Secrets and lies: digital security in a networked world, New York 2000

Simon, H., Management strategischer Wettbewerbsvorteile, in: ZfB 58. Jg., 1988,S. 461 – 480

Staehle, W.H., Management, 8. Auflage, München 1999

Welge, M. K. , - AL-Laham, A., Strategisches Management, 4. Auflage, Wiesbaden 2003

Welter, F., Strategie, KMU und Umfeld, Handlungsmuster und Strategiegenese in kleinen und mittleren Unternehmen, Berlin 2003

Welter, F. – Höhmann, H.H. et al., Vertrauensbeziehungen in KMU, RWI Materialien Heft 10, Essen 2004

Frank Sassenscheidt-Grote, Bundesamt für Verfassungsschutz

„Globalisierung im Fokus politischer Extremisten“

Bedrohung der Wirtschaft durch Linksextremisten

Auf den ersten Blick mag das Thema, „Globalisierung im Fokus politischer Extremisten“ eine vergleichende Darstellung erwarten lassen hinsichtlich der jeweiligen spezifischen Globalisierungskritik, wie sie in den verschiedenen extremistischen Phänomenbereichen zu finden ist – dass also ideologische und aktionistische Unterschiede wie Gemeinsamkeiten von Rechtsextremisten, Linksextremisten, Ausländerextremisten und Islamisten herausarbeitet und analysiert werden. Dies würde sich allerdings in weiten Teilen mit Vorträgen beim BfV-Symposium 2002 überschneiden.

Statt dessen wird sich dieser Vortrag stärker auf das Oberthema der Veranstaltung fokussieren und folglich der Frage nachgehen, inwieweit bzw. welche Bedrohung der Wirtschaft von globalisierungskritischen Extremisten ausgeht.

Diese Frage ist auch deshalb gerade in diesem Jahr besonders interessant, weil sich in 2007 die Bedrohung der deutschen Wirtschaft durch globalisierungskritische Extremisten in ganz besonderer Weise manifestierte. Der Grund lag bzw. liegt im diesjährigen deutschen G8-Vorsitz sowie der deutschen EU-Ratspräsidentschaft in der ersten Jahreshälfte, was bedeutet, dass unter deutscher Führung zwei politische Bündnisse berieten und Entscheidungen trafen, die auch aus globalisierungskritischer Sicht kaum bedeutender sein könnten. Wer folglich in Deutschland Globalisierungskritik äußern wollte oder will – egal auf welche Weise und mit welcher Zielsetzung – der hatte dafür in 2007 hinreichend Gelegenheit, und der hatte als ganz speziellen Anlass den G8-Gipfel im mecklenburgischen Heiligendamm im Sommer dieses Jahres.

Bereits bei der Betrachtung der Protestmobilisierung und der dann auch tatsächlich durchgeführten Protestaktionen ist erkennbar, dass – soweit man ausschließlich die Beteiligung von Extremisten berücksichtigt – der weit überwiegende Teil dem linksextremistischen Lager zuzuordnen ist. Rechtsextremisten, und hier insbesondere die NPD, versuchten zwar, das Thema über die Medien propagandistisch für sich auszuschlachten. Was ihr tatsächliches Aktionspotenzial betrifft, stellten sie jedoch eher eine Marginalie dar. Für Islamisten waren – zum Glück – der G8-Vorsitz und der G8-Gipfel gar kein Thema. Und auch die sonstigen ausländerextremisti-

schen Gruppierungen agierten nicht eigenständig, sondern – wenn überhaupt – dann im Verbund mit ihren deutschen linksextremistischen Gesinnungsgenossen.

Bei der speziellen Fokussierung auf gegen die Wirtschaft gerichteten Aktionen stellt man dann schnell fest, dass hier eine konkrete Bedrohung derzeit ausschließlich von Linksextremisten ausgeht. D.h. die Propagierung von militanten Aktionen gegen die Wirtschaft oder gar deren Umsetzung findet in Deutschland lediglich im Linksextremismus statt – dafür dort allerdings umso deutlicher und handfester.

Linksextremistisches Personenpotenzial

Eingangs soll das linksextremistische Bedrohungspotential mit einigen wenigen Zahlen verdeutlicht werden. Das erscheint auch deshalb angebracht, weil die entsprechenden Daten zum Linksextremismus bisweilen in der öffentlichen Wahrnehmung etwas untergehen.

An gewaltbereiten Linksextremisten – und die sind ja in diesem Zusammenhang von besonderem Interesse – zählten die Verfassungsschutzbehörden in 2006 bundesweit ca. 6.000, nach ca. 5.500 in den Vorjahren. Der weit überwiegende Teil davon sind sog. „Autonome".

Ein Blick in die Statistik „PMK-links", also die vom BKA erhobenen Zahlen zur „politisch motivierten Kriminalität – links" zeigt für das Jahr 2006

- insgesamt 2.369 Straftaten, davon
- 862 Gewalttaten – das ist deutlich mehr als ein Drittel, wobei
- von diesen 862 Gewalttaten mehr als die Hälfte, nämlich 444, Körperverletzungen waren.

Dies sind absolut betrachtet schon recht bemerkenswerte Größenordnungen, die insofern auf ein nicht unbeträchtliches Gewaltpotenzial hindeuten.

Vergleicht man diese Zahlen noch mit denen der Vorjahre, stellt man fest, dass seit 2004 nahezu jede dieser Kategorien eine Steigerung aufweist, die teilweise zwischen etwa 30 und 50 % liegt. Auch dies ist durchaus bemerkenswert.

Wirtschaftsunternehmen als Feindbild

Bevor an konkreten Beispielen die Bedrohung der Wirtschaft bzw. von Wirtschaftsunternehmen durch Linksextremisten dargestellt wird, soll

kurz auf deren ideologisch-politischen Hintergrund eingegangen werden, d.h. auf die Frage, warum generell Wirtschaftsunternehmen ein Feindbild für Linksextremisten darstellen bzw. warum speziell Wirtschaftsunternehmen im Visier gewaltbereiter Linksextremisten stehen.

Wirtschaftsunternehmen sind Teil des kapitalistischen Systems. Sie sind sogar elementarer Bestandteil, sie sind - aus linksextremistischer Sicht - das Aushängeschild des Systems, quasi „Manifestationen des Bösen", d.h. eines Systems, das es zu bekämpfen und zu überwinden gilt.

Aus dieser Rolle bzw. Funktion messen Linksextremisten Wirtschaftsunternehmen natürlich eine Mitverantwortung zu für sämtliche sozialen Missstände und politischen Fehlentwicklungen. Diese Mitverantwortung gilt für jedes einzelne kapitalistische Unternehmen genauso wie für die Wirtschaft insgesamt. Diese Mitverantwortung gilt aber auch und insbesondere für handelnde Personen in diesen Unternehmen und speziell für dort führend handelnde Personen.

Der Vorwurf lautet folglich, dass es Wirtschaftsunternehmen ausschließlich darum gehe, ihre Gewinne zu maximieren und ihren wirtschaftlichen und politischen Einfluss zu sichern. Dafür würden – nach linksextremistischer Lesart – zum einen Menschen unterdrückt und ausgebeutet und zum anderen Natur und Umwelt beschädigt oder sogar nachhaltig zerstört.

Das könnte man jetzt natürlich noch ausführen – sowohl in die Tiefe als auch in die Breite – ist aber an dieser Stelle nicht notwendig. Diese kurze und knappe Zusammenfassung muss für einen groben Einblick ausreichen.

Gefährdete Wirtschaftsbereiche

Wenn man statt dessen versucht, diese allgemeine und etwas abstrakte Gefährdungsbeschreibung ein wenig zu konkretisieren, ist es ein recht sinnvoller Ansatz, nach Unternehmensbereichen zu unterscheiden und besonders gefährdete Unternehmensbereiche zu identifizieren. Eine solche Identifikation kann man am besten vornehmen mit Hilfe der „klassischen" Themen linksextremistischer Agitation und Aktion.

„Unterstützer des Faschismus"

Der „antifaschistische Kampf" ist und bleibt das linksextremistische Aktionsfeld Nummer 1. Besonders gefährdet sind folglich Unternehmen, die aus linksextremistischer Sicht dieses kapitalismusimmanente Übel des Faschismus unterstützen.

Dies sind in erster Linie

- Transport- und Reiseunternehmen, die (vermeintliche) Rechtsextremisten zu Veranstaltungen fahren (vor einigen Jahren Fa. Ruperti in Berlin)
- Betriebe aus dem Hotel- und Gaststättengewerbe, die diesen Personen oder Vereinigungen Räume für Veranstaltungen zur Verfügung stellen
- sowie Militaria-Händler.

„Profiteure der Asylpolitik"

Hier geht es also um das linksextremistische Aktionsfeld „Antirassismus". Besonders betroffen sind in diesem Bereich

- Unternehmen, die mit der Unterbringung, Versorgung und Rückführung von Asylbewerbern beauftragt sind, wie Hotelketten (ACCOR, SORAT), Fluggesellschaften (Lufthansa, LTU), Lebensmittellieferanten (Fa. Dussmann in Berlin) oder auch Betreiber von Unterbringungsheimen wie das DRK oder die AWO
- Es sind weiterhin im Fokus private Wach- und Sicherheitsdienste von sog. Abschiebehaftanstalten oder „Abschiebe"-Flughäfen selbst
- sowie am Chipkartensystem zur Versorgung von Flüchtlingen beteiligte Firmen (Fa. Sodexho).

„Profiteure des Sozialabbaus"

Hier stehen primär im Fokus Unternehmen oder Einrichtungen, die aus Sicht von Linksextremisten besonders

- von den Sozialreformen
- oder der zunehmenden Deregulierung des Arbeitsmarktes

profitieren. Stichworte sind hier insbesondere Hartz IV und 1-Euro-Jobs. Konkret betroffen bzw. in Taterklärungen exemplarisch genannt werden dabei beispielsweise die Discounter LIDL und Schlecker, die angeblich Billigjobber einstellen, keine Betriebsräte dulden u.ä.m., aber auch Zeitarbeitsfirmen, Wohlfahrtsverbände wie AWO und DRK oder bestimmte Um-

zugsunternehmen, die von Zwangsräumungen im Zusammenhang mit Hartz IV profitieren.

„Profiteure der Globalisierung"

Hier wird nun sozusagen die internationale Dimension des Sozialabbaus thematisiert. D.h. es geht um Unternehmen, die von der Globalisierung profitieren, etwa durch Verlagerung von Fertigungsprozessen in Billiglohnländer.

Tatsächliche oder potenzielle Anschlagsziele waren bzw. sind Firmen wie Tchibo, Adidas, KarstadtQuelle, H&M, C&A oder der Otto-Versand. Der Vorwurf ist, dass diese Unternehmen Kleidung von Billignäherinnen beispielsweise in Bangladesh oder Kolumbien produzieren lassen, dort also Menschen ausbeuten und hier Arbeitsplätze vernichten.

Im „Atomgeschäft" tätige Unternehmen

Die Atombranche gehört seit Jahren zu den bevorzugten Zielen militanter Linksextremisten. Betroffen sind hier regelmäßig Firmen und Einrichtungen, die in den Bereichen

- Nutzung von Kernenergie oder
- Lagerung und Transport von Atommüll tätig sind.

Das waren bzw. sind vor allem die Deutsche Bahn AG und SIEMENS oder aber Energieversorger wie z.B. Vattenfall.

An Projekten zur „Umstrukturierung" beteiligte Unternehmen

Hier geht es hauptsächlich um Firmen und Banken bzw. Investoren, die in Großstädten und Ballungszentren an Projekten zur Stadtsanierung und Strukturverbesserung beteiligt sind. Das neudeutsche Stichwort ist hier „Gentrifizierung" bzw. die Kritik daran. Damit wird bezeichnet die Umwandlung ehemaliger alternativer Stadtteile oder auch sogenannter Kieze in Yuppie- und Schicki-Micki-Viertel mit teuren Altbauwohnungen, Rechtsanwaltskanzleien und Werbeagenturen. Die linksextremistischen Aktionsschwerpunkte liegen derzeit in Berlin und insbesondere in Hamburg, wo es in den letzten Jahren z.B. um das sog. Schanzenparkhotel am Wasserturm ging. Folglich waren oder sind besonders die Fa. Mövenpick als Betreiber und die mit der Projektrealisierung beauftragte Patricia Immobilien AG im Visier, aber auch beteiligte Baufirmen.

Im Bereich der Bio- und Gentechnologie tätige Unternehmen und Einrichtungen

Die Bio- und Gentechnologie ist ebenfalls ein in der militanten linksextremistischen Praxis immer wieder bedientes Aktionsfeld. Anschlagsziele sind insbesondere Freilandversuchsanlagen oder aber Unternehmen wie die Bayer AG, Monsanto und Syngenta als große US-Agrarfirmen oder die deutsche Fa. Märka.

Rüstungsbetriebe und deren Zulieferer

Und schließlich noch ein weiteres klassisches linksextremistisches Aktionsfeld, der „Antimilitarismus". In diesem Bereich sind in der Vergangenheit u. a. betroffen gewesen Mercedes-Benz bzw. EADS, Krauss-Maffei oder Hako MultiCar in Bad Oldesloe.

G8-Gipfel als Symbol des Neoliberalismus

Es kann keinen ernsthaft überraschen, dass gerade Treffen der acht wichtigsten und stärksten Wirtschaftsnationen der Welt in ganz besonderer Weise von Linksextremisten kritisch betrachtet werden. Für Linksextremisten handelt es sich dabei um ein Gipfeltreffen selbsternannter Eliten, die über das Schicksal der Welt und das von Milliarden von Menschen bestimmen und entscheiden,

- ohne dafür demokratisch legitimiert zu sein,
- ohne, dass der größte Teil der Weltbevölkerung repräsentiert wäre und ein Mitspracherecht hätte
- und mit dem ausschließlichen Ziel der Sicherung oder gar Vermehrung des eigenen Wohlstands auf Kosten der Armen und Unterdrückten in der Dritten Welt.

Der jährliche G8-Gipfel ist somit für sie ein Symbol des weltweiten Neoliberalismus, der „Macht des globalen Kapitalismus" und dessen „politischer und militärischer Gewalt".

Entsprechend kündigten Linksextremisten im Vorfeld des diesjährigen Gipfeltreffens in Heiligendamm an, „die Show der Herrschenden in Tage des Widerstands und der globalen Solidarität von unten (zu) verwandeln". Dabei verwendete Parolen lauteten beispielsweise „G8 angreifen – Zusammen kämpfen gegen Kapitalismus, rassistische Ausgrenzung, patriarchale Gesellschaftsordnungen und Krieg!".

Bereits an diesen Parolen ist erkennbar, dass für Linksextremisten die Globalisierung, d.h. der weltweit betriebene Kapitalismus eine allgemeine ideologische Klammer bildet. Nahezu sämtliche linksextremistischen Themen- und Aktionsfelder lassen sich unter den Begriff Globalisierung subsumieren. Sei es Rassismus, Imperialismus, Militarismus, Faschismus, staatliche Repression, Umweltzerstörung – für alle diese Themen ist der Neoliberalismus als globalisierte Form des Kapitalismus zumindest mitursächlich.

Entsprechend war der G8-Gipfel in Heiligendamm für Linksextremisten das Ereignis schlechthin, auf das man sich seit dem Gipfel 2005 im schottischen Gleneagles intensiv vorbereitet hatte. Vorbereitet, natürlich in erster Linie um entsprechend präsent zu sein und den politischen Protest deutlich zum Ausdruck zu bringen. Von den Gipfelprotesten erhoffte man sich aber auch eine Signalwirkung für ein Wiedererstarken der linken Bewegung, die seit einigen Jahren zumindest national aber auch in weiten Teilen international vor sich hindümpelt. Denn immerhin gab es auch ein – wenig bescheidenes – Fernziel: So sollten nämlich die Gipfelproteste letztlich mit dazu beitragen – und das wurde auch genauso verbalisiert – den perspektivisch angestrebten revolutionären Prozess in Gang zu bringen.

Die Ziele waren also gleichermaßen hoch und weit gesteckt. Und folglich war und ist auch die Bedeutung des Gipfels für die linksextremistische Szene nicht zu unterschätzen.

Vielleicht an dieser Stelle eine kleine, aber nicht unwichtige Anmerkung: Die globalisierungskritische Bewegung in Deutschland und im Ausland stellt keine politische Einheit dar. Und sie ist vor allem auch nicht per se linksextremistisch. Im Gegenteil, auch hier ist zu betonen: die überwiegende Mehrheit der Globalisierungskritiker und auch die überwiegende Mehrheit der in Heiligendamm und Rostock aktiven Demonstranten sind Nicht-Extremisten, die dort friedlich ein ihnen grundgesetzlich verbrieftes Recht wahrnehmen wollten und wahrgenommen haben. Auch dies soll hier gerade von Seiten des Verfassungsschutzes deutlich zum Ausdruck gebracht werden.

Es liegt allerdings auch ein Stück weit in der Natur der Sache, dass es die linksextremistischen Aktivitäten sind, die Aufmerksamkeit hervorrufen, und zwar konkret die militanten Aktivitäten. Darunter zählen zwar auch die Ausschreitungen, die man unter dem Oberbegriff Massen- oder Straßenmilitanz kennt. Präsent sind sicher noch die entsprechenden Fernseh-

bilder von der Großdemonstration am 2. Juni in Rostock, die bisweilen erinnert haben an die Proteste anlässlich des WTO-Treffens in Seattle 1999, des EU-Gipfels in Göteborg im Juni 2001 oder des G8-Treffens in Genua im Juli 2001. Vor allem aber sind gemeint – und hier muss man deutlich zu den Straßenprotesten unterscheiden – klandestine militante Aktionen, und zwar insbesondere Brandanschläge im Rahmen der sog. militanten Kampagne gegen das G8-Treffen in Heiligendamm.

„Militante Kampagne" gegen den G8-Gipfel

Vorab sind einige Rahmendaten zu dieser militanten Kampagne zu nennen:

Insgesamt gab es in diesem Zusammenhang 29 Brandanschläge auf Kraftfahrzeuge bzw. auf Gebäude mit zum Teil beträchtlichen Sachschäden.

Von diesen insgesamt 29 Anschlägen richteten sich 19 gegen Wirtschaftsunternehmen, die übrigen 10 Anschläge gegen staatliche Einrichtungen bzw. gegen Institute, die jedoch allesamt auf die ein oder andere Weise mit dem Thema Wirtschaft in Bezug stehen oder aber die aus Sicht der Täter für die negativen Folgen der Globalisierung in der Mitverantwortung stehen.

Neben diesen Brandanschlägen wurden nach Polizeizählung über 600 weitere Straftaten mit G8/EU-Bezug verübt, und zwar überwiegend Sachbeschädigungen. Bei diesen handelt es sich vorwiegend um Farbschmierereien. Im Vergleich zu Brandanschlägen sind diese zwar strafrechtlich von minderer Bedeutung; auch ist der verursachte Schaden in der Regel erheblich geringer. Man darf aber nicht die politische Bedeutung vergessen, die durchaus auch von derlei Aktionen ausgehen kann. Dies wird beispielsweise deutlich an der Farbattacke auf das Wohnhaus des Ministerpräsidenten von Mecklenburg-Vorpommern, Harald Ringstorff, am 28. August 2006 oder auf das Kempinski Grand Hotel in Heiligendamm selbst, also auf den Tagungsort des G8-Treffens, das mit der Farbe – wie es in der Bekennung heißt – als „Ziel markiert" wurde.

Diese über 600 Straftaten sind zwar im engeren Sinne nicht Bestandteil der militanten Kampagne, sie widerspiegeln aber gleichwohl eine nicht übersehbare Breite linksextremistischer bzw. mutmaßlich linksextremistischer Militanzbereitschaft.

Ausgewählte Beispiele

Anhand einiger ausgewählter Anschläge gegen Wirtschaftsunternehmen

soll die Praxis der militanten Kampagne etwas genauer dargestellt werden:

- In der Nacht zum 28. Juli 2005 verübten Unbekannte einen Brandanschlag auf das Dienstfahrzeug des Vorstandsvorsitzenden der Norddeutschen Affinerie AG Hamburg, Dr. Werner Marnette, vor dessen Privathaus in Hollenstedt (Niedersachsen). Dabei entstand Sachschaden in Höhe von etwa 70.000 Euro.

  Am 1. August 2005 ging bei der Hamburger Morgenpost eine sechsseitige Taterklärung ohne Gruppenbezeichnung ein. Darin heißt es: Dr. Marnette vereinige in seiner Person mehrere Funktionen, die geeignet seien, „unterschiedliche Facetten imperialistischer Herrschaft aufzuzeigen und anzugreifen." So sei er nicht nur seit mehr als 30 Jahren Vorstandsvorsitzender der Norddeutschen Affinerie (NA), sondern stehe zusätzlich dem Industrieverband Hamburg vor und sei stellvertretender Präses der Hamburger Handelskammer. Seine Postensammlung habe er erst unlängst mit einem Sitz im Bundespräsidium des CDU-Wirtschaftsrates gekrönt.

  Dr. Marnette repräsentiere Organisationen, die wesentlich für Privatisierung gesellschaftlichen Eigentums, Verschärfung sozialer Repression und bedingungslose Unterordnung sozialer Fragen unter die Wettbewerbslogik stünden. Die NA sei als größter europäischer Kupferhersteller an der Ausbeutung von Minen und Menschen im „Trikont" und an der Produktion von Giftmüll beteiligt. Der Industrieverband Hamburg, eine Filiale des Bundesverbandes der deutschen Industrie (BDI), verstehe sich als Schnittstelle zwischen Industrie, Politik und Verwaltung. Seine Funktion in dem Verband nutze Dr. Marnette, um für eine Wirtschaftspolitik zu trommeln, die ausschließlich der Profitrate verpflichtet sei.

  Unter der Zwischenüberschrift „Sich jetzt auf den Weg machen zum Gipfel 2007 in Heiligendamm/Rostock" skizzieren die anonymen Autoren das eigentliche Ziel ihres Anschlags:

  „Mit unserer Aktion gegen NA Vorstandschef Werner Marnette verbinden wir den Vorschlag für eine breite, auch militante Kampagne zum G8 Gipfel 2007 in Heiligendamm bei Rostock, die jetzt

direkt nach Gleneagles an die Proteste anknüpft.“ [1]

Kritische Einwände vorwegnehmend räumen die Autoren ein, reine „Kampagnenpolitik“ und isoliertes „Gipfelhopping“ stießen bei vielen Genossen zu Recht auf Skepsis. Auch sei ihnen bewusst, dass militante linksradikale Zusammenhänge in der BRD rar gesät seien:

„Trotzdem halten wir eine langfristige Orientierung auf Heiligendamm, die militant begleitet wird, für wichtig und notwendig. Der G8 Gipfel in Heiligendamm wird spätestens im Frühjahr 2007 ein zentrales Thema für Linksradikale in der BRD und wahrscheinlich auch in Europa werden. Erstes Interesse in der Szene ist in den letzten Wochen bereits erkennbar. Es scheint uns sinnvoll, nicht erst Anfang 2007 in einer Art Feuerwehrpolitik in die Mobilisierung der Antiglobalisierungsbewegung einzusteigen, sondern die nächsten zwei Jahre zu nutzen, an konkreten praktischen Initiativen darüber zu diskutieren, wo und wie wir Strukturen kapitalistischer Ausbeutung und imperialistischer Unterdrückung angreifen können und müssen.“

Der Anschlag Marnette war also nicht nur ein Anschlag, wie es ihn in der Vergangenheit immer wieder gegeben hat, beispielsweise unter der Überschrift „Karossentod“ oder von der „militanten gruppe“ in Berlin. Es wurde vielmehr bewusst ein Startsignal gegeben und ein Aufruf initiiert für eben diese militante Kampagne. Diese soll – nach dem ausdrücklichen Willen der Initiatoren – integraler Teil einer breiten Gesamtkampagne sein, wobei der spezielle Beitrag darin besteht, noch zahlreiche weitere gleich- oder ähnlich gelagerte militante Aktionen durchzuführen.

Bekanntermaßen stieß dieses Signal leider nicht auf taube Ohren, sondern wurde vielmehr in den nachfolgenden fast zwei Jahren in bemerkenswerter Intensität aufgegriffen.

- Als zweites Beispiel soll ein Brandanschlag dargestellt werden, der sich in der Nacht zum 27. März 2006 ereignete. Seinerzeit setzten unbekannte Täter auf dem Firmengelände der Gleis- und Schienenbaufirma Thormählen Schweißtechnik AG (TST) in Bad Oldesloe (Schleswig-Holstein) fünf Werkstattwagen sowie einen

1 „INTERIM“ Nr. 622 vom 15.09.2005, S. 15-20

Spezialtraktor in Brand. Die Fahrzeuge brannten nahezu vollständig aus; dabei kam es auch zu mehreren Explosionen, weil zwei der angegriffenen Fahrzeuge mit großen Gasflaschen beladen waren. Menschen waren gleichwohl nicht gefährdet. Der Gesamtschaden belief sich auf immerhin ca. 250.000 Euro.

In einer Taterklärung bezichtigten sich ebenfalls bis dato unbekannte „Internationalistische Zellen" des Brandanschlags.

Unter der Überschrift „ES FÄHRT KEIN ZUG NACH NIRGENDWO" nahmen die Verfasser darin die Beauftragung der TST mit dem Bau eines Eisenbahnschienennetzes im Südsudan zum Anlass. Umfassend kritisieren sie die - wie es heißt - ökonomische Ausbeutung des von jahrzehntelangem Bürgerkrieg heimgesuchten Sudan durch imperialistische Kräfte, zu denen auch die Bundesrepublik Deutschland gehöre. Das Eisenbahnprojekt der TST stehe beispielhaft für die konkrete Umsetzung eines „neuen deutschen Imperialismus, der nicht vordergründig auf militärische Eroberung setzt, sondern auf die ökonomische Durchdringung potenziell produktiver Zonen überall auf dieser Welt, und der ihre (Re)Integration in den kapitalistischen Weltmarkt zum Ziel hat" [2]. Das Eisenbahnprojekt - so die Verfasser weiter - mache die Zusammenhänge und das Wechselverhältnis kapitalistischer Ausbeutung und imperialistischer Kriege sichtbar. Dieses Prinzip habe man dort angegriffen, wo man es habe erreichen können.

- Im nächsten Beispiel wurden zwei Repräsentanten des Thyssen-Krupp-Konzerns die Opfer.

  In der Nacht zum 26. Januar 2007 verübten unbekannte Täter wiederum in Hamburg einen Brandanschlag auf das am Wohnhaus des Sprechers der Firma ThyssenKrupp Marine Systems (TKMS) abgestellte Firmenfahrzeug. Das Fahrzeug brannte vollständig aus. Im selben Zeitraum beschädigten unbekannte Täter das Wohnhaus eines Mitglieds des Managements der TKMS in Hamburg mit Farbe und zerstörten die Windschutzscheibe seines Firmenwagens.

  Zur Tat bekannte sich eine – wie fast immer – bislang unbekannte Gruppe, dieses Mal mit dem Namen „Revolutionäre Anti-Milita-

2 „INTERIM" Nr. 634 vom 06.04.2006, S. 12-15

ristische AktivistInnen". In ihrem Bekennerschreiben mit der Überschrift „NATO-Kriegskonferenz in München angreifen G8-Treffen in Heiligendamm lahmlegen" wenden sich die Täter gegen die jährliche Münchener „Sicherheitskonferenz", die nur wenige Tage später zum 43. Mal stattfand. Die als „Kriegskonferenz" bezeichnete Veranstaltung werde von der Rüstungsindustrie als Forum genutzt, um „mögliche Hürden für ihre Exportinteressen besser aus dem Weg zu räumen und die technische Weiterentwicklung der Waffensysteme auf die strategischen Anforderungen der Militärs auszurichten". Der ThyssenKrupp-Konzern sei „als Waffenschmiede ein wichtiger Baustein im Krieg, den die Bundeswehr in einer stetig wachsenden Zahl von Ländern" führe. Der Konzern sei zudem eine „Stütze des deutschen Kaiserreichs und des Nationalsozialismus" gewesen und stelle nunmehr „eine Stütze des aktuellen parlamentarischen deutschen Imperialismus" dar.
Weiter heißt es:

„Der Anschlag gilt einem Konzern, der an zwei von Deutschland initiierten Weltkriegen verdient hat, an der tausendfachen Zwangsarbeit von KZ-Häftlingen und dem millionenfachen Tod von Menschen überall auf der Welt." [3]

Ausdrücklich weisen die Verfasser darauf hin, dass ihr „Kampf für eine Welt ohne Krieg" gegen das kapitalistische System geführt werden müsse und verbinden deshalb „die Kampagne gegen die NATO-Kriegskonferenz in diesem Jahr mit der Mobilisierung gegen den G8-Gipfel" in Heiligendamm.

Noch eine Anmerkung:
Bereits ein Jahr zuvor, konkret am 31. Januar 2006 und folglich im unmittelbaren Vorfeld der 42. Sicherheitskonferenz, hatte sich der bis dato fünfte Brandanschlag im Rahmen der militanten Kampagne ereignet. Damals hatten unbekannte Täter unter ebenfalls ausdrücklichem Bezug auf das G8-Treffen 2007 in Heiligendamm in zwei Hamburger Stadtteilen jeweils einen Lkw des Rüstungszulieferers Imtech in Brand gesetzt. Zu der Tat hatte sich eine unbekannte „Militante Antimilitaristische Initiative" (M.A.M.I.) bekannt.

3 „INTERIM" Nr. 649 vom 01.02.2007, S. 16-18

- Bereits zu Beginn wurde die Fa. Dussmann als Ziel militanter linksextremistischer Aktionen im Aktionsfeld „Antirassismus“ genannt.

  Im Rahmen der militanten Kampagne war sie gleich zwei Mal kurz hintereinander von Anschlägen betroffen, und zwar am 23. Februar und am 6. März 2007. Zuerst wurden vier Firmenfahrzeuge in Hamburg angezündet, dann erfolgte ein weiterer Brandanschlag auf ein von Dussmann genutztes Gebäude in Berlin.

  Begründet werden die Taten mit der Rolle des Unternehmens als Profiteur angeblicher rassistischer Asylpolitik. So kritisieren die Verfasser der Taterklärungen die Verpflegung von Asylsuchenden durch die Firma Dussmann. Dussmann sei in der Vergangenheit und mit entsprechenden Aktionen wiederholt aufgefordert worden, „sich aus der Zwangsverpflegung von Flüchtlingen mit miesem Essen zurückzuziehen, was die Konzernverantwortlichen jedoch ganz offensichtlich nicht zur Kenntnis“ nähmen. In einem von Dussmann belieferten und von der Arbeiterwohlfahrt (AWO) unterhaltenen Ausreisezentrum in Berlin-Spandau würden Asylsuchende und geduldete Flüchtlinge „durch Internierung, fortgesetzte Schikanen, unwürdige Lebensbedingungen und mangelhafte Versorgung so sehr unter Druck gesetzt, dass sie Deutschland ‚freiwillig‘ “ verließen. Als „Überzeugungstäter kapitalistischer Modernisierung“ seien die Konzernverantwortlichen von Dussmann immun gegen Argumente und „offen für alles, woran sich in Zeiten des Neoliberalismus verdienen“ lasse.

  Zugleich stellen sie ihre Tat in einen inhaltlichen Zusammenhang mit der „militanten Kampagne“ gegen das G8-Treffen in Heiligendamm. Dabei begrüßen sie nicht nur den speziellen Aktionstag zum „Antirassismus“ während der Protestwoche in Heiligendamm. Vielmehr werten die Verfasser Militanz als „ein Mittel, um einerseits radikale antirassistische Positionen mit einem gewissen Nachdruck bekannter zu machen und um andererseits konkret gegen staatlichen und gesellschaftlichen Rassismus vorzugehen und die Selbstorganisation von Flüchtlingen wie auch linksradikale Antira-Politik allgemein zu unterstützen“.

- Das vorletzte Beispiel wurde insbesondere ausgewählt wegen des

Anschlagsziels, nämlich der Bild-Zeitung, einem langjährigen linksextremistischen Feindbild par excellence. Konkret betroffen war der Bild-Chefredakteur Kai Diekmann, dessen Privat-PKW am 22. Mai 2007 bei einem Brandanschlag unmittelbar vor seinem Privatgrundstück vollständig zerstört wurde.

Entsprechend ist auch die Taterklärung an Deutlichkeit kaum noch zu überbieten. Unter der Aktionsbezeichnung „Militante Kampagne kämpft für Sie“ bezeichnen die Verfasser ihre Aktion als „Antwort auf die G8-Razzia der Bundesanwaltschaft vom 9.5.07“.

Zur Erinnerung: Am 9. Mai vollzog das Bundeskriminalamt (BKA) im Auftrag der Bundesanwaltschaft im Rahmen zweier Ermittlungsverfahren wegen des Verdachts von Straftaten nach § 129 a StGB Durchsuchungsbeschlüsse des Bundesgerichtshofs. Die Maßnahmen richteten sich gegen 21 Beschuldigte - 18 im Verfahren „militante Kampagne“, drei im Verfahren „militante gruppe (mg)“ - insgesamt wurden 42 Objekte in Berlin, Brandenburg, Bremen, Hamburg, Niedersachsen und Schleswig-Holstein durchsucht, darunter auch einschlägige Szeneobjekte wie die „Rote Flora“ in Hamburg.

Der Bild-Zeitung sowie dem Springer-Konzern werfen die Täter vor, „den emanzipatorischen Widerstand“ gegen den G8-Gipfel „durch den Dreck zu ziehen“. Wörtlich: „Bild lügt, hetzt, erniedrigt, mordet, vergewaltigt jeden Tag neu mit 3,5 Millionen verkauften Exemplaren.“ Mit bis zu zwölf Millionen Lesern stelle die Bild-Zeitung zudem eine „bedeutende Säule für den Erhalt des kapitalistischen Systems in der BRD“ dar. Und im weiteren Textverlauf ist dann zu lesen: „Bild mobilisiert, formuliert und legitimiert den xenophoben, sexistischen, sozialdarwinistischen Hass und die Verachtung unter den Ausgebeuteten und Unterdrückten, mit Schlagzeilen, mit Bildern, mit Lügen und mit der Macht eines riesigen Medienkonzerns.“ [4]

Und schließlich senden die Verfasser dann auch noch Grüße an „alle, die in diesen zwei Jahren viel Kraft und Phantasie in den Widerstand gegen das Weltwirtschaftstreffen gesteckt haben und

4 „INTERIM“ Nr. 657 vom 21.06.2007, S. 21/22

ihren Beitrag dafür leisten, dass die Wahrheit von der Notwendigkeit einer Revolution hier und jetzt laut und unüberhörbar formuliert wird".

- Ein letzter Brandanschlag mit ausdrücklichem Bezug auf die militante Kampagne fand statt am 25. Juni 2007 in Berlin, d. h. gut zwei Wochen nach Beendigung des G8-Gipfels. Betroffen waren zwei Fahrzeuge der Deutschen Post AG bzw. konkret deren Tochtergesellschaft DHL.

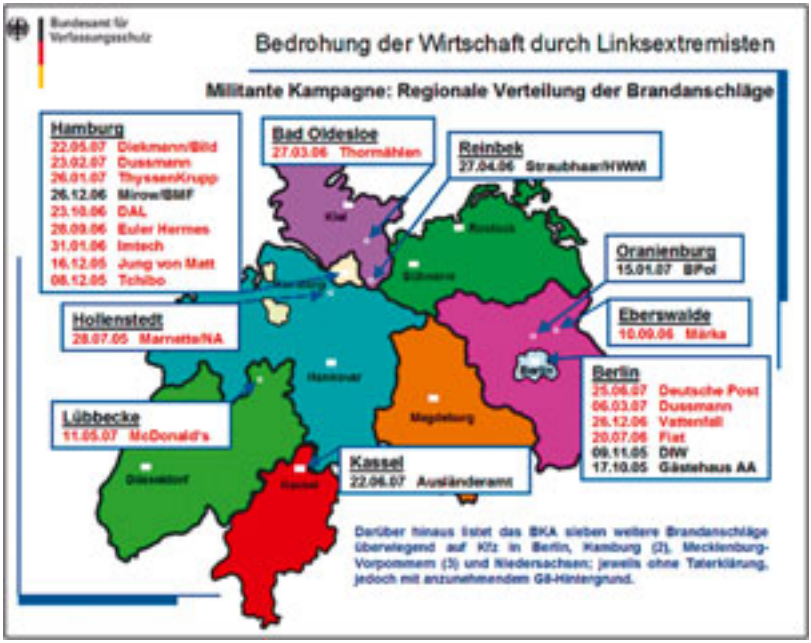
  Zu den Anschlägen bekannte sich eine Gruppe „AG 2. Juni 2007", die mit ihrer Namensgebung offensichtlich an die Ausschreitungen im Rahmen der G8-Proteste in Rostock an eben diesem Tag erinnern wollte.

  Die Tatbegründung fällt erneut in das Aktionsfeld „Antimilitarismus". So wird der DHL vorgeworfen, den US-amerikanischen Krieg im Irak zu unterstützen, indem sie die dortigen US-Truppen mit Post und Gütern aller Art beliefere. Man habe die Fahrzeuge in Brand gesetzt, um „ein wenig Sand in die Kriegsmaschinerie zu streuen und auf die Beteiligung Deutschlands auch in diesem Krieg aufmerksam zu machen". Zudem sei man der Meinung, „dass der Hauptfeind immer noch im eigenen Land steht", weshalb sich „diese Aktion nicht ausschließlich gegen den Irak-Krieg, sondern gegen imperialistische Kriege im Allgemeinen" richte.

  Die Aktion sei als Fortsetzung der militanten Kampagne zu sehen. Und so wird das Schreiben mit den Parolen beendet: „Die Proteste gegen den Gipfel in Heiligendamm haben einen angenehmen Aufwind mit sich gebracht – aber das war erst der Anfang! Jetzt erst recht! ... Es gibt kein ruhiges Hinterland!" [5].

5 „INTERIM" Nr. 658 vom 05.07.2007, S. 6

Regionale Verteilung der Brandanschläge



Auf dieser Übersicht ist die regionale Verteilung der Anschläge dargestellt. Im Einzelnen aufgeführt sind 22 Anschläge, nämlich die, zu denen eine Taterklärung vorliegt und insofern auch ein expliziter Bezug auf die militante Kampagne. Bei den übrigen sieben Anschlägen ist allerdings ebenfalls von einem G8-Hintergrund auszugehen.

In roter Schrift aufgeführt sind die Anschläge gegen Wirtschaftsunternehmen bzw. gegen deren Vertreter. In schwarzer Schrift dargestellt sind die Anschläge auf staatliche Einrichtungen und Wirtschaftsforschungsinstitute bzw. auf deren Repräsentanten, wie z.B. im Falle des Staatssekretärs im Bundesfinanzministerium Thomas Mirow am 2. Weihnachtstag 2006 in Hamburg, dem ebenso ein Privat-Pkw in Brand gesetzt wurde wie dem Direktor des Hamburgischen Welt-Wirtschaftsinstituts (HWWI), Prof. Straubhaar, am 27. April 2006 im schleswig-holsteinischen Reinbek. Die jeweiligen Tatbegründungen waren in bekannter Weise gehalten. Die Täter bezogen sich stets auf die Rolle der Geschädigten und ihre daraus abgeleitete angebliche Mitverantwortung im eingangs erwähnten Sinne.

Der Anschlag mit dem höchsten Sachschaden, nämlich über 2,2 Mio Euro, wurde übrigens am 17. Oktober 2005 gegen das Gästehaus des Auswärtigen Amtes in Berlin-Reinickendorf verübt. Dass insofern der Staat und nicht die Wirtschaft betroffen war, hat sicherlich nichts zu bedeuten und ist insofern auch nur ein schwacher Trost für die ansonsten betroffenen Wirtschaftsunternehmen. Zumal auch dieser Anschlag begründet wurde mit der „neuen deutschen Außenpolitik, sprich Großmachtpolitik im ökonomischen und militärischen Sinne". Schon ist die Wirtschaft wieder mit im Boot.

Aufgeschlüsselt nach Bundesländern verteilen sich die 29 Anschläge wie folgt:

Berlin 7

Brandenburg 2

Hamburg 11

Hessen 1

Mecklenburg-Vorpommern 3

Niedersachsen 2

Nordrhein-Westfalen 1 und

Schleswig-Holstein 2.

Sowohl aus dieser Auflistung als auch aus der Grafik sind schnell eindeutige regionale Schwerpunkte zu erkennen. Deutlich wird also, dass die Anschläge nicht nur ausschließlich in Norddeutschland stattfinden, sondern allesamt in und um Hamburg sowie in und um Berlin verübt wurden.

Bemerkenswert daran ist, dass man die Anschläge in Berlin erwarten musste, wenn auch vielleicht nicht in dieser Häufigkeit. Sie stellen nämlich leider nichts wirklich grundsätzlich Außergewöhnliches dar. Dort passieren seit Jahren immer wieder Anschläge – zumeist unter den Namen „militante gruppe" oder „Autonome Gruppen". Insofern bedeutet dies für Berlin, dass hier Bekanntes fortgeführt wird, jetzt allerdings unter dem Logo „G8".

Etwas anders ist die Situation in Hamburg. Hier hat es zwar früher auch schon Anschläge gegeben. In den letzten Jahren jedoch nicht mehr – zumindest nicht mehr in dieser Qualität und mit einem Begründungshintergrund, der eher allgemeinpolitisch ist und nicht spezifische Hamburger Probleme aufgreift.

Insofern muss man hier festhalten, dass es offenkundig in Hamburg ein linksextremistisches Potenzial gibt, das zu militanten Anschlägen bereit

und in der Lage ist und durch das Ausrufen der militanten Kampagne geweckt bzw. zu entsprechenden Taten animiert worden ist.

Bewertung und Ausblick

Abschließend sei ein Ausblick gewagt, also zur Frage Stellung genommen, wie es weiter gehen wird.

So ist davon auszugehen, das Wirtschaftsunternehmen auch zukünftig im Zielspektrum militanter Linksextremisten stehen werden, d. h. auch außerhalb einer Sondersituation wie einem G8-Gipfel. Da hat uns leider auch bereits die Realität insbesondere in Berlin eingeholt.

Denn auch nach Heiligendamm ist in Berlin eine bislang beispiellose Serie von Brandanschlägen auf Kfz zu registrieren - inzwischen hat es davon in 2007 bereits über 100 mit belegtem oder mutmaßlichem linksextremistischem Hintergrund gegeben. Hinzu kommen zahlreiche weitere Brandanschläge auf Gebäude sowie Sachbeschädigungen an Kfz u. a. durch eingeschlagene Scheiben.

Betroffen waren davon in großem Maße auch Wirtschaftsunternehmen, wie z. B. die Deutsche Bahn bzw. die DB Carsharing, von der allein mindestens 16 Fahrzeuge abgebrannt wurden – wohlgemerkt alleine in diesem Jahr und nur in Berlin. Weiterhin betroffen waren Siemens, Renault, die Allianz, Europcar und Sixt, immer wieder Vattenfall oder auch die Deutsche Telekom und die Deutsche Post AG.

Offenkundig haben die verschiedenen Exekutivmaßnahmen im Laufe des Jahres u. a. gegen die mutmaßlichen Initiatoren der militanten Kampagne sowie gegen die „militante gruppe“ dies nicht verhindern können. Im Gegenteil: Man muss sogar befürchten, dass diese Maßnahmen provozierend und insofern möglicherweise sogar animierend gewirkt haben, weil sie szeneintern als rundweg unrechtmäßig und völlig unverhältnismäßige Repression empfunden wurden und werden.

Dennoch gab es aus Sicht der Sicherheitsbehörden - auch rückblickend bewertet - keine Alternative zu diesem Vorgehen.

Möglicherweise wäre die Situation ohne die polizeilichen Maßnahmen auch noch brisanter. Denn in verschiedenen Erklärungen militanter Kreise ist in der Vergangenheit mehrfach die Forderung laut geworden, die „militante Kampagne“ auch über den G8-Gipfel hinaus fortzusetzen.

Letztlich ist es allerdings unerheblich, ob die Anschläge als Teil der „militanten Kampagne“ verübt werden oder nicht. Tatsache ist jedenfalls, dass es einige, wenn auch wenige Strukturen im Linksextremismus gibt, die

– wie sie es nennen – praktische, d.h. militante Intervention propagieren und sowohl willens als auch in der Lage sind, dies auch umzusetzen.

In einem erst vor wenigen Tagen im Berliner Szeneblatt „Interim" veröffentlichten Aufsatz wird ebenso direkt wie plakativ propagiert: „der militante Kampf ist immer richtig." Und weiter: „Militante Aktionen sind legitim und notwendig. ... Aus einer Kontinuität militanter Aktionen – und deswegen werden sie auch mit Repression verfolgt – kann sich ein bewaffneter Kampf gegen Staat und Kapital" – sprich die Wirtschaft – „entfalten. Rote Armee Fraktion, Bewegung 2. Juni und Revolutionäre Zellen sind in einer anderen Zeit entstanden. Aber die Verhältnisse, gegen die sie angetreten waren, sind harmlos, verglichen mit den heutigen und dem, was sich die Herrschenden gegenwärtig trauen durchzuziehen." [6] Klarer kann ein Bekenntnis zur Militanz bzw. eine Ankündigung zur militanten Intervention kaum formuliert werden.

Aktionsniveau geht gegenwärtig nicht über Sachschäden hinaus

Wenn man der Situation überhaupt etwas Positives abgewinnen kann, dann ist es die sehr hohe Wahrscheinlichkeit, dass es z.Zt. bei diesen militanten Interventionen nicht zu beabsichtigten Personenschäden kommt, d.h. das militante Aktionsniveau gegenwärtig nicht über die Ebene sachschadenbezogener Anschläge hinausgeht.

In diesem Zusammenhang soll aus einer anderen, ebenfalls erst kürzlich in der „Interim", aber auch in der „Zeck" aus Hamburg veröffentlichten Stellungnahme einer Gruppe zitiert werden, die sich nach eigenem Bekunden selbst an der „militanten Kampagne" aktiv beteiligt hat: „So werden sich viele Vorstöße vorerst darauf beschränken müssen, das Establishment mit militanten Aktionen kurzfristig zu erschrecken und unsere Vorstellungen von sozialer Befreiung indirekt zu vermitteln: durch den radikalen Bruch mit Reformismus und Legalismus, durch gezielte Angriffe, die Personenschäden grundsätzlich ausschließen, durch phantasievolle neue Aktionsformen...". [7]

Bewusst soll also gegenwärtig die Schwelle zum Terrorismus nicht überschritten werden. Dies ist natürlich keine Garantie für alle Zeit, aber gegenwärtig darf man annehmen, dass alle Tätergruppen keine Personenschäden beabsichtigen. Diese wären innerhalb der Szene auch nicht vermittelbar, d. h. man würde sich politisch isolieren und den notwendigen szeneinternen Rückhalt verlieren. Dies ist - wie gesagt - zur Zeit nicht erkennbar. Allerdings - und auch das sollte man nicht verschweigen - besteht der Eindruck an der ein oder anderen Stelle, dass Personenschäden billi-

6 „INTERIM" Nr. 663 vom 09.11.2007, S. 15/16
7 „INTERIM" Nr. 662 vom 26.10.2007, S. 17-21

gend in Kauf genommen werden. Damit soll kein Schreckensszenario heraufbeschworen werden. Es bleibt dabei: Personenschäden sind nicht intendiert, sie sind insofern sehr unwahrscheinlich. Gleichwohl ist an dieser Stelle naturgemäß größte Aufmerksamkeit geboten.

Zieleingrenzung kaum möglich

Es ist leider in der Tat so, dass eine Zieleingrenzung so gut wie unmöglich ist. Das limitiert natürlich dann auch die denkbaren präventiven Maßnahmen. Man kann den oder die nächsten Tatorte zwar wieder im Hamburger und Berliner Raum vermuten. Wer jedoch wann Opfer werden kann, ist aufgrund der thematischen Breite möglicher politischer Begründungszusammenhänge sowie der daraus resultierenden Anzahl potenzieller Anschlagsziele nicht prognostizierbar.

Man kann lediglich bzw. muss sogar davon ausgehen, dass auch in Zukunft sowohl staatliche Einrichtungen als auch Wirtschaftsunternehmen betroffen sein werden.

Was die staatlichen Einrichtungen als Angriffsziele betrifft, hat sich die bereits zitierte Gruppe in ihrer Stellungnahme in der „Interim“ und in der „Zeck“ unmissverständlich geäußert. Mit Blick auf die genannten Maßnahmen von Bundesanwaltschaft und BKA, denen nun das vorrangige Interesse linksradikaler Politik gelten müsse, wird dort unmissverständlich angemerkt: „Wir denken, dass es genügend Ansatzpunkte gibt, militante Antirepressionspolitik auch thematisch offensiv zu wenden. In diesem Zusammenhang sind für uns Bullen und Justiz, aber auch die Bundeswehr, Rüstungsindustrie und alle Agenturen imperialistischer Herrschaft gute Ziele.“

Als Beleg für die Prognose, dass auch zukünftig Wirtschaftsunternehmen Angriffsziel sein werden, soll ebenfalls ein Zitat angeführt werden, das für sich spricht. Es stammt aus einer Taterklärung zu einem kürzlich verübten Anschlag auf Fahrzeuge des Allianz-Konzerns:

„Am 17.9. liessen wir zwei Autos der Allianzversicherung am Strausberger Platz (Berlin) in Flammen aufgehen und rufen hiermit zu weiteren Attacken gegen Gross-Kapitalunternehmen auf. ... Die Allianz Versicherung steht für ein wirtschaftlich starkes Unternehmen mit ausgezeichneten Gewinnen und Bilanzen auf Kosten der Solidargemeinschaft. Hier ist die Allianz Versicherung exemplarisch für alle Unternehmen gemeint, die sich allein an der kapitalistischen Gewinnmaximierung orientieren.
Nur im Interesse von Großkonzernen und Kapitalbesitzenden werden die

sozialen Sicherungssysteme demontiert.“ [8]
Aus dieser Logik ergibt sich: Wenn also alle Einrichtungen der „staatlichen Repression“ und alle Unternehmen, die sich an der Gewinnmaximierung orientieren, als potenzielles Angriffsziel ausgerufen werden, ist eine Zieleingrenzung nahezu unmöglich.

Dies wird das BfV – ebenso wie beim Versuch der Identifizierung der Täter - nicht davon abhalten, buchstäblich die Stecknadel im Heuhaufen zu suchen. Man muss allerdings wissen, dass dafür viel Einsatz, kontinuierliche Bemühungen und ein langer Atem erforderlich sind.

8 „INTERIM“ Nr. 662 vom 26.10.2007, S. 16

Herbert Kurek, Bundesamt für Verfassungsschutz

Wirtschaftsspionage: Herausforderung für den Verfassungsschutz

Die weltweiten politischen Veränderungen der vergangenen 17 Jahre, deren Ausgangs- und zugleich Kulminationspunkt das Ende der Ost-West-Konfrontation markiert, führte zum Wegfall einer Reihe von äußeren Sicherheitsrisiken für die Bundesrepublik Deutschland.
Ihre Abwehr bestimmte maßgeblich die Arbeit der bundesdeutschen Sicherheitsbehörden über vier Jahrzehnte hinweg.
Wer geglaubt hat, dass das Zeitalter immerwährender Freundschaft und grenzenlosen Vertrauens zwischen den Völkern angebrochen sei, sah sich in seinen optimistischen Prognosen widerlegt.
Viele sicherheitspolitische Herausforderungen überlebten diese Zeit des globalen Umbruchs und beschäftigen die Sicherheitsbehörden unseres Landes nach wie vor.
Neue - globale - Herausforderungen kamen hinzu, an erster Stelle der internationale islamistische Terrorismus.

Zu den dauerhaft virulenten Gefahren für die innere Sicherheit der Bundesrepublik Deutschland zählt auch die Spionage durch fremde Nachrichtendienste, ein Problem, das sich aus unserer Sicht trotz Auflösung der Dienste des ehemaligen Ostblocks nicht gänzlich entschärft hat. Die Bedrohung durch Spionage - und hier insbesondere durch Wirtschaftsspionage - ist vielmehr in den vergangenen Jahren in dem Maße gestiegen, in dem auch die Liberalisierung der Weltmärkte den globalen Wettbewerb um nachhaltiges Know-how und Wissenspotentiale erhitzt hat.

Folgerichtig erklärt das Bundesamt für Verfassungsschutz - in Deutschland zentral verantwortlich für die Belange der Spionageabwehr - in seinem aktuellen Verfassungsschutzbericht, dass die Bundesrepublik Deutschland ungebrochen ein bedeutendes Aufklärungsziel für die Nachrichtendienste einer Reihe fremder Staaten ist.

Unser Land ist aufgrund seiner geopolitischen Lage, der wichtigen Rolle innerhalb der EU und der NATO und nicht zuletzt als Standort zahlreicher Unternehmen der Spitzentechnologie ein begehrtes Ausspähungsziel. Diese Begehrlichkeiten, d.h. nachrichtendienstliche Aktivitäten richten sich in Deutschland neben den klassischen Aufklärungszielen wie Politik

und Militär verstärkt auf die Bereiche Wirtschaft, Wissenschaft und Forschung sowie Hochtechnologie.

Insbesondere durch die Gesetzmäßigkeiten der Globalisierung bemisst sich das internationale Gewicht eines Landes nicht mehr primär nach seinem militärischen, sondern auch - und vor allem - nach seinem ökonomischen Potenzial.
Heute wird die ökonomische Leistungsfähigkeit als Basis für die Stärke eines Staates verstanden.
Darüber hinaus ist das wirtschaftliche Handeln heute mehr denn je durch globale Präsenz der Unternehmen und starke internationale Verflechtungen geprägt. Neben den positiven wirtschaftlichen Effekten der Internationalität liegen genau in der hohen Komplexität auch enorme Risiken.

Die Stärke unseres Landes basiert im Wesentlichen auf den Kernkompetenzen

- Ideenreichtum
- Innovation
- Wissensvorsprung sowie
- der schnellen Umsetzung von Ideen in marktfähige Produkte.

Durch Wirtschaftsspionage und dem damit verbundenen illegalen Know-how-Abfluss wird nicht nur der Wettbewerb negativ beeinflusst, Wirtschaftsspionage bedroht vielmehr den Standort Deutschland, d.h. den wirtschaftlichen Erfolg unseres Landes und damit auch die innere Stabilität und letztlich unseren Wohlstand.

Die Spionageabwehrbereiche der Verfassungsschutzbehörden des Bundes und der Länder setzen sich mit den Herausforderungen der Wirtschaftsspionage offensiv auseinander.

In der Öffentlichkeit und in den Medien wird häufig nicht zwischen Wirtschaftsspionage und Konkurrenzausspähung deutlich unterschieden. Das aber ist wichtig, da sich hieran nicht nur unterschiedliche Rechtsfolgen knüpfen, sondern auch eindeutige Zuständigkeiten ergeben. Daher möchte ich zunächst beide Begriffe erläutern und abgrenzen.

Unter Wirtschaftsspionage versteht man die staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben.
Ihre Strafbarkeit ist im § 99 des Strafgesetzbuches niedergelegt.

Dieser Bereich nachrichtendienstlicher Tätigkeit ist Aufgabe der Spionageabwehr der Verfassungsschutzbehörden.

Unter Konkurrenzausspähung oder auch „Industriespionage“ hingegen versteht man die Ausforschung, die ein konkurrierendes Unternehmen gegen ein anderes betreibt.
Sie ist privatwirtschaftlicher Natur, denn hier geht es in der Regel um Verrat von Geschäfts- und Betriebsgeheimnissen.
Also einen Tatbestand des § 17 des Gesetzes gegen den unlauteren Wettbewerb.

Es besteht kein Zweifel darüber, dass eine Grenzziehung zwischen beiden Phänomenbereichen - insbesondere im Anfangsstadium - im Einzelfall durchaus schwierig sein kann und sich der Modus operandi der „Täter“ häufig kaum unterscheidet.

Daher befasst sich die Spionageabwehr bei hinreichenden Anhaltspunkten analytisch mit beiden Sachverhalten, insbesondere wenn die Täterseite noch unklar ist.

Wirtschaftsspionage gibt es, seit es wirtschaftlichen Wettbewerb gibt.
Doch was sind die Motive im Zeitalter der Globalisierung?
Die Motive eines fremden Staates, seine Nachrichtendienste auf die deutsche Wirtschaft anzusetzen, erklären sich primär aus den Rahmenbedingungen der wirtschaftlichen Globalisierung und den damit verbundenen gravierenden inneren Umwälzungen der nationalen Volkswirtschaften.
Die seit dem Ende der Ost-West-Konfrontation beschleunigte Entwicklung, zwischenstaatliche Konflikte um Macht und Ressourcen auf neue, wirtschaftliche Schauplätze zu verlagern, hat in der Konsequenz dazu geführt, dass die Wirtschaftskraft eines Landes mittlerweile gleichzusetzen ist mit seiner internationalen Bedeutung.
Diese Wirtschaftskraft mit allen Mitteln - so auch durch Spionage - zu erhalten bzw. zu stärken, gehört mithin zur Staatsräson vieler Nationen.
Folglich zählt insbesondere in Ländern, in denen Wirtschaft und staatliche Strukturen eng miteinander verflochten sind, aktive nachrichtendienstliche Aufklärung im wirtschaftlichen und technologischen Bereich zum normalen Instrumentarium staatlicher Existenzvorsorge.
Zu diesen Ländern zählen insbesondere die Russische Föderation und die Volksrepublik China, auf die ich noch später zurückkomme.

Abgesehen von diesen eher staatspolitischen Motiven, die den Bezugsrahmen für Wirtschaftsspionage gegen unser Land markieren, diktiert auch die drastische Veränderung der globalen Wissens- und Informationskul-

tur die fortdauernden Bestrebungen fremder Staaten, ökonomisch wertvolles Wissen von potenziellen Konkurrenten zu erlangen.
In der globalen Informationsgesellschaft des 21. Jahrhunderts ist der strategische Wert von Informationen auch im wirtschaftlichen Bereich enorm gestiegen, da auf der Zeitachse der Einführung neuer Produkte die durch Spionage erlangten Informations- und Wissensvorsprünge unmittelbare Wettbewerbsvorteile eröffnen.
Zudem helfen die auf nachrichtendienstlichem Wege beschafften Informationen, z.B. im Bereich der Produktentwicklung Zeit und - angesichts des harten globalen Wettbewerbs mindestens ebenso wichtig - hohe Kosten für eigene Forschung einzusparen.
Deutschland investiert bekanntlich enorme Summen in Forschung und Entwicklung.
Welche Wirtschaftsbereiche sind besonders gefährdet?
Unternehmen der Hochtechnologie sowie Wissenschaft und Forschung sind bevorzugte Ziele der Wirtschaftsspionage.
Das besondere Interesse fremder Nachrichtendienste richtet sich in diesem Zusammenhang auf Unternehmen und Forschungseinrichtungen der

- Informations- und Kommunikationstechnologie
- Werkzeugmaschinenindustrie, insbesondere CNC-Technologie
- Optoelektronik
- Röntgen-Lasertechnologie
- Luft- und Raumfahrttechnik
- Automobilbau
- Energie- und Umwelttechnologie.

Kurzum, auf Branchen, in denen deutsche Unternehmen führend sind.

Die Schwerpunkte fremder Nachrichtendienste bei der Ausspähung der deutschen Wirtschaft variieren naturgemäß je nach dem ökonomischen Hintergrund des beteiligten Staates.
So sind die Begehrlichkeiten hochentwickelter Länder eher im wirtschaftsstrategischen Bereich angesiedelt. Sie richten sich auf die wirtschaftliche Infrastruktur der Bundesrepublik Deutschland im Ganzen, auf energiewirtschaftliche lnformationen sowie auf Unternehmens-, Wettbewerbs- und Marktstrategien. Aber auch finanzpolitische Planungen und Investitionen sowie Absprachen und Zusammenschlüsse von Unternehmen sind von hohem strategischen Interesse.

Technologisch weniger entwickelte Staaten (sog. Schwellenländer) hingegen versuchen vor allem, sich das technische und wissenschaftliche Know-how zu beschaffen, um Kosten für eigene Entwicklungen oder Lizenzgebühren zu sparen. Darüber hinaus sind sie stark an lnformationen über spezielle Fertigungstechniken interessiert, um auf dem Markt mit kostengünstigeren Nachbauten schnell konkurrenzfähig zu sein.
Insgesamt gilt für diesen Bereich der eher produktgebundenen Wirtschaftsspionage, dass die entsprechenden Ausforschungsbemühungen auf alle Entwicklungsstufen abzielen: von der Forschung und Entwicklung bis zur Fertigung und Vermarktung neuer Produkte.

Für einige Länder ist Wirtschaftsspionage ein legitimes Instrument staatlicher Existenzvorsorge.

Vor allem die Russische Föderation und die Volksrepublik China begleiten ihren wirtschaftlichen Aufstieg mit intensiver Wirtschaftsspionage und setzen ihre Nachrichtendienstapparate entsprechend ein.

Beide Staaten sehen im übrigen keinerlei Widerspruch darin, einerseits gute Beziehungen zu Deutschland zu unterhalten und es andererseits mit Spionage zu überziehen.

Russland will zügig die Folgen des Transformationsprozesses überwinden, sich als gleichrangige Macht neben den USA positionieren und den technologischen Abstand zum Westen verringern.
Der zivile Auslandsnachrichtendienst SWR ist auch für die Aufklärung in den Bereichen Ökonomie sowie Wissenschaft und Technologie zuständig. Es sind zahlreiche Äußerungen von russischen Politikern und Nachrichtendienstlern bekannt, wonach die Dienste die nationale Wirtschaft zu unterstützen haben.
Der ehemalige Leiter des SWR, Lebedew, erklärte im November 2005, dass der Nachrichtendienst für den russischen Staat ein gewinnbringendes Unternehmen sei, das für jeden investierten Rubel hundertfachen Profit abwerfe. Insgesamt unterstütze der SWR nicht nur die staatliche Sicherheit Russlands, sondern auch seine Wirtschaft und seine wissenschaftlich-technische Entwicklung.

Ziel der Aufklärung sei es, Informationen über richtungsweisende Entwicklungen in der Wissenschaft und Technik und über neueste Technologien im Ausland zu beschaffen.

Ganz aktuell hat Präsident Putin anlässlich der Amtseinführung des Nachfolgers von Lebedew, des früheren Ministerpräsidenten Fradkow, am 19.

Oktober 2007 erneut den SWR aufgefordert, seine Anstrengungen zu verstärken, um die heimische Wirtschaft und die Interessen russischer Unternehmen im Ausland aktiver zu unterstützen.

Die Beziehungen zwischen der Volksrepublik China und Deutschland entwickeln sich seit Jahren in allen Bereichen.
Für unsere exportorientierte Wirtschaft ist China als einer der wichtigsten Wachstumsmärkte von größter Bedeutung.

Die VR China strebt seit etwa zwei Jahrzehnten mit ansteigender Vehemenz den wirtschaftlichen, wissenschaftlichen und rüstungstechnischen Gleichstand mit den führenden westlichen lndustrienationen an.
Spätestens im Jahre 2020 will China wirtschaftlich und militärisch den USA auf Augenhöhe gegenübertreten können; ein sehr ehrgeiziges Ziel. Fachleute sind sich indes einig, dass diese Aufholjagd nur gelingen kann, wenn u.a. Spitzentechnologie in großem Umfang aus dem Westen beschafft wird. Deutschland ist dabei ein primäres Operationsgebiet.

Die chinesische Führung hat zahlreiche Regierungsprogramme verabschiedet und viele Institutionen und Staatsunternehmen beauftragt, konsequent an der Verwirklichung dieses nationalen Zieles mitzuwirken. Ein ganzer Wust von Gesetzen, Regelungen und Auflagen zwingt deutsche Unternehmen in China ihre Technologien sog. Design-Instituten, Zertifizierungsstellen oder in Joint Ventures offen zulegen.

Zahlreiche Firmen berichten davon, wie schwierig es ist, beim Engagement in China die eigene Technologie und das geistige Eigentum zu schützen.

Auch der chinesische Nachrichtendienstapparat spielt in diesem Prozess eine wichtige Rolle, allen voran das Ministerium für Staatssicherheit MSS. Es zählt zu den Hauptträgern der nachrichtendienstlichen Aktivitäten gegen ausländische Ziele im In- und Ausland.

Das Ministerium für Staatssicherheit ist wahrscheinlich der größte Nachrichtendienst der Welt mit einem geschätzten Personalbestand von mehr als 800.000 Mitarbeitern.

Wenn man weiß, welche Möglichkeiten und vor allem Ressourcen ausländische Nachrichtendienste, z.B. Russlands und Chinas, zur Beschaffung vertraulicher Wirtschaftsinformationen haben, ist es naiv zu glauben, dass diese nicht genutzt werden.

Nachrichtendienste haben ihren Modus operandi, d.h. ihre Vorgehensweisen und Methoden bei der Beschaffung von lnformationen den Bedingungen der Globalisierung angepaßt.

Wir leben heute in einer offenen Informationsgesellschaft.
Das hat u.a. zufolge, dass rund 80% aller lnformationen heutzutage aus frei zugänglichen Quellen erschlossen werden können. Nur noch die restlichen 20% bestehen aus Interna, sowie aus vertraulichen und geheimen Informationen. Laut wissenschaftlichen Erhebungen beträgt der Umfang der geheimen, d.h. der wirklich schützenswerten lnformationen in den Unternehmen im Durchschnitt nur noch 5%. Dieser Teil der Informationen, der natürlich von Unternehmen zu Unternehmen variiert, wird in der Wissenschaft als das „kritische Erfolgswissen" bezeichnet. Das sind sozusagen die ,,Kronjuwelen" oder auch der Wissensvorsprung eines Unternehmens, den es zu bewahren gilt.
Die Globalisierung und die moderne Informationstechnik haben die Arbeitsmethoden der Nachrichtendienste auch noch in anderer Hinsicht verändert. Fast alle Daten und lnformationen sind heute digital verfügbar und können in großen Mengen auf kleinsten Speichern, z.B. einem USB-Stick oder einer CD oft risikolos verbracht werden, sofern sie nicht per lnternet ohnehin weltweit abgerufen werden können. Spionage findet heute auch virtuell statt.

Vor diesem Hintergrund vollzieht sich nachrichtendienstliche Aufklärung und Beschaffung heutzutage subtiler als noch vor Jahren.

Die offene lnformationsbeschaffung gehört eindeutig zu den bevorzugten Methoden fremder Nachrichtendienste in Deutschland.

So zählt hierzu eine gezielte, intensive und kontinuierliche Auswertung aller relevanten Veröffentlichungen in Fachzeitschriften, in Dissertationen, im Internet, in wissenschaftlichen Datenbanken und Firmenpublikationen. Aber auch Werkszeitungen, Handbücher, Patent- und Lizenzunter- lagen und nicht zuletzt Firmenpräsentationen im lnternet können Nachrichtendiensten sehr interessante und aufschlussreiche Einblicke gewähren.
Die Bereitschaft der Unternehmen zu kundenfreundlicher Transparenz bietet auf der anderen Seite fremden Nachrichtendiensten ideale Ansatzpunkte für diese Form der lnformationsbeschaffung .

Die systematische Auswertung offener Quellen lässt nicht nur wertvolle Rückschlüsse auf aktuelles Know-how und zukünftige Projekte zu, sondern liefert auch detaillierte Persönlichkeitsbilder.

Interessante Zielpersonen in den Unternehmen oder im Forschungsbereich können mit diesem Hintergrundwissen gezielt nachrichtendienstlich angegangen werden.

Der Besuch öffentlicher Veranstaltungen, wie Messen, Kongresse und son-

stiger Foren bietet den Nachrichtendienstoffizieren eine ideale Plattform zur lnformationsbeschaffung durch Gesprächsabschöpfung.
Nach Erkenntnissen der Spionageabwehr erlangen Mitarbeiter fremder Nachrichtendienste im Zuge der Gesprächsabschöpfung, bei dem der jeweilige Gesprächspartner nicht um die nachrichtendienstliche Anbindung seines Gegenübers weiß, eine Fülle von Informationen und lnsiderwissen.
Seit etwa 2005 stellen wir auf breiter Ebene elektronische Angriffe über das lnternet auf deutsche Behörden und Unternehmen fest.
Elektronische Spionage stellt eine große Gefahr dar, denn auf diesem Wege können Rechner unbemerkt ausgespäht und dadurch hohe Schäden den Unternehmen zugefügt werden.
Diese Angriffsmethode ist für den Gegner auch deshalb so effizient, weil diese Angriffe risikofrei vom eigenen Territorium unternommen werden können und sowohl der Angreifer als auch der Angriffsweg weitgehend verschleiert werden kann.
Gerade im Zusammenhang mit E-Mail-basierten elektronischen Angriffen auf Computernetzwerke über das lnternet wird der Begriff
des „Social Engineering“ gebraucht.

In der Spionageabwehr verstehen wir darunter das geschickte Abschöpfen von insbesondere persönlichen lnformationen durch Mitarbeiter fremder Nachrichtendienste. Die so erlangten lnformationen werden später in E-Mail-basierten elektronischen Angriffen genutzt; sie sollen dem Empfänger suggerieren, die E-Mail sei in ehrlicher Absicht an ihn gerichtet. Beim Öffnen der E-Mail wird dann unbemerkt ein Trojaner oder andere Schadsoftware installiert.
Doch nicht alle Wissenslücken lassen sich durch offene lnformationsbeschaffung oder Computerspionage schließen.
Nach wie vor setzen fremde Nachrichtendienste auf menschliche Quellen, um an sehr sensible Informationen, an die „Kronjuwelen“ von Unternehmen und Forschungsinstitutionen heranzukommen.

Ihr besonderer Wert besteht darin, dass sie nicht nur aus einem Zielobjekt z.B. einem Unternehmen agieren, sondern zugleich auch beschaffte lnformationen hinterfragen, Produkte fachlich bewerten und Absichten eruieren können.
Bei den Aufklärungsaktivitäten russischer Nachrichtendienste in Deutschland spielen getarnte Stützpunkte in amtlichen russischen Vertretungen, die sog. Legalresidenturen nach wie vor eine wichtige Rolle.
Besonders sensible Agentenverbindungen werden allerdings aus den Zen-

tralen in Russland geführt, da das Entdeckungsrisiko dann deutlich geringer ist.
Auch die VR China nutzt zur lnformationsbeschaffung in Deutschland ihre diplomatischen und konsularischen Vertretungen.
Die dort als Diplomaten abgetarnten Nachrichtendienstoffiziere betreiben vornehmlich offene lnformationsbeschaffung.
Zu Gesprächspartnern mit wertvollen Zugängen wird der Kontakt zielstrebig ausgebaut und als „Freundschaftsbeziehung" fortgesetzt und gepflegt.
Die Angehörigen der offiziellen chinesischen Vertretungen in Deutschland pflegen auch intensive Kontakte zur hiesigen chinesischen Gemeinde; das sind u.a. die zahlreichen chinesischen Fachkräfte, postgraduierte Studenten, Austauschwissenschaftler, Praktikanten und sonstige Fachleute, die Zugang zum deutschen Know-how haben. Sie sind in aller Regel sehr gut organisiert, hochmotiviert und mit Bildungshunger, Karrieredenken und einem hohen Maß an Patriotismus ausgestattet.

Sie sind stolz, am Aufstieg ihres Landes mitwirken zu können und betrachten die umfassende Aneignung deutschen Know-hows nicht unbedingt als etwas Unrechtmäßiges.

Nach der Beschreibung des Phänomens Wirtschaftsspionage in seinen wesentlichen Facetten, stellt sich die berechtigte Frage, welchen Beitrag leisten das BfV und die Verfassungsschutzbehörden der Länder, um diese Gefahr abzuwehren oder zumindest zu minimieren.

Doch zunächst sollte hervorgehoben werden, dass Sicherheit und Schutz des technischen und wirtschaftlichen Know-hows primär in der Eigenverantwortung jedes Unternehmens liegt; optimal ist es, wenn Sicherheit Chefsache ist.

Unabhängig davon ist die systematische und methodische Beobachtung fremder Nachrichtendienste und deren Aktivitäten in Deutschland eine Kernkompetenz der Spionageabwehr des BfV.
Auf der Basis langjähriger nachrichtendienstlicher Erfahrungen und Analysen - die oft mit Partnerdiensten abgeglichenen werden - werden Beratungs- und Sensibilisierungskonzepte erarbeitet, die zielgruppengerecht über die verschiedenen Ausspähungsmethoden fremder Nachrichtendienste aufklären und zugleich Empfehlungen ableiten.

Doch der Schutz sensibler Informationen im Unternehmen ist selbstverständlich mehr als nur die Sicherheit der IT-Systeme.

Der Mitarbeiter ist der wichtigste und wertvollste Produktionsfaktor eines Unternehmens. Mitarbeiter müssen verstehen, dass sie bei unbefugter oder leichtfertiger Weitergabe von Know-how das Unternehmen schädigen, für das sie arbeiten und damit auch ihre Arbeitsplätze gefährden.

Das BfV bietet Awareness- und Sensibilisierungsvorträge und Gespräche an, denn es gilt die Überzeugung, dass Prävention die sicherste Art ist, Schaden im Unternehmen zu vermeiden.

Prävention durch die Zusammenarbeit zwischen Verfassungsschutzbehörden und Unternehmen hat - erfahrungsgemäß - hohe Bedeutung und Akzeptanz. Sie ist Teil der beabsichtigten Optimierung einer Sicherheitspartnerschaft zwischen Staat und Wirtschaft.

Es besteht eine enge Zusammenarbeit mit der Arbeitsgemeinschaft für Sicherheit der Wirtschaft (ASW), der Zentralorganisation der deutschen Wirtschaft in Sicherheitsfragen auf Bundesebene. Die hierzu bestehenden Rahmenregelungen wurden aktuell überarbeitet und weiter optimiert.

Deutsche Unternehmen haben viel zu bieten, allerdings auch viel zu verlieren. Know-how-Schutz ist daher eine besondere Herausforderung für die Wirtschaft und den Staat mit globaler Dimension und strategischer Erfolgsfaktor zugleich.

Das Bundesamt für Verfassungsschutz ist ein kompetenter Ansprechpartner der Unternehmen in Sachen Wirtschaftsspionage.

Grundlage unserer Arbeit sind Vertrauen und Vertraulichkeit.

Nur in enger Zusammenarbeit mit den Unternehmen und aufbauend auf deren Erfahrungen können wirksame Präventivmaßnahmen implementiert werden.

Spionageabwehr ist Teamwork!

Dr. Thomas Menk, Vorsitzender der Arbeitsgemeinschaft für Sicherheit der Wirtschaft (ASW) Leiter Konzernsicherheit Daimler AG

Die Sicherheit der Wirtschaft -Veränderte Bedingungen durch die Globalisierung-

Sicherheit gehört nach herrschendem betriebswirtschaftlichem Verständnis – auch im Zeitalter wirtschaftlicher und politischer Globalisierung - nicht zu den bevorzugten Investitionsfeldern der Wirtschaftsunternehmen. Dieser Sachverhalt muss überraschen, da die Sicherheitsgefährdungen für die Wirtschaft im Zusammenhang der Globalisierung national und besonders international signifikant zunehmen. Die Geschäftsprozesse sind ganz allgemein und mit steigender Tendenz von einer wachsenden Komplexität der mit ihnen verbundenen Sicherheitsrisiken gekennzeichnet.

I. Sicherheitsrisiken im globalen Wettbewerb

Die gegenwärtig vorherrschenden Sicherheitsrisiken und -gefährdungen für weltweit tätige Unternehmen werden bestimmt durch:

- Die voranschreitende Destabilisierung der bisherigen internationalen politischen Ordnungssysteme und ihre Rückwirkungen auf wirtschaftliche Zusammenhänge.
- Angriffe auf schützenswertes Unternehmenswissen durch Wirtschafts- und Konkurrenzspionage sowie reputationsschädigende Desinformationskampagnen.
- Interne und externe kriminelle Angriffe mit standort- und grenzüberschreitenden Deliktsmustern, einschließlich Markenpiraterie und korruptiven Handlungen.
- Häufiges Fehlen verlässlicher Sicherheits- und Krisenmanagementstrukturen in Wirtschaft und Staat.

Dabei ist festzuhalten, dass nicht nur Terrorismus und andere vermeintlich wirtschaftsexterne Faktoren wie Krieg, Bürgerkrieg und sonstige politische Krisen die Wirtschaft bedrohen. Es sind vor allem die immanenten Risiken des weltweiten ökonomischen Netzwerkes, die in Zeiten einer volatilen Wirtschaftsentwicklung zur unberechenbaren Gefahr werden. Zu diesen Risiken gehört vor allem ein aggressiver Wettbewerb, dessen Formen und Instrumente zwischen traditionellem Handel und Wirtschaftskrieg oszil-

lieren.

Gerade Handlungen wie Wirtschafts- und Konkurrenzspionage sowie Markenpiraterie bestimmen zunehmend das Verhältnis der Wettbewerber und ihrer Herkunftsländer zueinander und werden von manchen bereits als „Wirtschaftskrieg“ bezeichnet.

Dabei ist zuzugeben, dass der Begriff des Wirtschaftskrieges ein schwieriges Thema berührt.

Der Begriff „Wirtschaftskrieg“ bezeichnet im deutschen Sprachgebrauch ein Phänomen, das in der Sphäre des Politischen und des Völkerrechts angesiedelt ist. Bisher versteht man darunter einen Konflikt zwischen Staaten oder anderen Völkerrechtssubjekten - der unterhalb der Schwelle des klassischen Krieges - mit wirtschaftlich wirksamen Mitteln ausgetragen wird.

Dem gegenüber geht der Sprachgebrauch in anderen westlichen Staaten, z.B. der französische Begriff der „guerre économique“, weit darüber hinaus, weil er auch nichtstaatliche Akteure, vor allem Wirtschaftsunternehmen und unterstützende Dienstleister aller Art, als „Kriegspartei“ anerkennt und berücksichtigt.
Wirtschaftskrieg ist nach diesem Verständnis in erster Linie ein neuer Modus des Wettbewerbs, der sich durch große Härte und einem weitgehenden Fehlen von Regeln auszeichnet und sowohl staatliche als auch private Akteure umfasst.

Es wird sich zeigen, ob sich ein solchermaßen gewandelter Begriff des „Wirtschaftskrieges“ durchsetzen kann. Die damit verbundenen Handlungen und Gefährdungen sind - oft unterschätzt - längst Realität und keineswegs ein Thema nur für Regierungen und Wissenschaftler. Sie gehören zu den oben erwähnten Herausforderungen des globalisierten Wettbewerbs und betreffen die Unternehmen unmittelbar.

II. Traditionelles Sicherheitsmanagement

Trotz der beschriebenen Risiken nehmen viele Unternehmen Investitionen für ihre Sicherheit nur zurückhaltend vor oder denken sogar darüber nach, bestehende Sicherheitsstrukturen abzubauen. Nach allgemeiner Erfahrung sind hierfür die nachfolgenden Meinungen und Beweggründe ausschlaggebend:

- Das Bewusstsein für die tatsächliche Bedrohung von Wirtschaftsprozessen fehlt oder ist lückenhaft.

- Soweit dieses Sicherheitsbewusstsein besteht, dominiert die häufig zur Überzeugung gewordene Hoffnung, dass mögliche Gefährdungen und Schadensereignisse das Unternehmen nicht betreffen oder „Übertreibungen“ der Sicherheitsmanager sind.

Folgerichtig werden Investitionen in das Sicherheitsmanagement ihrem Wesen nach als unerwünschte, ökonomische Belastungen empfunden. Das Sicherheitsmanagement trägt nach diesem Verständnis nur in geringem Umfang zur Wertschöpfung und damit zum Unternehmenserfolg bei. Die legitime Frage „Was bringt uns das?“ wird in diesem Fall unvermeidlich und überwiegend negativ beantwortet, weil der Zusammenhang zwischen Sicherheit und Unternehmenserfolg entweder verneint oder nur zum Teil anerkannt wird.

Entsprechend häufig ist die Meinung anzutreffen, Sicherheit könne sich auf den Schutz von Mitarbeitern und materiellen Ressourcen (physische Sicherheit) beschränken. Die Neigung, Sicherheitsfunktionen jenseits der physischen Sicherheit - auch solche von großer Empfindlichkeit - kostengünstig an externe Dienstleister zu vergeben (outsourcing), kann vor diesem Hintergrund nicht überraschen.

Es ist offensichtlich, dass das hier beschriebene traditionelle Sicherheitsmanagement Risikofelder von strategischer Bedeutung (Sicherheit der Geschäftsprozesse im In- und Ausland, Informationsschutz und Kriminalitätsbekämpfung) nicht berücksichtigt. Vor allem enthält dieses Konzept keine Elemente der frühen Risikoidentifizierung (Frühwarnsystem) und sieht deshalb kaum präventive Maßnahmen zur Gefahrenabwehr vor. Es folgt überwiegend einem reaktiven Handlungsmuster, dass heißt: Maßnahmen erfolgen in vielen Fällen erst nach Schadenseintritt.

Darüber hinaus berücksichtigt das traditionelle Sicherheitsmanagement den Wertschöpfungsprozess der Unternehmen nur unzureichend. Es fehlt häufig an der engen Verzahnung der Sicherheitsprozesse mit dem jeweiligen Kerngeschäft. Wirtschaftlich relevante Sicherheitsziele (z.B. Schutz des Knowhow) können so nicht erreicht werden. Die Akzeptanz des Sicherheitsmanagements im Unternehmen ist regelmäßig gering.

III. Integriertes Risiko- und Sicherheitsmanagement

Das traditionelle, auf physische Sicherheit fokussierte Sicherheitsmanagement, kann den Herausforderungen des globalen Wettbewerbs nicht begegnen. Seine Grundannahmen und seine Methodik entsprechen weder

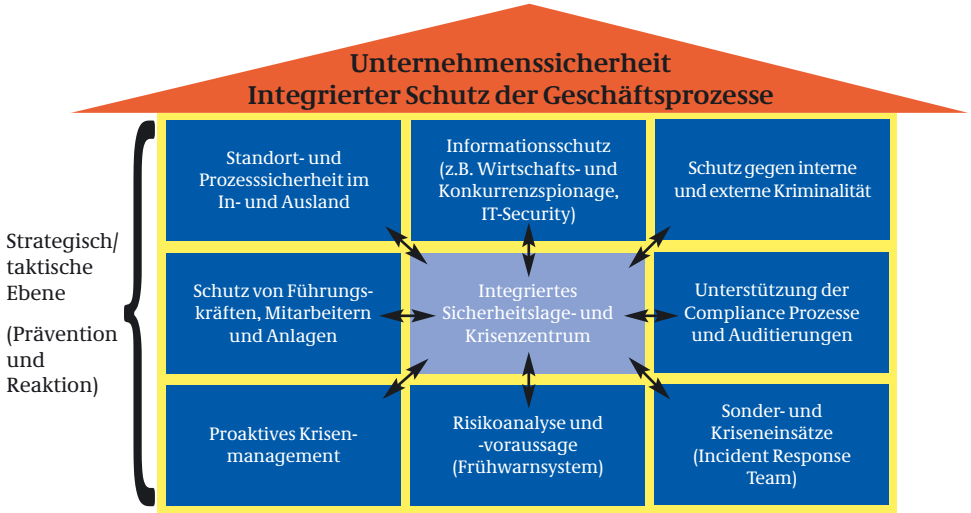
ordnungspolitisch noch betriebswirtschaftlich den Interessen der Unternehmen.

Im Einzelnen gilt:

Die Tatsache vielfältiger Sicherheitsgefährdungen im Zusammenhang eines weltweiten wirtschaftlichen Handelns kann nicht ernsthaft bestritten werden. Das Leugnen oder Verharmlosen der möglichen Bedrohungsszenarien führt nur vordergründig zur Kostenreduzierung und belastet das wirtschaftliche Handeln mit nicht identifizierten und damit tatsächlich nicht beherrschbaren Risiken. Das gilt auch für den Fall, in dem die Hoffnung auf den Nichteintritt von Gefahren und Schäden oder Kostendruck eine verteidigungsfähige Sicherheitsorganisation vereitelt.

Darüber hinaus ist es sicher richtig, dass die Herstellung vollkommener Sicherheit unmöglich ist. Jedoch können Sicherheitsrisiken - je nach Lage und Ressourcen – wirksam verringert und begrenzt werden. Voraussetzung hierfür ist aber das Bestehen eines professionell eingerichteten und ausgeübten Sicherheitsmanagements.

Ein solches Sicherheitsmanagement ist als integriertes Risiko- und Sicherheitsmanagement aufzufassen und beruht methodisch auf dem Grundsatz der umfassenden und frühen Aufklärung und Identifizierung aller Sicherheitsrisiken sowie ihrer integrierten Bearbeitung durch eine unternehmensweit zuständige Sicherheitsorganisation. Die Kernaufgaben einer solchen Organisation stellen sich wie folgt dar:



Dabei ist zu beachten, dass die operative Realisierung der hier beschriebenen Sicherheitsziele methodisch notwendige Grundlagenprozesse voraussetzt. Hierzu gehören u.a.:

- die kontinuierliche Sammlung und Auswertung von sicherheitsrelevanten Informationen mit Unternehmensbezug
- die Identifizierung und Klassifizierung von Sicherheitsrisiken und Gefahren unter Berücksichtigung der Unternehmensstrategie, bzw. der Kerngeschäftsziele und -prozesse (Risikoanalyse)
- die ständige Anpassung von Aufgaben und Maßnahmen an die Sicherheitslage und Geschäftsprozesse

Diesem Verständnis eines präventiv wirksamen integrierten Risiko- und Sicherheitsmanagements hat sich offensichtlich auch der Gesetzgeber angeschlossen, als er im Bereich der Risikohaftung des Vorstandes von Aktiengesellschaften die Haftungsregelung des Aktiengesetzes zum Organisationsverschulden durch die Einführung des KontraG verschärft hat. Das Gesetz präzisiert die Organisationspflicht des Vorstandes und fordert von ihm, „geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden".

Bestandsgefährdende Risiken – hierzu können auch Sicherheitsrisiken gehören – sollen so früh erkannt werden, dass Maßnahmen zur Sicherung des Fortbestandes des Unternehmens rechtzeitig ergriffen werden können.

Im Hinblick auf Funktion, Aufgaben und wirtschaftlichen Nutzen eines effizienten Sicherheitsmanagements bedeutet dies z.B.:

- Die ständige Beobachtung und Prognose von Sicherheitsgefährdungen im In- und Ausland (risk forecast) sind für Erhalt und Fortentwicklung von Unternehmensressourcen und Geschäftsprozessen sowie für Investitionsentscheidungen ein tägliches Erfordernis.
- Der Schutz des Unternehmenswissens gegen Wirtschafts- und Konkurrenzspionage und sonstigen Informationsabfluss gewährleistet die Abwehr potentieller wirtschaftlicher Verluste, vor allem aber die Sicherung der Wettbewerbsfähigkeit.
- Der Schutz gegen sonstige vermögensschädigende und kriminelle Angriffe einschließlich Korruption bedeutet gleichermaßen die Abwehr von wirtschaftlichen Verlusten und damit den Erhalt der Handlungsfähigkeit von Unternehmen.

- Der Schutz vor reputationsschädigender Desinformation bewahrt Ansehen und Integrität der Unternehmen und damit ihre Marktchancen.
- Die Existenz eines schnellen und effektiven Krisenmanagements zeigt, dass die Geschäftstätigkeit von Unternehmen auch unter schwierigen Bedingungen möglich ist.

IV. Sicherheit als Wirtschaftsfaktor

Ein modernes, weit über die traditionelle Aufgabe des physischen Schutzes hinausreichendes Sicherheitsmanagement schützt die für den erfolgreichen Wettbewerb unverzichtbare Überzeugungskraft der Unternehmen und ihrer Produkte, denn im Zentrum erfolgreicher Geschäftstätigkeit steht das Vertrauen der Geschäftspartner und Kunden in die Qualität und wirtschaftliche Beständigkeit von Marke und Produkt. Sicherheit ist deshalb ein an Bedeutung gewinnender Wirtschafts- und Erfolgsfaktor für alle Unternehmen, vom Global Player bis hin zu mittleren und kleinen Unternehmen.

Produktion, Vertrieb und Finanztransaktionen finden nicht in einem virtuellen friedlichen Wirtschaftsraum statt, in dem politische, wettbewerbsbedingte und kriminelle Unsicherheit nicht existiert. Im Gegenteil, nach dem Zusammenbruch der bipolaren Weltordnung unterliegen ökonomische und politische Bedingungen im Weltmaßstab einem beständigen und raschen Wandel mit Auswirkungen auf Wettbewerb und Sicherheitslage bis in die nationalen Volkswirtschaften hinein.

Sicherheit kann deshalb nicht mehr allein als physischer Schutz von Mitarbeitern und materiellen Ressourcen der Unternehmen verstanden werden, sondern als Verteidigung ihres Gesamtgeschäftes gegen Angriffe und Gefährdungen aller Art. Der physische Schutz steht – obwohl nach wie vor erforderlich – deshalb nicht mehr im Vordergrund. Entscheidend ist vielmehr die Sicherheit der Gesamtheit aller Geschäftsprozesse, von der Produktentwicklung bis hin zur Produktvermarktung einschließlich der Sicherung vorteilhafter Wettbewerbsbedingungen.

Nach diesem Verständnis ist Sicherheitsmanagement weder geschäftshemmender Selbstzweck noch kontraproduktive Investition. Im Gegenteil, Sicherheitsmanagement als integraler Produkt- und Geschäftsschutz werden in einer unsicheren Wirtschaftslandschaft zu einem entscheidenden Wettbewerbsfaktor und strategischen Wettbewerbsvorteil. Es kann inso-

weit nicht überraschen, dass Qualität und Erfolg des Sicherheitsmanagements beim Rating von Unternehmen erstmalig und zunehmend an Bedeutung gewinnen.

Sicherheit wird deshalb im Zusammenhang der ökonomischen und politischen Globalisierung zu einem bedeutsamen Wirtschaftsfaktor und unbestreitbar ein aktiver Beitrag zur Wertschöpfung. Investitionen in die Sicherheit von Unternehmen sind daher ein strategisches Element zur Sicherung der Funktions– und Zukunftsfähigkeit von Unternehmen.

Alain Juillet, Haut responsable chargé de l'intelligence économique au près du Premier Ministre

Protection of the French Economy in the Age of Globalization

Der Schutz der französischen Wirtschaft im Zeitalter der Globalisierung

A New World in a New Century

- A new world will be multipole with the pivot of economic exchanges moving west towards Asia.
- A new world will be full of opportunities and threats, with economic pressure being used as a military weapon for an asymetric fight.
- The fast development of information technology will open new possibilities and speed up industrial and commercial processes.

Six Key Factors in a Tough Competition

1. The trade exchange system is not adapted to the new reality of globalization where all poles want to keep an increasing part of their creation of value.
2. States are changing their laws and rules, or exerting pressure to modify standards and use of patterns, in order to protect their home key markets.
3. Willingness to improve financial results or shares of markets and criminial organizations entering the business generate a lack of ethics, a lot of corruption, and a need for public-private partnership.
4. All managers being trained in the same kind of schools, it is increasingly difficult to create and surprise with a really new product or service.
5. The time to place a product on the market is decreasing as well as the time to respond. To be the first in a new market implies the abilitity to respond with the ability to anticipate.

6. The use of legal (alliance or joint venture) or illegal (copy) means allows to speed up the date of entry into the market or to stay in the race.

The Successful Response to Globalization: Develop a New Competitive Advantage

The Need for a New Competitive Advantage

- The development or survival of companies is secured by the creation and defence of a specific advantage which requires to analyse one's own strengths and weaknesses.
- Mastering of information and communications is a strategic issue which allows to improve expertise and the ability to respond.
- Information does not give power anymore but creates value if shared with others.
- All managers must be able to create a gap through the management of expertise and search of information in order to develop a competitive offer or generate a real demand.
- In case you have neither raw materials nor low labour costs, you must become innovative through investing in research and development.
- To strengthen your position you could be at the same time partner and competitor, ally and enemy.

Economic Intelligence: The Right Answer for an Efficient Business

Chosen by the leading countries in the world as the best existing tool and concept to find out and implement succesfully the right answers.

Principles

Collect through a network, within a defined framework, all the data useful for a centralized and published analysis aiming to provide managers with winning options.

It requires control of the sources of information, their management, and use of the contents for setting up strategic actions.

Concept Evolution

This concept has been used for a very long time by states pursuing an offensive trade.

- Japan: Watching out for formal and informal information focused on industry, science and technology
- USA: Competitive intelligence focused on competitors
- UK: Business intelligence focused on competitors and market

Definitions

- French global definition: Economic intelligence aims to master and secure the strategic information which is pertinent for all economic players. It focuses on business plus the social and cultural environment, strategy and technologies.
- French state – oriented definition: Economic intelligence aims to implement a mode of governorship for the search and control of strategic information whose final aim is the competitiveness and safety of the national economy and strategic companies.

Mastering Strategic Information

- 80 to 95 % of the existing information can be legally obtained through human and open technical sources.
- To master it requires the control of the complete process of its acquisition and treatment using adapted and modern tools.
- Starting from the perspective of defining a framework, it implies data research, to select and collect data, to transfer and analyze information, to realize a synthesis and to end with a delivery.

Securing Strategic Information

- As 20 % of the published information is wrong, it is a must to cross-check through multiple sources.
- Knowing that the same tools can be used to master the process, to destroy it, to enter false information into it or to control it externally, security necessitates the protection, flow, storage and publishing of data.

- Among the 100 main financial powers worldwide there are less than 50 states.

Influencing

- Nowadays a good strategy is necessary but not enough to win. Therefore more and more states and companies are using influence techniques.
- Due to increasing media influence, success requires you to communicate on your strategy value at the time when you are developing it.
- Competitors are using more and more indirect tools and techniques to reduce or destroy the efficiency of your strategy.

A Public Policy to implement Economic Intelligence

The French Experience

Reasons for a Public Policy

- To keep your position in the world economic race requires you to use the same tools and techniques as your main competitors.
- Only the state is able to give an impulse and coordinate an action plan on both public and private level.
- A Coordination center managed at top administration level will have to produce an action plan, detect failures, and come up with answers and proposals.

Public Policy Objectives

- The first objective of economic intelligence is to give more competitiveness to companies facing world competition in order to secure tomorrow's employment.
- The second objective is to specially focus on medium-size and small companies to help them to use the method in order to be more offensive and competitive despite their size.
- The third objective is to maintain the state's involvement until economic intelligence operations become one of the standard tools for every company management. After that the state will go back to its own specific segment: defence and security.

Six Main Public Policy Axes

1. Information

- Continuous flow of infomation and adapted communications towards the public and the administration.
- Operations as poles of competitiveness used to promote the concept and show its efficiency.
- Coordination, synthesis and supply of all the information collected worldwide through open sources by the French administration.
- Informal meetings to exchange views with top management level of the companies and senior administration staff.

2. Education and Training

- Agreement on a basic program to be used by all schools and teachers.
- Coordinating the teaching of national institutes, universities, state-controlled and public schools, and chambers of commerce.
- Training for the students and managers of private companies and public administration.
- Definition of all the jobs involved in economic intelligence and establishment of adapted teaching according to special needs.

3. Strategic Areas and Companies

- Definition of strategic high-tech segments using key technologies and listing of the companies involved.
- Safeguarding of selected strategic companies and setting up of regular exchanges on their situation through domestic intelligence services.
- Adaption of our laws, within a European framework, in the field of merger and purchase of strategic companies by foreign investors.
- Implementation of investment funds to finance the development of strategic companies and the control of foreign funds acitivities and policies.

4. International Monitoring and Lobbying

- Support of export companies by checking if competition is fair and balanced with others competitors.
- Regular surveys to check whether countries are using protectionism in order to guarantee equal treatment.
- Creation of task forces on specific issues, e.g. to monitor the compliance of other countries to international agreement.
- Research and lobbying on international organizations to monitor new rules, international laws, standards, patents, etc...

5. Research and Development

- Assessment of monitoring and analysis tools as to their efficiency and safety.
- Promotion of new national and European tools.
- Development of new operation methods adapted to the technical evolution.
- Implementation and promotion of new laboratories and setting scientist to work on economic intelligence.

6. International Relations

- Promotional campaigns to set up links with other countries in order to facilitate exchanges and develop a partnership network.
- Development of a cooperation between allied countries through the support of companies investing and producing there.
- Development of joint actions for international negociations based upon common views or the same objectives.

Public Policy requires Domestic Organization

- At national level, the coordination and impulse are realized through two committees: the Economic Intelligence Group including all the ministries, and the Strategic Segment Group with the main ministries.
- At regional level, the <<prefet>>, as head of the local administration, coordinates the action of all his services and transfers information to the national level.
- At regional level, a Pool of Competitiveness is run by the <<prefet>> but coordinated at national level by the ministry of the interior.

Future of the Economic Intelligence

- For the next fifty years economic intelligence will be what marketing has been for the past fifty years. The way to create a competitive and sustainable advantage.
- We still have a lot to discover about the potential of this discipline, both internally and externally.
- Some people work on legal application, others on sports, others on tourism showing enormous possibilities for the concept, ranging from economic to strategic intelligence.

For further information go to:
www.intelligence-economique.gouv.fr

MDirig Dr. Markus Maurer

„Geheimschutz in der Wirtschaft -Vorbild für den Schutz von Unternehmensgeheimnissen?“-

Die staatliche; d.h. von fremden Nachrichtendiensten gelenkte Ausforschung von Unternehmen und privaten Einrichtungen – allgemein als „Wirtschaftsspionage“ bezeichnet, stellt eine ernstzunehmende Bedrohung für die Kernkompetenzen und Fertigungskapazitäten von Unternehmen und damit natürlich auch indirekt eine Bedrohung von Arbeitsplätzen am Standort Deutschland dar. Ebenso ernst zu nehmen ist aber auch die Ausspähung von Firmengeheimnissen zwischen den Unternehmen – was mit dem gängigen Begriff „Konkurrenzspionage“ umschrieben wird. Dabei verwischen sich die Grenzen zwischen nachrichtendienstlich gesteuerter Ausforschung von Unternehmen – die sich im übrigen nicht auf die Erlangung amtlich geheim zu haltender Informationen beschränkt – und der auf die Ausforschung fremder Unternehmensgeheimnisse gerichteten Aktivitäten von Wettbewerbern zunehmend. Letztlich können beide zu den gleichen wirtschaftlichen Schäden führen, nämlich wenn sie Wettbewerbsvorteile – seien sie technisch/organisatorischer Art oder in Marketingvorteilen begründet - zunichte machen.

Effizienter Schutz von Staats- und Unternehmensgeheimnissen wird zu einem wichtigen Wettbewerbs- und Standortfaktor, denn nicht nur einzelne Unternehmen sind dadurch bedroht, sondern ganze Branchen oder sogar Volkswirtschaften. Die Globalisierung hat die Risiken und Gefährdungen, insbesondere für solche Unternehmen verstärkt, die die Chancen des Weltmarktes durch ihre Exportaktivitäten oder mittels Investitionen im Ausland nutzen. Die Verantwortung für Sicherheitsmaßnahmen sowohl zum Schutz von im staatlichen Interesse geheim zu haltenden Informationen – sog. „Verschlusssachen“ – als auch für den Schutz von Firmengeheimnissen liegt gleichermaßen zunächst in der Verantwortung des Unternehmens. Der Staat kann keinen umfassenden Schutz vor diesen Gefährdungen bieten. Er kann die Unternehmen zwar im Bereich des amtlichen Geheimschutzes zu Schutzmaßnahmen im einzelnen verpflichten, nicht aber generell zum Schutz ihrer eigenen Unternehmensgeheimnisse.

Insofern ist zunächst einmal jedes Unternehmen und insbesondere jede Unternehmensleitung aufgerufen, die notwendigen Schutzmaßnahmen zu treffen. Sicher ist: Nur wer Staats- und Geschäftsgeheimnisse wirksam schützt, qualifiziert sich für sensible Forschungs- oder Entwicklungsauf-

träge. Wer dies nicht tut, kann sich selber erheblich gefährden und verliert an Ansehen bei Auftraggebern und Kunden. Soweit der Schutz staatlicher Geheimnisse (Verschlusssachen) betroffen ist, kann die Wirtschaft schon bisher auf die Unterstützung des Bundesministeriums für Wirtschaft (BMWI) in Zusammenarbeit mit dem Bundesministerium des Innern (BMI) und dem Bundesamt für Verfassungsschutz (BfV) bauen.

Die in diesen Fällen praktizierte „Geheimschutzbetreuung", d.h. die Sicherheitsüberprüfung von Unternehmen und von deren Mitarbeitern, sowie die Beratung und Kontrolle in allen Geheimschutzangelegenheiten sind ein wichtiger und im übrigen auch gebührenfreier Beitrag zur Sicherheit der Unternehmen.

Die Entwicklung des Geheimschutzes

Das BMWI betreut derzeit etwas über 2000 Unternehmen und Firmenniederlassungen mit insgesamt ca. 55 000 sicherheitsüberprüften und zum Zugang zu Verschlusssachen ermächtigten Mitarbeitern und Führungspersonen. Der Anteil von Rüstungsaufträgen oder anderen sicherheitsrelevanten Aufträgen am Gesamtumsatz dieser Firmen ist recht unterschiedlich und rangiert von über 50 % bis unter 5 %. Entsprechend variiert der Anteil der sicherheitsüberprüften Mitarbeiter.

Immer stärker beruhen Rüstungsaufträge - aber auch zivile Großprojekte -, die staatlicherseits gefördert oder insgesamt finanziert werden – wie z.B. das europäische Satellitennavigationssystem Galileo oder das gemeinsam mit Großbritannien und den Niederlanden betriebene Gas-Ultrazentrifugenprogramm - auf internationalen Kooperationen. Internationale Arbeitsteilung, die Bildung von projektbezogenen Konsortien und die Gründung von transnationalen Unternehmen, wie z.B. EADS, machen nicht nur einen grenzüberschreitenden Austausch von schützenswerten Informationen und den Transport sensibler Bauteile und Systemkomponenten zwischen den verschiedenen Produktionsstätten erforderlich, sondern führen auch zunehmend zu einer Intensivierung des internationalen Personalaustauschs. Hier ist das BMWi u.a. bei der Veranlassung von Sicherheits- überprüfungen für ausländische Firmenmitarbeiter, der Genehmigung grenzüberschreitender Verschlusssachentransporte von Dokumenten und Material oder bei den Genehmigungsverfahren für ausländische Besucher in deutschen Betriebsstätten oder umgekehrt (Internationales Besuchskontrollverfahren) eingebunden.

Manche Waffensysteme werden auch an Länder außerhalb der NATO oder der EU verkauft. Da hierbei oft auch Verschlusssachen weitergegeben werden, sind entsprechende Geheimschutzvereinbarungen der Bundesregierung mit den Empfängerländern erforderlich. Die großen Rüstungsunternehmen haben meist aufwändige Sicherungsverfahren und zuverlässige Geheimschutzstrukturen zum Schutz eingestufter Komponenten von Waffensystemen oder militärischem Großgerät aufgebaut und besitzen eine langjährige Erfahrung im Umgang mit Verschlusssachen.

Diese Unternehmen haben naturgemäß ein gesteigertes Interesse am Schutz ihrer Firmengeheimnisse und ihrer Technologie. Um diesem essentiellen Bedürfnis Rechnung zu tragen, sind dort auch ohne spezielle Anforderungen des Geheimschutzes häufig bereits entsprechende Mechanismen etabliert und Vorkehrungen zum Schutz von Firmen-Know-how getroffen worden.

Bei Unternehmen, die nicht ständig Aufträge haben, die unter die Geheimschutzvorschriften fallen, ist die Betreuung naturgemäß aufwändiger. Es müssen oft erst das Bewusstsein für Erfordernisse des Geheimschutzes geweckt und entsprechende Strukturen geschaffen werden.

Schutz von Unternehmensgeheimnissen: Effektives Risikomanagement – Vorbeugung zahlt sich aus

Während große Firmen zum Teil einen erheblichen personellen, organisatorischen und auch finanziellen Aufwand betreiben bzw. betreiben müssen, um ihren Verpflichtungen zum Schutz von Verschlusssachen in Form von Dokumenten oder Gerät nachzukommen, wird Geheimschutz bei kleinen oder mittelständischen Firmen sozusagen „ nebenher“ betrieben und manchmal auch etwas vernachlässigt. Dies gilt auch für den Schutz von Betriebs- und Geschäftsgeheimnissen.

Dabei sollten die Unternehmen selbst ein erhebliches Eigeninteresse am „Wirtschaften in Sicherheit“ haben, um ihre Wettbewerbsfähigkeit als Voraussetzung für die wirtschaftliche Existenz zu erhalten. Das gilt für die DAX – Schwergewichte ebenso wie für mittelständische Unternehmen, deren Wettbewerbsvorteile wesentlich sind für ihren Erfolg und vielleicht sogar für ihren Bestand.

Im Rahmen eines effektiven Risikomanagements gilt es, Bedrohungen frühzeitig zu erkennen, Gefährdungen zu analysieren und über geeignete Vorbeugemaßnahmen einen angemessenen Schutz von Firmen- und Betriebsgeheimnissen sicherzustellen.

Effektives Risikomanagement auf dem Gebiet der Wirtschafts- und Konkurrenzspionage sollte ebenso wie beim Geheimschutz mit zu den wichtigen Unternehmenszielen zählen und – das ist besonders hervorzuheben -: es muss zur Chefsache werden.

Diesem Erfordernis hat auch der Gesetzgeber zur Geltung verholfen, indem er die Haftungsregelung des Aktiengesetzes zum Organisationsverschulden in diesem Punkt verschärft hat. Mit dem „Gesetz zur Kontrolle und Transparenz im Unternehmensbereich", das am 1. Mai 1998 in Kraft getreten ist, werden Unternehmensleitungen verpflichtet, ein unternehmensweites Früher- kennungssystem für Risiken einzuführen und zu betreiben. Wörtlich heißt es in § 91 Abs. 2 Aktiengesetz: „Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden." Es besteht unter anderem eine Schadens- ersatzpflicht für Vorstandsmitglieder, die ihre diesbezüglichen Pflichten verletzen.

Auch wenn es kein Patentrezept für ein „ideales Risikomanagement" gibt, so gibt es doch allgemein anwendbare Handhabungsschemata, die im wesentlichen einen Katalog an Prüf- und Umsetzungsschritten vorgeben. Unter Hinweis auf die unterschiedliche Größe der Unternehmen und die Vielgestaltigkeit der Branchen und Strukturen hat der Gesetzgeber die Entwicklung der Risikomanagementsysteme letztlich aber der Praxis überlassen. In Zeiten sich intensivierender globaler Risiken lassen sich sicherheitsrelevante Erfordernisse allerdings nicht länger als lästige zusätzliche Kosten und bürokratische Belastungen darstellen. Es sind vielmehr notwendige Investitionen in die mittel- und langfristige Wettbewerbsfähigkeit von Unternehmen.

Geheimschutz in der Wirtschaft Vorbild für den Schutz von Unternehmensgeheimnissen?

Im folgenden möchte ich nun die Vorkehrungen und Grundsätze zum Schutz von Verschlusssachen im Rahmen des amtlichen Geheimschutzes in der Wirtschaft näher erläutern und dabei versuchen aufzuzeigen, inwieweit diese Maßnahmen auch generell zum Schutz von Unternehmensgeheimnissen taugen können.

Schutzvorkehrungen aus dem amtlichen Geheimschutz sind keine Wunderwaffen zum Schutz von Firmen-Know-how. Dazu sind die Maßnahmen in vielen Bereichen zu spezifisch und manche aus rechtlichen Gründen außerhalb des Geheimschutzes nicht praktikabel.

Die angewandten Schutzmaßnahmen sind aber – in angepasster Form - durchaus dazu geeignet, Unternehmensgeheimnisse und Firmen-Know-how auch außerhalb der geheimschutzbetreuten Industrie wirksam zu schützen. Es sind schlichtweg Maßnahmen, deren Umsetzung und Beachtung sich bewährt haben.

Ich will und kann nun nicht alle Maßnahmen aufzählen, die im amtlichen Geheimschutz Anwendung finden. Ich will nur ein paar Punkte nennen, die von fundamentaler Bedeutung sind und mehr oder weniger auch allgemein zum Instrumentarium gehören sollten, wenn ein Unternehmen seine Unternehmensgeheimnisse angemessen schützen will.

1. Identifizierung von schützenswerten Informationen

Im amtlichen Geheimschutz ist die zu schützende Information klar definiert: Hier geht es um den Schutz von im staatlichen Interesse geheim zu haltenden Angelegenheiten, die von einer amtlichen Stelle oder auf deren Veranlassung als solche identifiziert, im Geheimhaltungsgrad eingestuft und als solche gekennzeichnet worden sind. Dies nennen wir Verschlusssachen. Hierfür gibt es klare Behandlungsvorschriften. Damit fallen Informationen, die aus anderen Gründen geschützt werden sollen (z.B. personenbezogene Daten, kommerziell sensitive Informationen, andere Geschäftsgeheimnisse oder firmeneigenes Know-how), nicht unter den amtlichen Geheimschutz.

Bei jedem Konzept zum Schutz von Unternehmensgeheimnissen muss – entsprechend wie beim amtlichen Geheimschutz – zunächst Klarheit geschaffen werden, welche Informationen oder Gegenstände vor unbefugtem Zugriff von innerhalb und von außerhalb des Unternehmens geschützt werden müssen.

Dabei ist von Bedeutung, welche Informationen oder Unternehmens-Interna für ein Konkurrenzunternehmen oder einen Dritten überhaupt interessant sein können und welche Art Schaden der Firma durch den Abfluss der Information entstehen könnte.

Dies gestaltet sich zwar oft als sehr schwierig, ist aber Vorraussetzung dafür, um ein praktikables Know-how-Schutzkonzept zu entwickeln und umzusetzen. Sobald man innerhalb eines Unternehmens Klarheit darüber hat, welche Informationen oder Gegenstände vor unbefugten Dritten geheim gehalten werden sollen, müssen solche Informationen und ggf. auch Gegenstände, Geräte oder Anlagen entsprechend gekennzeichnet werden,

damit diese Dokumente oder Gegenstände auch innerhalb des Unternehmens klar und eindeutig als „sensibel“ erkennbar sind und besonderen Behandlungskriterien unterliegen.

2. Baulich-Technische Schutzmaßnahmen

Nach dem aus den NATO-Sicherheitsvorschriften bekannten Prinzip „Defence in Depth“ (soll heißen: Staffelung von Schutzmaßnahmen von außen nach innen) beginnt Geheimschutz bereits mit der Sicherung von Betriebsgelände und Gebäuden. Diese müssen zuverlässig gegen das Eindringen durch Unbefugte von außen geschützt werden. D.h. u.a., dass an den Eingängen Zugangskontrollen erfolgen müssen. Heutzutage geht es nicht mehr nur um diese konventionellen Sicherungsmaßnahmen, sondern z.B. um Lauschabwehrmaßnahmen für Besprechungen, den Umgang mit den von Mitarbeitern benutzten persönlichen elektronischen Geräten, Mobiltelefonen usw. Hier bestehen erhebliche Gefahren, denen vorzubeugen ist. Die entsprechenden Maßnahmen, die im Bereich des Geheimschutzes getroffen werden, können selbstverständlich als Vorbild für den Schutz von Unternehmensgeheimnissen dienen.

3. IT-Schutzmaßnahmen

Die IT – Sicherheit gehört heute sicherlich zu den am meisten unterschätzten Risikobereichen. Psychologen haben dieses Phänomen als das „It won’t happen-to-me-Syndrom“ beschrieben. Bestärkt wird diese Einstellung dadurch, dass ein potentieller Schaden im Regelfall nicht unmittelbar eintritt und oft auch gar nicht bemerkt wird. Es ist im übrigen auch falsch, zu glauben, dass die Datenausspähung immer von außen kommt – wogegen man ja durch eine Firewall geschützt sei. Man macht sich nicht klar, dass eine Firewall kein absolut sicherer Schutz ist und dass die Gefahr häufig von innen kommt. Häufig sind es eigene Mitarbeiter, die sich – bewusst oder auch unbewusst - zum Werkzeug von interessierten externen Konkurrenten machen. Sofern Verschlusssachen auf IT-Systemen bearbeitet werden sollen, muss hierfür eine besondere Sicherheitsanweisung, die sog. „IT-Geheimschutzanweisung“, erstellt werden. Diese Anweisung legt die einzuhaltenden technischen und organisatorischen Sicherheitsmaßnahmen sowie die Zugangsberechtigungen zum IT-System fest.

Auch außerhalb des Geheimschutzes könnten entsprechende Sicherheitsanweisungen generell den Umgang mit IT-Systemen regeln sowie die Nutzung von privaten Geräten festlegen. Deren Nutzung ist im Geheimschutz

generell nicht zulässig und sollte auch sonst in sensiblen Bereichen zum Schutz von Unternehmensgeheimnissen eher restriktiv gehandhabt werden. In den für jedermann verfügbaren Empfehlungen zum IT-Grundschutz beschreibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) im übrigen in ausführlicher Form die Risiken und die möglichen Schutzmaßnahmen für IT–Systeme.

Erhöhte Risiken bestehen generell bei der Nutzung von Telekommunikationseinrichtungen, insbesondere Mobiltelefonen. Das BMWi hat hier in Zusammenarbeit mit dem BSI spezielle Leitfäden für die geheimschutzbetreute Industrie erarbeitet, in denen auf die besonderen Risiken beim Betrieb von Telekommunikationsanlagen sowie der Nutzung von Mobil- telefonen hingewiesen wird. Sie geben Orientierungshilfen für firmeninterne Schutzvorkehrungen und Regelungen. Für die elektronische Übertragung von Informationen über Internet, z.B. per Email sollte der Einsatz von speziell zertifizierten Verschlüsselungssystemen in Betracht gezogen werden, wie diese z.B. für die Übermittlung von VS–NfD vorgeschrieben sind.

Zuverlässige Verschlüsselungsverfahren existieren auch für Festplatten von Laptops und USB – Sticks, die es bei Verlust oder Diebstahl einem Dritten nur mit erheblichem Aufwand möglich machen, Zugriff zu den Daten zu erhalten.

4.Verbleibskontrolle von Dokumenten und Datenträgern

Die Verbleibskontrolle von Dokumenten und Datenträgern ist beim Geheimschutz ein wichtiges Thema, das sicher nicht vernachlässigt werden darf. Hierbei ist selbstverständlich auch die zuverlässige Vernichtung und Löschung von Dokumenten oder Datenträgern ein Thema. Dasselbe gilt auch für den folgenden Punkt.

5. Weitergabe und Veröffentlichung von Informationen

Die Weitergabe von Verschlusssachen an Dritte sowie die Verbringung von Verschlusssachen unterliegt, abhängig vom Geheimhaltungsgrad, strengen Regelungen. Auch wenn dies in Deutschland anders sein sollte, so ist doch – wie gerade der Verlust zweier CD – ROMs mit Personaldaten auf dem Postweg in Großbritannien gezeigt hat - der Versand auf dem normalen Postweg auch bei uns keine ratsame Versandart für sensible Firmendaten, zumal, wenn sie nicht einmal verschlüsselt sind.

6. Benennung eines Sicherheitsverantwortlichen im Unternehmen

In der geheimschutzbetreuten Industrie muss durch die Geschäftsleitung ein sog. „Sicherheitsbevollmächtigter" sowie ein ständiger Vertreter vor Ort benannt werden. Dieser soll der Geschäftsleitung unmittelbar unterstellt sein und muss als eine Art „zentrales Sicherheitsorgan" im Unternehmen mit den entsprechenden Befugnissen ausgestattet werden, um die vom Unternehmen übernommenen Verpflichtungen im Rahmen des amtlichen Geheimschutzes wirksam erfüllen zu können. Der Sicherheitsbevollmächtigte ist gleichzeitig auch Ansprechpartner des BMWi und der Verfassungsschutzbehörden. Der Sicherheitsbevollmächtigte wird vom BMWi ausführlich in seine Aufgaben im Rahmen des amtlichen Geheimschutzes eingewiesen. Zudem werden weitergehende Schulungen und Fachseminare angeboten.

Für die Verwaltung von Verschlusssachen ist außerdem ein im Umgang mit Verschlusssachen geschulter „Verschlusssachenverwalter" zu benennen. Sofern Verschlusssachen auch auf IT-Systemen bearbeitet werden, ist von den Firmen ferner ein sog. „IT-Sicherheitsbevollmächtigter" zu benennen, der für die Einhaltung der IT-Sicherheitsmaßnahmen zum Schutz von Verschlusssachen verantwortlich ist.

Auch unabhängig vom Geheimschutz ist die Benennung eines Sicherheitsverantwortlichen in einem Unternehmen sinnvoll. Die benannte Person soll die Geschäftsleitung bei der Umsetzung von Sicherheitsmaßnahmen beraten und kann auch als „Vertrauensperson" Ansprechpartner der Sicherheitsbehörden sein. Für die Umsetzung von Maßnahmen im Rahmen der IT-Sicherheit benötigt man selbstverständlich entsprechend spezifisches Fachwissen. Dies ist manchmal nicht verfügbar, sodass Hilfe von außen benötigt wird. Auch bei der Erstellung von Risikoanalysen und Informationsschutzkonzepten in Firmen benötigt man entsprechende Erfahrung, die sich Unternehmen oft von außerhalb holen müssen. Auf der anderen Seite sind leider nicht alle Firmen, die Sicherheitsdienstleistungen oder Sicherheitsberatung anbieten, auch wirklich kompetent. Hier ist die Frage, inwieweit Fachverbände oder Industrie- und Handelskammern in der Lage sind, kompetente Firmen nachzuweisen.

7. Grundsatz „Kenntnis nur, wenn nötig"

Zu einem der wichtigsten Grundsätze im Geheimschutz zählt, dass Verschlusssachen nur an entsprechend ermächtigte Personen nach dem Grundsatz „ Kenntnis nur, wenn nötig" zugänglich gemacht werden dür-

fen. Dies bedeutet in der Praxis, dass Verschlusssachen – auch wenn der Mitarbeiter die generelle Ermächtigung zum Zugang zu Verschlusssachen hat – diesem nur dann zugänglich gemacht werden dürfen, wenn seine Kenntnisnahme für die Wahrnehmung seiner Aufgaben in der Firma oder die konkrete Mitarbeit an einem Projekt unbedingt erforderlich ist. Dieses Prinzip ist - wenn es konsequent umgesetzt wird - besonders geeignet, um dem unerwünschten Abfluss von Unternehmensgeheimnissen und Know-how entgegenzuwirken. Nicht jeder in der Firma – auch auf der Führungsetage - muss alles wissen. Praktikanten und Aushilfskräfte, aber auch vorübergehend tätige Mitarbeiter von Service- oder Beratungsfirmen, sollten aber auf keinen Fall schon nach wenigen Tagen uneingeschränkt oder unkontrolliert Zugang zu Betriebsräumen oder zu Firmennetzwerken erhalten. Besondere Aufmerksamkeit verdienen im übrigen auch Besucher. Nur eine effektive Kontrolle von Besuchern, d.h. ggf. über eine permanente Beaufsichtigung, kann verhindern, dass vermeintliche Kunden oder interessierte ausländische Delegationen unkontrolliert etwa Zugang zu Entwicklungsabteilungen haben oder sich anderweitig Kenntnis von neuen Entwicklungen oder sonstigen sensiblen Firmendaten verschaffen können.

8. Innerbetriebliche Anweisungen, Schulungen, Kontrollen

Die Maßnahmen zum Schutz von Verschlusssachen sind in dem vom BMWi herausgegeben „Handbuch für den Geheimschutz in der Wirtschaft“ zusammengefasst. Auf dieser Grundlage erstellen die geheimschutzbetreuten Unternehmen entsprechende firmeninterne Sicherheitsanweisungen, in denen – neben den Verpflichtungen zum Schutz von Verschlusssachen – oft auch weitergehende Verhaltensregeln zur allgemeinen Unternehmenssicherheit sowie zur Behandlung anderer sensibler Informationen aufgenommen werden. Diese firmeninternen Anweisungen haben sich in der Praxis bewährt, zumal sie häufig auch in einem einheitlichen Sicherheitshandbuch zusammengefasst sind. Besonders wichtig ist im Geheimschutz die regelmäßige Unterweisung der Mitarbeiter über ihre Geheimschutzverpflichtungen sowie die Strafbarkeit bei Zuwiderhandlungen. Die zum Zugang zu Verschlusssachen ermächtigten Mitarbeiter müssen regelmäßig entsprechende Belehrungsnachweise unterschreiben. Die Aufklärung und Sensibilisierung von Mitarbeitern über die Risiken des Informationsabflusses sowie eine regelmäßige Schulung von Mitarbeitern im Umgang mit sensiblen Firmendaten oder Belehrungen über geltende firmeninterne Sicherheitsregelungen sind generell ein wesentlicher Bestandteil innerbetrieblicher Informationsschutzkonzepte und daher un-

verzichtbar. Auch firmeninterne Kontrollen sind unerlässlich, sind sie doch dazu geeignet Schwachstellen aufzuzeigen oder sogar Fehlverhalten von Mitarbeitern aufzudecken.

9. Vertragliche Verpflichtungen von Mitarbeitern

Im Rahmen des Geheimschutzes in der Wirtschaft ist es eine Voraussetzung, dass die Verpflichtung zur Geheimhaltung über eine Zusatzvereinbarung zum Arbeits- oder Anstellungsvertrag gleichzeitlich Bestandteil der arbeitsrechtlichen Beziehung zwischen Unternehmen und Mitarbeitern wird. Verstößt ein Mitarbeiter gegen seine Geheimhaltungspflichten, dann verstößt er damit gleichzeitig gegen seinen Arbeitsvertrag und ermöglicht in der Folge arbeitsrechtliche Maßnahmen, bis zu einer fristlosen Kündigung.
Außerhalb des Geheimschutzes kommen vergleichbare vertragliche Geheimhaltungsvereinbarungen mit Beschäftigten in Betracht, die neben einer fristlosen Kündigung, ggf. auch Schadensersatzforderungen an den Mitarbeiter/die Mitarbeiterin ermöglichen. Zusätzlich können spezielle Wettbewerbsverbote oder Kundenschutzvereinbarungen und deren Absicherung über Vertragsstrafen ein wirksames Mittel sein. Natürlich kann es hier im Einzelfall Beweisschwierigkeiten geben. Dies sollte aber nicht dazu führen, von vorneherein auf eine arbeitsvertragliche Absicherung zu verzichten.

10. Zuverlässigkeitsüberprüfungen von Beschäftigten

Bekanntermaßen ist der größte Risikofaktor der Mensch. Mehrere Untersuchungen zu Fall- und Schadensanalysen bei Know-how/Informationsverlusten sowie zuletzt auch die Studie zu Industriespionage in Deutschland von Corporate Trust, kommen zum Ergebnis, dass der größte Teil der Täter in der Mitarbeiterschaft zu suchen ist. Darunter durchaus auch Personen aus dem Top-Management.

Ein besonderes wichtiges Mittel im Rahmen des personellen Geheimschutzes ist deshalb die vorherige Durchführung einer Sicherheitsüberprüfung nach den Vorschriften des Sicherheitsüber- prüfungsgesetzes für Beschäftigte von Firmen, die Zugang zu Verschlusssachen ab dem Geheimhaltungsgrad VS-VERTRAULICH erhalten sollen. Auch dies ist natürlich keine Gewähr dafür, dass einzelne Mitarbeiter/innen sich in diesem Zusammenhang immer korrekt verhalten. Trotzdem lassen sich mit diesen Überprüfungen doch in manchen Fällen Risiken feststellen und durch entsprechende Maßnahmen ausschalten.

Sicherheitsüberprüfungen sind auch im Rahmen des vorbeugenden Sabotageschutzes für die Überprüfung von Personen in lebens- und verteidigungswichtigen Einrichtungen möglich. Durch diese Sicherheitsüberprüfungen sollen Mitarbeiter/innen identifiziert werden, die eine politisch oder weltanschaulich extremistische Haltung und damit eine gegenüber unserer freiheitlich demokratischen Grundordnung feindliche Einstellung manifestiert haben, eine mangelnde charakterliche Eignung aufweisen oder aufgrund finanzieller Schwierigkeiten oder anderer Umstände besondere Angriffspunkte für fremde Geheimdienste bieten. Falls sie auf Grund fachkundiger Bewertung durch den Bundesverfassungsschutz und das BMWi deswegen ein Sicherheitsrisiko darstellen, müssen sie von Verschlusssachen oder sensiblen Einrichtungen ferngehalten werden. Dieses Instrument steht aber nach der derzeitigen Rechtslage für andere Zwecke als für die nach dem Sicherheitsüberprüfungsgesetz nicht zur Verfügung.

Für effektive Zuverlässigkeitsüberprüfungen von Mitarbeitern oder künftigen Mitarbeitern stehen den Firmen außerhalb des Geheimschutzes kaum effiziente Mittel zur Verfügung. Maßnahmen im Rahmen des sog. „Pre-Employment-Screening" stoßen sehr schnell auch datenschutzrechtlich an ihre Grenzen. Das bedeutet aber nicht, dass es für Unternehmen keine Möglichkeiten gibt, Auskünfte über einen künftigen Mitarbeiter einzuholen. Wichtig ist in diesem Zusammenhang zunächst einmal, dass sich das Unternehmen vor der Einstellung Gedanken darüber macht, ob der zukünftige Mitarbeiter oder die Mitarbeiterin mit sensiblen Informationen oder sensiblen Tätigkeiten in Berührung kommt. Daraus ergibt sich dann, ob eine vertiefte Zuverlässigkeitsprüfung erforderlich ist. Wie im Geheimschutz kann der Bewerber gebeten werden, Auskunfts- oder Referenzpersonen entweder bei seinem früheren Arbeitgeber oder aus seinem persönlichen Umfeld zu benennen, die dann auch über den Betroffenen befragt werden können. Unverzichtbar erscheint mir, dass das Unternehmen, welches eine(n) Bewerber/in einstellen möchte, ein persönliches Bewerbungsgespräch vornimmt. Neben Tests zur Feststellung der fachlichen Eignung kommt hier das Gespräch eines mit der Einstellung von Personal erfahrenen Fachmannes mit psychologischen Kenntnissen in Betracht. Auf jeden Fall sollten Unternehmen sich beglaubigte Kopien von Zeugnisdokumenten oder sonstigen wichtigen Zertifikaten und nicht nur einfache Kopien vorlegen lassen. Die vermehrt in großen Unternehmen gängige Praxis von „Online-Bewerbungen" sollte auf jeden Fall durch das persönliche Auswahlverfahren ergänzt werden. Mitarbeiter, die Zugang zu sensiblen Firmendaten haben und diese - gleich aus welcher Motivation heraus - unbefugt nach außen weitergeben wollen, sind mit technischen Schutzvorkehrungen und meist auch durch organisatorische

Maßnahmen nur schwer daran zu hindern. Weder die Personenüberprüfung nach dem SÜG im Geheim- und Sabotageschutz noch die sonst vor Einstellungen durch Unternehmen angestellten Prüfungen und Tests können verhindern, dass sich aufgrund von Fehlentwicklungen oder Enttäuschungen im Berufsleben möglicherweise einmal Loyalitätsverstöße ergeben. Dies kann wahrscheinlich nur durch sorgfältige und konsequente, aber auch sensible Personalarbeit vermieden werden.

11. Vertraulichkeitsvereinbarungen zwischen den Unternehmen

Im Geheimschutz muss die Verpflichtung zum Schutz von Verschlusssachen und die Einhaltung der geltenden Sicherheitsvorschriften in einer sog. „ Geheimschutzklausel“ in einen Liefer- oder Leistungsvertrag zwischen Auftraggeber und Auftragnehmer aufgenommen werden, sofern im Rahmen des Vertrages die Überlassung oder Erstellung von Verschlusssachen vorgesehen ist. Auch außerhalb des Geheimschutzes empfehlen sich entsprechende vertragliche Vertraulichkeitsvereinbarungen sowie besondere Nutzungs- und Weitergabebeschränkungen von überlassenem Know-how, auch in Bezug auf Produktionstechniken und Anlagen. Sie alle wissen aber auch, dass der Schutz von geistigem Eigentum bzw. Know-how bei der Kooperation mit ausländischen Geschäftspartnern in einigen Ländern nicht ausreichend gewährleistet, bzw. schwer durchzusetzen ist. Ferner ist zu berücksichtigen, dass Informationen auch über die gezielte Beteiligung an Unternehmen durch ausländische Konkurrenten beschafft oder im Rahmen von Joint Ventures, Kooperations-, Forschungs- oder Entwicklungsverträgen abfließen können. Bei Joint Ventures im Ausland sind die Gefahren für den Schutz des geistigen Eigentums und Unternehmens-Know-hows besonders groß. Hier muss jedes Unternehmen prüfen, wie es sich schützen kann, oder ob es das Risiko eines Know-how-Abflusses in Kauf nehmen kann.

Wegen der volkswirtschaftlichen Bedeutung solcher Gefahren beabsichtigt die Bundesregierung, im Außenwirtschaftsrecht ein besonderes Kontrollverfahren vorzusehen, das eine Prüfung und eine Untersagung von ausländischen Investitionen in Deutschland ermöglicht, wenn dies aus Gründen der öffentlichen Ordnung oder Sicherheit unerlässlich ist. Das Außenwirtschaftsgesetz sieht sie bereits vor bei Investitionen in Unternehmen, die Kriegswaffen, bestimmte Rüstungsgüter oder Kryptosysteme herstellen oder entwickeln.

Zusammenfassung

Der Staat kann keinen umfassenden Schutz vor Bedrohungen oder Gefährdungen bieten, die sich aus der Globalisierung der Weltwirtschaft ergeben. Das einzelne Unternehmen, das die Chancen des Marktes - und das heißt auch der Globalisierung - wahrnimmt, muss sich auch mit den Risiken auseinandersetzen. Nur das einzelne Unternehmen, das im Markt operiert und sich entsprechend organisiert, kann über das Erfordernis und die Angemessenheit von Schutzmaßnahmen entscheiden. Der Staat kann und sollte auch nicht einzelne Schutzmaßnahmen vorschreiben. Das heißt aber wiederum nicht, dass dem Staat und seinen Behörden das Schicksal seiner Unternehmen gleichgültig sein kann. In erster Linie hat er aber die Verantwortung für den Schutz amtlicher Geheimnisse. Daneben muss er Rahmenbedingungen, d.h. Schutzinstrumente für die Wirtschaft, zur Abwehr von Bedrohungen zur Verfügung stellen, z.B. über die Strafbewehrung von Bedrohungsaktivitäten und ihre strafrechtliche Verfolgung. Er hat die Aufgabe, das geistige Eigentum in seinen verschiedenen Formen - sowohl national als auch international – zu schützen. Er kann – wie ausgeführt – sein außenwirtschaftliches Instrumentarium zum Schutz von Verteidigungs- und Sicherheitsinteressen einsetzen. Im Hinblick auf die Sicherung des Wirtschafts-und Technologiestandortes Deutschland liegt es im Interesse des Staates, die Wirtschaft darüber hinaus gegen Wirtschaftsspionage im weiteren Sinne, gegen Sabotage und terroristische Bedrohungen zu unterstützen. Die Weitergabe von Wissen über die im Geheimschutz erprobten und bewährten Maßnahmen könnten den Unternehmen beim Schutz ihrer Unternehmensgeheimnisse sicherlich helfen. Entscheidend aber dürfte sein, dass sich in den Unternehmen überhaupt das Bewusstsein entwickelt, dass es schützenswerte Informationen in den Betrieben gibt, und dass man Schutzmaßnahmen aktiv ergreifen muss.

Das Bundesministerium für Wirtschaft begrüßt ausdrücklich die Initiative des BfV, diese Problematik vertieft zu erörtern und dabei die unterschiedlichen Risikofaktoren und Verantwortungsbereiche sowie Abwehr- und Schutzmaßnahmen zu identifizieren. Nach meinem Eindruck ist es darüber hinaus erforderlich, zu überlegen, in wieweit ein sicherheitspartnerschaftliches Zusammenwirken von Bundes- und Landesbehörden auf der einen und Wirtschaftsverbänden und Unternehmen auf der anderen Seite erforderlich ist und - soweit vorhanden - intensiviert werden kann.

Einige Bundesländer engagieren sich in diesem Bereich bereits seit längerem. Sie haben Sicherheitsforen oder Sicherheitspartnerschaften begrün-

det und scheinen auf einem guten Weg zu sein. Ich habe allerdings den Eindruck, dass die Kommunikation und der Informationsfluss zwischen diesen Partnern, insbesondere auch bei Auslandsaktivitäten - im Interesse einer wirksamen und erfolgreichen Gefahrenabwehr – noch verbessert werden kann.

Die Autoren

Merkel, Wilma, Prof. Dr.	Universität Lüneburg
Kahle, Egbert, Prof. Dr.	Universität Lüneburg
Sassenscheidt-Grote, Frank	Bundesamt für Verfassungsschutz
Kurek, Herbert	Bundesamt für Verfassungsschutz
Menk, Thomas, Dr.	Arbeitsgemeinschaft für Sicherheit der Wirtschaft (ASW) Leiter Konzernsicherheit Daimler AG
Juillet, Alain	Haut responsable chargé de l'intelligence économique au près du Premier Ministre
Maurer, Markus, Dr.	Bundesministerium für Wirtschaft und Technologie