Wirtschafts- und Industriespionage im deutschen Wirtschaftsraum: eine analytische Betrachtung von Akteuren, Methoden und Gefahren

Wolff, Daniel

Arbeitspapier / working paper

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
SSG Sozialwissenschaften, USB Köln

AIPA 3/2009

Arbeitspapiere zur Internationalen Politik und Außenpolitik

Daniel Wolff

Wirtschafts- und Industriespionage im deutschen Wirtschaftsraum: Eine analytische Betrachtung von Akteuren, Methoden und Gefahren

Lehrstuhl Internationale Politik
Universität zu Köln

ISSN 1611-0072

AIPA 3/2009

Arbeitspapiere zur Internationalen Politik
und Außenpolitik

Daniel Wolff

Wirtschafts- und Industriespionage im deutschen Wirtschaftsraum: Eine analytische Betrachtung von Akteuren, Methoden und Gefahren

ISSN 1611-0072

Herausgeber:

Lehrstuhl Internationale Politik

Universität zu Köln, Gottfried-Keller-Str. 6, 50931 Köln

Druck:

Hausdruckerei der Universität zu Köln

Redaktionelle Bearbeitung:

Anna Daun, Linda Müller

Köln 2009

Abstract

Sieht sich der deutsche Wirtschaftsraum einer Bedrohung durch Wirtschafts- und Industriespionage ausgesetzt? Zur Beantwortung dieser Frage beleuchtet die vorliegende Studie die gestiegene Bedeutung ökonomisch ausgerichteter Spionage in einem sich rapide verändernden Marktumfeld. Der Autor gibt einen Überblick über die in diesem Umfeld handelnden *Gruppierungen*, die von ihnen zur Informationsabschöpfung eingesetzten *Methoden* und darüber, welche *Gefahren* aus der höchst unterschiedlichen Rezeption und Verarbeitung des Phänomens erwachsen. Ein Schwerpunkt der Analyse liegt dabei auf den Auswirkungen eines veränderten, durch Globalisierung und Transnationalisierung geprägten Marktumfeldes.

Die Analyse zeigt, dass der deutsche Wirtschaftsraum nicht zuletzt aufgrund einer unter seinen defensiven Akteuren vorherrschenden *Schweige- und Stillhaltekultur* Teil eines besonderen Gefahrenraums in Bezug auf Vorgänge von Wirtschafts- und Industriespionage ist. Es besteht daher ein dringender Bedarf an ganzheitlichen Informationsschutzkonzepten für Staat und Wirtschaft, auf deren erste Ansätze abschließend verwiesen wird.

Daniel Wolff

hat Wirtschaftswissenschaften mit politikwissenschaftlichem Schwerpunkt an den Universitäten Bonn und Köln studiert.

Kontakt: dwolff@deloitte.de

INHALT

Abbildungsverzeichnis

Abkürzungsverzeichnis

ATTAC	Association pour une taxation des transactions financières pour l'aide aux citoyens, dt.: Vereinigung für eine Besteuerung von Finanztransaktionen zum Nutzen der Bürger; ein globalisierungskritisches Netzwerk
BfV	Bundesamt für Verfassungsschutz
BKA	Bundeskriminalamt
BND	Bundesnachrichtendienst
BSI	Bundesamt für Sicherheit in der Informationstechnik
CI	Competitive Intelligence
CIA	Central Intelligence Agency, dt.: Zentraler Nachrichtendienst; US-amerikanischer Auslandsgeheimdienst
CNC	Computerized Numerical Control; computergestützte Steuerungsmethode im Werkzeugmaschinenbau
CRT	Cathode Ray Tube, dt.: Kathodenstrahlröhre; Element eines herkömmlichen Röhrenbildschirms, auch Braun'sche Röhre genannt
DCI	Director of Central Intelligence; Koordinator der amerikanischen Intelligence Community und de facto Leiter der CIA
DGSE	Direction Générale de la Sécurité Extérieure, dt.: Generaldirektion für Äußere Sicherheit; französischer Auslandsgeheimdienst
FBI	Federal Bureau of Investigation, dt.: Bundesamt für Ermittlung; bundespolizeiliche Strafverfolgungsbehörde der USA
FSB	Federalnaya Sluzhba Besopasnosti, dt.: Föderaler Sicherheitsdienst; Inlandsgeheimdienst der Russischen Föderation
GIT	Globalisierung, Internationalisierung, Transnationalisierung
GRU	Glavnoye Razvedyvatelnoye Upravlenie, dt.: „Hauptverwaltung Aufklärung"; militärischer Geheimdienst der Russischen Föderation

HVA	Hauptverwaltung Aufklärung; Auslandsnachrichtendienst der ehemaligen DDR
HUMINT	Human Intelligence Collection; klandestine Informationsgewinnung durch interpersonellen Kontakt
ICE	InterCity Express; deutscher Hochgeschwindigkeitszug
IMINT	Imagery Intelligence Collection; Unterkategorie von TECHINT, klandestine Informationsgewinnung mit Hilfe bildgebender Systeme
KGB	Komitet Gossudarstwennoy Besopasnosti, dt.: Komitee für Staatssicherheit; 1991 aufgelöster Geheimdienst der Russischen Föderation
KTX	Korea Train Express; koreanischer Hochgeschwindigkeitszug
LGT	Liechtenstein Global Trust; ein Finanzunternehmen des liechtensteinischen Fürstenhauses
MAD	Militärischer Abschirmdienst
MASINT	Measurement and Signature Intelligence Collection; Unterkategorie von TECHINT, klandestine Informationsgewinnung mit Hilfe nicht bild- oder tongebender Sensoren
MBA	Master of Business Administration; angelsächsischer Hochschulabschluss im Bereich der Betriebswirtschaftslehre
MID	Militärischer Informationsdienst der Volksrepublik China
MSS	Ministerium für Staatssicherheit der Volksrepublik China
NGO	Non-Governmental Organization, dt.: Nichtregierungsorganisation
NSA	National Security Agency, dt.: Nationale Sicherheitsbehörde; mit Telekommunikationsüberwachung und Verschlüsselungswesen befasster amerikanischer Geheimdienst
OSINT	Open Source Intelligence Collection; Informationsgewinnung aus öffentlich zugänglichen Quellen
PKS	Polizeiliche Kriminalstatistik

SIGINT	Signals Intelligence Collection; Unterkategorie von TECHINT, klandestine Informationsgewinnung durch abgefangene Funksignalen
SORM	Sistema Operativno-Rozysknykh Meropriyatii, dt.: System für operativ-investigative Tätigkeiten; Name russischer Gesetze zur Telekommunikationsüberwachung
StGB	Strafgesetzbuch
SVR	Sluzhba Vneshnogo Razvedky, dt.: Auslandsgeheimdienst; russischer Auslandsgeheimdienst
TECHINT	Technical Intelligence Collection; klandestine Informationsgewinnung durch technische Mittel
TFT	Thin-Film Transistor, dt.: Dünnschichttransistor; ein spezieller Transistor, welcher in herkömmlichen Flachbildschirmen zum Einsatz kommt
TGV	Train á grande vitesse; französischer Hochgeschwindigkeitszug
TNT	Trinitrotoluol; verbreiteter militärischer wie ziviler Sprengstoff, seine Sprengkraft wird als Maßstab der Sprengkraft anderer Explosivstoffe verwendet
UMTS	Universal Mobile Telecommunications System; ein Mobilfunkstandard
USB	Universal Serial Bus; Schnittstelle, welche die Verbindung mit ihr ausgestatteter Geräte mit einem laufenden PC ermöglicht
UWG	Gesetz gegen den unlauteren Wettbewerb
WiFi	Wireless Fidelity; Bezeichnung für drahtlose Netzwerktechnik

Wirtschafts- und Industriespionage im deutschen Wirtschaftsraum: Eine analytische Betrachtung von Akteuren, Methoden und Gefahren

1 Einleitung

1.1 Zur thematischen Relevanz

Sieht sich der deutsche Wirtschaftsraum einer steigenden Bedrohung durch Wirtschafts- und Industriespionage ausgesetzt? Einer gemeinsamen Studie des Handelsblatt und der Münchener Sicherheitsberatung Corporate Trust zufolge schließen sich mehr als 70% der befragten deutschen Unternehmen dieser Einschätzung an (Corporate Trust 2007: 39). Knapp ein Fünftel der Befragten ist bereits *wissentlich* zum Opfer von Industriespionage geworden (ebd.: 13). Aufgrund der hohen Dunkelziffer dieses Deliktfeldes (Bundeskriminalamt 2005: 63; Lux/Peske 2002a: 107) ist jedoch zu vermuten, dass die Gesamtzahl der Fälle wesentlich höher liegt.

In Anbetracht dieser Zahlen ist es nicht verwunderlich, dass sich die jährlich durch Industriespionage verursachten Schäden für die deutsche Wirtschaft in Summe auf bis zu 20 Milliarden Euro belaufen, wie jüngst durch Dr. August Hanning[1] geschätzt (Bundesministerium des Innern 2007). Die Relevanz dieser Summe wird besonders deutlich, wenn man sie in Beziehung zu den Größen der volkswirtschaftlichen Gesamtrechnung setzt: Sie entspricht zum Beispiel 0,82% des deutschen Bruttoinlandsproduktes im Jahre 2007 (Statistisches Bundesamt 2007a), was für eine Volkswirtschaft, die in den letzten fünfzehn Jahren nur um durchschnittlich 1,64%

1 Dr. August Hanning bekleidete von 1998 bis 2005 das Amt des Präsidenten des Bundesnachrichtendienstes und ist heute als Staatssekretär im Bundesministerium des Innern tätig.

pro Jahr (Statistisches Bundesamt 2007b) gewachsen ist, eine beachtliche Zahl darstellt.

Doch nicht nur die Schäden für die deutsche Volkswirtschaft sind immens, auch die Schadenssummen der einzelnen Unternehmen sind beträchtlich. So erlitten knapp 30% der betrachteten Unternehmen Schäden in Höhe von über 100.000 Euro, 7,2% sogar Schäden von über einer Million Euro (Corporate Trust 2007: 17).

Trotz dieser Datenlage neigen die deutschen Unternehmen noch dazu, die Gefahr dramatisch zu unterschätzen: Die oben genannte Studie zeigt, dass lediglich 33,7% der Befragten glauben, dass die Gefahr durch Industriespionage auch für das eigene Unternehmen zukünftig steige. Bei eigenen Untersuchungen zeigten sich ebenfalls lediglich 58% der Befragten darüber besorgt, selbst Opfer von Spionage zu werden (siehe Anhang 1).

Zusätzlich zum mangelnden Risikobewusstsein der potentiellen Opfer von Spionagestraftaten unterliegt die Sphäre der Täter und der potentiellen Täter einer ganzen Reihe Besorgnis erregender Veränderungen sowohl in politischer als auch in ökonomischer Hinsicht. So hat zum Beispiel der zu Beginn der 90er Jahre einsetzende, massive Zerfall von Staatlichkeit in Osteuropa zu Umschichtungen in der Organisation der ehemals sowjetisch geführten Geheimdienste geführt. Viele in diesen Umschichtungen entlassene Nachrichtendienstoffiziere stehen nun auf den Lohnlisten der russischen Wirtschaft und versorgen diese mit nachrichtendienstlichem Know-how (Strong 1994: 166).

Auch für Deutschland stellt sich die Frage, in welchem Umfang ehemals professionelle Geheimdienstmitarbeiter ihre beruflichen Erfahrungen am freien Markt anbieten konnten: Obwohl viele der mehr als 4.000 ehemaligen Mitarbeiter des Auslandsnachrichtendienstes der ehemaligen DDR (offiziell „Hauptverwaltung Aufklärung des Ministeriums für Staatssicherheit“, kurz HVA) trotz der verworrenen Verhältnisse zur Zeit von Mauerfall und Wiedervereinigung enttarnt wurden[2], ist nicht

2 Für eine umfassende Darstellung der Auflösung der HVA vgl. Sontheimer (1999).

auszuschließen, dass ein Teil dieses Personenkreises beruflich gewonnenes Methodenwissen heute in den Dienst privatwirtschaftlicher Interessenten stellt.

Auch der beginnende Aufstieg der Volksrepublik China zu einer wirtschaftlichen Großmacht wird von chinesischen Behörden mit Hilfe von Wirtschaftsspionage aggressiv unterstützt. So ist zum Beispiel die Kontaktaufnahme mit jedweden ins Ausland reisenden oder dort arbeitenden Chinesen für das chinesische Ministerium für Staatssicherheit eine Routineaktivität (Bundesamt für Verfassungsschutz 2007: 321; Rustmann 2002: 117), Anwerbungen dauerhafter Zuträger sind im Zuge dieses Prozesses nicht ausgeschlossen. Gerade die Nachrichtendienste Russlands und Chinas betreiben nach Auffassung des Kölner Bundesamtes für Verfassungsschutz verstärkt Wirtschaftsspionage in Deutschland (Bundesamt für Verfassungsschutz, 2006, S. 10-12). Generell ist zu bemerken, dass die staatlich geförderte Industriespionage seit dem Ende des Kalten Krieges einem exponentiellen Wachstumstrend unterliegt (Rustmann 2002: 120).

Auch der wirtschaftliche Sektor ist massiven Veränderungen unterworfen: So schafft zum Beispiel die zunehmende wirtschaftliche Öffnung der Staaten des ehemaligen Warschauer Paktes, durch deren relative geografische Nähe, einen immensen Kostendruck für mitteleuropäische Produktionsstandorte, der durch einen Vorsprung in Innovation und Qualität kompensiert werden muss. Fortschreitende Deregulierung ehemals geschützter Märkte, ein von der Informationstechnologie getriebener rapider technologischer Wandel und eine zunehmende Internationalisierung von Beschaffungs- und Absatzmärkten erzeugen in vielen Branchen weltweit einen massiven Wettbewerbsdruck, welcher sich am ehesten durch das Phänomen der „Hypercompetition“ nach d’Aveni (1994; siehe dazu auch Kapitel 3.2) beschreiben lässt.

Einige Wettbewerber etablieren angesichts dieses massiven Drucks Geschäftspraktiken, die über den jeweiligen nationalen und internationalen Gesetzes-

rahmen hinausgehen. Klassische Methoden der HUMINT[3], wie Erpressung, Bestechung und Manipulation finden sich im Einsatz zwischen Unternehmen genauso wieder, wie im Repertoire staatlicher Geheimdienste. Ebenso finden im Zuge der verstärkten freien Verfügbarkeit (miniaturisierter) Überwachungstechnologie die Methoden der TECHINT[4], wie etwa Lausch- und Spähangriffe, im Unternehmensumfeld mittlerweile Verwendung.

Weiterhin müssen Wirtschaftsspione in Deutschland mit denkbaren geringen Strafen rechnen, unerheblich ob es sich dabei um einzelne Innentäter als Selbstanbieter oder ganze Konzerne handelt: Natürliche Personen haben mit nur geringen Freiheitsstrafen zu rechnen, juristische Personen werden oftmals nur mit geringen Geldbußen belegt. Somit gilt in den meisten Fällen, dass das Entwenden von Forschungsergebnissen oft preiswerter ist als eine eigene Entwicklung, dass ein Blick in Vertragsangebote der Konkurrenz jede Preisverhandlung auf eine sicherere Basis stellt und dass ein Auszug aus der Kundendatei des Wettbewerbers jede noch so kostspielige Werbekampagne in ihrer Wirkung übertrifft.

All diese Fakten geben berechtigten Anlass zu den Fragen, inwieweit der deutsche Wirtschaftsraum durch Wirtschafts- und Industriespionage gefährdet ist, wo diese Gefahren herrühren und wie diesen Gefahren wirksam zu begegnen ist. Gegenstand dieser Arbeit ist daher eine Bestandsaufnahme der für den deutschen Wirtschaftsraum relevanten Akteure, Methoden und Gefahren im Bereich der Wirtschafts- und Industriespionage.

1.2 Aufbau der Arbeit

Im folgenden Kapitel 2 soll zunächst ein gemeinsames Verständnis der Kernbegriffe dieser Arbeit aufgebaut werden. Es gilt die beiden stark umgangssprachlich geprägten Begriffe der „Wirtschaftsspionage“ und der „Industriespionage“ auf eine klar

3 Human Intelligence Collection: klandestine Informationsgewinnung durch interpersonellen Kontakt, siehe dazu Kapitel 5.1.

4 Technical Intelligence Collection: klandestine Informationsgewinnung durch technische Hilfsmittel, siehe dazu Kapitel 5.2.

umrissene definitorische Basis zu stellen und sie von verwandten Konzepten wie dem der Produktpiraterie und dem der Competitive Intelligence abzugrenzen.

Einen Überblick darüber, welche nationalen und internationalen Rahmenbedingungen das Feld der Wirtschafts- und Industriespionage seit dem Ende des Kalten Krieges beeinflusst haben, gibt Kapitel 3. Dazu werden politische, ökonomische, technologische und rechtliche Einflüsse, sowie ihre Veränderungen im Zeitablauf untersucht.

Kapitel 4 befasst sich mit den Akteuren der Wirtschafts- und Industriespionage in Form staatlicher oder privatwirtschaftlicher Institutionen. Diese erfahren eine Betrachtung getrennt nach offensiven Akteuren, welche wirtschaftliche Vorteile aus der illegalen Informationsbeschaffung zu ziehen versuchen und defensiven Akteuren, welche dies zu verhindern suchen oder Ziel dieser Vorgänge werden. Die dabei verwendeten Methoden werden in Kapitel 5 besprochen. Grob unterteilen lassen sich diese, wie bereits oben angedeutet, in die zwei Sphären der HUMINT und der TECHINT. Es werden sowohl klassische Methoden aus dem Bereich der nachrichtendienstlichen Spionage, als auch auf eigenen Recherchen basierende Praxisfälle erläutert. Das abschließende Kapitel 6 fasst die vorangehenden Betrachtungen zusammen und gibt Aufschluss darüber, ob der deutsche Wirtschaftsraum in besonderem Maße durch Wirtschafts- und Industriespionage gefährdet ist.

Insbesondere die Kapitel 4 und 5 werden durch anonymisierte Interviewdaten ergänzt, die im Jahre 2007 im Rahmen der Technologiemessen Medica, NanoSolutions und Euromold erhoben wurden. Diese werden in aufbereiteter Form im Anhang wiedergegeben.

2 Definitorische Abgrenzung

Die Kernbegriffe „Wirtschaftsspionage“ und „Industriespionage“ bedürfen einer inhaltlichen Präzisierung. Dies resultiert vor allem daraus, dass ihre Inhalte in der wissenschaftlichen Diskussion nicht deckungsgleich sind, oder deckungsgleiche

Inhalte nicht unter einheitlichen Termini geführt werden. Beispiele hierfür sind etwa die Bezeichnungen Konkurrenzausspähung (Corporate Trust 2007: 6), Konkurrenzspionage oder nachrichtendienstlich geführte Wirtschaftsspionage (Lux/Peske 2002b: 16). Auch im englischen Sprachraum kann durch Bezeichnungen mit mangelnder Trennschärfe wie etwa denen der Business Intelligence, der Competitor Intelligence und der Competitive Intelligence (Lux/Peske 2002a: 28), der Competitive Espionage, der Economic Espionage, der Industrial Espionage oder der Industrial Intelligence (Strong 1994: 162) ein ähnliches Phänomen beobachtet werden. Für die Betrachtung der *öffentlichen* Diskussion dieser Bereiche ist zu beachten, dass die Begriffe eine umgangssprachliche Prägung erfahren haben, welche häufig für eine synonyme Verwendung sorgt.

Im Gegensatz zum literaturüblichen Ansatz, beide Begriffe einer vollständig getrennten Definition zu unterwerfen, wird im Rahmen dieser Arbeit zunächst deren gemeinsamer Kern erarbeitet. Darauf aufbauend werden Kriterien entwickelt, die eine trennscharfe Unterscheidung von „Wirtschaftsspionage“ und „Industriespionage“ ermöglichen. Weiterhin werden verwandte Prozesse und Sachverhalte, wie etwa die der Produktpiraterie und der Competitive Intelligence, aus dem betrachteten Themenkreis ausgeschlossen.

2.1 Gemeinsamer Begriffskern

Verbindendes Element beider Begriffe ist die Tatsache, dass es sich bei beiden Vorgängen um eine Art der *Spionage* handelt. Einen ersten Anhaltspunkt zur Definition dieses Oberbegriffs bieten die Einträge gängiger Begriffswörterbücher. So versteht zum Beispiel die Onlineausgabe der Encyclopædia Britannica (o.J.) unter „Espionage” folgendes:

> „Process of obtaining military, political, commercial, or other secret information by means of spies, secret agents, or illegal monitoring devices. Espionage is sometimes distinguished from the broader category of intelligence by its aggressive nature and its illegality.”

Dieser Beschreibung lassen sich folgende Elemente entnehmen:

- Spionage ist ein Prozess
- Gegenstand des Prozesses ist das Aneignen geheim gehaltener Informationen
- Der Prozess bedient sich klandestiner[5] und illegaler Mittel (z.B. gesetzeswidrig installierter Aufzeichnungsgeräte oder der Erpressung von Entscheidungsträgern)

Diese Elemente geben bereits Aufschluss über den *Prozessgegenstand*, sowie die Frage nach dem *modus operandi*, der Art der Durchführung des Prozesses. Diese ist vergleichbar mit der zweiten Phase des *Intelligence Cycle* (siehe Abb. 1), eines Prozessstufenmodells zur Erklärung nachrichtendienstlicher Tätigkeit, wie es z.B. von den 18 Mitglieds-organisationen der US-amerikanischen Intelligence-Community angewandt wird (Federation of American Scientists, o.J.; US-Intelligence Community o.J.a).

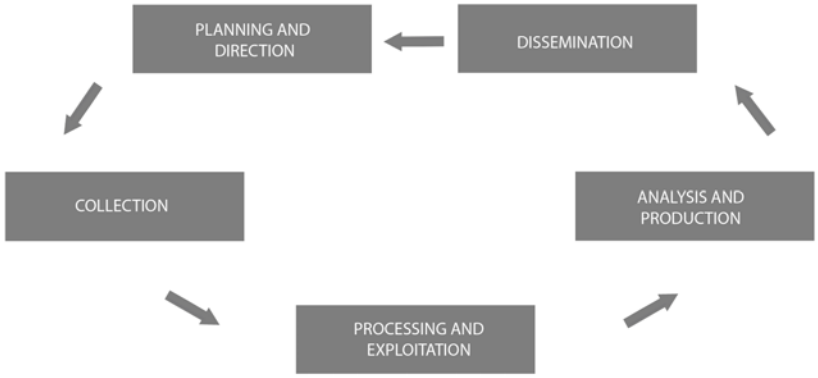

Abb. 1: Intelligence Cycle

Nach der ersten Phase („Planning and Direction"), in der die Ziele nachrichtendienstlicher Aktivität festgelegt und ihnen zum Zwecke der Aufklärung zur Verfügung stehende Ressourcen zugewiesen wurden, erfolgt die zweite Phase, „Collection" genannt. Diese wird von der Intelligence Community definiert als „Gathering

5 Als klandestin wird im Rahmen dieser Arbeit eine Tatsache bezeichnet, die vor anderen Akteuren geheim gehalten wird, um eigene Kenntnisse und Fähigkeiten vor diesen verborgen zu halten.

of raw data from which finished intelligence is produced." (US-Intelligence Community o.J.b), was im weitesten Sinne dem oben beschriebenen Vorgang der Spionage entspricht. Die sich daran anschließenden Phasen der Aufbereitung („Processing and Exploitation"), Analyse („Analysis and Production") und Verbreitung („Dissemination") stehen nicht mehr im eigentlichen Fokus des Begriffs und gehören daher nicht mehr zum eigentlichen Umfang dieser Arbeit.

Welches Kriterium unterscheidet nun aber die „Spionage" von der „Wirtschafts- und Industriespionage"? Im Rahmen dieser Arbeit wird hierbei nach der Art der angeeigneten Information unterschieden. Von „Wirtschafts- und Industriespionage" soll im weiteren Verlauf der Arbeit die Rede sein, wenn durch das Aneignen der Information wirtschaftliche Vorteile, zumeist gegenüber dem ursprünglichen Besitzer dieser Information zu erlangen sind.

Dies muss eine unmittelbare kommerzielle Verwendbarkeit der Information jedoch nicht mit einschließen. Das illegale und klandestine Aneignen einer Kundenkontaktdatei fällt somit ebenso unter Wirtschafts- und Industriespionage, wie das illegale und klandestine Aneignen der Standortplanung einer Unternehmung. Während sich aus der umsichtigen Nutzung einer fremden Kundendatei eine direkte Umsatzsteigerung erzielen lässt, eröffnet die Kenntnis der Standortplanung eines Wettbewerbers keinerlei Möglichkeiten, die sich unmittelbar positiv auf ökonomische Kennziffern auswirken. Dennoch lassen sich hierdurch strategische wirtschaftliche Vorteile erzielen, indem etwa anhand dieser Daten Grundstücke aufgekauft werden, die ein Mitbewerber in die Bauplanung eines neuen Standorts einbezogen hatte. Eine direkt positive Auswirkung auf die eigenen ökonomischen Kennziffern ist hierbei zwar nicht festzustellen, der wirtschaftliche Vorteil gegenüber dem ursprünglichen Eigner der Information ist jedoch gegeben. Auch das Aneignen solcher Informationen fällt dementsprechend unter Wirtschafts- und Industriespionage. Darunter zu verstehen ist, gemäß der obigen Ausführungen, der „**Prozess des Aneignens geheim gehaltener Informationen mit Hilfe illegaler und klandestiner Mittel. Ziel ist hierbei das Erlangen eines wirtschaftlichen Vorteils"**.

Weiterhin stellt sich die Frage nach den handelnden Subjekten. Diese soll genutzt werden, um aus dem gemeinsamen Begriffskern heraus eine Abgrenzung zwischen den einzelnen Tatbeständen der „Wirtschaftsspionage“ und der „Industriespionage“ zu ermöglichen.

2.2 Begriffsabgrenzung Wirtschaftsspionage

Bei Wirtschaftsspionage im Sinne dieser Arbeit erfolgt das Aneignen der Information stets durch einen **Nationalstaat** beziehungsweise durch eine **staatliche Institution**. Dies bedeutet jedoch nicht zwangsläufig, dass dieser bzw. diese gleichzeitig Nutznießer des auf diese Weise zu erlangenden wirtschaftlichen Vorteils sind. Analog zum Modell des *Intelligence Cycle* kann die Dissemination der aufgearbeiteten Information, auch wenn diese durch staatliche Stellen gesammelt wurde, durchaus in den privaten Sektor erfolgen. Ein Beispiel hierfür ist der oft zitierte Fall der Auftragsvergabe für den südkoreanischen Hochgeschwindigkeitszug KTX: Das TGV-Konsortium GEC-Alsthom erlangte (durch ein vermutlich vom französischen Auslandsgeheimdienst DGSE abgefangenes Fax) Kenntnis von den Angebotsbedingungen des von Siemens geführten ICE-Konsortiums und konnte die Ausschreibung in letzter Sekunde durch eine Anpassung des eigenen Vertragsangebotes für sich entscheiden (Homann et. al. 2005: 4; Ulfkotte 1999: 66; o.V. 1996; Office of the National Counterintelligence Executive o.J.: 287).

Diese Art der Betrachtung kommt dem von Lux und Peske hierfür verwendeten Begriff der „nachrichtendienstlich geführten Spionage“ (2002a: 30) recht nahe. Ihre Definition greift vom Inhalt her jedoch etwas kürzer, insofern als das Aneignen der Information gemäß obiger Definition nicht zwangsweise durch nachrichtendienstliche Kanäle geschehen muss, sondern vielmehr auch auf Erkenntnissen beruhen kann, die durch andere staatliche Institutionen gewonnen wurden. Ein Diplomat, der eigene Beobachtungen über ungewöhnliche Freizeitaktivitäten von Topmanagern seines Einsatzlandes anstellt, fällt genauso wenig unter die Definition nach Lux und Peske, wie eine Zentralbank, die durch verdeckte Mittelsmänner in

ausländischen Zentralbanken Aussagen über deren zukünftige Leitzinsveränderungen oder Anlageentscheidungen treffen kann. Um diese Fälle mit einzuschließen sei der Begriff „Wirtschaftsspionage" im Rahmen dieser Arbeit folgendermaßen definiert: **„Wirtschaftsspionage ist der Prozess des Aneignens geheim gehaltener Informationen mit Hilfe illegaler und klandestiner Mittel staatlicher Institutionen. Ziel ist hierbei das Erlangen eines wirtschaftlichen Vorteils."**

Eine Auswahl Wirtschaftspionage betreibender staatlicher Institutionen findet sich in Kapitel 4.1.1, eine Übersicht über die dabei zum Einsatz kommenden illegalen und klandestinen Mittel wird in Kapitel 5 gegeben.

2.3 Begriffsabgrenzung Industriespionage

Bei Industriespionage im Sinne dieser Arbeit erfolgt das Aneignen der Information stets durch eine **privatwirtschaftliche Institution** oder eine **Privatperson**. Diese sind überwiegend selbst Nutznießer der erlangten Information. Gründe hierfür liegen in dem persönlichen Risiko, das mit einer weiteren Dissemination der Informationen einhergeht und in der Gefahr, einen eventuellen wirtschaftlichen Vorteil nicht selbst in vollem Umfang ausnutzen zu können. Für eine Privatperson, die zum Beispiel aufgrund von illegal erlangten Kenntnissen über eine bevorstehende Unternehmensakquise in der Lage wäre Vermögensvorteile zu erlangen, besteht bei Entdeckung ein persönliches Risiko in Form von Geld- oder Freiheitsstrafe (siehe dazu auch Kapitel 3.4.1). Ebenso läuft die Person Gefahr, den potentiellen wirtschaftlichen Vorteil zu verlieren, wenn die erlangte Information als Folge der Dissemination allgemein zugänglich wird und andere Institutionen oder Personen den Vorteil so für sich beanspruchen können.[6]

Der Begriffswahl „Industriespionage" liegt (genau wie den Begriffen „Konkurrenzspionage" oder „Konkurrenzausspähung") eine gewisse Willkür inne, weil hierbei nicht nur „die Industrie" oder „die Konkurrenz" sondern durchaus auch Verbände, staatliche Organe und andere Institutionen des Wirtschaftsraumes Ziel

6 Zu den allgemeinen Risiken der Intelligence-Kooperation siehe auch Westerfield (1996: 539-543).

des Prozesses sein können. Die Wahl der Bezeichnung „Industriespionage“ erfolgt daher vor allem wegen deren umgangssprachlicher Geläufigkeit. Sie ist im Rahmen dieser Arbeit wie folgt definiert: **„Industriespionage ist der Prozess des Aneignens geheim gehaltener Informationen mit Hilfe illegaler und klandestiner Mittel privatwirtschaftlicher Institutionen und Einzelpersonen. Ziel ist hierbei das Erlangen eines wirtschaftlichen Vorteils.“**

Eine Beschreibung der am Prozess beteiligten Akteure findet sich in Kapitel 4, eine Auswahl der dabei eingesetzten illegalen und klandestinen Mittel wird in Kapitel 5 erläutert.

2.4 Verwandte Maßnahmen

Zur weiteren Veranschaulichung der Begriffe ist es sinnvoll, mit Wirtschafts- und Industriespionage verwandte Maßnahmen kurz aufzuführen und aufzuzeigen, inwiefern sich diese von ihnen abgrenzen.

2.4.1 Produktpiraterie

Unter Produktpiraterie ist laut dem Verbraucherleitfaden „Schutz vor Produkt- und Markenpiraterie“ der Bundesanstalt für Arbeitsschutz folgendes zu verstehen: „Bei Produkt- und Markenpiraterie handelt es sich um die Verletzung bzw. illegale Verwendung von Urheber-, Marken-, Patent-, sowie sonstigen gewerblichen Schutzrechten durch Nachahmung oder Fälschung.“ (Bundesanstalt für Arbeitsschutz 2007).

Die Veräußerung dieser Waren erfolgt meist weit unter dem Preis der Originalprodukte, da die Nachahmer nur einen Bruchteil an Forschungs-, Design-, und Vermarktungsaufwendungen zu tragen haben. Schätzungen der Aktion Plagiarius[7] zufolge wird die deutsche Wirtschaft dadurch jährlich mit Schäden in Höhe von 29

7 Die Aktion Plagiarius (Initiator: Prof. Rido Busse, Weißensee-Kunsthochschule Berlin) beschäftigt sich mit Produktimitationen auf dem deutschen Markt und vergibt seit über 30 Jahren einen jährlichen Negativpreis (einen schwarzen Zwerg mit goldener Nase) für die dreistesten Plagiate. Vgl.: www.plagiarius.com .

Milliarden Euro belastet (Aktion Plagiarius o.J.), der Hauptteil der Fälschungen stammt dabei laut dem „Jahresbericht Gewerblicher Rechtschutz 2006“ des deutschen Zolls aus dem asiatischen Raum. War Thailand im Jahre 2003 in der Statistik der Aufgriffe nach Herkunftsländern mit knapp 25% noch führend, so hat China seinen Anteil bis ins Jahr 2006 von 12,7% auf über 32% gesteigert (Bundeszollverwaltung 2006).

In welcher Beziehung steht nun aber die Produktpiraterie zur Wirtschafts- und Industriespionage? Zunächst einmal erfordert die erfolgreiche Nachahmung eines Produktes die Aneignung des Produktes selbst. Das Aneignen zusätzlicher, nicht frei erhältlicher Informationen über das Produkt ist nur dann erforderlich, wenn die Komplexität des zu kopierenden Produktes das technische Know-How des Plagiators übersteigt oder das Produkt nicht frei erhältlich ist. So stehen die Nachahmer elektronischer Geräte (wie etwa von Kernspintomographen oder Industrierobotern) zumeist vor ungleich größeren technischen Problemen als die Nachahmer von Wohnraumaccessoires (wie etwa Designermöbeln oder Küchenutensilien) oder Kleidung. Im ersteren Fall kann erfolgreiche Wirtschafts- oder Industriespionage zur Voraussetzung von Produktpiraterie werden, zwingend erforderlich ist sie dafür aber nicht.

2.4.2 Competitive Intelligence

Im Gegensatz zur betriebswirtschaftlichen Marktforschung klassischer Prägung, die sich vornehmlich auf das Studium der Absatzmärkte eines Unternehmens konzentriert, verfolgt die „Competitive Intelligence“ einen breiteren Ansatz. Nach Michaeli ist sie: „[...] der systematische Prozess der Informationserhebung und -analyse […], durch den aus fragmentierten (Roh-)Informationen über Märkte, Wettbewerber und Technologien den Entscheidern ein plastisches Verständnis für ihr Unternehmensumfeld und damit eine Entscheidungsgrundlage geliefert wird.“ (Michaeli 2006: 3).

Der Gegenstand der „Competitive Intelligence“ ist also die systematische Beobachtung des gesamten Wettbewerbsumfeldes. Auch dieser Begriffsinhalt wird wiederum mit einer Vielzahl unterschiedlicher Bezeichnungen belegt. Gängige

deutsche Synonyme sind Wettbewerbsforschung, Wettbewerbsaufklärung, Wettbewerberforschung, Konkurrenz-analyse oder Konkurrenzbeobachtung (Michaeli 2004: 2). Im englischen Sprachgebrauch sind zudem die Begriffe Competitor Intelligence und Business Intelligence in Gebrauch (Lux/Peske 2002b: 15).

Trotz dieser terminologischen Differenzen ist sich die Fachliteratur jedoch über den Unterschied zwischen Competitive Intelligence (CI) und Wirtschafts- und Industriespionage einig. „Von CI ist die Wirtschaftsspionage als vereinfacht ausgedrückt illegale Form der Informations- und Wissensbeschaffung zu unterscheiden. […] CI sollte somit die Beschaffung und Auswertung von öffentlich zugänglichen Quellen unter Beachtung der Datenschutzvorschriften und zusätzlich ethischer Gesichtpunkte sein.“ (Lux/Peske, 2002b, S. 15).

Die Abgrenzungskriterien *Legalität, ethisch sozialkonformes Verhalten* und *ausschließliche Verwertung ubiquitärer Quellen* finden sich auch bei Michaeli: „Competitive Intelligence ist weder unethisch noch kriminell. Die einem CI-Analysten zur Verfügung stehenden Daten stammen überwiegend aus öffentlich zugänglichen Quellen […]. Wirtschaftsspionage und -kriminalität basieren hingegen auf illegal erworbenen Informationen.“ (Michaeli 2006: 24).

Zu beachten ist jedoch, dass die Grenzen zwischen CI und Wirtschaftsspionage, aufgrund einer unterschiedlichen Gesetzgebung auf nationaler Ebene, auf internationaler Ebene eher fließend sind (Lux/Peske 2002b: 16).

3 Rahmenbedingungen des deutschen Wirtschaftsraums

Der Analyse nationaler und internationaler Einflussfaktoren auf die Wirtschafts- und Industriespionage im deutschen Wirtschaftsraum sei eine kurze Erläuterung dieses Begriffs vorangestellt.

Bei einer Volkswirtschaft, welche seit 2002 weltweit führend im Warenexport ist (Bundesministerium für Wirtschaft und Technologie 2007; Statistisches

Bundesamt 2007c: 479) liegt es auf der Hand, dass bundesdeutsche Wirtschaftsinteressen nicht an den eigenen Landesgrenzen halt machen. Genauso wenig beschränken sich jedoch auch die Spionageaktivitäten gegen deutsche Unternehmen auf das Staatsgebiet der Bundesrepublik: Immerhin 15% aller erkannten Spionagefälle geschahen in den Auslandsniederlassungen und -tochterunternehmen deutscher Firmen (Corporate Trust 2007: 20). Sei es eine Reinigungskraft, die in einer im Ausland gelegenen Vertriebszentrale ein waches Auge auf die auf den Schreibtischen liegenden Papiere hat, die technische Inspektion einer im Ausland errichteten Produktionsanlage durch die dortige Regierung oder der Diebstahl eines Laptops während einer Verhandlungsreise: Überall dort, wo deutsche Unternehmen im Ausland präsent sind, bieten sie eine Angriffsfläche für die Spionagetätigkeiten von Konkurrenz und ausländischen Regierungen.

Die Bezeichnung *deutscher Wirtschaftsraum* rekurriert daher neben dem deutschen Staatsgebiet auch auf die physische Präsenz[8] deutscher Unternehmen und Interessen im Ausland.

Im folgenden Kapitel soll untersucht werden, inwiefern sich die Veränderung (respektive das Fortbestehen) nationaler und internationaler Rahmenbedingungen auf das Phänomen der Wirtschafts- und Industriespionage ausgewirkt hat und wie diese Bedingungen die Gefährdungslage des deutschen Wirtschaftsraums beeinflussen. Dazu werden Entwicklungen des internationalen Systems, des ökonomischen und technologischen Fortschritts, sowie des (speziell für den deutschen Wirtschaftsraum) geltenden Rechtsrahmens herangezogen.

Zu beachten ist, dass die aufgezeigten politischen, technologischen und ökonomischen Entwicklungen vielfach interdependent sind: Der technologische Fortschritt bedingt Prozesse der Globalisierung, die Globalisierung wiederum nimmt Einfluss auf das ökonomische Umfeld des Staates. Die Aufteilung der einzelnen Faktoren entbehrt nicht einer gewissen Willkür, erfolgt aber in einer Form, welche

8 In Form von Handlungsbevollmächtigten oder von Strukturen, die durch Auslandsinvestition geschaffen wurden. Eine rein virtuelle Präsenz wie etwa eine Website, ein Konzernintranet oder ein Rechenzentrum ist ohnehin global zugänglich und somit auch global angreifbar.

den bestmöglichen Überblick über die einzelnen Entwicklungen bietet. Eine Untersuchung der individuellen Interdependenzen kann an dieser Stelle aufgrund der thematischen Fokussierung jedoch nicht geleistet werden.

3.1 Wechsel zu einer unipolaren Weltordnung

Seit Beginn der 1990er Jahre unterliegt die internationale politische Ordnung massiven Veränderungen durch punktuelle Ereignisse wie auch durch beständig fortschreitende Prozesse. Die für das Feld der Wirtschafts- und Industriespionage wohl bedeutendste Veränderung dieser Rahmenbedingungen innerhalb der letzten 20 Jahre stellt jedoch der politische Zusammenbruch der Sowjetunion und der daher rührende Übergang von einer bipolaren zur unipolaren Weltordnung dar. Dies hatte für alle ehemals im Ost-West-Konflikt verstrickten Nachrichtendienste nach dem „Fall des eisernen Vorhangs" die Notwendigkeit einer Neuausrichtung ihrer Aktivitäten zur Konsequenz, da nun zunehmend die wirtschaftliche Stärke eines Staates dessen Einfluss auf das internationale System bestimmte (Shulsky/Schmitt 2002: 6). Zur Veranschaulichung seien hier die Entwicklungen in den USA und der Russischen Föderation aufgeführt.

USA

Bereits 1992 betonte der damalige DCI[9] Robert Gates in einer Rede vor dem „Economic Club of Detroit" die dramatisch gestiegene Bedeutung ökonomischer Themen für die Arbeit der Geheimdienste: Knapp 40% der bei den Diensten eingehenden Anforderungen seien zur Zeit wirtschaftlicher Natur, daher sei die oberste Entscheidungsebene der US-Regierung davon überzeugt, dass sogar über das Ende der Dekade hinaus in diesem Bereich die größten Herausforderungen und Chancen zu finden seien (Kober 1992).

9 DCI: Director of Central Intelligence, Koordinator der amerikanischen Intelligence Community und de facto Leiter der Central Intelligence Agency (CIA).

Eine dauerhafte Grundlage der nachrichtendienstlichen Beschäftigung mit diesem Feld legte die Clinton-Administration in einem im Jahre 1995 erschienen Strategiepapier. Unter anderem konstatiert diese Veröffentlichung unter dem Titel „A National Security Strategy of Engagement and Enlargement", dass der Begriff der Nationalen Sicherheit der beginnenden Ära nach dem Kalten Krieg eine „breitere Definition" (The White House 1995: 17) erhalten habe. Zur Verbindung ökonomischer Belange und der Arbeit der US-amerikanischen Geheimdienste heißt es hierin: „In order to adequately forecast dangers to democracy and to *U.S. economic well-being*, the intelligence community must track political, *economic*, social and military developments in those parts of the world where U.S. interests are most heavily engaged and where overt collection of information from open sources is inadequate." (ebd.; Hervorhebungen eingefügt). Hier wurde also geheimdienstlicher Einsatz zur Verfolgung ökonomischer Interessen gebilligt und angekündigt.

Zu den Gründen für dieses Vorgehen heißt es weiterhin: „[…] collection and analysis can help level the economic playing field by identifying threats to U.S. companies from foreign intelligence services and unfair trading practices." (ebd.) Die Tätigkeit der US-Geheimdienste auf dem ökonomischen Sektor dient demnach der Verteidigung gegen das offensive Vorgehen fremder Dienste; eine Auffassung, die in Kapitel 4.1.1 weitergehend untersucht wird.

Russland

Auch die Nachrichtendienste der ehemaligen Sowjetunion erfuhren durch den Fall des eisernen Vorhangs massive Veränderungen. So wurde das ehemals gefürchtete KGB[10] auf Anweisung Boris Jelzins, des damaligen Präsidenten der russischen Teilrepublik, am 6. November 1991 aufgelöst und seine Zuständigkeiten größtenteils an die Nachfolge-organisationen FSB[11] und SVR[12] übergeben. Diese Veränderungen führten jedoch nicht zu einer direkten Neuausrichtung auf wirt-

10 *Komitet Gossudarstwennoy Besopasnosti*, wörtlich: „Komitee für Staatssicherheit".

11 *Federalnaya Sluzhba Besopasnosti*, wörtlich: „Föderaler Sicherheitsdienst", russischer Inlandsgeheimdienst.

12 *Sluzhba Vneshnogo Razvedky*, wörtlich: „Auslandsgeheimdienst".

schaftliche Themen, soweit dies für den Fall der (im Vergleich zur Informationspolitik ihrer westlichen Pendants) immer noch vergleichsweise verschlossenen russischen Dienste zu überschauen ist. Dennoch finden sich bereits früh einzelne Beiträge, die eine Verbindung zwischen der Anfang der 90er Jahre boomenden russischen Wirtschaft und ehemaligen KGB-Offizieren herstellen (Strong 1994: 166). Eine Validierung dieser Aussagen gestaltet sich jedoch infolge schlechter Quellenlage schwierig.

Dennoch finden sich auch für Russland in jüngerer Zeit immer wieder Anzeichen eines veränderten Verhältnisses zwischen Geheimdiensten und Wirtschaft. Diese finden jedoch nicht, wie im Beispiel der amerikanischen Intelligence Community auf institutioneller, sondern vielmehr auf persönlicher Ebene statt. Viele ehemalige FSB- (und KGB-) Offiziere haben einem Artikel der New York Times zu Folge heutzutage einen Sitz in den Vorstandsetagen staatseigener Unternehmen. Hierzu nennt der Artikel prominente Namen: Sergey I. Chemezov, Vorstandsvorsitzender von Russian Technologies (Rohstoffzulieferer für Boeing), Igor I. Sechin, Aufsichtsratvorsitzender von Rosneft, einem der größten russischen Energiekonzerne oder Aleksandr Y. Lebedev, milliardenschwerer russischer Airline-Tycoon (Kramer 2007).

Als Förderer solcher Maßnahmen gilt der ehemalige FSB-Dienstherr, der zum Zeitpunkt der Abfassung dieser Arbeit amtierende Präsident der Russischen Föderation Vladimir Putin (ebd.). Diese Entwicklung hat mittlerweile derartige Formen angenommen, dass die russische Ausgabe des „Smart Money Magazine“ im November mit „KGB ist besser als MBA“ titelte (ebd.).

Eine detaillierte Besprechung aktueller US-amerikanischer und russischer Spionagebestrebungen im wirtschaftlichen Sektor erfolgt in Kapitel 4.1.1. Vorab lässt sich jedoch für den Fall der US-amerikanischen und russischen Dienste eine zunehmende Verflechtung mit wirtschaftlichen Interessen feststellen - seien diese nun staatlicher oder privater Natur.

3.2 Globalisierung, Internationalisierung, Transnationalisierung

Neben der Ablösung der bipolaren Weltordnung sorgen die sogenannten GIT-Prozesse – die Prozesse der Globalisierung, Internationalisierung und Transnationalisierung – für ein weltweites „Zusammenrücken", was nachfolgend am Beispiel der Begriffe Transnationalisierung und Globalisierung erläutert wird.[13]

3.2.1 Transnationalisierung

Das Auftreten gesellschaftlicher Akteure, die eigenständig und dauerhaft über nationale Grenzen hinweg handeln, geht zurück bis in die Zeiten der Gründung der britischen East India Company am 31. Dezember 1600 (Robins 2006). Einzigartig für das mit Transnationalisierung bezeichnete Phänomen ist jedoch die schiere Zahl der heutzutage auf diese Art und Weise verfahrenden gesellschaftlichen Akteure und ihre Bedeutung für das außenpolitische Handeln von Nationalstaaten, auch und gerade im Bereich der Ökonomie (Jäger/Beckmann 2007).

Im Themenfeld Wirtschafts- und Industriespionage ist zu bemerken, dass private, transnationale Akteure verstärkt Know-How in Bereichen ausbilden, die traditionelle Domänen staatlicher Geheimdienste waren. So war zum Beispiel die Beurteilung der Wirtschaftskraft einzelner Zielstaaten und ihrer Unternehmen eine Aufgabe, welche sich (speziell staatenblockübergreifend zur Zeit des Kalten Krieges) fast ausschließlich mit Insiderwissen lösen ließ, das durch geheimdienstliche Methoden gewonnen war. Was früher somit gemäß Definition als Wirtschaftsspionage zu bezeichnen war, ist mittlerweile – nicht zuletzt dank der Leistungsfähigkeit moderner Datenbanken und spezieller Prognosesoftware, siehe Kapitel 3.4 – Teil der tagtäglichen Arbeit global präsenter Finanzdienstleister, wie etwa

13 Die Konsequenzen der zunehmenden Internationalisierung, d.h. der Prozesse mit denen Staaten versuchen, den teilweisen Verlust ihrer Gatekeeper-Funktion zu kompensieren und ihre Handlungsfähigkeit in veränderter Umwelt zu reproduzieren, liegen für das Feld der Wirtschafts- und Industriespionage in der Neuausrichtung nachrichtendienstlicher Aktivitäten, wie sie bereits in Kapitel 3.1 beschrieben wird.

Dun&Bradstreet oder McGraw-Hill geworden (Harbich 2006: 64). Illegale und klandestine Methoden sind wohlgemerkt hierzu nicht mehr erforderlich.

Ein weiteres, der Wirtschafts- und Industriespionage dienliches Gebiet technologischer Neuerungen ist das Feld der Satellitenaufklärung. Mit Hilfe dieser Technologie lassen sich bestimmte wirtschaftlich relevante Fragestellungen zeitnah, kosteneffizient und ohne unmittelbare Präsenz im aufgeklärten Gebiet beantworten: Welchen Umfang haben die Aushubarbeiten auf den nigerianischen Besitzungen von Konkurrent X? Hat die Tabakernte auf den brasilianischen Plantagen von Konkurrent Y schon begonnen? Ist die arktische Forschungsstation Z durch das Abschmelzen der Polkappen bedroht?

Dieses Know-How befand sich, genau wie die oben angeführte Wirtschaftsaufklärung, noch vor wenigen Jahren fest in staatlich-geheimdienstlicher Hand und fand klandestin statt[14]. Mittlerweile ist auch diese, ehemals von einer hohen Exklusivität gekennzeichnete Technologie, durch die Verwertung in den Händen finanzstarker, transnationaler Akteure öffentlich zugänglich geworden. Das US-amerikanische Unternehmen GeoEye zum Beispiel verfügt ab 2008 über Satelliten mit „41cm-Auflösung“. Dies entspräche einer Bildschärfe, wie sie lediglich von staatlichen Satelliten neuerer Generationen erreicht wird (GeoEye 2007).

In beiden aufgezeigten Fällen ist für den Bereich der Wirtschafts- und Industriespionage zu beobachten, dass ehemals als Wirtschaftsspionage zu bezeichnende Handlungen mit dem Aufstieg transnationaler Akteure zu kommerziell verfügbaren Dienstleistungen geworden sind.[15] Sie sind daher dem Bereich der Competitive Intelligence zuzurechnen. Die Konsequenzen dieser Verschiebung sind durchaus ambivalent: Zum einen steigt mit der Zahl der Akteure, welche über oben genannte Möglichkeiten verfügen, die Gefährdung von Staat und Unternehmen, zum anderen aber agieren die neuen privaten Akteure nicht mehr klandestin. Sie

14 Eine Beurteilung der *Legalität* dieser Vorgehensweise unter Betrachtung völker- und weltraumrechtlicher Aspekte würde an dieser Stelle jedoch zu weit führen.

15 Ergänzend ist anzumerken, dass die freie Verfügbarkeit der ehemals strikten staatlichen Kontrollen unterworfenen Bildaufklärungstechnologie ebenfalls durch das Ende des Kalten Krieges bedingt ist (Harbich 2006: 39ff).

müssen sich staatlicher Gesetzgebung und Kontrolle beugen und sind – je nach gewählter Rechtsform – verpflichtet, umfangreiche Einblicke in ihre geschäftliche Tätigkeit zu bieten.

3.2.2 Globalisierung

Die ökonomische Entwicklung des deutschen Wirtschaftsraums wird zu einem nicht unwesentlichen Teil auch von der Globalisierung beeinflusst. Unter Globalisierung sind Prozesse zu verstehen, durch die „Bereiche des menschlichen Handelns […] zeitlich und räumlich eine Komprimierung gegen Null erfahren." (Jäger/Beckmann 2007: 25).

Auslöser hierfür sind unter anderem die mit den Anfängen des Informationszeitalters[16] und dem Aufkommen des Internet drastisch gestiegene Fähigkeit zur interpersonellen Echtzeitkommunikation in Form von E-Mail und E-Mailanhängen, Videokonferenzen oder NetMeetings, sowie die zunehmende globale Vernetzung von Geschäftsprozessen, vor allem im Bereich Forschung und Entwicklung (Jäger/Beckmann 2007: 26).

Problematisch am Phänomen der Globalisierung ist, dass sie Druck auf die Angebotsseite der Gütermärkte ausübt, indem sie für eine stetig steigende Innovationsgeschwindigkeit sorgt (Lux/Peske 2002a: 11), welche zusammen mit weiteren Faktoren das Überleben von Unternehmen am Markt zusehends erschwert. Bei diesen Faktoren handelt es sich um:

- Intensivierung des Wettbewerbs in Bezug auf Zeit und Know-How
- Stagnationsphasen der wirtschaftlichen Entwicklung
- Abbau von Hemmnissen grenzüberschreitenden Handels
- Zunehmende Fragmentierung von Kundenansprüchen in angestammten Märkten
- Deregulierung monopolistisch oder oligopolistisch geprägter Märkte, zum Beispiel in den klassischerweise netzgebundenen Sparten Energie und Telekommunikation (Rifkin 1996; Lux/Peske 2002a: 11f).

16 Siehe hierzu auch den nächsten Abschnitt, Kapitel 3.3.

Diese Faktoren sorgen in ihrer historisch einzigartigen Kombination auf vielen Märkten für einen Zustand, welcher mit „Hypercompetition“ bezeichnet wird: Ein Marktzustand, in dem es für ein Unternehmen nicht mehr möglich ist, nachhaltige Wettbewerbsvorteile aufzubauen, sondern diese durch eine permanente und kurzfristige Neuausrichtung seiner *strategischen* Ziele verteidigen oder neu aufbauen muss (d’Aveni 1994).

Für Unternehmen und ihre Bevollmächtigten, welche ihr wirtschaftliches Überleben in der Konfrontation mit diesen Phänomenen in Frage gestellt sehen, steigt der Anreiz auf Methoden der Wirtschafts- und Industriespionage zurückzugreifen (Lux/Peske 2002a: 12).

Untermauert wird diese Ansicht durch die Rational Choice Theory von Cornish und Clarke (1986): Dieser kriminologischen Theorie zu Folge beruht vorsätzliches kriminelles Verhalten auf einer durch den Täter ad hoc vorgenommenen Kosten-Nutzen-Analyse. Hierbei wägt er das Risiko, sich für die Tat verantworten zu müssen, und die Schwere der dafür zu erwartenden Strafe gegen die durch die Tat zu erlangenden Werte und seinen unmittelbaren Bedarf dieser Werte ab. Übertragen auf das Beispiel der Wirtschafts- und Industriespionage bedeutet dies Folgendes: Sobald der zu erwartende Nutzen des Täters in der Sicherung des eigenen wirtschaftlichen Überleben besteht, steigt die Wahrscheinlichkeit, dass er hierfür eine illegale Handlung vornimmt, im Vergleich zu einer Tat, welche ihm in wirtschaftlich guter Lage lediglich zusätzlichen Profit sichert, immens[17].

Auch aufgrund seiner hohen Know-How-Intensität unterliegt speziell der deutsche Wirtschaftsraum einer besonderen Gefährdung durch Wirtschafts- und Industriespionage. Gelingt es nämlich fremden Mächten deutsche Forschungsergebnisse auszuspähen und in marktfähige Produkte zu verwandeln, können sie diese auf dem Weltmarkt zu weitaus günstigeren Preisen anbieten, da sie nicht auf eine Amortisierung der Kosten für Forschung und Entwicklung angewiesen sind.

17 Dies zeigt natürlich nur die Neigung auf, generell straffällig zu werden. Welcher Art das verübte Delikt ist, ob es zum Beispiel im Bereich des Betruges oder in der Wirtschafts- und Industriespionage anzusiedeln ist, bleibt hierbei offen.

Gerade ein forschungsintensiver Standort wie Deutschland kann aber von einer globalen Entwicklungsvernetzung auch profitieren, auch wenn ihre Auswirkungen von den sogenannten „globalisierungskritischen" Gruppen (ATTAC 2006) kontrovers diskutiert werden. Ein Blick in die Jahresstatistik des Europäischen Patentamts verdeutlicht, dass Deutschland in Forschung und Entwicklung zu den führenden Nationen der Welt gehört. Laut Jahresstatistik des Europäischen Patentamts (2006: 1) wurden im Jahr 2006 an deutsche Unternehmen insgesamt 14.274 Patente erteilt. Dies sind mehr als 40% der an europäische Unternehmen vergebenen Patente und fast ein Viertel der an alle Unternehmen weltweit vergebenen Patente[18]. Es ist somit zu vermuten, dass die führende Stellung Deutschlands im Export forschungsintensiver Güter nicht zuletzt eine Folge dieser außergewöhnlichen Innovativität ist.

Eine vollständige Betrachtung der wirtschaftlichen Auswirkungen des Phänomens der Globalisierung – ganz zu schweigen von ihrer politischen und kulturellen Dimension – kann an dieser Stelle nicht geleistet werden. Für den Bereich der Wirtschafts- und Industriespionage ist jedoch zu vermuten, dass die Neigung kriminelle Handlungen zu vollziehen mit steigendem Druck auf die Angebotsseite der Märkte wächst, und dass Deutschland als innovativer Forschungsstandort aufgrund erhöhter globaler Transparenz weiterhin zunehmend im Fokus illegaler und klandestiner Aktivitäten der Informationsbeschaffung stehen wird.

3.3 Das Informationszeitalter

> „Imagine, if you can, a small room, hexagonal in shape, like the cell of a bee. […] An armchair is in the centre, by it's side a reading desk - that is all the furniture. And in the armchair there sits a swaddling lump of flesh - a woman, with a face as white as fungus. It is to her that the little room belongs. An electric bell rang. […] „I suppose, I must see who it is.", she thought, and set her chair in motion. The chair […] was worked by machinery and rolled her to the other side of the room where the bell rang importunately. „Who is it?" she called. […] She knew several thousand people, in certain directions human intercourse had advanced

18 Einzig die USA haben 2006 mehr Patente in Europa angemeldet: Mit 14.834 erfolgreichen Anmeldungen liegen sie an erster Stelle, es folgen Deutschland (14.274), Japan (12.044), Frankreich (4.498) und Italien (2.317) (Europäisches Patentamt 2006: 1).

> enormously. […] The round plate that she held in her hands began to glow. A faint blue light shot across it, darkening to purple, and presently she could see the image of her son, who lived on the other side of the earth, and he could see her." Auszug aus „The machine stops" (Forster 1909)

Der obige literarische Auszug sieht, trotz seiner Erstveröffentlichung vor fast 100 Jahren, bereits verschiedene Charakteristika des menschlichen Zusammenlebens der heutigen Zeit voraus, eine Zeit die häufig durch das Schlagwort „Informationszeitalter" (Information Age) (Keohane/Nye 1998; Alberts/Papp 1997; Lallana/Uy 2003) beschrieben wird. Doch was ist unter diesem, dem Werk sogenannter Futurologen (Toffler 1980) entstammendem Schlagwort zu verstehen und welchen Einfluss hat es auf die Belange von Wirtschafts- und Industriespionage?

Das „Information Age" bezeichnet:

> „[…] the current stage in societal development, which began to emerge at the end of the twentieth century. This period is marked by the increased production, transmission, consumption of and reliance on information." (Center for International Development at Harvard University o.J.)

Gemäß dieser Definition ist die gegenwärtige Gesellschaftsform in hohem Maße vom vermehrten Umgang mit dem Phänomen Information geprägt. Im Nachsatz wird deutlich, dass diese einen massiven Einfluss auf das menschliche Sozial- und Marktverhalten ausübt: „Many consider the new role of information to be changing our social and economic behavior as dramatically as did the Industrial Revolution." (ebd.). Man kann also von einem von Information abhängigen Wirtschaftssystem, der Information Economy sprechen. Kennzeichen dieser Informationsökonomie sind:

- Globale Verknüpfung in Echtzeit (Vgl. Kapitel 3.1.2)
- Weltweites Reservoir qualifizierter Arbeitskräfte
- Freier, grenzüberschreitender Kapitalverkehr in Echtzeit
- Hohe Produktivität
- Profit durch hohe Innovationsgeschwindigkeit (Vgl. Kapitel 3.2)(Lallana/Uy 2003: 14f)

In dieser Gesellschaft ist also Information, ergänzend zur klassischen Gutenbergschen Einteilung in Elementar-[19] und dispositive[20] Faktoren (Gutenberg 1983) zu einem den Elementarfaktoren zuzurechnenden Produktionsfaktor avanciert (Jehle/Müller/Michael 1994: 1), auch wenn dies (meist jedoch aus formellen Gründen) noch verschiedentlich bezweifelt wird (Seidenberg 1998: insb. 35f).

Die technologische Grundlage dieser Entwicklungen liegt in der Ubiquität moderner digitaler Mikroprozessoren, welche durch die von Ihnen verliehenen Fähigkeiten der massenhaften Datenerhebung, -verarbeitung und -speicherung die „digitale Revolution" erst ermöglichten (Lallana/Uy 2003: 6).[21] Die Veränderung technologischer Rahmenbedingungen resultierte somit also auch in Veränderungen gesellschaftlicher und ökonomischer Rahmenbedingungen.

Neben dem bereits in Abschnitt 3.2 gezogenen Fazit, das eine positive Korrelation zwischen einem steigendem Innovations- und damit auch Wettbewerbsdruck und dem Anreiz zum Einsatz illegaler Methoden feststellt, lassen sich aus den obigen Ausführungen weitere Konsequenzen für das Feld der Wirtschafts- und Industriespionage, vor allem für den Bereich der Methodik ableiten:

Vor dem Beginn des Informationszeitalters war das Entwenden großer Mengen von Informationen aufgrund von Schwierigkeiten mit deren Übertragung und Speicherung ein aufwändiges Unterfangen. Informationen wurden vor allem auf beschriebenem oder bedrucktem Papier oder in Form analoger Abbildungen, wie etwa Fotografien oder Mikrofiche, aufbewahrt. Diese mussten, um eine spätere geordnete Aufbereitung zu ermöglichen (vgl. Konzept des Intelligence Cycle, Kapitel 2.1) entweder an Ort und Stelle reproduziert, oder in Gänze entwendet werden. Beides konnte je nach Umfang der Operation zu massiven logistischen Problemen führen. Als Beispiel mag hier der im Januar 2007 begonnene Prozess gegen ehema-

19 Menschliche Arbeitsleistung, Betriebsmittel, Werkstoffe.

20 Diese kombinieren die drei Elementarfaktoren zu einer produktiven Einheit.

21 Obgleich Lallana und Uy die bloße „Erfindung" dieser Prozessoren als ausschlaggebend herausstellen, stellt der Vorgang der Schöpfung einer Technologie meist nur die notwendige Bedingung für die von ihr ausgelösten gesellschaftlichen Veränderungen dar, während nach Meinung der Autoren die Ubiquität (Allgegenwart, allgemeine Verfügbarkeit) oder zumindest die Marktreife hierzu zwingend die hinreichende Bedingung darstellt.

lige Mitarbeiter der insolventen Fluggesellschaft Swissair gelten. Dessen Anklageschrift hätte jeden, der sich ihr vor ihrer Veröffentlichung hätte bemächtigen wollen, vor kaum zu bewältigende Schwierigkeiten gestellt, da sie beachtliche 4.200 Aktenordner umfasste (Dunsch 2007).

Eine Begleiterscheinung der sich stetig fortentwickelnden Informationsgesellschaft ist die ebenso stetig fortschreitende Miniaturisierung elektronischer Systeme. Dies zeigt sich zum einen am prominenten Beispiel des Mooreschen Gesetzes (Intel o.J.), einer empirisch fundierten Faustregel, welche besagt, dass sich die Anzahl der Transistoren eines marktüblichen Prozessors bei gleich bleibendem Preis alle 24 Monate verdoppelt (ein Zusammenhang dessen Gültigkeit seit 1971 belegt ist), zum anderen auch an der stetigen Miniaturisierung von Speichermedien. Nahm eine Datenmenge von einem Gigabyte gegen Anfang der 90er Jahre noch den gesamten Speicherplatz Dutzender handelsüblicher Festplatten in Anspruch, so sind zum gegenwärtigen Zeitpunkt (Februar 2008) selbst Festplatten mit Größen im einstelligen Gigabytebereich bereits nicht mehr marktüblich. Dies verwundert nicht: USB-Massenspeichermedien („Memory Sticks“) mit einer Speicherkapazität von 32 Gigabyte (Herstellerseite: Corsair 2008) und portable Festplatten mit einer Kapazität von bis zu 2 Terabyte sind seit einiger Zeit im Handel verfügbar (Herstellerseite: Western Digital 2008). Ein kurzes gedankliches Experiment soll die Bedeutung dieser Dimensionen verdeutlichen:

- Ein vollständig gefüllter DIN A4 Aktenordner enthält bei einer üblichen Papierstärke von 70 - 80 g/m2 geschätzte 500 Blatt Papier.
- Versuche zeigen, dass eine 500 Seiten starke, formatierte Textdatei (ohne Abbildungen) einer handelsüblichen Office-Anwendung ohne Dateikomprimierung eine Dateigröße von ca. 1,5 Megabyte umfasst.
- Die im obigen Beispiel genannten 4.200 Aktenordner ergäben also eine Datenmenge von 6.300 Megabyte, d.h. 6,3 Gigabyte.
- Digitalisiert auf einem USB-Massenspeicher neuester Generation (32 Gigabyte Speicherkapazität), belegen also 4.200 Standardformat-Aktenordner (je

8x29x32 cm = 7.424cm³) mit einem Raumvolumen von ca. 31 Kubikmetern (fast die Kapazität eines 20-Fuß-ISO-Containers) gerade mal knapp 20% des zur Verfügung stehenden Speicherplatzes.

Die Möglichkeit, eine Textdatei mit zusätzlichen Mediadaten (Bild und Ton) anzureichern, sowie die Möglichkeiten der Dateikomprimierung oder des Duplexdrucks lassen diese Größenangaben stark schwanken, die Dimensionen der rasant fortschreitenden Miniaturisierung dürften dennoch klar geworden sein.[22]

Doch was bedeutet dies nun für den Themenkomplex der Wirtschafts- und Industriespionage?

1. Information liegt aus Gründen der Effizienz zunehmend vor allem in digitalisierter Form vor.

2. Das Informationszeitalter sorgt für immense Fortschritte bei der Verarbeitung, Übertragung und Speicherung von Information (siehe obiges Experiment und vgl. Shulsky/Schmitt 2002: 7).

Daraus folgt, dass – unter methodischen Gesichtspunkten – der nicht autorisierte Zugang zu Information in vielerlei Hinsicht vereinfacht worden ist. Vor allem der Vorgang des Entwendens von Informationen ist von logistischen Problemen befreit worden: Besagte 4.200 Aktenordner finden auf einem Speichermedium Platz, welches – am Körper getragen – nur mit Hilfe einer Leibesvisitation zu finden ist. Unzugänglichere Orte, wie zum Beispiel das Innere eines hohlen Schuhabsatzes, stellen Sicherheitsverantwortliche vor ungleich größere Probleme.

Die obigen Überlegungen gelten für den Fall, dass der Diebstahl eine physische Präsenz am Ort der Datenaufbewahrung erfordert. In einer global vernetzten Welt ist es jedoch nicht unüblich, dass digitalisierte Informationen in Firmen-, NGO- oder Regierungsnetzwerken von außen zugänglich sind.[23] „Außen“ meint hier je-

22 Selbst die gesammelten multimedialen Daten der von der Wikimedia Foundation gehosteten Onlineenzyklopädie Wikipedia, immerhin 15 Gigabyte in 243 Sprachen (Stand: September 2006; Quelle: Wikimedia Foundation 2008), hätten Platz auf einem Speichermedium von der Größe eines Fingers.

23 Dies geschieht vor allem um eine enge Zusammenarbeit räumlich getrennter Organisationen und Dienststellen zu ermöglichen. Ein Beispiel wäre eine Forschungs- und Entwicklungszusammenarbeit verschiedener Landesdivisionen eines Automobilkonzerns.

den beliebigen Personalcomputer der Welt, welcher mit dem Internet verbunden, aber nicht Teil eines der oben genannten Netzwerke ist. Gelingt es eventuell mit den zu entwendenden Daten verbundene Sicherheitsmaßnahmen zu überwinden, muss der betreffende Täter hierfür nicht einmal die Sicherheit der eigenen vier Wände verlassen; ein Vorgang wie er vor Ubiquität der Personal Computer und des Zugangs zum Internet nicht möglich gewesen wäre.

Eine weitere Verschärfung der Gefährdungslage ergibt sich aus der fortschreitenden Miniaturisierung der Überwachungstechnologie, auf welche das Methodikkapitel noch einmal kurz Bezug nimmt. Insgesamt ist somit zu bemerken, dass die Gefährdung durch Wirtschafts- und Industriespionage durch den rasanten technologischen Wandel eine neue, ungleich höhere Qualität erfahren hat.

3.4 Rechtliche Rahmenbedingungen

Nicht zuletzt hängt es vom Augenmaß des nationalen (oder internationalen) Gesetzgebers ab, wann eine Handlung vor dem Gesetz als Wirtschafts- oder Industriespionage zu gelten hat. Diese Beurteilung stellt sich jedoch je nach angelegtem Gesetzesrahmen durchaus unterschiedlich dar. Entgegen der oben angeführten weiten Auslegung des Begriffs des „Deutschen Wirtschaftsraumes“, kann an dieser Stelle allein schon aus Platzgründen nur eine zusammenfassende Diskussion der wichtigsten Normen des bundesdeutschen Strafrechts geleistet werden.[24] Verwandte zivilrechtliche Ansprüche auf Schadenersatz oder Unterlassung können zwar in Folge von Wirtschaftsspionage entstehen, an dieser Stelle sollen jedoch die gesetzlichen Instrumente mit der höheren Abschreckungswirkung gegenüber dem potentiell straffälligen Individuum – mehrjährige Freiheitsstrafen im Gegensatz zu zivilrechtlichen Schadenersatzzahlungen – diskutiert werden.

24 Alle Normen, welche in diesem und den folgenden Kapiteln erläutert werden, finden sich alphabetisch gegliedert, und paragraphenweise mit URLs zu ihrem Fundort auf den Seiten des Bundesjustizministeriums versehen, im Literaturverzeichniss wieder.

Für eine umfassende Betrachtung der Thematik einschließlich völker- und europarechtlicher Verknüpfungen sei an dieser Stelle auf die Dissertation von Sule (2006) verwiesen.

3.4.1 Rechtlicher Rahmen im Bereich der Industriespionage

Die zentralen Vorschriften zur Bekämpfung von Delikten, welche durch privatwirtschaftliche Institutionen und Einzelpersonen begangen wurden, finden sich in den §§17ff UWG, des Gesetzes gegen den unlauteren Wettbewerb.

Zu beachten ist hierbei, dass der Begriff der Industriespionage (oder eines seiner zahlreichen Synonyme) nicht im Gesetzestext zu finden ist. Dieser kommt im deutschen Recht weder als Tatbestand vor, noch erfährt er eine wie auch immer geartete Legaldefinition (Lux/Peske 2002a: 115). Delikte dieser Art werden stattdessen unter dem Oberbegriff des Geheimnisverrats behandelt, wobei zwischen dem Verrat von Staatsgeheimnissen (siehe dazu Kapitel 3.4.2) einerseits und dem Verrat von Geschäfts- und Betriebsgeheimnissen andererseits unterschieden wird (Lux/Peske 2002a: 115).

Zentrale Norm im Bereich des Verrats von Betriebs- und Geschäftsgeheimnissen ist §17 I UWG: „Wer als eine bei einem Unternehmen beschäftige Person ein Geschäfts- oder Betriebsgeheimnis, das ihr im Rahmen des Dienstverhältnisses anvertraut worden oder zugänglich gemacht worden ist, während der Geltungsdauer des Dienstverhältnisses unbefugt an jemand zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, mitteilt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft."

Entscheidend bei der Anwendung dieser Norm ist die Unterscheidung, wann es sich bei einer Tatsache um ein Betriebs- oder Geschäftsgeheimnis handelt. Többens (2000: 506) macht dies an vier maßgeblichen Kriterien fest: Zunächst einmal muss die geheim zu haltende Tatsache eine *Beziehung zu einem Geschäftsbetrieb* aufweisen. Auskünfte über private Beziehungen der Unternehmensmitarbeiter untereinander sind hiervon zum Beispiel nicht erfasst. Eine bereits marktbekannte Re-

zepturzutat kann jedoch als Betriebsgeheimnis eine Beziehung zum Geschäftsbetrieb aufweisen, wenn geheim ist, dass diese für ein Produkt verwendet wird.

Weiterhin muss die Tatsache dem Kriterium der *Nichtoffenkundigkeit* genügen. Ist diese Tatsache allgemein bekannt, wurde sie zum Beispiel im Jahresabschluss eines Unternehmens publiziert, erfüllt sie dieses Kriterium nicht. Ihr Verrat ist demnach nicht strafbar. Nichtoffenkundig ist sie demnach, wenn sie nur einem eng begrenztem Personenkreis bekannt ist. Eine Festlegung, wie viele Mitglieder ein solch eng begrenzter Kreis umfassen darf, ist sicherlich von Fall zu Fall verschieden und liegt im Auge des zuständigen Gerichtes. Entscheidend ist hierbei, dass bei Anzahl und Auswahl der Mitglieder davon auszugehen ist, dass das Geheimnis gegenüber dem Wettbewerb gewahrt bleibt.

Das dritte Kriterium ist der erkennbare *Geheimhaltungswille* des Betriebsinhabers. Dieses Kriterium verlangt lediglich, dass sich aus der Natur der geheim zu haltenden Sache ein Geheimhaltungswille des Inhabers vermuten lässt.

Schließlich wird von der Rechtsprechung ein *berechtigtes wirtschaftliches Geheimhaltungsinteresse des Geschäftsinhabers* an der Tatsache verlangt. Dies ist immer dann der Fall, wenn das Unternehmen durch das Bekanntwerden dieser Tatsache Wettbewerbsnachteile zu erleiden hat. Fraglich ist jedoch, wann solch ein Interesse berechtigt ist. Hat eine Bank ein berechtigtes Interesse an der Geheimhaltung von Praktiken, mit denen sie Großkunden bei der Steuerhinterziehung im Ausland behilflich ist? Többens (2000: 506) bejaht dies mit dem knappen Hinweis, der Arbeitnehmer sei „weder Sittenrichter noch Kontrollorgan“ gegenüber seinem Arbeitgeber. Die dahinter stehende und entscheidende Frage ist jedoch: Sollte es einem Arbeitnehmer erlaubt sein, aus sitten- und gesetzeswidrigen Geschäftspraktiken seines Arbeitgebers einen explizit wirtschaftlichen Vorteil zu ziehen? Ein überhöhtes Maß an Täterschutz kann hier ebenso wenig im Interesse des Staates liegen wie die Aussicht, seine Bürger als bezahlte Denunzianten durch Aussicht auf Belohnung in mit-

unter prekäre Rechtslagen zu bringen[25]. Für eine weitere Diskussion der Frage sei hier auf die einschlägige juristische Fachliteratur verwiesen, welche speziell vor dem Hintergrund der aktuellen Kontroverse (Februar 2008) um den Handel mit gestohlenen Kontodaten der liechtensteinischen LGT Gruppe sicher zu neuen Erkenntnissen finden wird[26].

Selbst wenn die Qualität einer Tatsache als Betriebs- oder Geschäftsgeheimnis zweifelsfrei feststeht, gilt es im Geltungsbereich des §17 I UWG zwei wichtige Ausnahmen zu beachten: Zum einen ist fraglich, ob dieser gegenüber freiberuflich für das Unternehmen tätigen Personen – wie etwa Wirtschaftsprüfern oder Steuerberatern – Anwendung findet (Lux/Peske 2002a: 119), zum anderen schließt er die Strafwürdigkeit von Personen, welche ihre redlich im Unternehmen erworbenen Kenntnisse nach Ablauf ihres Anstellungsverhältnisses im Dienst eines anderen Unternehmens einsetzen, aus (Többens 2000: 507). Aus diesem Ausschluss ergibt es sich, dass Arbeitsverträge vielfach durch über den eigentlichen Arbeitsvertrag hinausgehende Geheimhaltungsvereinbarungen ergänzt werden (Corporate Trust 2007: 36; für eigene diesbezügliche Untersuchungen siehe Anhang 1).

Der zweite Absatz stellt das Ausspähen eines Betriebes (hier wörtlich: unbefugtes Verschaffen und Sichern) in §17 II (1) UWG unter Strafe. Als Täter kommt hier jedermann, also nicht nur ein Angehöriger des betreffenden Unternehmens in Betracht. Explizit eingeschlossen wird hier das Ausspähen durch technische Mittel, die Herstellung einer verkörperten Wiedergabe des Geheimnisses und die Wegnahme einer das Geheimnis verkörpernden Sache. Die schließt Tätigkeiten wie Diebstahl, Abschreiben oder Fotografieren mit ein, weist aber eine unmittelbare Lücke auf: Der bloße Vorgang des Aneignens steht nicht unter Strafe sofern dies rein mittels Gedächtnisleistung erfolgt und keine Verwertung oder Mitteilung nach §17 II (2) UWG erfolgt (Lux/Peske 2002a: 120). Ein Täter, welcher zum Beispiel durch Belauschen eines Gespräches ohne technisches Gerät von Betriebs- und Ge-

25 Man stelle sich vor, ein Arbeitnehmer verkauft solche Daten an den Staat, der Arbeitgeber kann aber nachweisen, dass sein Geheimhaltungsinteresse *doch* berechtigt war.

26 Siehe hierzu die Pressemitteilungen des betroffenen Geldinstituts: LGT Gruppe (2008).

schäftsgeheimnissen erfährt, dem man aber eine Verwendung oder Mitteilung nicht nachweisen kann, bleibt nach §17 UWG straffrei.[27]

Weiterhin wird im zweiten Absatz das unbefugte Verwerten oder Mitteilen von Geschäfts- und Betriebsgeheimnissen unter Strafe gestellt. §17 II (2) UWG sieht dafür den gleichen Strafrahmen vor wie in §17 I UWG. Der straffreie Spezialfall aus Absatz 2 Nummer 1 wird hier in der Generalklausel der sonstigen unbefugten Verschaffung oder Sicherung ausgeschlossen.

§17 III UWG enthält die Bestimmung, dass bei Delikten nach Absatz 1 und 2 auch der Versuch strafbar ist, §17 IV UWG sieht in besonders schweren Fällen eine Verschärfung des Strafmaßes bis zu einer Freiheitsstrafe von fünf Jahren oder eine Geldstrafe vor. Ein besonders schwerer Fall liegt dann vor, wenn der Täter gewerbsmäßig handelt[28], bei Mitteilung Kenntnis von einer bevorstehenden Verwertung im Ausland hat oder eine Verwertung im Ausland selbst vornimmt. Die genauere Auslegung des unbestimmten Rechtsbegriffs „Ausland" ist in diesem Zusammenhang Többens (2000: 509) zu entnehmen.

Ein Absatz mit größeren Konsequenzen für die Praxis deutsche Strafverfolgungspraxis ist §17 V UWG. Er konstatiert, dass Delikte nach Absatz 1 und 2 nur auf Antrag verfolgt werden. Die Strafverfolgungsbehörden schreiten von Amts wegen nur im Falle besonderen öffentlichen Interesses ein, es handelt sich hierbei also um so genannte Anzeigedelikte. Der letzte Absatz, §17 VI UWG, verweist schließlich auf §5 Nr. 7 StGB, welcher verfügt, dass eingangs beschriebene Delikte auch dann unter das deutsche Strafrecht fallen, wenn davon ein Tochterunternehmen eines deutschen Konzerns betroffen ist.

Weiterhin von Bedeutung sind die §§18 und 19 des UWG, welche hier noch in aller Kürze erläutert werden sollen. Im Gegensatz zum Schutz der inneren betrieblichen Sphäre des §17 UWG schützt §18 UWG das Unternehmen und dessen Geheimnisse im Umgang mit der Außenwelt. Nach Absatz 1 wird das unbefugte

27 Die praktische Relevanz dieser Lücke dürfte jedoch äußerst gering sein.

28 Gewerbsmäßig handelt in diesem Zusammenhang, wer sich mit der fortlaufenden Straftat eine auf Dauer angelegte, finanzielle Einnahmequelle schaffen will, die Tat also wie einen Beruf betreibt.

Verwerten oder Mitteilen von im geschäftlichen Verkehr anvertrauten Vorlagen mit einer Freiheitsstrafe von bis zu zwei Jahren oder mit einer Geldstrafe bestraft. Die Formulierung „Geschäftlicher Verkehr" verkörpert hier den Umgang mit Geschäftspartnern oder Beauftragten, welche nicht dem Unternehmen angehören. Unter Vorlagen und Vorschriften technischer Art fallen zum Beispiel Blaupausen, Fertigungsanweisungen, Bühnenmanuskripte und ähnliche Aufzeichnungen (siehe dazu Többens 2000: 510). Die Ausführungen zu den Abschnitten 3, 5 und 6 des §17 UWG gelten analog für die Abschnitte 2, 3 und 4 des §18 UWG.

§19 UWG schließlich stellt die zu obigen Delikten gehörenden Vorbereitungshandlungen unter Strafe. Absatz 1 bedroht die Anstiftung zu einem Vergehen nach §17 und §18 UWG mit einer Freiheitsstrafe von bis zu zwei Jahren oder Geldstrafe. Dabei ist es unerheblich, auf welche Art und Weise die Anstiftung erfolgte, und ob der prospektive Täter ein Unternehmensangehöriger oder ein außenstehender Mittelsmann ist. Ebenso wird nach Absatz 2 bestraft, wer einem anderen anbietet, eine Straftat nach §17 und 18 UWG zu begehen, oder den Antrag eines anderen, eine derartige Tat zu begehen oder zu ihr anzustiften, annimmt. Zu beachten ist, dass nach §19 III UWG straffrei bleibt, wer von einer derartigen Tat nachprüfbar zurücktritt.

Auch hier gilt jedoch wieder (nach §19 IV UWG), dass analog §17 V UWG eine Strafverfolgung von Amts wegen nur im Falle besonderen öffentlichen Interesses stattfindet, und eine derartige gegen den ausländischen Teil eines deutschen Konzerns gerichtete Tat analog §17 VI UWG in Verbindung mit §5 Nr. 7 StGB nach §19 V UWG ebenfalls verfolgt wird.

Weitere für die Strafverfolgung relevante Tatbestände ergeben sich aus einer Reihe von Normen, die über die unterschiedlichsten Gesetze verteilt sind, als da wären: §404 Aktiengesetz, §120 Betriebsverfassungsgesetz, §151 Gesetz betreffend die Erwerbs- und Wirtschaftsgenossenschaften, §85 Gesetz betreffend die Gesellschaften mit beschränkter Haftung, §333 Handelsgesetzbuch, §19 Gesetz über die Rechnungslegung von bestimmten Unternehmen und Konzernen und §138 Gesetz

über die Beaufsichtigung der Versicherungsunternehmen (Lux/Peske 2002a: 122).[29] Für diese Delikte sieht das Gesetz in der Regel eine Freiheitsstrafe bis zu einem Jahr oder Geldstrafe, in besonders schweren Fällen bis zu zwei Jahren oder Geldstrafe vor. Auch diese Delikte werden nur auf Antrag verfolgt, der Versuch ist jedoch nicht strafbar (Lux/Peske 2002a: 123).

Welchen Einfluss hat diese Rechtslage nun auf das Gefährdungsniveau des deutschen Wirtschaftsraumes?

Als uneingeschränkt positiv stellt sich der Bezug des rechtlichen Rahmens auf den gesamten deutschen Wirtschaftsraum dar, welcher wie bereits oben erwähnt durch §§17 VI, 18 IV und 19 V UWG in Verbindung mit §5 Nr. 7 StGB gesichert ist, da laut Corporate Trust Studie aus dem Jahre 2007 immerhin 15% der Spionagestraftaten gegen deutsche Unternehmen in deren Auslandsniederlassungen registriert werden (Corporate Trust 2007: 20).

Die Abschreckungswirkung der im Fall des §17 UWG bei fünf Jahren angesetzten Höchstfreiheitsstrafe muss jedoch als durchaus ambivalent betrachtet werden. Zwar dürfte von der Höhe des Strafmaßes eine gewisse Signalwirkung ausgehen, jedoch sollte man sich auch darüber im Klaren sein, dass der sogenannte schwere Fall nur unter engen Voraussetzungen erfüllt ist, andernfalls liegt die Höchststrafe lediglich bei drei Jahren. Hierzu ist, wie bei allen anderen Straftaten auch, zu bemerken, dass dieser Strafrahmen in vollem Maße nur von Gerichten ausgeschöpft wird, die geneigt zu glauben sind, dass die Straftat mit einem nachweisbar hohen Maß an krimineller Energie begangen wurde („Art der Ausführung und verschuldete Auswirkungen der Tat“ nach §46 II StGB). Andernfalls ist die Verhängung einer milderen Freiheitsstrafe, die Verhängung einer Geldbuße oder gar eine Aussetzung zur Bewährung zu erwarten.

Auch im Vergleich mit dem Ausland ist der Strafrahmen relativ gering angesetzt. So sieht sich zum Beispiel der verurteilte amerikanische Straftäter für Delikte

29 Das ebd. erwähnte Schwerbehindertengesetz ist inzwischen in das Sozialgesetzbuch IX übernommen worden. Dort findet sich unter §130 zwar eine Geheimhaltungspflicht, jedoch keine Strafandrohung mehr.

dieser Kategorie nach §1832 des Economic Espionage Act von 1996 einer zehnjährigen Freiheitsstrafe, in den Fällen des §1831 sogar einer fünfzehnjährigen Freiheitsstrafe ausgesetzt.

Wenig hilfreich für die Abschreckungswirkung der verschiedenen Normen dürfte weiterhin sein, dass es sich bei den in den einschlägigen Normen verankerten Delikten ausnahmslos um Antragsdelikte handelt, bei denen die zuständigen Strafverfolgungsbehörden nur bei besonderem öffentlichen Interesse einschreiten. Da Unternehmen den aus einem Spionagefall resultierenden Imageschaden vielfach als sehr hoch einschätzen sind sie oft wenig geneigt, Vorfälle dieser Art öffentlich publik zu machen (Bundesamt für Verfassungsschutz 2006: 22; Corporate Trust 2007: 29).

Ganz allgemein scheint es um das Vertrauen der Wirtschaft gegenüber den deutschen Strafverfolgungsbehörden nicht gut bestellt: In nur einem guten Viertel aller Spionagefälle werden staatliche Ermittlungsbehörden eingeschaltet, größer scheint dagegen das Vertrauen in private Ermittler, diese wurden in knapp 40% aller Fälle zu Rate gezogen (Corporate Trust 2007: 29). Diese erfahren dadurch gerade in jüngster Zeit einen ungeahnten Aufschwung (Reppesgaard 2007).

Auch das in Kapitel 1.2 angeführte, auf diversen Technologiemessen erhobene Stimmungsbild ist in Bezug auf die Strafverfolgung dieser Delikte durch die deutschen Behörden eher negativ geprägt: Bekannt gewordene Vorfälle wurden den zuständigen Stellen nur zu einem geringen Teil gemeldet und angezeigte Vorfälle führten nur selten zu den gewünschten Ergebnissen (siehe Abb. 1).

Die Aussteller waren daher mehrheitlich der Meinung, dass diese Vorgehensweise mit nur geringer Wahrscheinlichkeit einen greifbaren Nutzen für das Unternehmen haben würde. Bei denjenigen Fällen, die aktenkundig gemacht wurden, war zu beobachten, dass zivilrechtlichen Unterlassungs- und Schadenersatzklagen im europäischen Raum ein gewisser Erfolg beschieden war. Im asiatischen Raum dagegen waren diese aussichtslos, strafrechtliche Konsequenzen konnten ebenfalls nicht erwirkt werden.

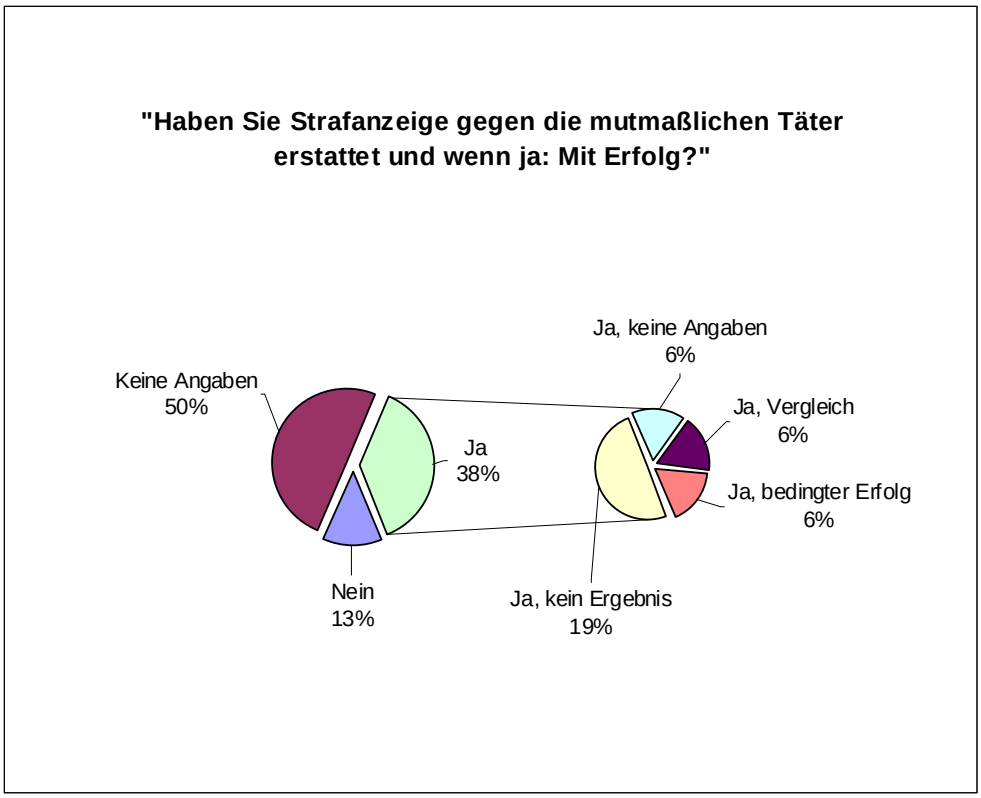

Abb. 2: Ergebnisse der Strafverfolgung

Insgesamt scheint die deutsche Gesetzgebung in Bezug auf Industriespionage weder das Vertrauen der Unternehmen zu besitzen, noch von vorzeigbaren Ergebnissen geprägt zu sein. Eine restriktivere Gesetzgebung könnte durch eine höhere Abschreckungswirkung zu einer Minderung der Gefährdung des deutschen Wirtschaftsraumes beitragen.

3.4.2 Rechtlicher Rahmen im Bereich der Wirtschaftsspionage

Strafrechtliche Sanktionen einer geheimdienstlichen Tätigkeit für ausländische Mächte innerhalb des Staatsgebietes der Bundesrepublik Deutschland sind Gegenstand der §§ 93-99 StGB. Zentraler Begriff der §§94-97 StGB ist der Verrat eines Staatsgeheimnisses, welcher in §93 StGB eine Legaldefinition erfährt. Wann ist nun das (nach Kapitel 2.2) definitionsgemäße Aneignen geheim gehaltener Informationen zur Erlangung eines wirtschaftlichen Vorteils mit dem Aneignen (und dem anschließenden Verrat) von Staatsgeheimnissen gleichzusetzen?

Hierzu heißt es in §93 I StGB: „Staatsgeheimnisse sind Tatsachen, Gegenstände oder Erkenntnisse, die nur einem begrenzten Personenkreis zugänglich sind und vor einer fremden Macht geheim gehalten werden müssen, um die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland abzuwenden." Nach Lux und Peske (2002a: 128) scheitert der Versuch Wirtschaftsspionagetätigkeiten mit dem Verrat von Staatsgeheimnissen gleichzusetzen regelmäßig daran, dass aus dem Verrat eines bestimmten Wirtschaftsgeheimnisses der Regel nach kein schwerer Nachteil für die Bundesrepublik Deutschland (das heißt für ihren Bestand, ihre äußere Sicherheit) droht. Ausnahmen von dieser Regel wären zum Beispiel bahnbrechende neue Erkenntnisse im industriellen Rüstungsbereich, welche geeignet wären, für eine Verschiebung der machtpolitischen Kräfteverhältnisse zu sorgen. Diese Fälle werden allerdings aufgrund ihres seltenen Vorkommens von der Betrachtung ausgenommen.

Spionagestraftaten im Dienst ausländischer Mächte, welche das oben genannte Tatbestandsmerkmal nicht erfüllen, werden in den Auffangtatbeständen der §§ 98 und 99 StGB erfasst. §98 StGB befasst sich hierbei unter dem Titel „Landesverräterische Agententätigkeit", ähnlich wie §19 UWG in Kapitel 3.4.1, mit auf den Verrat von Staatsgeheimnissen bezogenen Vorbereitungshandlungen.

Eine ungleich größere Relevanz besitzt im Rahmen dieser Arbeit §99 I StGB über „Geheimdienstliche Agententätigkeit": „Wer (1.) für den Geheimdienst einer fremden Macht eine geheimdienstliche Tätigkeit gegen die Bundesrepublik Deutschland ausübt, die auf die Mitteilung oder Lieferung von Tatsachen, Gegenständen oder Erkenntnissen gerichtet ist, oder (2.) gegenüber dem Geheimdienst einer fremden Macht oder einem seiner Mittelsmänner sich zu einer solchen Tätigkeit bereit erklärt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in § 94 oder § 96 Abs. 1, in § 97a oder in § 97b in Verbindung mit § 94 oder § 96 Abs. 1 mit Strafe bedroht ist." Seine besondere Relevanz ergibt sich daraus, dass er Spionagetätigkeiten, welche sich nicht mit dem Verrat von Staatsgeheimnissen nach §93 StGB befassen, und demnach nicht unter die Tat-

bestandsmerkmale der §§94-97 fallen, unter Strafe stellt. Hierzu muss allerdings auch wieder eine Reihe von Voraussetzungen erfüllt sein:

Erstens muss der Täter im Dienste einer fremden Macht stehen. Nach herrschender Meinung ist unter einer fremden Macht ausschließlich eine souveräner Staat oder eine staatlich gelenkte Organisation zu verstehen, ein Unternehmen fällt demnach im Allgemeinen nicht unter diese Definition (Lux/Peske 2002a: 129). Zweitens muss diese Tätigkeit gegen die Bundesrepublik Deutschland gerichtet sein. Lux und Peske sprechen hier von einer Vorverlegung der Abwehr von Spionageangriffen auf Unternehmensgeheimnisse (2002a, S. 129), daher ist anzunehmen, dass die Bundesrepublik hier auch in Form ihrer Wirtschaftslandschaft gemeint ist.

Der besonders schwere Fall wird in Absatz 2 betrachtet: „In besonders schweren Fällen ist die Strafe Freiheitsstrafe von einem Jahr bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter Tatsachen, Gegenstände oder Erkenntnisse, die von einer amtlichen Stelle oder auf deren Veranlassung geheimgehalten werden, mitteilt oder liefert und wenn er (1.) eine verantwortliche Stellung missbraucht, die ihn zur Wahrung solcher Geheimnisse besonders verpflichtet, oder (2.) durch die Tat die Gefahr eines schweren Nachteils für die Bundesrepublik Deutschland herbeiführt.“ Sollte also aus dieser Tätigkeit auch ohne den Verrat eines Staatsgeheimnisses – welcher ja nach Absatz 1 zur Anwendung der dort genannten Normen führen würde – die Möglichkeit eines schweren Nachteils erwachsen, wirkt dies erheblich strafverschärfend. Selbiges gilt für einen Täter, welcher eine verantwortliche Stellung, wie zum Beispiel ein Amt, welches ihn mit geheimhaltungspflichtigem Material in Berührung bringt, nutzt, um diese fremden Mächten zur Verfügung zu stellen. Auch hierbei muss es sich nicht um Staatsgeheimnisse handeln.

Absatz 3 nimmt schließlich Bezug auf §98 II StGB, welcher dem Tatrichter die Möglichkeiten der Strafmilderung und des Straferlasses gibt. Bedingung hierfür ist, dass der Täter sein Verhalten freiwillig aufgibt und er sein Wissen einer Dienststelle offenbart.

Zusammenfassend ist anzumerken, dass eine geheimdienstliche Agententätigkeit mit weitaus höheren Freiheitsstrafen bedacht wird (bis zu fünf Jahren Freiheitsstrafe, in schweren Fällen zehn) als eine Spionagetätigkeit für eine privatwirtschaftliche Institution (bis zu drei Jahren Freiheitsstrafe, in schweren Fällen fünf). Ob hier eine signifikant höhere Abschreckungswirkung erzielt werden kann ist jedoch fraglich:

Geheimdienste verfügen bei ihrer Tätigkeit über die Möglichkeit, einer rechtsstaatlichen Strafverfolgung durch die Behörden ihrer Einsatzländer zu entgehen, wenn sie als Agenten die Angehörigen einer ihrer Botschaften im Einsatzland verwenden. Der Grund hierfür liegt im Wiener Übereinkommen vom 24. April 1963 über konsularische Beziehungen. Nach diesem von fast allen Staaten der Erde ratifiziertem Abkommen verfügt ein akkreditierter Handlungsbefugter einer fremden Macht über diplomatische Immunität in seinem Gastland. Im Falle eines Vergehens gegen die Rechtsordnung dieses Gastlandes kann der Betreffende nicht gerichtlich belangt, sondern höchstens als *persona non grata* ausgewiesen werden. Für im Einsatzland rekrutierte Agenten oder nachrichtendienstliches Personal, welches nicht unter diplomatisch akkreditierter „Legende“[30] aktiv ist, dürften Strafen dieser Höhe jedoch eine gewisse Abschreckungswirkung erzielen.

3.5 Zwischenfazit

Die Untersuchung der Auswirkungen der für den Bereich der Wirtschafts- und Industriespionage geltenden Einflussfaktoren zeigen eine bereits seit Beginn der 90er Jahre stetig steigende Gefährdung des deutschen Wirtschaftsraumes. Eine Isolation der Einflussfaktoren gestaltet sich jedoch schwierig: Technologische Entwicklungen wie der Fortschritt moderner Echtzeitkommunikationstechnologie stehen in einem engem Zusammenhang mit dem Phänomen der Globalisierung, welches wiederum

30 „Legende“: Nachrichtendienstliche Bezeichnung für die Tarnidentität eines Geheimdienstmitarbeiters im Einsatz.

unter dem Einfluss eines bestehenden Ost-West-Konflikts kaum denkbar gewesen wäre.

Als entscheidend können jedoch folgende Faktoren betrachtet werden:

- Der Wechsel zur unipolaren Weltordnung sorgte zu Beginn der 90er Jahre für veränderte Informationsbeschaffungsprioritäten bei den staatlichen Geheimdiensten.
- Die zunehmende Globalisierung stellt Deutschland als Forschungsstandort stärker in den Fokus von Spionageaktivitäten.
- Der Eintritt der industrialisierten Welt in das Informationszeitalter vereinfacht die illegale und klandestine Informationsbeschaffung.
- Die einschlägige deutsche Rechtsordnung ist nicht dazu angetan, dass Vertrauen deutscher Unternehmen in die Strafverfolgung im Bereich der Wirtschaft- und Industriespionage zu gewinnen.

Die Statistik hilft, diesen Eindruck zu untermauern: Lag der Anteil von Wirtschaftsspionage an den gesamten nachrichtendienstlichen Spionageaktivitäten Schätzungen zufolge im Jahre 1994 weltweit bei 43%, so hatte er sich im Jahre 1997 bereits auf 87% erhöht (Lux/Peske 2002a: 12).

Ebenfalls im Anstieg begriffen ist die wahrgenommene Bedrohung durch derartige Phänomene: 81% der befragten Unternehmen fürchten, dass das Risiko durch Wirtschafts- und Industriespionage weltweit weiter steigen wird, über 70% befürchten dies auch für den deutschen Wirtschaftsraum (Corporate Trust 2007: 39).

4 Akteure der Wirtschafts- und Industriespionage

Die Interaktion zwischen den verschiedenen staatlichen und privaten Akteuren im Bereich der Wirtschafts- und Industriespionage ist durch ein komplexes Beziehungsgeflecht mit ambivalenten Rollen charakterisiert: Jeder Nationalstaat kann hierbei als Betreiber von Nachrichtendiensten in der Rolle eines offensiv informationsbeschaffenden Akteurs, sowie in der Rolle seiner staatlichen Schutzorgane, wel-

che solch ein Vorgehen zu verhindern suchen, auftreten. Gleiches gilt für die privaten Akteure, welche wiederum offensiv Industriespionage betreiben oder das Ziel derartiger Bestrebungen werden können.

Die Behandlung von ausländischen Nachrichtendiensten als offensive Akteure sowie die Behandlung von deutschen Unternehmen und Behörden als defensive Akteure ist allein der Perspektive dieser Arbeit geschuldet, die vom deutschen Wirtschaftsraum ausgeht. Gleichermaßen können deutsche Unternehmen Nutznießer von Spionagestraftaten sein (siehe dazu auch das Beispiel in Kapitel 4.1.2) und ausländische Nachrichtendienste sich illegaler und klandestiner Beschaffung wirtschaftlich relevanter Information innerhalb ihrer Wirtschaftsräume erwehren müssen, eventuell sogar gegenüber den Zuträgern der deutschen Nachrichtendienste, wie in der jüngsten Affäre um die Liechtensteiner LGT Gruppe und den Bundesnachrichtendienst deutlich wurde.

4.1 Offensive Akteure

Als offensiv gelten im Rahmen dieser Arbeit sowohl Akteure, die aktiv aus eigener Initiative heraus Wirtschafts- und Industriespionage betreiben, als auch diejenigen Akteure, die unter opportunistischer Ausnutzung der Gegebenheiten zu passiven Nutznießern derartiger Vorgänge werden. Ein staatlicher Geheimdienst, welcher dauerhaft einen Teil seiner Ressourcen für Wirtschaftsspionage verwendet, gilt daher ebenso als offensiv, wie ein Unternehmen, welches durch lose Kooperation mit einem Selbstanbieter[31] unregelmäßig mit vertraulichen Informationen versorgt wird. Entscheidend ist hierbei der Versuch des Akteurs, durch geheime Informationen einen wirtschaftlichen Vorteil zu erlangen. Die nachfolgenden Abschnitte sollen Aufschluss über die an Wirtschafts- und Industriespionage beteiligten Gruppierun-

31 Selbstanbieter: Privatperson, welche sich einem Nachrichtendienst oder einem Unternehmen in der Absicht anbietet, vertrauliche Informationen gegen Bezahlung oder Gewährung anderer Vorteile zu verschaffen.

gen geben. Diese werden getrennt nach staatlichen und privaten Akteuren betrachtet.

4.1.1 Staatliche Institutionen als offensive Akteure

Ausländische Nachrichtendienste betreiben aktiv und systematisch Wirtschafts- und Industriespionage im deutschen Wirtschaftsraum. Sie lassen sich in drei grobe geografische Kategorien einteilen: Nachrichtendienste Osteuropas (Bundesamt für Verfassungsschutz 2007: 300-309), Nachrichtendienste des Nahen und Fernen Ostens, (Bundesamt für Verfassungsschutz 2007: 310-318) und Nachrichtendienste westlicher Alliierter (Bundesamt für Verfassungsschutz 2006: 13-14). Nachfolgend werden exemplarisch Vertreter der einzelnen Kategorien anhand von Beispielen erläutert[32]. Im Fokus der Betrachtung liegen die *Struktur*, die *Vorgehensweise* und die *Motive* der handelnden Dienste.

Die Nachrichtendienste Osteuropas am Beispiel Russlands

Russland verfügt als politischer Erbe der Sowjetunion über eine bemerkenswerte Vorgeschichte im Bereich systematischer, staatlich gelenkter Wirtschaftsspionage. Federführend im größten je bekannt gewordenen Programm dieser Art war die Verwaltungsstelle T innerhalb der Ersten Hauptverwaltung des KGB.

Das Ziel des Programms bestand darin, die zwischen der Sowjetunion und den USA klaffende technologische Lücke zu schließen. Trotz großer wissenschaftlicher Erfolge in ausgewählten Gebieten (wie etwa der bemannten Raumfahrt) hinkte die technologische Entwicklung der Sowjetunion speziell auf dem Gebiet der Computerforschung und sonstiger Mikroelektronik den Standards der USA um bis zu 15 Jahre hinterher (Sagdeev 1994: 298). Um diesem Mangel zu begegnen schleuste das KGB, mit Beginn der von der Nixon-Administration maßgeblich geförderten Détente (Weiss 1996: 122), zu Beginn der siebziger Jahre Hunderte von Agenten in Wissenschaft und Forschung der Westmächte ein (ebd.: 124). Das Programm wurde zu

32 Einen detaillierten Überblick über die in Deutschland tätigen Nachrichtendienste geben Lux und Peske (2002a: 54f)

einem durchschlagenden Erfolg: Zwischen 2/3 und 3/4 der zu beschaffenden Technologien konnten gemäß späterer amerikanischer Schätzungen akquiriert werden (ebd.). Der Schwerpunkt der Beschaffung lag hierbei auf technischen Spezifikationen und Produkten aus den Bereichen Halbleitertechnologie, Radaraufklärung und Werkzeugmaschinen (ebd.).

Mit Hilfe des Doppelagenten Vladimir Vetrov (Codename „Farewell"), eines sowjetischen Überläufers innerhalb der Verwaltungsstelle T gelang es, das Programm aufzudecken und in zwei Phasen aufzurollen. In der ersten Phase wurden den Agenten des sowjetischen Netzwerks sorgfältig manipulierte Informationen untergeschoben, welche authentisch wirkten, aber im produktiven Einsatz zu teilweise verheerenden Problemen führten. So löste die Manipulation einer Software zur automatischen Pipelinesteuerung kurz nach Ihrer Inbetriebnahme durch Umgehung von Sicherheitssperren und durch gegeneinander arbeitende Pumpen und Ventile die bis dato größte je auf der Erde gemessene nicht-nukleare Detonation aus: Eine wichtige sibirische Gaspipeline explodierte mit einem Äquivalent von 3.000 Tonnen TNT (Saffire 2004). Wachgerüttelt von diesem Ereignis stand bei den russischen Behörden von da an jedwede erbeutete Technologie unter Generalverdacht. Mit Phase 2 wurde das Spionage-Projekt schließlich vollständig gestoppt: Etwa 200 enttarnte sowjetische Spione wurden aus den betroffenen NATO-Staaten ausgewiesen (Weiss 1996: 125).

Diese Vorgänge zeigen deutlich, dass trotz aller immer wieder zitierten Schwierigkeiten großer und systematischer Spionageprogramme (vgl. Lowenthal 2003: 196) diese durchaus im Bereich des Möglichen liegen. Es kann allerdings davon ausgegangen werden, dass in „gemeinschaftlichen" Gesellschaften, welche einen hohen Grad der Verflechtung zwischen Staat und Wirtschaft aufweisen die Wahrscheinlichkeit systematischer Wirtschaftsspionage wesentlich höher liegt als in „individualistischen" Gesellschaften, in denen diese Verknüpfung nur in geringem Maße gegeben ist (Harbich 2006: 36).

Obwohl seit dem Ende des Kommunismus Staat und Wirtschaft auf dem Gebiet der heutigen russischen Föderation formell keine Einheit mehr bilden, finden sich dort dennoch viele Anzeichen einer gemeinschaftlichen Gesellschaft. Es existiert zum Beispiel, wie bereits oben erwähnt, eine regierungsseitig protegierte personelle Verknüpfung zwischen staatlichen Stellen und Wirtschaftsunternehmen in Form sogenannter „bürokratischer Oligarchen" (Kononczuk 2006: 50)[33]. Weiterhin erstarkt die wirtschaftliche Zentralgewalt im „System Putin" zu Ungunsten des privaten Sektors. Bedenkt man nun noch den Trend der fast schon gewaltsamen Verstaatlichung einst privater Großunternehmen[34] so scheint es nur eine Frage der Zeit zu sein, bis zum einen die größten russischen Wirtschaftszweige wieder staatlich gelenkt sind, und zum anderen erneut und massiv staatliche Ressourcen aus dem Bereich der Nachrichtendienste zur Durchsetzung russischer Wirtschaftsinteressen eingesetzt werden[35].

Nicht verwundern mag vor diesem Hintergrund, dass das deutsche Bundesamt für Verfassungsschutz drei der russischen Nachrichtendienste schon jetzt zu den in Deutschland im Bereich der Wirtschaftsspionage aktivsten Diensten zählt (Bundesamt für Verfassungsschutz 2006: 10f). Deren Struktur soll nachfolgend kurz charakterisiert werden.

Eine zentrale Rolle in der Beschaffung im Ausland nimmt seiner Aufgabe gemäß der russische Auslandsgeheimdienst SVR ein. Aus der ehemaligen Ersten Hauptverwaltung des KGB entstanden, beschäftigt er ca. 12.000 bis 15.000 Mitarbeiter (Henderson 2003: 160; Bundesamt für Verfassungsschutz 2006: 10) und wurde bis Anfang Oktober 2007 vom Deutschlandexperten General Sergej Lebedew geführt. Als „Erbe" der Ersten Hauptverwaltung des KGB umfasst die organisatorische Struktur des SVR auch die bereits oben erwähnte Verwaltungsstelle T, zustän-

33 Wie zum Beispiel an der in Kapitel 3.1.1 genannten Person Igor Sechins deutlich wird, der neben seinem Amt als Aufsichtsratsvorsitzender des Rosneft-Konzerns auch als stellvertretender Leiter der russischen Präsidialverwaltung tätig ist.

34 Wie am Beispiel des Yukos-Konzerns zu sehen (Für eine ausführliche Darstellung vgl. Kononczuk 2006).

35 Die Zeit wird zeigen, ob die erweiterte staatliche Kontrolle vornehmlich *russischen* Interessen oder den *persönlichen* Interessen der machthabenden Eliten dient.

dig für das Sammeln wissenschaftlicher und technischer Informationen im Ausland. Ziel des SVR in Deutschland ist unter anderem das Sammeln von Hintergrundinformationen zu Produkten in den Bereichen Telekommunikation, Bio-, Informations-, Sicherheits- und Messtechnik (Bundesamt für Verfassungsschutz 2007: 303). Die häufigste *Vorgehensweise* bei der Sammlung ist die Gewinnung aus offenen Quellen wie etwa Vorträgen, Messen, Medienauswertungen und Abschöpfung im Gespräch. Die Beschaffung sensitiver Informationen erfolgt jedoch nach wie vor auch durch verdeckt handelnde Agenten mit offizieller oder nicht-offizieller Legende (Bundesamt für Verfassungsschutz 2007: 304f). Eine ausführlichere Diskussion verschiedener Methoden der Informationsbeschaffung erfolgt in Kapitel 5.

Vornehmlich an Produkten mit militärischen Verwendungsmöglichkeiten ist die GRU[36] des russischen Verteidigungsministeriums interessiert. Der Dienst unterhält einen Personalstab von geschätzten 12.000 Mitarbeitern und nutzt seine schwerpunktmäßige Zuständigkeit für die Beschaffung von militärpolitisch und wehrstrategisch relevanten Informationen auch zum Ausspähen von Rüstungstechnik und verwandter Bereiche (Bundesamt für Verfassungsschutz 2006: 10). Methodisch handelt er grob analog zur Vorgehensweise des SVR (Bundesamt für Verfassungsschutz 2007: 305).

Ebenfalls aktiv im deutschen Wirtschaftsraum ist der russische Inlandsgeheimdienst FSB, und zwar insofern, als ihm nach dem SORM II[37] - Gesetz von 1998 die routinemäßige Überwachung der russischen Internetkommunikation obliegt. Nach diesem Gesetz sind russische Internetprovider verpflichtet, dem FSB eine kostenlose Überwachungsschnittstelle mit Glasfaserverbindung einzurichten (Deppe 2000). Ein deutsches Unternehmen, welches eine Dependance in Russland einrichtet, sollte sich also im Lichte der oben erwähnten zunehmenden Verflechtung von Politik und Wirtschaft über das Risiko potentiell überwachter Telekommunikationskanäle im Klaren sein.

36 *Glavnoye Razvedyvatelnoye Upravlenie,* wörtlich „Hauptverwaltung Aufklärung".

37 *Sistema Operativno-Rozysknykh Meropriyatii,* wörtlich: „System für operativ-investigative Tätigkeiten".

Nach dieser Analyse von Struktur und Vorgehensweise stellt sich schließlich die Frage nach den *Motiven*. Es wird hier jedoch nur der Ausschnitt nationalstaatlicher Motive betrachtet, aktuelle persönliche Interessen machthabender Eliten seien außen vor.

Zur Frage der Motive treffen Lux und Peske (2002a: 65) die generelle Aussage, dass hochentwickelte Industriestaaten Wirtschaftsspionage betreiben um sich eine ökonomische und technologische Führerschaft aufzubauen oder um diese zu sichern. Ferner gehen sie davon aus, dass wirtschaftlich weniger entwickelte Staaten an einer kostengünstigen Schließung ihrer technologischen Lücke zu den Führungsstaaten interessiert sind. Im Falle Russlands sind aber branchenspezifisch hochgradig unterschiedliche wirtschaftliche Positionen innerhalb eines Staates vereint. Einer ökonomischen Führerschaft in der Energieversorgung Mittel- und Osteuropas steht zum Beispiel eine vergleichsweise unterentwickelte Mikroelektronikbranche gegenüber. Eine Einteilung in diese Kategorien gestaltet sich demnach schwierig. Es steht vielmehr zu vermuten, dass die im Bereich der Wirtschaftsspionage an die russischen Dienste gestellten Anforderungen vor allem mit den tagesaktuellen Bedürfnissen russischer Einflusspolitik zusammenhängen, und dass die tatsächliche Beschaffung branchenspezifische Schwerpunkte setzt: Bei der Penetration eines Halbleiterfabrikanten wird demnach eher Wert auf technische Details der Wertschöpfungskette gelegt, eine Quelle in einem Energieversorgungskonzern wird aller Voraussicht nach strategisch relevante Einzelheiten der Geschäftspolitik und -entwicklung zu beschaffen versuchen.

Auf Deutschland als Land mit hoher Forschungsintensität und bedeutender Wirtschaftskraft liegt jedenfalls das besondere Augenmerk russischer Dienste: Laut Bundesamt für Verfassungsschutz sind diese der Personalstärke nach deutlich überrepräsentiert, was den Stellenwert des deutschen Wirtschaftsraumes als Ziel nachrichtendienstlicher Aktivität weiterhin unterstreicht (Bundesamt für Verfassungsschutz 2007: 304f).

Die Nachrichtendienste des Fernen Ostens am Beispiel Chinas

Auch das Beispiel der kommunistisch-sozialistisch geprägten Volksrepublik China unterstützt die These, dass in Staaten, deren Gesellschaft durch eine hohe Verflechtung von Politik und Wirtschaft gekennzeichnet ist, die Wahrscheinlichkeit einer systematisch betriebenen Wirtschaftsspionage ungleich höher ist als in eher individualistisch geprägten Systemen. So zählen auch die chinesischen Geheimdienste zu den auf deutschem Boden aktivsten fremden Diensten. Motivation und Methodik sind bei ihnen jedoch – wie im Folgenden erläutert – grundsätzlich anders gelagert als bei ihren russischen Pendants.

Im Besonderen benannt werden vom Bundesamt für Verfassungsschutz sowohl das chinesische Ministerium für Staatssicherheit[38] (MSS) für den zivilen Teil der Aufklärung wie auch dessen Schwesterdienst, den militärischen Informationsdienst (MID) der Zweiten Hauptverwaltung des Generalstabshauptquartiers der Volksbefreiungsarmee[39] (Bundesamt für Verfassungsschutz 2006: 12). Beide sind sowohl mit Kompetenzen zur Inlandsüberwachung als auch zur Auslandsaufklärung versehen, eine *strukturelle* Betrachtung gestaltet sich jedoch schwierig, da die genauen Organisationspläne, Mitarbeiterzahlen und Budgets für beide Dienste scheinbar eine äußerst geringe Verbreitung erfahren haben. Als eine der wenigen Quellen hierzu ist ein von chinesischer Seite aus massiv kritisierter (o.V. 2007) Artikel aus dem Spiegel 35/2007 zu nennen, welcher den chinesischen Diensten ein Netz von 800.000 Spitzeln weltweit zurechnet. Wie für ein journalistisches Produkt nicht unüblich, wird dafür jedoch kein dezidierter Nachweis erbracht, sondern lediglich auf die „Einschätzungen der westlichen Konkurrenz" der chinesischen Dienste verwiesen (Dahlkamp et. al. 2007: 26).

Als *Motiv* für die Arbeit beider Dienste nennt der Verfassungsschutz das Schließen der im Vergleich zur westlichen Welt erheblichen technologischen Lücke des Großteils chinesischer Industriezweige (Bundesamt für Verfassungsschutz 2007: 317). Eigene Untersuchungen zeigen, dass diese Gefahr seitens der deutschen In-

38 Chinesisch: „*Guojia Anaquaanbu*", kurz „*Guanbu*".
39 Chinesisch: „*Zhong Chang Er Bu*".

dustrie maßgeblich unterschätzt wird. So gab zum Beispiel ein Hersteller von CNC-Fräsen zu verstehen, dass er es für höchst unwahrscheinlich halte, wegen seiner Produkte ausspioniert zu werden, da diese zum Teil bereits seit zehn Jahren auf dem Markt und außerdem frei erhältlich seien. Selbst wenn jemand Interesse am Nachbau seiner Maschinen hätte, so seine Auffassung, könne dieser seine Maschinen am ehesten auf regulärem Wege erwerben.[40] Dieses Statement kann stellvertretend für viele andere Aussagen dieser Art angeführt werden.

Unterschätzt wird dabei jedoch, dass diese und weitere Technologien, welche im westeuropäischen Raum weit verbreitet sind, nicht ohne weiteres mit den Möglichkeiten ostasiatischer Technologieträger einem erfolgreichen „Reverse Engineering"-Prozess[41] unterzogen werden können. Hier entsteht also durchaus ein Bedarf an durch nachrichtendienstliche Methoden gewonnenem Insiderwissen.

Auf die *Methodik* chinesischer Nachrichtendienste geht vor allem Rustmann ein (Rustmann 2002: 113-119). Rustman führt als Grundlage der Auslandsaufklärung eine routinemäßige Kontaktaufnahme des MSS zu aus China ausreisenden und nach China einreisenden Chinesen an. Bei diesem Kontakt werden die Reisenden aufgefordert, zum Wohle des chinesischen Volkes mit den Behörden zu kooperieren, d.h. für staatliche Stellen interessante Informationen an diese weiterzuleiten (ebd.: 117). Es werden dabei sowohl positive Anreize, etwa in Form von Geldgeschenken und Privilegien, als auch negative Anreize, etwa in Form politischen Drucks auf in China verbliebene Familienmitglieder oder generelle Ein- und Ausreisebeschränkungen bzw. -verbote eingesetzt (ebd.: 117).

Der ehemalige chinesische Diplomat und spätere Überläufer Chen Yonglin erklärte hierzu: „Jeder Student, jeder Geschäftsmann, der ins Ausland gelassen wird, steht in der Schuld der Partei. Er revanchiert sich als Spitzel, als Denunziant" (Bundesamt für Verfassungsschutz 2007: 321). Inwieweit die Aussage eines – zur Unterstützung seines in der Schwebe befindlichen Asylantrags – um mediale Auf-

40 Vertrauliches Gespräch am Rande der Euromold, Frankfurt am Main, 07.12.2007.

41 Reverse Engineering: Der Versuch durch Analyse von Aufbau und Funktionsweise industrieller Produkte eine Möglichkeit des originalgetreuen Nachbaus abzuleiten.

merksamkeit bemühten Gegners des chinesischen Regimes (Ya 2005) den Kriterien objektiver Belastbarkeit entspricht ist jedoch fraglich.

Ebenfalls fraglich ist, in wieweit das *Guanxi*, das traditionelle chinesische Netzwerk interpersoneller sozialer Beziehungen, eine Rolle bei der Beschaffung geheimgehaltener Informationen spielt. Zum einen beziehen sich die im Guanxi aufgebauten Beziehungen stets auf die Beziehungen zwischen zwei (Privat-)Personen, nicht etwa auf die Beziehung einer Person zum Staat. Zum anderen wird das Guanxi zwischen Privatpersonen und Parteioffiziellen als inhärent korrupt und ethisch fragwürdig angesehen (Fan 2002: 22). Betrachtungen speziell asiatischer Ansätze von Wirtschafts- und Industriespionage betonen jedoch, dass ein Guanxi ausnutzender Informationsaustausch, auch wenn er gegen die rechtlichen Normen des Landes auf dessen Boden er stattfindet verstößt, nicht als unethisch erachtet wird, sondern sogar akzeptierte Norm ist.

In seiner Rede vor einem Sicherheitskongress der Firma OSS Inc. führte der Journalist Doug Tsuruoka dazu folgendes Beispiel an: Ein chinesisch-stämmiger Ingenieur, welcher für ein sensibles US-Verteidigungsprojekt arbeitet, verfügt über eine Guanxi-Verpflichtung gegenüber einem alten Freund, der Offizier in einem Programm für strategische Waffen der Volksrepublik China geworden ist. Man kann nicht annehmen, dass bei einem Treffen dieser beiden Personen zwangsläufig Informationen ausgetauscht werden, aber durch die informelle Art des Guanxi wäre ein Nachweis eines solchen verbalen Austausches nur schwer möglich und gelte zudem im asiatischen Kontext als nicht verwerflich. Es sei somit davon auszugehen, dass in Fragen von Wirtschaftsgeheimnissen fremder Länder eine gewisse Menge an Information auf diese Weise beschafft wird (Tsuruoka 1997: 8f). Chinas Geheimdienste gelten daher auch als „very proficient in the art of seemingly innocuous elicitations of information" (Global Security o.J.).

Weitere Quellen bestätigen diese Vorgehensweise (Innenministerium des Landes Nordrhein-Westfalen o.J.). *Potentielle* Zuträger der staatlichen Dienste Chinas sind somit die ein- und ausreisenden Bürger dieses Landes, unter anderem auch

Touristen, Studenten, Praktikanten, Geschäftsleute und Austauschwissenschaftler (Global Security o.J.), ein Befund der leider geeignet ist, xenophoben gesellschaftlichen Tendenzen Vorschub zu leisten.

Nachrichtendienste westlicher Staaten

„Die Spionageabwehr geht nach derzeitiger Kenntnislage davon aus, dass von westlichen Staaten keine systematische Wirtschaftsspionage gegen die Bundesrepublik Deutschland durchgeführt wird", so die offizielle Aussage des Verfassungsschutzes (2006: 14) zur Bedrohung durch eine von befreundeten Staaten ausgehende Wirtschaftsspionageaktivität. Weiterhin heißt es, dass die deutsche Gesetzgebung Bedrohungen dieser Art nicht „nach der Himmelsrichtung", aus der diese erfolgen, unterscheide: Die Abwehrbehörden bewahrten sich in dieser Hinsicht einen „360°-Blick" (ebd. 2006: 13).

Diese Position verdient eine differenzierte Betrachtung: Sie schließt nämlich durch die Verwendung des Adjektivs „systematisch" eine nicht-systematische, das heißt *nicht* in Form eines auf Dauer angelegten Programms stattfindende Wirtschaftsspionage *nicht* aus. Über diese nicht-systematische Wirtschaftsspionage befreundeter Staaten werden dagegen keinerlei Aussagen getroffen, obwohl derartige Vorgänge in der Literatur immer wieder beschrieben werden.

Eines der prominentesten Beispiele ist wohl die Unterstützung des französischen Auslandsnachrichtendienstes DGSE[42] für den französischen TGV-Hersteller GEC- Alsthom im Jahre 1993 (Homann et. al. 2005: 4; Ulfkotte 1999: 66; o.V. 1996; Office of the National Counterintelligence Executive o.J.: 287). Im September 1993 erteilte die südkoreanische Regierung diesem Konsortium den Auftrag zum Bau einer neuen Generation von Hochgeschwindigkeitszügen, dem KTX (Korea Train Express). Daraufhin beschuldigte das von Siemens geführte ICE-Konsortium, welches sich im Spätsommer 1993 kurz vor Abschluss eben jenes Kontraktes wähnte, das DGSE, die Telefon- und Faxleitungen der Siemens-Niederlassung in Seoul ab-

42 *Direction Générale de la Sécurité Extérieure,* wörtlich: „Generaldirektion für Äußere Sicherheit".

gehört und vertrauliche Kostenkalkulationen an GEC-Alsthom weitergeleitet zu haben. Aufgrund dessen seien diese in der Lage gewesen, ihr Angebot entscheidend nachzubessern und so in letzter Sekunde den Zuschlag für den Bau von Streckennetz und zwölf Zügen zu erhalten. Eine offizielle Anklage wurde von Siemens nie eingereicht; Ulfkotte (1999: 66) berichtet von einer anschließenden vertraulichen Klärung der Affäre auf der Vorstandsebene der beiden Konzerne.

Auch auf derartige Aktivitäten amerikanischer Nachrichtendienste gibt es zahlreiche Hinweise: So verwies die Bundesrepublik Deutschlands 1997 einen im Bundesministerium für Wirtschaft platzierten CIA-Agenten des Landes, welcher mit der Sammlung von Informationen über High-Tech-Produkte betraut war (Office of the National Counterintelligence Executive o.J.: 283). Die amerikanische Seite rechtfertigt solche Bestrebungen gerne mit dem Argument, dass man sich lediglich unfairer Geschäftspraktiken europäischer Unternehmen erwehre (Woolsey 2000)[43].

Ein anderes Beispiel dafür, dass sich die USA in einer Opferrolle sehen, ist der Abschlussbericht einer Intelligence-Reformkommission der „Woodrow Wilson School of Public and International Affairs“ an der Princeton-University (Gregory 1997). In dem Abschnitt *A Role for Economic Espionage* spricht sich der Bericht explizit für das Betreiben von Wirtschaftsspionage aus: „The United States' economic intelligence effort should continue to keep up the good work and identify unfair "playing surfaces" abroad“. Im Abschnitt *Why we are targets* wird als Grund hierfür wieder – analog zum Artikel von Woolsey – eine wahrgenommene Überlegenheit amerikanischer Technologie angeführt: „Everybody wants it and tries to get it one way or another. Most nations – friend or foe – have either used American technology as a springboard to economic development (France, Japan, etc.), or become 'hooked' on it for their very survival (the former USSR).” Der Abschnitt schließt: “So, the picture should be clear. The United States is a victim of industrial espionage, with a considerable cost to United States business.”

43 Jener lesenswerte Artikel des Ex-CIA-Direktors Woolsey mag auch als Maßstab für die Seriosität derartiger Darstellungen dienen, wenn man die darin enthaltenen Behauptungen darüber in Betracht zieht, dass europäische Technologie im Vergleich zum amerikanischen Standard viel zu rückständig sei, als dass sich Spionage dafür lohnen würde.

Trotz der vielfältigen Betonung, dass amerikanische Wirtschaftsspionage nur eine Verteidigung gegen illegale Aktivitäten fremder Mächte darstelle (Vgl. den Airbus-Fall: Office of the National Counterintelligence Executive o.J.:. 283) und nur dem Zwecke gleicher Chancen aller Marktteilnehmer zu Gute komme („The point is fair competition, not advantage for an American firm." (Gregory 1997)) ist nicht auszuschließen, dass solche Versuche in der Praxis über jene eventuell nur vorgeschobenen Zwecke hinausgehen, und sich in ihr Gegenteil, in eine wettbewerbsverzerrende Unterstützung amerikanischer Firmen verkehren. Vorfälle dieser Art werden jedoch in der oben zitierten Broschüre des Bundesamtes für Verfassungsschutz – mit Ausnahme einer kurzen Besprechung des ECHELON-Systems[44] – nicht angesprochen (Bundesamt für Verfassungsschutz 2006).

Der Eindruck, dass von Seiten der zuständigen deutschen Behörden kein Interesse daran besteht, öffentlich gegen Wirtschafts- und Industriespionage westlicher Staaten vorzugehen, verstärkt sich im Lichte der Geschehnisse um den WDR-Journalisten Jörg Heimbrecht und das Bundesamt für Verfassungsschutz. Ersterer gelangte 1998 an Informationen über Aktivitäten der amerikanischen NSA[45] in der deutschen Wirtschaft. Durch einen Mitarbeiter des Verfassungsschutzes wurden ihm daraufhin 14.000 DM für die Preisgabe seiner Quellen geboten. Auf Nachfrage teilt jener Mitarbeiter ihm mit, dass diese Aktion nur dem „Abschalten" von Heimbrechts Quelle diene. Ein Interesse daran, die betroffenen Unternehmen über bezahlte Spitzel in ihren eigenen Reihen zu informieren bestehe nicht. Zudem gäbe eine Weisung von Bundeskanzler Kohl persönlich, Informationen dieser Art im Interesse der deutsch-amerikanischen Freundschaft *nicht* an die Wirtschaft weiterzuleiten (Heimbrecht/Schultze 1998).

Als Gründe für dieses Stillhalten führt Heimbrecht weiterhin eine Aussage des Geheimdienstexperten Erich Schmidt-Eenboom darüber an, dass die Bundesrepublik in Form ihrer Nachrichtendienste „viel zu abhängig von den Kapazitäten,

44 Eine ausführliche Darstellung der Kapazitäten des Systems findet sich im Abschlussbericht eines Untersuchungsausschusses des Europäischen Parlaments (2001).

45 *National Security Agency*, wörtlich: „Nationale Sicherheitsbehörde".

von der Hilfestellung der amerikanischen Dienste, insbesondere im Bereich der Satellitenaufklärung, aber auch bei der Agentenaufklärung in manchen Zielregionen dieser Erde [ist], als dass man das gute Verhältnis zu den Amerikanern dadurch trüben könnte, dass man die deutsche Wirtschaft warnt." (Heimbrecht/Schultze 1998).

In Summe der aufgezeigten Zusammenhänge scheint es, als würde die Arbeit der Bediensteten des Verfassungsschutzes aus politischen Gründen systematisch eingeschränkt: Einer jener Bediensteten gab zu verstehen, dass Ermittlungen über Wirtschaftsspionage westlicher Mächte von staatlicher Seite aus unerwünscht sind (Ulfkotte 1999: 20). Diesbezügliche Nachfragen Ulfkottes beim Bundesamt für Verfassungsschutz blieben unbeantwortet (ebd.: 21).

Erkenntnisse über den Umgang mit Spionagefällen durch die hiervon betroffenen Unternehmen finden sich in Kapitel 4.2.1.

4.1.2 Privatwirtschaftliche Institutionen als offensive Akteure

Internationale Unternehmen, die in einer zunehmend komplexen Umwelt agieren, stehen einem stetig steigenden Informationsbedarf gegenüber. Zur Deckung des nicht-legalen Teils dieses Bedarfs greifen Unternehmen gegebenenfalls auf die drei Gruppen der privaten offensiven Akteure in Wirtschafts- und Industriespionage zurück: Innentäter, Intelligence Trader und Nischenexperten[46] (Lux/Peske 2002a: 49). Diese drei Kategorien werden nachfolgend anhand der Strong (1994: 170) entnommenen, erklärenden Variablen *Motivation*, *Bereitschaft*, *Methodenkenntnis* und *Gelegenheit*[47] klassifiziert.

Angeworbene und nicht angeworbene Innentäter

„[Eigene] Mitarbeiter stellen aufgrund ihrer internen Kenntnisse für den Know-How-Schutz ein noch größeres Sicherheitsrisiko dar als Eindringversuche

46 Der Fall so genannter „Inhouse-Agenten"– Unternehmensmitarbeiter mit nachrichtendienstlicher Ausbildung – sei hiermit aufgrund der Seltenheit dieser Fälle ausgeschlossen (Lux/Peske,2002a: 49).

47 Im Original: Motivation, Willingness, Expertise, Opportunity.

von außen“ befindet ein Bericht der Arbeitsgemeinschaft für Sicherheit der Wirtschaft (2005: 53). Sowohl die bereits mehrfach zitierte Corporate Trust-Studie (Corporate Trust 2007: 18) als auch eigene Erhebungen (vgl. die in Anhang 2 aufgeführten Fälle) bestätigen diese Ansicht. Doch worin liegen nun die Gründe für diesen Zusammenhang?

Zunächst einmal stellt sich die Frage nach der *Motivation* der Täter. Gleich ob diese von außen angeworben werden oder als Selbstanbieter auftreten, kommen hierbei vor allem die klassischen Motive des Geheimnisverrats in Betracht. Am häufigsten zu nennen wären dabei: Geldgier, Abenteuerlust, Unzufriedenheit am Arbeitsplatz (bzw. Rache an ehemaligen oder aktuellen Arbeitgebern) und ein übersteigertes Geltungsbedürfnis (Bundesamt für Verfassungsschutz 2006: 17), oder etwas kürzer gefasst: „Money, revenge, and ego“ (Rustmann 2002: 39). Ideologische Gründe, das heißt die explizite Unterstützung anderer politischer Systeme (z.B. Chinas) sind im speziellen Feld der Wirtschafts- und Industriespionage als eher nachrangig zu betrachten (Bundesamt für Verfassungsschutz 2006: 17).

Die Frage, woher die *Bereitschaft* gewisser Personen stammt, sich mit dem Verrat von Unternehmensgeheimnissen strafbar zu machen, hängt oft eng mit deren Motivation zusammen. Ein primär finanziell motivierter Produktdesigner mag von der Tatsache angetrieben werden, dass er im Gegensatz zu seinen vorgesetzten Managern einen (subjektiv betrachtet) wesentlich elementareren Beitrag zum Erfolg eines gewissen Produktes leistet, im Verhältnis dazu aber ein wesentlich geringeres Gehalt bezieht und sich kühl berechnend zu seinen Taten entschließen. Ein unzufriedener Vertriebsagent, der von einem direkten Vorgesetzten mit persönlicher Kritik seiner Ergebnisse oder Arbeitsweise vor den Kollegen bloßgestellt wurde, könnte dagegen derart gekränkt solche Pläne ad hoc fassen und sein nächstes Mittagessen schon mit einem Mitarbeiter der Konkurrenz verbringen.

Generell sei zur Frage der Bereitschaft wieder auf die Rational Choice Theory von Cornish und Clarke (1986) verwiesen, nach der einem Verbrechen eine un-

mittelbare Abwägung von Nutzen und Risiko der Tat vorausgeht und Verbrechen dann geschieht, wenn der zu erwartende Nutzen das Risiko entsprechend aufwiegt.

Die Besonderheit des Innentäters liegt in seinem typischerweise auftretenden Missverhältnis zwischen geringer *Methodenkenntnis* und häufiger *Gelegenheit*.

Es scheint bei einem kaufmännischen oder technischen Angestellten eines mitteleuropäischen Unternehmens einleuchtend, keine über die Inhalte von Agentenromanen oder -filmen hinausgehende Kenntnis nachrichtendienstlicher Methoden zu erwarten. Dementsprechend gehen solche Mitarbeiter bei dem Versuch, ihnen nicht zugängliche Daten zu entwenden und weiterzugeben, ein verhältnismäßig hohes Risiko ein. Im Verdachtsfall ist es daher meist nur mit geringem Aufwand verbunden, die Aktivitäten eines solchen nachrichtendienstlich ungeschulten Mitarbeiters zu überprüfen und diesen gegebenenfalls zu überführen.

Im Gegensatz dazu bieten sich für einen Innentäter im Allgemeinen mehr Chancen, an sensible Daten zu gelangen, als für Mitglieder der beiden anderen Gruppen. Er erhält routinemäßig Zugriff auf vertrauliche Dokumente seines Geschäftsbereichs, kann weitere Informationen aus Gesprächen mit seinen Kollegen beziehen, muss seine Präsenz in den Geschäftsräumen der Unternehmung im Gegensatz zu Unternehmensfremden nicht rechtfertigen und unterliegt auch nicht den eventuell auf letztere Gruppe zutreffenden Beschränkungen, wie zum Beispiel dem Verbot Fotohandys oder Datenträger mit sich zu führen.

Eine zusätzliche Gefahr ergibt sich aus der prinzipiellen Vertrautheit des Mitarbeiters mit den internen Vorgängen des Unternehmens. Er weiß im Allgemeinen, welcher Kollege mit der Bearbeitung welcher Vorgänge betraut ist, wo gewisse Daten in den Archivsystemen des Unternehmens abgelegt werden und ob und wie diese gesichert werden.

Bestimmte Gruppen von Angestellten verlangen eine gesonderte Betrachtung. Dies sind diejenigen, die aufgrund ihrer beruflichen Fachkenntnisse die Möglichkeit besitzen, Daten einzusehen, zu manipulieren oder zu entwenden, die anderen Angestellten verborgen bleiben. Im Besonderen trifft dies auf die Gruppe der

Archivare oder in neuerer Zeit auf die Mitarbeiter der unternehmensinternen IT-Abteilungen zu, speziell auf die dort ansässigen Systemadministratoren. Als potentielle Innentäter verfügen diese über ein hohes Maß an *Gelegenheit*. Ihre außergewöhnliche Fachkenntnis erlaubt ihnen jedoch einen wesentlich umfassenderen Zugriff auf die Datenablage des Unternehmens, als dies anderen Mitarbeitern gleichermaßen unverdächtig möglich wäre. Es empfiehlt sich daher, gerade bei der Auswahl und Überwachung dieser Mitarbeiter besondere Sorgfalt walten zu lassen.

Ein Beispiel für einen *angeworbenen* Innentäter stellt die Person von José Ignacio Lopez dar. In seiner Position als Vizeeinkaufschef von General Motors wurde er vom Chef des VW-Konzerns Ferdinand Piëch im Verlauf mehrerer persönlicher Zusammenkünfte angeworben, um mit einem Stab von sechs engen Mitarbeiter zum VW-Konzern zu wechseln (Rustmann 2002: 40f.). Lopez gelang es, seine Mitarbeiter ebenfalls von Piëchs Angebot zu überzeugen und machte sich, von diesem beauftragt, daran, vor seinem Ausscheiden aus dem Unternehmen möglichst viele für seinen neuen Arbeitgeber verwendbare Informationen zusammenzutragen. Entsprechend seiner ranghohen Position erlangte er dabei Zugriff auf hochvertrauliche Dokumente wie etwa die Kostenkalkulationen für diverse General-Motors-Fahrzeugmodelle, Projektstudien zu Einkaufs- und Einsparstrategien, Entwürfe eines neuen Kleinwagens und Pläne einer neuartigen Fabrikanlage (Office of the National Counterintelligence Executive o.J.: 286). Insgesamt umfasste das entwendete Material zwanzig Kartons, welche Lopez und seine Helfer über die Adresse von Lopez Schwager in Spanien an VW weiterleiteten (Rustmann 2002: 40).

Aufgedeckt wurde die Affäre unter anderem durch den Mitschnitt persönlicher Videokonferenzen zwischen Lopez und Piëch durch die amerikanische NSA, die diese Informationen der Darmstädter Staatsanwaltschaft zuspielte (Ellwart 2000). Der deutschen Polizei gelang es daraufhin vier Boxen mit General-Motors-Dokumenten und einen Brief, der sich auf die vorangegangene Vernichtung der restlichen Dokumente bezog, sicherzustellen. In einem aufwändigen juristischen Nachspiel wurde der VW-Konzern zu einer Zahlung von 100 Millionen US-Dollar

und einem auf sieben Jahre gestreckten Bezug von General-Motors-Fahrzeugteilen im Wert von einer Milliarde US-Dollar verurteilt.

Das Beispiel verdeutlicht die für Innentäter typische Diskrepanz zwischen Gelegenheit und Methodenkenntnis. Erstere war bei José Ignacio Lopez, wie man an der Aufstellung der entwendeten Daten sehen kann, sehr stark ausgeprägt, an letzterer bestand ein entscheidender Mangel: Hätte die Kommunikation zwischen Piëch und Lopez über anonyme, verschlüsselte E-Mails stattgefunden, hätten Lopez und seine Mitarbeiter General Motors nicht gleichzeitig innerhalb einer denkbar kurzen Zeitspanne in Richtung VW verlassen, sondern Intermezzi bei anderen Firmen eingelegt, hätte man die Dokumente anstatt sie zu entwenden mit etwas mehr zeitlichem Anlauf fotokopiert, wäre die strafrechtliche Aufarbeitung der Geschehnisse erschwert, wenn nicht vereitelt worden.

Intelligence Trader

Zur Gruppe der Intelligence Trader gehören häufig Gruppierungen, die unter Bezeichnungen wie Informationshändler, (Wirtschafts-)Detekteien, „Private Intelligence Services“, Sicherheitsberatungs- oder Risikomanagement-Gesellschaften firmieren. Sie bieten zwar in der Regel Dienstleistungen an, die aus ihrer eigentlichen Unternehmensbezeichnung zu ersehen sind, fungieren aber bisweilen auch als Beschaffer oder Vermittler von Informationen, die mit Hilfe illegaler und klandestiner Mittel erlangt wurden (Lux/Peske 2002a: 49).

Im Gegensatz zu den Innentätern mit ihrem weit gefassten Motivationsspektrum liegt die *Eigenmotivation* der Intelligence Trader jedoch in der Regel einzig in der Gewinnerzielungsabsicht, die ihrer Organisationsform als privaten Dienstleistungs-unternehmen typischerweise innewohnt. Aus diesem Grund unterhalten sie die weitläufigen Informations- und Informantennetze, die für ihre Arbeit unabdingbar sind. Die auslösende *Fremdmotivation* hinter ihren Handlungen liegt dagegen wieder im Motivationsspektrum der sie beauftragenden Akteure begründet. Dabei kann es sich ebenfalls wieder um die Gewinnerzielungsabsicht eines Un-

ternehmens, die sozialen Ziele einer NGO, Einflussziele eines Verbandes oder auch um die politischen Ziele einer staatlichen Gruppe handeln.

Die *Bereitschaft* aus Gewinnstreben heraus gegen strafrechtliche Bestimmungen zu verstoßen ist es, was den Intelligence Trader im Sinne dieser Arbeit von den eigentlichen Sicherheitsberatern, Risikomanagern und ähnlichen unterscheidet. Durch den nicht-legalen Teil ihrer Arbeit verschaffen sich die Trader einen Wettbewerbsvorteil gegenüber ihren mit ausschließlich legalen Mitteln operierenden Pendants. In der Konkurrenz um die in diesem Berufsfeld gezahlten, zum Teil „enormen Summen" (Lux/Peske 2002a: 49), kann dieser Vorteil durchaus ausschlaggebend sein.

Im Falle der Entdeckung und Verfolgung solcher Praktiken verkehrt sich ein solcher Wettbewerbsvorteil natürlich leicht in sein Gegenteil. Dies ist etwa dann der Fall, wenn Unternehmen, die ihre Beratungskosten häufig vor internen Aufsichtsgremien verantworten müssen, nicht mehr bereit sind, mit diesen Mitteln operierende Berater unter Vertrag zu nehmen. Andere könnten sich dagegen durch ein implizites Angebot dieser Möglichkeiten angezogen fühlen. Nichtsdestotrotz erfüllen die Intelligence Trader für den auftraggebenden Akteur eine wichtige Funktion: Da diese den illegalen Teil ihrer Arbeit weder bewerben noch vertraglich vereinbaren können, verschaffen sie dem Auftraggeber einen Zugang zu geheimgehaltenen Informationen, ohne ihn dem Risiko einer Strafverfolgung auszusetzen.

Bezüglich ihrer *Methodenkenntnis* und *Gelegenheit* verfügen die Intelligence Trader (wie auch die Nischenexperten) über ein höchst variables Profil.

Im Allgemeinen verfügen sie nicht über die ungehinderten Zugriffsmöglichkeiten eines Innentäters (siehe dazu Kapitel 4.1.1). Eventuell gelingt es ihnen jedoch mittels positiver Anreize (zum Beispiel Bestechung mittels Geld, Privilegien oder sexuellen Gefälligkeiten) oder negativer Anreize (zum Beispiel Bedrohung oder Erpressung) einen solchen Innentäter anzuwerben oder eine ihnen gegenüber loyale Person als „Maulwurf" in das Ziel ihrer Wahl einzuschleusen. Zumindest letztere

Vorgehensweise dürfte aufgrund ihrer Komplexität und des zeitlichen Aufwandes über die Möglichkeiten vieler Trader hinausgehen.

Ebenso variabel stellt sich der Faktor Methodenkenntnis dar, da dieser stark von dem Humankapital abhängt, das dem Trader zur Verfügung steht. Dieses ist bei einigen privaten Nachrichtendiensten in hohem Maße vorhanden, da diese zum Teil ehemalige Nachrichtendienstoffiziere unter ihren Mitarbeitern haben. Ein Beispiel dafür ist die amerikanische „Private Intelligence Agency" (Selbstbezeichnung) CTC-International Group. Gegründet wurde sie im Jahre 1992 von dem oben bereits zitierten Frederick W. Rustmann Jr., welcher sich nach 24-jähriger Tätigkeit für die CIA mit diesem Unternehmen selbständig machte. Die Principal Associates weisen weiterhin die gesammelte Erfahrung von insgesamt mehr als 100 Jahren in verschiedenen Laufbahnen innerhalb der CIA auf, so dass dem Unternehmen ein weites Reservoir nachrichtendienstlicher Methodenkenntnis zur Verfügung stehen dürfte[48] (CTC International Group o.J.a).

Der Kreis der Privatiers unter den ehemaligen Nachrichtendienstoffizieren umfasst weiterhin so prominente Mitglieder wie James Woolsey (CIA-Direktor von 1993 bis 1995), William H. Webster (FBI-Direktor von 1978 bis 1987, CIA-Direktor von 1987 bis 1991) und Shabtai Shavit (Mossad[49]-Direktor von 1989 bis 1996) (Harbich 2006: 70), was die Methodenkenntnis mancher Intelligence Trader anschaulich illustrieren dürfte. Es ist zu vermuten, dass es sich dabei nicht um Einzelfälle handelt (siehe dazu auch Kapitel 3.1.1).

Nischenexperten

Experten für bestimmte Fachbereiche gehören ebenfalls zu den potentiell offensiv auftretenden Akteuren der Wirtschafts- und Industriespionage, sind aber

48 Die CTC International Group dient in diesem Zusammenhang nur als Veranschaulichung der *Möglichkeiten* hochkarätiger Private Intelligence Services. Die Anwendung illegaler Informationsbeschaffungsmethoden soll hier nicht unterstellt werden. Gleichwohl sei darauf hingewiesen, dass das Unternehmen auf seiner Profilseite die zur Verfügung stehenden „clandestine collection methods" explizit bewirbt (CTC International Group o.J.b).

49 Kurzform von *Hamossad Lemodi'in Uletafkidim Meyuchadim*, israelisch für Institut für Aufklärung und besondere Aufgaben.

nicht dem originär nachrichtendienstlichen Bereich zuzuordnen. Dieser Personenkreis umfasst unter anderem Experten für den Bau von Alarmanlagen, die Sicherheit von IT-Systemen oder den Betrieb von Abhöranlagen.

Gleich ob sie von Dritten angeworben wurden oder eigenverantwortlich agieren ist zu vermuten, dass die *Motivation* von Nischenexperten in der Regel finanzieller Art ist. Als Privatpersonen sind sie analog zu den Innentätern jedoch ebenfalls für die klassischen Motive des Geheimnisverrats anfällig.

Ein relativ schwieriger Punkt bei der Behandlung dieser Gruppe ist die Frage der *Bereitschaft* zur Ausführung ungesetzlicher Handlungen zum Schaden Dritter. Während ein Angestellter eines Unternehmens noch aus Gründen schlechter Behandlung oder mangelnder Berücksichtigung bei Beförderungen bereit sein könnte seinem Unternehmen zu schaden, und ein Unternehmen bereit sein könnte sein Überlebenschance am Markt durch den Einsatz illegaler Methoden zu verbessern, so ist fraglich, warum ein Nischenexperte bereit sein könnte, Dritten zu schaden. Zu vermuten wäre ein übersteigertes Vertrauen in die eigene Fähigkeit illegale Handlungen vertuschen zu können, extreme Geldgier, eine laxe Einstellung in Bezug auf die Verantwortung für das eigene Handeln, von außen einwirkende negative Anreize (wie etwa Erpressung oder Bedrohung) oder eine beliebige Kombination der genannten Faktoren. Generell ist jedoch zu vermuten, dass es Vertretern dieser Gruppe ferner liegt als anderen, illegale Handlungen zu begehen.

Bei der Frage der *Gelegenheit* unterscheidet sich diese Gruppe als eine Gruppe von Tätern ohne originären Innenzugriff kaum von der Gruppe der Intelligence Trader. Auch ihnen ist es jedoch potentiell möglich, sich diesen durch den Einsatz ihrer spezifischen Fähigkeiten zu verschaffen. Ein Beispiel wäre hier ein versierter Fälscher, der sich mittels eines gefälschten Werksausweises Zutritt zu einem bestimmten Betriebsgelände verschafft. Es ist jedoch wahrscheinlich, dass dieser, außer wenn er eigenverantwortlich handelt, nicht an der eigentlichen Operation teilnimmt, sondern nur „im zweiten Glied“ aktiv sein wird.

Entscheidend für die Tätigkeit der Nischenexperten ist jedoch ihre besondere *Methodenkenntnis* in ihrem jeweiligen Feld, welche sie sich bei der illegalen und klandestinen Informationsbeschaffung zu Nutze machen können. Seien es ihre besonderen Fähigkeiten im Bereich der Penetration von IT-Sicherheitssystemen, ihre Fähigkeit bei der Umgehung von Alarmanlagen oder ihr besonderes Geschick beim Fälschen offizieller Dokumente: Nischenexperten können den zum Gelingen einer Beschaffungsoperation entscheidenden Unterschied ausmachen.

Ein Beispiel für einen versierten Nischenexperten ist Kevin Mitnick. Obwohl er es 1999 als „Most notorious hacker" sogar auf einen Eintrag im Guinness Buch der Rekorde brachte (Whittacker 2003: 235), sieht sich Mitnick – nach Verbüßen einer mehrjährigen Haftstrafe inzwischen Eigentümer eines kalifornischen Sicherheitsberatungsunternehmens – laut eigener Aussage als einen Experten für das Fachgebiet des „Social Engineering", das sein Unternehmen wie folgt definiert:

> „Social engineering is a method where the intruder deceives his target into complying with a request based on false pretenses and psychological manipulation." (Mitnick Security Consulting 2003: 1).

Social Engineering basiert auf der von ihm vertretenen These, dass der Mensch der größte Schwachpunkt der IT-Sicherheit ist (ebd.). Hierzu führt er in seinem Buch „The Art of Deception" (Mitnick/Simon 2002) eine Vielzahl standardisierter Vorgehensweisen[50] auf, mit denen es Außenstehenden gelungen ist, an sensible Firmendaten zu gelangen. Der dabei betriebene technische Aufwand geht dabei kaum über einige Telefonanrufe hinaus. Ein Experte für derartige Methoden stellt daher eine wertvolle Ressource für jeden Versuch von Wirtschafts- und Industriespionage dar.

4.2 Defensive Akteure

Als defensiv gelten im Rahmen dieser Arbeit sowohl private Akteure, welche die Wirtschafts- und Industriespionage im deutschen Wirtschaftsraum zur Wahrung

50 Einige der Methoden des Social Enginering werden in Kapitel 5.1 erläutert.

ihrer eigenen Interessen zu erschweren oder unterbinden suchen, als auch Akteure, die dieser Aufgabe in hoheitlichem Auftrag nachgehen. Ein Autor, der ein Buch über betriebliche Spionageabwehr verfasst und ein Unternehmen, das ein die Spionagegefahr einbeziehendes System von Sicherheitsmaßnahmen errichtet, gelten daher ebenso als defensiv, wie eine staatliche Institution, die damit ihrer verfassungsgemäßen Bestimmung nachkommt. Entscheidend ist dabei das Interesse des Akteurs die Betreiber von Wirtschafts- und Industriespionage am definitionsgemäßen Erlangen eines wirtschaftlichen Vorteils zu hindern.

Die nachfolgenden Abschnitte sollen Aufschluss über alle für die Abwehr von Wirtschafts- und Industriespionage relevanten Akteure geben. Dabei werden staatliche und private Akteure unterschieden.

4.2.1 Staatliche Institutionen als defensive Akteure

Hervorzuheben unter den staatlichen Institutionen zum Schutz des deutschen Wirtschaftsraums vor Wirtschafts- und Industriespionage sind vor allen Dingen die inländischen Geheimschutz- und Polizeibehörden. Namentlich sind dies das Kölner *Bundesamt für Verfassungsschutz* und die Verfassungsschutzämter der Länder, das Wiesbadener *Bundeskriminalamt* und die Landeskriminalämter, sowie das Bonner *Bundesamt für Sicherheit in der Informationstechnik*.

Eine eher untergeordnete Rolle spielen in diesem Zusammenhang der Bundesnachrichtendienst (BND) und der Militärische Abschirmdienst (MAD) der Bundeswehr. Letzterer ist nach §1 des Gesetz über den militärischen Abschirmdienst nur insofern für den Geheimschutz zuständig, wie der Geschäftsbereich des Bundesministeriums für Verteidigung betroffen ist, und kann seine Tätigkeit nach §2 dieses Gesetzes nur in besonderen Fällen und unter Einbezug der Verfassungsschutzbehörden über diesen Bereich hinaus ausdehnen. Die Tätigkeit des BND hingegen ist nach §1 des Gesetzes über den Bundesnachrichtendienst auf das Ausland beschränkt, Spionageabwehr wird lediglich innerhalb des BND selbst betrieben.

Verfassungsschutzbehörden

Die Verfassungsschutzbehörden in Bund und Ländern bezeichnen sich selbst auch als das „Frühwarnsystem der Demokratie“ (Bundesamt für Verfassungsschutz 2008: 8). Ihr Auftrag besteht im Schutz der freiheitlich-demokratischen Grundordnung der Bundesrepublik Deutschland, in der Wahrung des Bestandes des Bundes und der Länder sowie in der Spionagebekämpfung im Bundesgebiet (ebd.: 9). Zu diesem Zweck beobachten sie extremistische und potentiell extremistische Umtriebe sowie fremde Nachrichtendienste auf deutschem Boden. Sie verfügen aber auf Wunsch der Alliierten nach dem Kriege über keinerlei polizeiliche Befugnisse wie etwa die zum Verhör, zur Festnahme, zur Hausdurchsuchung, über das Anhalterecht oder zur Personenüberprüfung (Lux/Peske 2002a: 57).

Das im Kölner Stadtteil Chorweiler beheimatete Bundesamt für den Verfassungsschutz (BfV) ist mit der Koordination und Auswertung der Arbeit der 16 Landesämter für den Verfassungsschutz betraut. Diese Behörden sind dem BfV allerdings nicht unterstellt.[51] Darüber hinaus ist das BfV auch selbst zur Auswertung und Sammlung von Informationen nach §3 des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz befugt und untersteht in diesem Zusammenhang den Weisungen den Bundesministerium des Innern. Zur Erfüllung seiner Aufgaben stehen dem BfV rund 2.500 Mitarbeiter und ein Budget (offiziell „Zuschuss aus dem Bundeshaushalt“) von 137 Mio. € zur Verfügung (Bundesamt für Verfassungsschutz 2007: 17).

Im Bereich der Abwehr von Wirtschafts- und Industriespionage wird das BfV in zweierlei Hinsicht tätig: Zum einen in der *aktiven Bekämpfung* von Wirtschaftsspionage, zum anderen in der *präventiven Bekämpfung* in Form von Aufklärung und Beratung von Wirtschaftsunternehmen und staatlichen Institutionen.

Ein Problem bei der *aktiven Bekämpfung* von Spionagestraftaten im wirtschaftlichen Umfeld besteht in der Aufteilung der Zuständigkeitsbereiche: Zu Be-

51 Die Verfassungsschutzbehörden der Länder sind im Allgemeinen den jeweiligen Innenressorts auf Länderebene gegenüber weisungsgebunden.

ginn etwaiger Ermittlungen lässt sich nur sehr schwer sagen, ob es sich beim vorliegenden Fall um einen Fall von Wirtschaftsspionage handelt, bei dem der Verfassungsschutz aufgrund seines hoheitlichen Auftrags der Spionagebekämpfung befugt ist ermittlerisch tätig zu werden, oder ob es sich um einen Fall von Industriespionage handelt, bei dem die ermittlerische Zuständigkeit in den Händen der Kriminalbehörden liegen würde. Dies führt zu häufigen Kompetenzstreitigkeiten zwischen Verfassungsschutz und den Polizeibehörden, welche meist damit enden, dass der Verfassungsschutz so lange ermittelt bis zweifelsfrei feststeht, dass es sich um von Privatpersonen an Privatpersonen begangene Verbrechen handelt (Lux/Peske 2002a:. 50).

Bei der *präventiven Bekämpfung* von Wirtschaftsspionage steht das BfV zunehmend unter Zugzwang. Dessen Aussagen zu Folge hält sich das Interesse der Industrie an diesem Themenkomplex jedoch in engen Grenzen. So antworteten auf eine diesbezügliche Untersuchung einer Industrie- und Handelskammer nur 16% von 2.000 befragten Unternehmen (Bundesamt für Verfassungsschutz 2006: 22), die Antwortquote der bereits oben zitierten Untersuchung des Handelsblattes in Zusammenarbeit mit der Hamburger Sicherheitsberatungsfirma Corporate Trust lag sogar nur bei 9,9% (Corporate Trust 2007: 11).[52] Von den befragten Unternehmen sind 10% (Bundesamt für Verfassungsschutz 2006: 22) respektive 18,9% (Corporate Trust 2007: 13) bereits einmal Opfer von Spionage geworden. Hiervon haben jedoch nur zwischen 0% (Bundesamt für Verfassungsschutz 2006: 22), und 26,1% (Corporate Trust 2007: 29) die Behörden eingeschaltet, ein Befund der weitere Fragen aufwirft, wie etwa ob dies am mangelnden Vertrauen der Unternehmen in die Fähigkeiten der deutschen Behörden liegt.

52 Eigene Interviewreihen zeigen, dass sich die Antwortquote durch persönliche Befragung der Verantwortlichen im Rahmen von Messen und Kongressen auf nahezu 100% steigern lässt. Verzerrungen aufgrund mangelnden thematischen Interesses der Unternehmen wird somit effektiv begegnet. Der Anteil der betroffenen Unternehmen lag dabei bei 32%, von diesen suchten 37,5% den Kontakt zu den Behörden. Ein Nachteil dieser Methodik liegt jedoch im ungleich höheren finanziellen und zeitlichen Aufwand.

Auf der Ebene von Geschäftsführung und Sicherheitsverantwortlichen deutscher Unternehmen herrscht zudem die Auffassung, dass das öffentliche Eingeständnis solcher Vorgänge im eigenen Unternehmen zu einem Gesichtsverlust der Verantwortlichen und Reputationsschäden für das Unternehmen führen kann (Bundesamt für Verfassungsschutz 2006: 22; Corporate Trust 2007: 29).

Um diesem Problem entgegenzuwirken betont das BfV ausdrücklich, dass alle eingehenden Anfragen absolut vertraulich behandelt werden, und dass eine Anzeigepflicht gegenüber Kriminalpolizei und Staatsanwaltschaften nicht besteht (Bundesamt für Verfassungsschutz 2006: 22). Weiterhin wurden in Zusammenarbeit mit den Wirtschafts- und Innenministerien der Länder sowie den Verbänden für Unternehmenssicherheit und den Industrie- und Handelskammern so genannte Sicherheitspartnerschaften ins Leben gerufen. Ihre Aufgabe besteht darin, die Wirtschaft zeitnah über aktuelle Entwicklungen und dazugehörige Gegenstrategien im Bereich der Wirtschafts- und Industriespionage zu informieren (Innenministerium des Landes Nordrhein-Westfalen 2001).

Kriminalbehörden des Bundes und der Länder

Das Verhältnis der Kriminalbehörden auf Bundes- und Landesebene ist analog zum Aufbau der Verfassungsschutzbehörden. Das Bundeskriminalamt (BKA) ist den einzelnen Landeskriminalämtern gegenüber nicht weisungsbefugt, dient aber als Zentralstelle des polizeilichen Auskunfts- und Nachrichtenwesens nach Artikel 87 I des Grundgesetzes. Die Landeskriminalämter sind – analog zu den Landesämtern für Verfassungsschutz – ebenfalls den Innenressorts der einzelnen Länder unterstellt. Sie sind die verantwortlichen Ermittlungsbehörden für alle Fälle des in Kapitel 3.4.1 dargelegten Deliktfeldes des Gesetzes gegen den unlauteren Wettbewerb.

Die Aktivitäten der Kriminalbehörden gegen die Betreiber von Industriespionage lassen sich anhand der polizeilichen Kriminalstatistik (PKS) und des jährlich erscheinenden Lagebildes zur Wirtschaftskriminalität verfolgen. In der polizeilichen

Kriminalstatistik wurden für das Jahr 2006 unter dem Straftatenschlüssel 7153 insgesamt 176 Straftaten nach dem oben erläuterten §17 I UWG und nach dem Straftatenschlüssel 7154 insgesamt 117 Straftaten nach §17 II UWG registriert, die schweren Fälle nach §17 IV UWG sind dabei mit eingeschlossen (Bundeskriminalamt 2007: 41). Ein Vergleich mit der Statistik der Jahre 2000-2004 offenbart für die Jahre 2005 und 2006 einen deutlichen Anstieg der Delikte im Bereich des §17 I UWG, und einen im Schnitt leichten Anstieg im Bereich des §17 II UWG (Bundeskriminalamt 2005: 63; Bundeskriminalamt 2007: 41). Dennoch scheint die Zahl der Delikte im Vergleich mit anderen Straftatenschlüsseln vergleichsweise gering, die Aufklärungsquote beider Straftatenschlüssel lag zudem bei über 90%.

Die zunächst positiv erscheinende Aussage dieser Zahlen relativiert sich jedoch angesichts zweier Fakten ungemein: Zum einen ist bei dieser Art von Delikten von einer sehr hohen Dunkelziffer auszugehen (Bundeskriminalamt 2005: 63; Lux/Peske 2002a: 107). Für das gesamte Feld der Wirtschaftskriminalität wird diese Dunkelziffer von Seiten deutscher Unternehmen auf 80% geschätzt (KPMG 2006: 6). Zum anderen handelt es sich bei den Delikten wie bereits in Kapitel 3.4.1 erläutert um Anzeigedelikte. Es steht zu vermuten, dass aus Angst vor eingangs erwähnten Reputationsschäden, nur in denjenigen Fällen von Industriespionage Anzeige erstattet wird, bei denen eine Überführung und Verurteilung als gesichert erscheint.

In Anbetracht der geringen Anzeigehäufigkeit derartiger Delikte scheint es nicht verwunderlich, dass das BKA auf seiner Jahrespressekonferenz 2008 im Bereich der Wirtschaftskriminalität lediglich die Zahlkartenkriminalität und den Identitätsdiebstahl (durch „Phishing“ und andere Methoden) zu seinen aktuellen kriminalistischen Herausforderungen zählt (Bundeskriminalamt 2008).

Bundesamt für Sicherheit in der Informationstechnik

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Zentralstelle des Bundes in Fragen der IT-Sicherheit. Es verfügt über einen Personal-

stamm von ca. 470 Mitarbeitern, welche vor allem mit Prüf-, Zertifizierungs- und Beratungsaufgaben betraut sind.

Im Gegensatz zu Verfassungsschutz und Kriminalbehörden verfügt das BSI jedoch über keinen wie auch immer gearteten Ermittlungsauftrag bezüglich Wirtschafts- und Industriespionage, es spielt mit seinen *vier Kernkompetenzen* jedoch eine wichtige Rolle in der passiven Gefahrenabwehr dieses Bereiches. Erstens *informiert* es über alle wichtigen Entwicklungen der IT-Sicherheit, zweitens *berät* es bei Einsatz und Entwicklung von IT-Sicherheitsmaßnahmen, drittens *entwickelt* es eigene sicherheitsbezogene Produkte (z.B. Verschlüsselungsmethoden) und viertens *zertifiziert* es die Sicherheitseigenschaften von IT-Systemen (Bundesamt für Sicherheit in der Informationstechnik 2006: 4).

Das Angebot des BSI richtet sich dabei gleichermaßen an staatliche Behörden, Unternehmen und Privatanwender und besteht unter anderem auch aus Penetrationstests[53] und Prüfverfahren der Lauschabwehr. Die Kosten für derartige Maßnahmen bemessen sich nach einem durch den Bundesminister des Innern festgelegten aufwandsgebundenen Gebührenkatalog. So beträgt der Tagessatz eines BSI-Mitarbeiters je nach dessen Laufbahngruppe zwischen 432 und 672 Euro (Basis: 8h / Tag, Quelle: Bundesministerium des Innern 2005: 521); Summen, die im unteren Normbereich der für Unternehmensberater gängigen Honorare liegen.

Im Rahmen seines Aufgabenbereichs sieht das BSI die Wirtschafts- und Industriespionage in Deutschland auf dem Vormarsch. Während Wirtschaftsspionage, Informationsdiebstahl und unbefugte Kenntnisnahme im „Bericht zur Lage der IT-Sicherheit in Deutschland 2007“ in der Rangfolge der größten Gefahrenbereiche für Unternehmen nur den fünften Rang von zwölf einnimmt, prognostiziert das BSI, dass diese zukünftig auf Rang drei zu finden sein werden (Bundesamt für Sicherheit in der Informationstechnik 2007:15).

53 Die Mitarbeiter des 2001 eingerichteten „IT-Penetrationszentrums“ versuchen dabei unter Anwendung von Mitteln und Methoden, mit denen sich ein potentieller Angreifer Zutritt zu einem IT-System verschaffen würde, die Schwachstellen eines solchen Systems zu finden.

4.2.2 Privatwirtschaftliche Institutionen als defensive Akteure

Wie in Kapitel 3 gezeigt, erwächst aus den veränderten nationalen und internationalen Rahmenbedingungen ein für Nationalstaaten und Privatwirtschaft gleichermaßen erhöhtes Schutzbedürfnis gegenüber der Wirtschafts- und Industriespionage. Doch welche Akteure sind hier im Besonderen betroffen? Sind diese sich ihrer erhöhten Schutzbedürftigkeit überhaupt bewusst? Werden ausreichende Sicherheitsmaßnahmen getroffen und wie sind diese beschaffen? Diese Fragen sollen im nachfolgenden Abschnitt geklärt werden. Obwohl unter den privaten, defensiven Akteuren des Feldes Wirtschafts- und Industriespionage nicht nur das produzierende Gewerbe zu verstehen ist, konzentriert sich die Betrachtung auf diese am stärksten betroffenen Unternehmen (Corporate Trust 2007: 15). Zwar sind als private defensive Akteure die „eigentlichen“[54] Sicherheitsberatungen (wie z.B. die Hamburger Corporate Trust), verschiedene Industrieverbände (wie z.B. die „Arbeitsgemeinschaft für Sicherheit der Wirtschaft“) sowie nicht zuletzt die Universitäten und andere höhere Bildungseinrichtungen tätig, letztlich werden jedoch die für die individuelle Sicherheit des Unternehmens maßgeblichen Entscheidungen nur innerhalb des Unternehmens selbst getroffen.

Die nachfolgenden *Anzeichen für eine gesteigerte Gefährdung des Unternehmens*, die *empirische Bestandsaufnahme gängiger Sicherheitsmaßnahmen* und der *entscheidungstheoretische Erklärungsansatz* sind durch Interviewreihen entstanden, die während der Technologiemessen Medica, NanoSolutions und Euromold im Jahre 2007 mit ausgewählten Unternehmensvertretern durchgeführt wurden. Ergänzt werden diese Befunde durch die bereits zitierte Untersuchung von Corporate Trust.

Risikofaktoren für die Spionageanfälligkeit von Unternehmen

Der Grad der Anfälligkeit für Spionage variiert je nach Unternehmen. Maßgeblich dafür sind folgende wirtschaftliche Kenngrößen:

54 Im Gegensatz zur Kategorie „Intelligence Trader“ aus Kapitel 4.1.2.

- *Struktur des Absatzmarktes*: In einer Marktform mit vielen Anbietern, z.B. im heterogenen Polypol[55], muss ein offensiver Akteur der Wirtschafts- und Industriespionage aufgrund begrenzter Ressourcen eine Entscheidung darüber treffen, welche der vielen Konkurrenzunternehmen er ausspähen möchte. Je höher die Zahl der am Markt vertretenen Anbieter ist, desto geringer ist die Chance für jedes einzelne Anbieterunternehmen Opfer von Spionage zu werden. In Marktformen mit einer geringeren Anzahl von Anbietern, wie etwa dem inhomogenen Dyopol[56,] ist die Wahrscheinlichkeit Opfer eines der diversen, in Kapitel 4.1 vorgestellten offensiven Akteure zu werden entsprechend höher.
- *Markstellung des Unternehmens*: Die Marktstellung eines Unternehmens ist die Summe einer Vielzahl vom Unternehmen beeinflussbarer (z.B. Rohstoffgüte, Produktpalette, Vertriebsstrategie) und unabhängiger (Wechselkurse, Rohstoffpreise, Produkt- und Vermarktungsansprüche von Handel und Kundschaft) Variablen. Dasjenige Unternehmen, von dem aufgrund seiner herausgehobenen Marktstellung vermutet wird, dass es die beeinflussbaren Variablen geschickt gewählt hat, wird viel eher zum Ziel von Spionage werden als ein Unternehmen, welches über eine nur untergeordnete Marktstellung verfügt.
- *Grad der Produktinnovativität*: Wirtschafts- und Industriespionage unterliegt nach der Rational-Choice-Theory (Cornish/Clarke 1986) ebenfalls einem Kosten-Nutzen-Kalkül. Der potentielle Nutzen einer Spionagestraftat liegt umso höher, je innovativer die Produkte des ausgespähten Unternehmens sind. Daher werden innovative Unternehmen häufiger zum Ziel solcher Bestrebungen.

55 Makroökonomische Marktformklasse, die durch eine Vielzahl von Anbietern, eine Vielzahl von Nachfragern und nicht-homogene Produkte gekennzeichnet ist (in der Realität sehr häufig anzutreffen).

56 Makroökonomische Marktformklasse, die durch zwei Anbieter, eine Vielzahl von Nachfragern und nicht vollständig homogene Produkte gekennzeichnet ist (z.B. die Konkurrenz zwischen Airbus und Boeing).

- *Grad der Produktkomplexität*: Je komplexer die Produkte eines Unternehmens aufgebaut sind, desto geringer ist die Wahrscheinlichkeit, dass diese zum Zweck der Produktpiraterie einem erfolgreichen „Reverse Engineering"-Verfahren zu unterziehen sind. Scheitert der potentielle Produktpirat bei diesem, steigt die Wahrscheinlichkeit, dass er sich die Informationen auf klandestine und illegale Weise beschafft.
- *Komplexitätsgrad der Produktionsverfahren*: Selbst bei klar erkanntem Aufbau eines bestimmten Produktes steht ein potentieller Produktpirat eventuell vor dem Problem, bestimmte Bauelemente mit den ihm zur Verfügung stehenden Fertigungsverfahren nicht nachbilden zu können. Ist zudem nicht klar, welche Verfahren Verwendung fanden oder sind diese nicht auf dem freien Markt erhältlich, steigt wiederum das Spionagerisiko.
- *Internationales Tätigkeitsfeld*: Ein auf dem Weltmarkt tätiges Unternehmen macht sich durch seinen dadurch ungleich größeren Bekanntheitsgrad zu einem potentiell stärker gefährdeten Ziel als ein Unternehmen, welches seine Produkte nur national oder gar regional anbietet.
- *Wahrnehmbare Sicherheitsvorkehrungen*: Je mehr ein Unternehmen seine Sicherheitsüberlegungen in seinem Außenbild verankert, umso größer ist die davon ausgehende Abschreckungswirkung. Ein vollständig umfriedetes Firmenareal, sichtbare Videoüberwachung sensibler Bereiche, eine rigorose Anzeigepolitik gegenüber potentiellen Straftätern und eine in der Corporate Governance[57] verankerte regelmäßige Sicherheitsschulung der Mitarbeiter senken das Risiko, Opfer von Wirtschafts- und Industriespionage zu werden.

Je höher der anhand dieser Kriterien bestimmbare Risikograd des Unternehmens ist, desto höher ist auch dessen Bedarf an Sicherheitsmaßnahmen. Wie im Folgenden gezeigt, wird dieser Bedarf jedoch seitens der Unternehmen nur selten wahrgenommen.

57 Corporate Governance: Leitlinien der Unternehmensführung.

Empirische Bestandsaufnahme gängiger Sicherheitsmaßnahmen

Die Vertreter deutscher Technologieunternehmen besitzen ein stark unterschiedlich ausgeprägtes Sicherheitsbewusstsein, ähnlich unterschiedlich ausgeprägt ist in diesen Unternehmen der Einsatz grundlegender Sicherungsmaßnahmen.

So waren nur 58% der befragten Unternehmensvertreter der Meinung, sich einem Risiko durch Wirtschafts- und Industriespionage ausgesetzt zu sehen (siehe Anhang 1), unter denjenigen Unternehmen, welche noch nicht wissentlich von Industriespionage betroffen waren, liegt die Quote sogar nur bei 50%. Die geringe Höhe dieses Anteils verwundert, wurden die Befragungen doch alle auf durchweg technologieorientierten Messeveranstaltungen (Medizintechnik, Nanotechnologie, Werkzeugmaschinen- und Prototypenbau) durchgeführt.

Doch selbst von denjenigen Unternehmensvertretern, deren Firmen bereits wissentlich Opfer von Spionagestraftaten geworden sind, glaubten 25% nicht an eine diesbezügliche weitere Gefährdung des eigenen Unternehmens. Diese scheinbar irrationale Diskrepanz erklärt sich aus der Methodik der Studie[58]: Die persönliche Einschätzung der Gefährdung wurde im strukturierten Interview als erstes, bereits erfolgte Spionagestraftaten zuletzt abgefragt. Diese Struktur wurde bewusst gewählt, um diesbezügliche Wahrnehmungsverzerrungen auf Seiten der Befragten aufzudecken, eine direkte, umgekehrte Folge der Fragen (1.: „Ist Ihr Unternehmen schon einmal Opfer von Industriespionage geworden?“ 2.: „Sehen sie ihr Unternehmen als durch Industriespionage gefährdet?“) hätte eine verzerrende Suggestivwirkung auf die Beantwortung der zweiten Frage ausgeübt. So konnte festgestellt werden, dass ein Viertel der Befragten kein Bewusstsein für das Risiko durch Industriespionage entwickelt hatte, obwohl das eigene Unternehmen dadurch bereits Schäden erlitten hat.

Diese Daten bestätigen eine Studie des Handelsblatts. Laut dieser waren 81% der Befragten davon überzeugt, dass Industriespionage weltweit auf dem Vormarsch sei, 72,1% glaubten dies in Bezug auf Deutschland. Dagegen waren jedoch

58 Siehe dazu das Beispiel eines Interviewbogens in Anhang 3.

nur 33,7% der Meinung, dass ihr eigenes Unternehmen zukünftig stärker durch Industriespionage bedroht sei.

Doch worin liegt diese Verzerrung begründet? Unstrukturierte, dem Interview nachfolgende Gespräche ergaben, dass viele Unternehmen nicht erwarten, dass sich jemand für die Fertigungsgeheimnisse von Produkten interessieren könnte, die bereits einige Jahre auf dem Markt sind[59] und nicht bedenken, dass viele Unternehmen weniger entwickelter Länder nicht über die technischen Möglichkeit zur Herstellung dieser Produkte in gleicher oder ähnlicher Qualität oder gar zum „Reverse Engineering" verfügen. Andere wiederum verließen sich voll und ganz auf die in ihrem Unternehmen praktizierten Sicherheitsmaßnahmen.

Gerade bezüglich dieser Sicherheitsmaßnahmen ergab die Befragung jedoch Besorgnis erregende Lücken. Zwar verfügen die meisten Unternehmen (86%) laut Auskunft ihrer Vertreter über mindestens eine Form der Zugangskontrolle[60] zu ihren Firmengeländen bzw. -gebäuden und verpflichten die allermeisten Unternehmen (95%) ihre Arbeitnehmer vertraglich zur Geheimhaltung (siehe Kapitel 3.4.1 und Anhang 1). Fundamentalere Sicherheitskonzepte werden dabei jedoch oft übersehen. So unterziehen weniger als die Hälfte (44%) der befragten Unternehmen Bewerber für gehobene Positionen[61] einfachsten Sicherheitsüberprüfungen (ebd.). Eine dazu oft im Messegespräch geäußerte Ansicht war, dass man sich diese aufgrund des damit verbundenen Aufwandes nicht leisten könne.[62]

Auffällig ist auch, dass die Unternehmenssicherheit in den wenigstens Fällen „Chefsache" ist. Die mit 24% am häufigsten gegebene Antwort auf die Frage, wer im Unternehmen für die zentrale Planung und Realisation von Sicherheitsmaßnahmen zuständig ist, lautete schlichtweg „Niemand" – eine weitere Bestätigung für das mangelnde Sicherheitsbewusstsein deutscher Unternehmen (siehe Abb. 3).

59 Siehe dazu das Gespräch in Kapitel 4.1.1, S. 48.

60 Pförtner, Werksausweise, Codekarten etc.

61 Mittleres und Top-Management, leitende Entwickler und Designer.

62 Dieser Auffassung muss hier jedoch widersprochen werden, ein im Aufwand begrenzter Vorschlag zur Methodik grundsätzlicher Sicherheitsüberprüfungen findet sich in Kapitel 6.1.

Weitere 22% der Befragten sahen die IT-Abteilungen und -beauftragten ihres Unternehmens als federführend in der Realisierung von Sicherheitsmaßnahmen, was dafür spricht, dass über eine Firewall und einen Passwortschutz von Arbeitsplatzrechnern hinausgehende Sicherheitsmaßnahmen ebenfalls keiner zentralen Planung unterliegen (ebd.).

20% der Unternehmen beschäftigten schließlich einen hauptamtlichen Sicherheitsbeauftragten mit einem Aufgabenfeld, das ausdrücklich über die Belange des Arbeitsschutzes hinausgeht. In immerhin 17% der Unternehmen (ebd.) war Sicherheit schließlich „Chefsache", das heißt es erfolgte eine zentrale Planung durch Geschäftsführung bzw. Top-Management. Eine eigene Sicherheitsabteilung existierte nur in drei der befragten Firmen. Diese waren alle der Kategorie Industriegroßunternehmen mit mehr als 10.000 Beschäftigten zuzuordnen.

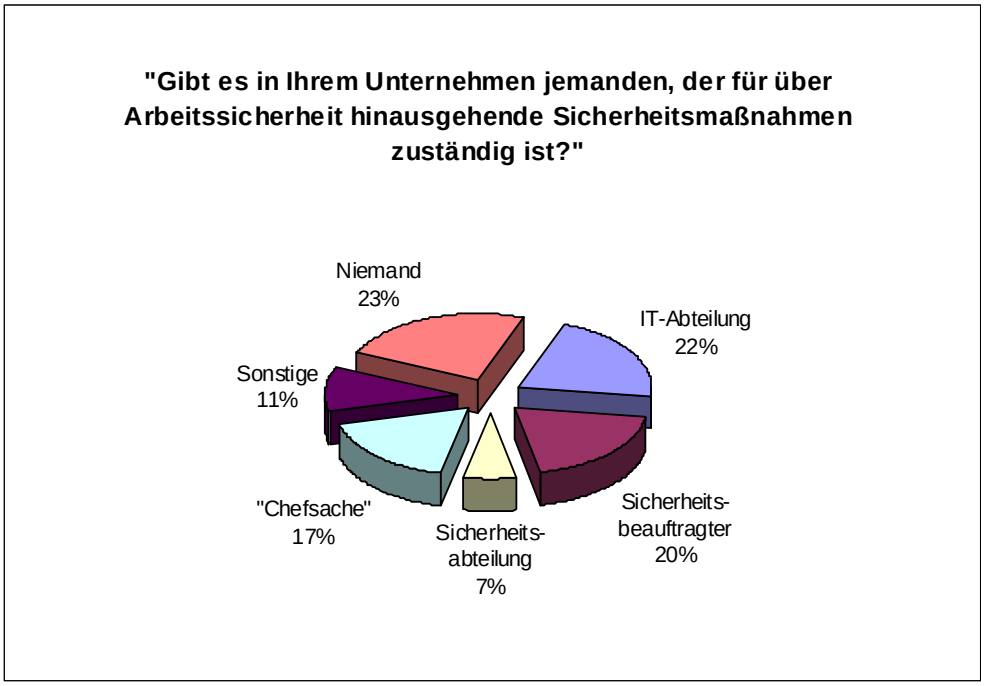

Abb. 3: Unternehmensinterne Zuständigkeit für Planung und Durchführung von Sicherheitsmaßnahmen

Diese Ergebnisse bestätigen die Corporate Trust-Studie, die deutschen Firmen ein desaströses Verhältnis zum Thema Unternehmenssicherheit bescheinigt (Corporate Trust 2007: 33-37):

Von 32 abgefragten Sicherheitsmaßnahmen aus den Bereichen Objektsicherheit, IT-Sicherheit, prozessuale Sicherheit und Mitarbeitersensibilisierung hat keine einzige Maßnahme eine flächendeckende Verbreitung (in mehr als 90% der befragten Unternehmen) gefunden. Lediglich zwei, nämlich der Einsatz einer Firewall zum Schutz der IT-Systeme und die Aufnahme von Geheimhaltungsklauseln in den Arbeitsvertrag fanden eine hohe Verbreitung (>75%). Immerhin fünf weitere Maßnahmen[63] bringen es noch auf eine Verbreitung von jeweils nahezu 50% oder mehr. Besonders desolat sieht die Lage im Bereich der prozessualen Sicherheit aus: Hier war keine der genannten Maßnahmen zu mehr als 50% verbreitet. Explizite Regeln zum Umgang mit geheimhaltungspflichtigem Material, Backgroundchecks strategischer Geschäftspartner, eine Clean-Desk-Policy oder abhörsichere Kommunikationsmittel fehlen in der Mehrzahl der Unternehmen.

Besonders hervorgehoben sei schließlich noch der Bereich der Lauschabwehr. Zwar ist das Abhören fremder Räumlichkeiten mit einer ganzen Reihe operativer Schwierigkeiten verbunden[64], gelingt es jedoch eine Abhöreinrichtung unentdeckt zu platzieren, ist es mit immensen Schwierigkeiten verbunden diese aufzuspüren und unschädlich zu machen (Bundesamt für Sicherheit in der Informationstechnik 2006: 68-70). Abhöreinrichtungen wurden immerhin für ein Zehntel aller bemerkten Spionageversuche eingesetzt (Corporate Trust 2007: 18). Dies scheint sich dem Bewusstsein deutscher Sicherheitsverantwortlicher jedoch zu entziehen: 58% der Befragten gaben an, dass sich niemand um die Belange des Abhörschutzes in ihrem Unternehmen kümmere (ebd.: 32). Doch selbst in Anbetracht der verbliebenen 42%, welche über diesbezüglich geregelte Verantwortlichkeiten verfügen, lässt sich nicht erklären, warum lediglich 5,8% der Unternehmen einen abhörsicheren

63 Als da wären: Technische oder personelle Zugangskontrollen zum Firmenareal (61,1%), gesonderte Überwachung besonders sensibler Bereiche (49,8%), personalfördernde Maßnahmen zur Steigerung der Verbundenheit mit dem Unternehmen (50,7%), Passwortschutz auf allen IT-Geräten (72,9%) und ein nicht näher spezifizierter Punkt namens „Hohe Standards bei der IT-Sicherheit" (56,2%).

64 Vgl. Rustmann 2002 50-73.

Konferenzraum ihr Eigen nennen und nur 6,3% ihre Räumlichkeiten regelmäßig auf Abhöreinrichtungen überprüfen lassen (ebd.: 33).

Entscheidungstheoretischer Erklärungsansatz

Auf dieses Problem verweist der Geschäftsführer einer Frankfurter Firma für integrale Sicherheitssysteme während eines Gesprächs auf der Medica: Er überprüfe gelegentlich für seine Großkunden die Sicherheit potentieller neuer Zulieferer. Dabei stoße er immer wieder auf Unternehmen, bei denen man sich ungehindert durch das Werkstor bis zu den Fertigungsbändern bewegen könne. Weitere Mängel seien die zu seltene Videoüberwachung sensibler Bereiche, welche zum einen eine Abschreckungswirkung habe, zum anderen die Identifizierung eventueller Täter ermögliche, sowie eine IT-Sicherheit, die über Firewall, Virenscanner und Passwortschutz meist nicht hinausgehe. Er erklärte die geringe Verbreitung grundlegender Sicherheitsmaßnahmen mit dem Hinweis, dass sich Sicherheit nicht auf dem Papier rechne; klar umrissenen Kosten könne man keinerlei kalkulierbare Rückflüsse gegenüberstellen.[65]

Sicherheitsverantwortliche in Unternehmen haben es in der Tat schwer, ihre Ausgaben sowohl *im Voraus* als auch *im Nachhinein* gegenüber den Budgetverantwortlichen zu rechtfertigen. Einen Erklärungsansatz der komplexen Entscheidungssituation bietet die Prinzipal-Agent Theorie[66]: *Im Voraus* erstellt der sicherheitsverantwortliche Agent im Auftrag des budgetverantwortlichen Prinzipals eine Analyse der Bedrohungslage. Dieser Auftrag lautet, die Unternehmung angemessen gegenüber möglichen Risiken durch Wirtschafts- und Industriespionage abzusichern. Die Motivation des Agenten liegt im eigenen beruflichen Fortkommen, welches im Falle einer Sicherheitspanne ernsthaft behindert werden könnte. Seine Entscheidungssituation stellt sich wie folgt dar:

65 Vertrauliches Gespräch am Rande der Medica, Düsseldorf, 16.11.2007.

66 Prinzipal-Agent-Theorie: Ein Ansatz der Neuen Institutionenökonomik, welcher das Hierarchieverhalten unter asymmetrischer Informationsverteilung zu erklären versucht.

- Eine Sicherheitslösung mit angemessenem Kosten-Nutzen-Verhältnis wird vom Prinzipal gewünscht.
- Eine anhand der eigenen Analyse gefertigte angemessene Lösung schließt aber typischerweise eine Anzahl sicherheitstechnischer Restrisiken nicht aus.
- Der Prinzipal kann allerdings mangels sicherheitstechnischen Fachwissens die Angemessenheit des Sicherheitspaketes nicht beurteilen, dies ist dem Agenten bekannt.
- Für den Agenten ergibt sich daraus ein Anreiz, eine unangemessene Sicherheitslösung zu wählen, welche die Restrisiken zu unverhältnismäßigen Kosten ausschließt.

Der Prinzipal kann *im Voraus* mangels Sachkenntnis im Allgemeinen nicht abschätzen, ob die geplanten Sicherheitsmaßnahmen in einem angemessenen Verhältnis zur tatsächlichen Bedrohungslage stehen. Seine Entscheidungssituation stellt sich wie folgt dar:

- Genehmigt er den Ausgabenvorschlag des Agenten, läuft er Gefahr, einen unangemessenen Teil seines Budgets auf Sicherheitsmaßnahmen zu verwenden.
- Kürzt er die zur Ausgabe vorgeschlagene Summe, läuft er Gefahr, kein angemessenes Sicherheitssystem zu erhalten.

Das Ergebnis der Entscheidungssituation hängt davon ab, inwieweit der Prinzipal (der wiederum um den Anreiz des Agenten weiß) dem Agenten vertraut, dass dieser zum Erreichen der eigenen Ziele keine übertriebene Sicherheitslösung gewählt hat. Der Ausgang der Entscheidungssituation ist somit ungewiss.

Im Nachhinein steht der Prinzipal vor folgender Problematik:

Ist nach Einrichtung des Sicherheitskonzeptes keine Straftat geschehen, kann nicht gesagt werden, ob der Agent mit seiner Bedrohungsanalyse richtig lag, das Sicherheitssystem also alle angreifbaren Lücken geschlossen und somit potentielle Spione von einer Straftat abgehalten hat, oder ob die Bedrohung aus Eigennutz des Agenten übertrieben dargestellt worden ist. Ein zur Abschreckung ausreichendes

Sicherheitssystem gibt also keinen Nachweis über seine Angemessenheit. Dies ist auch als das „Paradox of Warning“ bekannt (US-Joint Chiefs of Staff 2000: I-27; Strong 1994: 163).

Es ist somit anzunehmen, dass die dargestellten Unsicherheitsprobleme, wie im Interviewauszug dargestellt, zu unnötig restriktiven Anschaffungsentscheidungen im Sicherheitsbereich führen.

4.3 Zwischenfazit

Die durchgeführte Betrachtung aller relevanten Akteure führt zu der Schlussfolgerung einer besonderen Bedrohungslage für den deutschen Wirtschaftraum in Bezug auf die Gefahr durch Wirtschafts- und Industriespionage. Dafür ist eine Kombination verschiedenster Faktoren verantwortlich:

- Der deutsche Wirtschaftsraum ist das Ziel systematischer Wirtschaftsaufklärung einiger der größten Nachrichtendienste der Welt. Besonders aktiv sind dabei die Dienste der Russischen Föderation und der Volksrepublik China. Doch auch die Dienste westlicher Alliierter betreiben Wirtschaftsspionage gegen deutsche Interessen.
- Die Aktivität von Innentätern stellt nach wie vor eines der größten Spionagerisiken für Unternehmen dar. Im Bereich der Intelligence Trader und Nischenexperten ist eine zunehmende Kenntnis nachrichtendienstlicher Methoden und verwandter Techniken, welche sich auch zum Ausspähen von Staat und Wirtschaft nutzen lassen, zu beobachten.
- Die mit der Bekämpfung von Wirtschafts- und Industriespionage befassten Strafverfolgungsbehörden genießen bei den deutschen Unternehmen kein hohes Ansehen. Diese bezweifeln die Fähigkeit der Behörden, derartige Delikte effektiv zu bekämpfen, und schalten sie auch aus Angst vor Reputationsschäden selten ein. Weiterhin gibt es Anzeichen für die bewusste Vertuschung der Wirtschaftsspionage westlicher Alliierter durch bundesdeutsche Behörden.

- Der Verfassungsschutz bemüht sich in jüngster Zeit, seinem negativen Image mit Aufklärungskampagnen, Beratungsangeboten, zu Gunsten der Spionageabwehr veränderten Prioritäten und einer strikten Vertraulichkeitszusage aktiv entgegen zu treten (Bundesamt für Verfassungsschutz 2006: 21f; o.V. 2008a).
- Trotz immenser jährlicher Schäden sind sich die Unternehmen des deutschen Wirtschaftsraums der Problematik noch nicht in vollem Umfang bewusst. Die aufgezeigten Gefährdungskriterien treffen in hohem Maße auf viele deutsche Hightech-Unternehmen zu, professionelle Unternehmenssicherheit wird dort aufgrund unkalkulierbarer Rückflüsse jedoch nur rudimentär betrieben. Eine Zusammenarbeit mit den Behörden findet oft nur in klar erkannten und bereits aufgeklärten Fällen von Spionage statt. Auf Wirtschaftskongressen ist Spionage weiterhin eher ein Randthema. Es entsteht der Eindruck einer diesbezüglichen *Schweige- und Stillhaltekultur*.

5 Methodik klandestiner Informationsbeschaffung

Wie bereits in Kapitel 4.1.2 angedeutet, hängt eine erfolgreiche und dauerhafte Informationsbeschaffung auch im Bereich der Wirtschafts- und Industriespionage in hohem Maße von der Kenntnis dazu geeigneter Methoden aus dem Umfeld nachrichtendienstlicher Tätigkeit ab. Unter geeigneten Methoden sind dabei standardisierte Vorgehensweisen zu verstehen, welche darauf ausgelegt sind, die individuellen Verwundbarkeiten eines Zielobjektes auszunutzen. Das Zielobjekt ist dabei der Ausgangspunkt der Methodenplanung, es schränkt durch die Art seiner Verwundbarkeiten die Methodenwahl ein. So gibt zum Beispiel der Fall eines spielsüchtigen Fachbeamten in der Devisenverwaltung einer Zentralbank zwingend andere standardisierte Vorgehensweisen vor, als der Fall einer ungenügenden Beaufsichtigung von Fachbesuchern in den Montagehallen eines Automobilbau-Unternehmens.

Eine besondere Relevanz erfährt der Einsatz solcher Methoden bei Angriffen, die von Außentätern durchgeführt werden. Hierbei wird versucht, den in Kapitel 4.1.2 thematisierten Mangel an Gelegenheit durch den Einsatz nachrichtendienstlicher Methoden zu kompensieren. Ein Innentäter, d.h. ein Angestellter, der sich entschließt gegen seine eigene Organisation (Firma, Regierungsbehörde oder Verband) tätig zu werden, hat auch ohne Einsatz nachrichtendienstlicher Methoden Zugriff auf ein gewisses Maß an Informationen, welches ihm aufgrund seiner Position zur Verfügung steht. Möchte er sich jedoch über dieses Maß hinaus Informationen aneignen, so muss er sich wie der Außentäter nachrichtendienstlicher Methoden bedienen.

Die Methoden der klandestinen Informationsbeschaffung werden von Forschung und Praxis in eine Vielzahl unterschiedlicher Kategorien eingeteilt. So unterscheidet die grundlegende Intelligence-Publikation der US-Joint Chiefs of Staff zwischen zwölf[67] verschiedenen Kategorien von Sammlungsmethoden (2000: I-6); Lux und Peske führen sogar siebzehn auf (2002a: 85). Um im Rahmen dieser Arbeit einen Überblick über ausgewählte Methoden im Bereich der Wirtschafts- und Industriespionage zu geben, ist eine derartig feingliedrige und zumeist technikorientierte Unterteilung jedoch nicht notwendig. Die hier folgende Einteilung unterscheidet daher lediglich die übergeordneten Kategorien der Human Intelligence Collection (HUMINT), welche alle Methoden der Informationsgewinnung durch direkten zwischenmenschlichen Kontakt erfasst, und der Technical Intelligence Collection (TECHINT), welche alle Methoden der Informationsgewinnung mit technischen Hilfsmitteln umfasst (Shulsky/Schmitt 2002: 11). Häufig wird als dritte Kategorie die Open Source Intelligence Collection (OSINT), die Gewinnung von Informationen aus öffentlich zugänglichen Quellen genannt (ebd.), da sie einen großen Anteil an der Informationsbeschaffung der staatlichen Nachrichtendienste hat. Zur Abschöpfung öffentlich zugänglicher Quellen sind allerdings weder illegale noch

67 Counterintelligence ist keine originäre Sammlungsmethode und ist daher nicht mitgezählt worden.

klandestine Handlungen notwendig, sie liegt daher gemäß der Definition der Begriffe Wirtschaftsspionage und Industriespionage nicht im Fokus dieser Arbeit.[68]

Gelegentlich fällt die genaue Einordnung einer Methode dennoch schwer, wie etwa im Falle bestimmter kombinierter *Social-Engineering*-Ansätze (siehe Seite 86f) oder im Falle des *Zufallsfund-Köders* (siehe Seite 85). Diese stellen sich bei näherer Betrachtung jedoch als Kombination verschiedener grundlegenderer Methoden heraus. Entscheidend für die Einordnung ist letztlich, ob die Information ihren Weg von einer menschlichen Quelle oder aus einer technischen Quelle heraus zum Empfänger findet.

5.1 Methoden der Human Intelligence Collection

Die Methoden der Human Intelligence umfassen das Abschöpfen menschlicher Quellen unter verschiedensten Vorbedingungen: In der Betrachtung muss zum einen danach unterschieden werden, ob sich die Quelle des Abschöpfungsversuchs bewusst ist und zum anderen danach, ob die Quelle diesen Abschöpfungsversuch, so sie sich dessen bewusst ist, auch toleriert.

Ist sich die Quelle der Abschöpfung bewusst und toleriert sie diese (gleichgültig ob aufgrund von passiver Duldung oder aktiver Kooperation) liegt ein Fall von *freiwilliger Mitwirkung* vor. Ist sie sich der Abschöpfung bewusst und toleriert sie diese nicht, wird die Kooperation verschiedentlich mit Hilfe von Druckmitteln erzwungen. Es liegt dann der Fall *unfreiwilliger Mitwirkung* vor. Wenn sich die Quelle der Abschöpfung nicht bewusst ist, ist es für die Betrachtung der einzusetzenden Methoden nahezu gleichgültig, ob sie diese bei eventueller Kenntnisnahme tolerieren würde. Diese Methoden werden schließlich unter den Begriffen *Täuschung und Beeinflussung* zusammengefasst.

68 Im wirtschaftlichen Bereich wäre diese Kategorie am ehesten der Competitive Intelligence zuzurechnen.

Freiwillige Mitwirkung

Die freiwillige Mitwirkung ist der Lehrbuchfall der klassischen nachrichtendienstlichen Tätigkeit. Im Allgemeinen bedarf es dabei zweier Mitwirkender, eines Innentäters (vgl. Kapitel 4.1.2) und einer staatlichen oder privatwirtschaftlichen Institution, welche willens und in der Lage ist, aus den Kenntnissen des Innentäters einen wirtschaftlichen Vorteil zu ziehen. Die Beziehung zwischen beiden Akteuren kann dabei auf drei unterschiedliche Arten zustande gekommen sein: Der Innentäter kann ein Selbstanbieter sein, welcher Kontakt zu der betreffenden Institution aufnimmt, um ihr seine Dienste anzubieten. Er kann wie im Falle Lopez (siehe Seite 56) durch die beteiligte Institution angeworben worden sein oder er wurde als „Maulwurf" gezielt in das Zielobjekt eingeschleust. Die Kooperation zwischen dem Innentäter und der betreffenden Institution kann hierbei auf regelmäßiger Basis oder auch zeitlich (eventuell sogar nur ein einziges Mal) begrenzt stattfinden.

Eine besondere Gefahrensituation ergibt sich für das Zielobjekt, wenn – *Motivation* und *Bereitschaft* vorausgesetzt[69] – die häufige *Gelegenheit* eines Innentäters auf eine über gute nachrichtendienstliche *Methodenkenntnis* verfügende und zur Spionage entschlossene Institution trifft. In dieser Konstellation ist eine hohe Schadenswahrscheinlichkeit für das Zielobjekt gegeben, da die betreffende Institution versuchen wird, sich ihre „Quelle im Objekt" über einen möglichst langen Zeitraum zu erhalten und ihre Kenntnisse dazu einzusetzen, die Gefahr der Entdeckung des Innentäters entscheidend zu minimieren.

Der Fall freiwilliger Mitwirkung besitzt für die Praxis eine hohe Relevanz. Corporate Trust zufolge war die Anwerbung von Mitarbeitern durch Dritte in 18,7% der Fälle die Ursache nicht autorisierter Informationsabflüsse (Corporate Trust 2007: 18). Auch eigene Erhebungen zeigen, dass Anwerbungsversuche Dritter derart alltäglich sind, dass sie von vielen Unternehmensvertretern schon als „Tagesgeschäft" abgetan werden. Dies sei in der Branche nicht unüblich: Wer seine Mitarbeiter nicht genügend motiviere, müsse auch mit den daraus entstehenden Konsequenzen fertig

69 Verärgerung über den eigenen Arbeitgeber ist dabei nach finanziellen Anreizen das wichtigste Motiv (Lux/Peske 2002a: 87). Siehe zu den möglichen Motiven nochmals Seite 54 in Kapitel 4.1.2.

werden, so dass Statement eines Herstellers medizinischer Diagnostik. Weiterhin sei der gerichtliche Nachweis eines tatsächlichen Geheimnisverrats oftmals sehr schwierig, entsprechende Konkurrenzverbote[70] zudem mit einer Reihe juristischer Schwierigkeiten und einem hohem finanziellem Aufwand verbunden.[71]

Eine enorme Erleichterung erfahren Anwerbungsversuche in jüngster Zeit durch offene Geschäftskontaktnetzwerke wie etwa Xing (ehemals openBC). Dort können Unternehmensmitarbeiter auf der Suche nach neuen Jobs, Geschäftskontakten oder Absatzchancen auf einer Website kostenlos ein Profil ihres bisherigen Karrierepfades hinterlegen und dieses Profil über eine Kontaktliste mit den Profilen anderer Xing-Mitglieder verknüpfen. Einem potentiellen Anwerber wird so die Suche nach für ihn interessanten Zielpersonen in der auszuspähenden Institution ebenso vereinfacht wie eine diskrete persönliche Kontaktaufnahme.

Aber auch einem Selbstanbieter ist es auf diese Weise möglich, sich geeignete Ansprechpartner (vornehmlich bei der direkten Konkurrenz) zu suchen. Zwei der befragten Unternehmensvertreter klagten über Vorfälle dieser Art: In beiden Fällen hatten Selbstanbieter sensible Unternehmensdaten (in einen Fall Kundenlisten, in einem anderen neu entwickelte chemische Rezepturen) an Konkurrenzunternehmen zu verkaufen versucht. Offensichtlich wurde jedoch kein nachrichtendienstliches Know-How zur dauerhaften Abschöpfung dieser beiden Quellen eingesetzt: In einem der beiden Fälle versuchte der Selbstanbieter seinen illegalen Geschäftsverkehr über sein firmeninternes E-Mail-Konto abzuwickeln (vgl. Interviewreihen zur Medica und zur NanoSolutions).

Unfreiwillige Mitwirkung

Sollte die Mitwirkung einer Zielperson auf kooperativer Basis nicht zu erreichen oder nicht zu erwarten sein, lässt sich diese mitunter auch erzwingen. Die hierfür zur Verfügung stehenden Möglichkeiten lassen sich grundlegend in die Alterna-

70 Arbeitsvertragliche Klauseln, welche nach Beendigung des Arbeitsverhältnisses eine Anstellung bei einem Konkurrenzunternehmen für einen bestimmten Zeitraum verbieten.

71 Vertrauliches Gespräch am Rande der Medica, Düsseldorf, 16.11.2007.

tiven *Nötigung* und *Erpressung* unterteilen. Diese werden hier aber nicht im Sinne des Strafrechts unterschieden, nach welchem sich Erpressung von Nötigung durch eine Bereicherungsabsicht des Täters unterscheidet. Vielmehr soll der Begriff der Erpressung das Ausnutzen einer speziellen Verwundbarkeit der Zielperson zum Ausdruck bringen.

Eine *Nötigung* im Sinne dieser Arbeit liegt dann vor, wenn die Zielperson mittels Gewalt oder durch Drohung mit für sie nachteiligen Konsequenzen zur Kooperation veranlasst wird. Dabei ist die Drohung ohne nähere Recherche der speziellen Lebensumstände der Zielperson einsetzbar. Sie liegt typischerweise im Bereich von Gefahren für Leib und Leben sowohl der Zielperson als auch ihr nahe stehender Personen. Die Kooperation der Zielperson kann dabei in einem Handeln, Unterlassen oder Dulden liegen.

Eine *Erpressung* im Sinne dieser Arbeit ist ebenfalls stets mit einer Drohung verbunden, diese nimmt aber auf die Lebensumstände der Zielperson Bezug. Sie erfordert daher im Gegensatz zur Nötigung eine genauere Recherche über ihr Opfer. Ein Beispiel für den Gegenstand einer solchen Erpressung wäre eine Drohung mit der Offenlegung einer sozial nicht akzeptierten Handlung oder Eigenschaft der Zielperson, wie etwa einem Ehebruch, bestimmter sexueller Vorlieben, politischer Ansichten oder einer von der Zielperson begangenen Straftat. Gerade wegen letzterer Alternative ist zu bedenken, dass sich im Rahmen von Wirtschafts- und Industriespionage *freiwillig* mitwirkende Innentäter (sowie jeder andere Wirtschaftskriminelle auch) durch die Strafbarkeit ihrer Handlungen stets in die Gefahr begeben, aufgrund dieser Strafbarkeit zu einer weiteren Kooperation *gezwungen* zu werden.

Weiterhin lässt sich die zur Durchführung einer Erpressung nötige Verwundbarkeit der Zielperson auch herbeiführen. Ein Beispiel hierfür ist der Einsatz so genannter Romeo-Agenten, wie er von Seiten sowjetischer Nachrichtendienste im Bereich der Technologiespionage mit Erfolg eingesetzt wurde (Mellon 2001: 11): Mithilfe dieser auf die Anbahnung erotischer Affären spezialisierten Agenten gelang es die Zielpersonen erpressbar zu machen, indem diesen gedroht wurde, dass

ihre heimlich in Bild und Ton festgehaltenen außerehelichen sexuellen Kontakte mit dem betreffenden „Romeo“ ihren Ehepartnern zugespielt würden.

Täuschung und Beeinflussung

Ungleich komplexer als Nötigung und Erpressung sind die Methoden der Täuschung und Beeinflussung. Diese nutzen gezielt menschliche Verhaltensmuster aus, um ihre Zielperson zu einer bestimmten Handlung zu veranlassen. Vom gewöhnlichen Trickbetrug unterscheidet sich diese methodische Kategorie in zweierlei Hinsicht: Erstens dadurch, dass die Absicht des Trickbetrügers in der unmittelbaren Aneignung von Sach- und Geldwerten liegt, und nicht im Aneignen von Informationen (auch wenn diese dann wiederum zu einem wirtschaftlichen Vorteil führen können) und zweitens durch ihre für Wirtschafts- und Industriespionage typische, intendierte Klandestinität. Diese hat unter anderem den Sinn, die Zielperson nach Möglichkeit auch *nach* erfolgreich abgeschlossener Täuschungshandlung über diese im Unklaren zulassen, da die Methoden der Täuschung und Beeinflussung auch zur Vorbereitung der Anwendung von TECHINT-Methoden dienen können. Dies soll nachfolgend am Beispiel des *Zufallsfund-Köders*[72] erläutert werden:

Ein „interessantes“ oder „wertvolles“ Objekt wird an einer Stelle, an der eine hohe Wahrscheinlichkeit besteht, dass es dort von einer Zielperson wahrgenommen wird, auf dem Boden platziert. Es besteht nun eine gewisse Wahrscheinlichkeit, dass die Zielperson dieses Objekt an sich nimmt. Welche Köderobjekte der Zielperson interessant oder wertvoll genug scheinen, so dass sie diese an sich nimmt, ist dabei natürlich höchst subjektiv, es könnte sich beispielsweise um einen hochwertigen Füllfederhalter oder um ein Portemonnaie handeln. Weiterhin hängt die Art dieses Köders von dem intendierten Zweck der Methode ab. So wäre zum Beispiel ein neben dem gekennzeichneten Firmen-PKW-Stellplatz einer Zielperson ausgelegter Füllfederhalter von Größe und Format her gut geeignet, eine einfache Abhörein-

72 Die Bezeichnung wurde im Rahmen dieser Arbeit gewählt, da sich in der Literatur keine Beschreibungen dieser speziellen Methode finden.

richtung aufzunehmen oder zum Beispiel einen Sender, welcher es durch Dreiecks-peilung ermöglicht, ein Bewegungsprofil dieser Zielperson zu erstellen.

Eine im Bereich der Wirtschafts- und Industriespionage verwendete Variante dieser Methode dient zur Vorbereitung von Angriffen auf die IT-Systeme eines Unternehmens[73]: Ein ahnungsloser Angestellter sieht sich dabei mit einem morgens auf dem Firmenparkplatz herumliegenden USB-Stick konfrontiert. Um herauszufinden wem seiner Kollegen dieser gehört, nimmt er ihn an sich und steckt ihn in den USB-Port seines PC-Arbeitsplatzes. Was der Angestellte nicht weiß ist, dass der USB-Stick oder die sich auf ihm befindlichen Dateien von kundiger Hand so präpariert wurden, dass sie, sobald sie geöffnet werden, so genannte Spyware, d.h. Software die zum Ausspionieren von PCs oder ganzen Netzwerken dient[74], auf dem Rechner installiert.[75]

Eine weitere HUMINT-Methode, welche typisch menschliche Verhaltens-muster ausnutzt ist die Methode des *Social Engineering*. Im Gegensatz zum Zufalls-fund-Köder bedürfen die diversen Ausprägungen des Social Engineerings eines ausgeprägten zwischenmenschlichen Kontaktes. Der bereits weiter oben erwähnte Kevin Mitnick definiert Social Engineering wie folgt:

> „Social engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology." (Mitnick/Simon 2002: iv).

Gegenstand des Social Engineering ist also eine mittels Vorspiegelung einer falschen Identität oder einer sonstigen Manipulation vorgenommene Täuschung anderer, mit dem Ziel der Gewinnung vertraulicher Informationen.

---

73 Quelle: Vertrauliches Gespräch mit einem Mitarbeiter eines großen deutschen Industriekonzerns im Rahmen der Interviewreihe auf der NanoSolutions, Frankfurt a. M., 23.11.2007.

74 Ein Beispiel für Spyware wäre zum Beispiel ein so genannter *Keylogger*: Eine Software, die alle Tastatureingaben (wie z.B. auch Passwörter) aufzeichnet, speichert und ggf. an ein vordefiniertes Ziel versendet.

75 Die Voraussetzung hierfür ist natürlich, dass der PC über zugängliche USB-Ports verfügt, etwas was bei strikter IT-Sicherheit nicht der Fall sein dürfte.

Dieser Prozess läuft typischerweise nach folgendem Muster ab (ebd.: 331): Zu Anfang bedarf es umfangreicher *Nachforschungen* über das Zielobjekt. Dies beinhaltet zum Beispiel das aufmerksame Studium von Presseartikeln und Pressemitteilungen, von periodischen Geschäftsberichten, von Patentanmeldungen und der Unternehmenswebsite. Möglich ist auch eine visuelle Inspektion der Umgebung des Firmenstandortes, um einen Eindruck der dortigen Routineabläufe zu erhalten. Auch das „Dumpster Diving" (ebd.: 156), das Durchsuchen und Auswerten der (Papier-)Abfälle eines Unternehmens kann Teil dieser Nachforschungen sein.

Weitere Ansatzpunkte für Nachforschungen sind, neben dem Unternehmen als solchem, seine Mitarbeiter. Erste Ansätze zu diesen kann hier eines der offenen Geschäftskontaktnetzwerke (wie etwa Xing) bieten, mit Hilfe dessen sich unter Umständen die Namen von Angestellten des Zielobjektes finden lassen. Aber auch Xings mehr dem Privatleben seiner Nutzer zugewandten Pendants (wie etwa StudiVZ, Myspace oder Facebook) lassen sich nutzen, um für das Social Engineering nützliche Informationen über eine bestimmte Person zu sammeln.

Auf Basis der während der Nachforschungen erhaltenen Informationen versucht der Social Engineer nun im persönlichen Kontakt ein *Vertrauensverhältnis aufzubauen* oder ein bestehendes Vertrauensverhältnis auszunutzen. Dies kann zum Beispiel über das Verwenden unternehmenseigener Fachbegriffe, oder die Ansprache gemeinsamer Tätigkeitsbereiche oder gar gemeinsamer Hobbys geschehen.

Schließlich wird versucht, das *Vertrauensverhältnis auszunutzen*. Dies kann in einem vermeintlich dienstlichen Ersuchen um Hilfe bestehen, der Erteilung einer Anweisung aus dem Munde einer vermeintlich vorgesetzten Persönlichkeit oder in der Veranlassung eine bestimmte E-Mail zu öffnen bzw. eine Website zu besuchen. Dies sei nachfolgend an einem Beispiel erläutert:

Ein Social Engineer hat sich zum Ziel gesetzt (oder zum bezahlten Ziel gesetzt bekommen), Informationen über die neue Vertriebsstrategie eines großen Mobilfunkanbieters zu sammeln. Er beschließt zu diesem Zweck, mittels spyware-

infizierter Email-Anhänge die Kontrolle über die PCs möglichst hochrangiger Vertriebsmitarbeiter des Konzerns zu erlangen.

Vorbedingungen dafür, eine Person zum Öffnen eines spyware-infizierten Email-Anhangs zu bewegen, sind zum einen die Kenntnis von deren Email-Adresse und zum anderen das Wecken seines Interesses. Weiterhin muss die Spyware in der Lage sein, die IT-Schutzmechanismen des Unternehmens, in diesem Fall also den Email-Scanner zu überwinden.

Der Angriff startet mit Nachforschungen über das Unternehmen in einem offenen Geschäftsnetzwerk. Je größer das Unternehmen ist, je mehr Niederlassungen die Firma hat und je weiter diese räumlich getrennt sind, desto geringer sind wegen dessen tendenziell größerer Anonymität der Mitarbeiter untereinander die Chancen, dass eine angenommene oder vorgetäuschte Identität auffliegt (Mitnick/Simon 2002: 333). Hierbei werden die Namen von Zielpersonen des Vertriebsbereiches und aus dem IT-Bereich ermittelt.[76] Dann beginnt die Vorbereitung des technischen Teils der Aktion: Es muss getestet werden, ob der Email-Scanner des Unternehmens in der Lage ist, die Spyware zu erkennen. Dazu muss der Name der eingesetzten Software allerdings erst einmal bekannt sein. Um dies herauszufinden, genügt meist ein Anruf bei der Unternehmens-IT (zu der bei Unkenntnis der Durchwahl auch die Telefonzentrale des Unternehmens verbindet):

> „Hallo, hier ist Glasmann[77], vom Vertrieb. Ich soll gleich beim Kunden eine Präsentation halten, sitze gerade noch in einem Café mit WiFi-HotSpot[78] und mein Virenscanner spuckt mir beim automatischen Updateversuch eine Fehlermeldung nach der anderen um die Ohren. So kann ich natürlich nicht präsentieren, wie sieht das denn aus? Könnten Sie mir kurz die aktuelle Versionsnummer und wo ich die auf deren Website finde sagen, dann installier ich das Update manuell…“

Geht der IT-Mitarbeiter darauf ein, ist – sofern das eigene technische Know-How ausreicht um den Scanner zu umgehen – die erste Hürde genommen.

---

76 Eigene Versuche zeigen, dass dies für viele deutsche Großunternehmen problemlos möglich ist, sofern man selber Mitglied in einem solchen Netzwerk ist.

77 Der Name eines beliebigen Vertriebsmitarbeiters.

78 Möglichkeit des drahtlosen Zugangs zum Internet.

Die gewerbliche Email-Adresse einer Zielperson zu erfahren ist mit relativ geringen Schwierigkeiten verbunden. Viele Unternehmen verwenden bei der Vergabe ihrer Mailadressen Namenskonventionen. So ist das Finden der gewünschten Adresse, sollte sich diese nicht direkt über Xing, Google oder ähnliche Suchanwendungen herausfinden lassen, nur eine Frage der richtigen Konvention: svglasmann@firma.de, glasmann.sven@firma.de oder svgl@firma.de wären hier häufige Varianten. Oft wird diese schon durch einen Blick auf die Firmenhomepage klar, ansonsten findet sie sich bei einer Suche im WorldWideWeb oder durch das Erlangen einer Visitenkarte des Unternehmens während eines Messebesuchs. Die *Nachforschungen* sind somit erledigt, die technische Möglichkeit, das *Vertrauensverhältnis auszunutzen*, ist ebenfalls vorbereitet. Das eigentliche Herzstück der Methodik verbleibt: Der Versuch zu einer der Zielpersonen ein *Vertrauensverhältnis aufzubauen*. Eine hierzu geeignete Methode wäre zum Beispiel die Folgende:

Zunächst überprüft der Social Engineer die Kontakte des im Xing gefundenen Vertriebsmitarbeiters auf Interessen, die sie mit diesem gemeinsam haben. Gleichzeitig sucht man nach Anzeichen dafür, dass diese Personen einen nicht gewohnheitsmäßigen oder gar freundschaftlichen Umgang miteinander pflegen. In hohem Maße geeignet sind daher Kontakte, die zum einen räumlich weit entfernt von der ausgesuchten Zielperson arbeiten und zum anderen noch nicht lange für ihr Unternehmen tätig sind, nicht lange beruflich tätig sind oder deren Arbeitsplatz vorher bestenfalls in einer anderen, in keinerlei Beziehung zum Unternehmen der Zielperson stehenden Branche lag.

Nun schickt der Social Engineer der Zielperson eine fingierte Email, die so manipuliert wurde, dass sie als Absender eine der Adresse des Geschäftskontaktes ähnliche Absenderadresse enthält und im Text Bezug auf das gemeinsame Interesse nimmt, um das Vertrauen der Zielperson zu gewinnen:

> „Hallo Herr Geiger,
> ich hatte ja gar nicht gewusst, dass Sie ebenfalls Golf spielen, bis ich mir gerade zufällig Ihr Xing-Profil angeschaut habe. Könnten Sie mir vielleicht bei einer Sache weiterhelfen? Mein Abteilungsleiter plant für eine Auswahl an Key Account Managern unserer Großkunden in ihrer Region ein exklusives Golf-

> Wochenende als Incentive. Haben Sie zufällig einen der auf der Liste angehängten Plätze schon bespielt? Ich wäre Ihnen für Ihre Hilfe sehr dankbar.
> In Hoffnung auf weitere gute Zusammenarbeit,
> David Großer“

Der Anhang wurde vom Social Engineer so gestaltet, dass er neben entsprechenden Angebotsprospekten aus der Region des Geschäftskontaktes auch eine sich unbemerkt vom Anwender installierende beliebige Spyware, wie z.B. den Remote Access Trojaner „Back Orifice“[79] enthält. Ein Praxisbeispiel für diese Methode findet sich bei Nagaraja und Anderson (2009: 5ff.), ein von ihnen beschriebenes Spionagenetzwerk erschloss auf diese Weise neue Zielrechner.

In der Praxis sind allerdings auch weniger gut vorbereitete Angriffe verbreitet, wie z.B. der Anruf als vorgeblicher IT-Mitarbeiter mit der Aufforderung, bestimmte Passwörter in eine Maske auf einer Website einzugeben oder der Auftritt als persönlicher Kontakt eines Vorstandsmitgliedes, von dem man weiß dass es sich gerade im Urlaub befindet.

Doch gleich ob gut vorbereitet oder ad hoc durchgeführt, gegen die Methoden eines Social Engineers sind nur wenige Unternehmen gefeit. Penetrationstests verschiedener Sicherheitsberatungen ergaben eine Erfolgsquote von nahezu 100% bezüglich Social-Engineering-Attacken auf IT-Ziele (Mitnick/Simon: 245). Derzeit werden im Bereich der Wirtschafts- und Industriespionage bereits 8% der Fälle durch Social Engineering verursacht (ebd.: 8), aufgrund der anscheinend äußerst hohen Verwundbarkeit der Unternehmen und einem mit 28,4% äußerst geringen Anteil über diese Methoden aufgeklärter Mitarbeiter (Corporate Trust 2007: 35) ist jedoch eine zukünftig steigende Zahl von Delikten zu vermuten.

79 Remote Access Trojaner sind Programme, mit denen sich über das Internet Kontrolle über von ihnen infizierte Rechner erlangen lässt. Back Orifice verfügt zum Beispiel über die Möglichkeit Tastatureingaben aufzuzeichnen, die Festplatten des Rechners zu durchsuchen oder das Monitorbild samt eventueller Tonausgabe mitzuschneiden (Microsoft Technet 2002).

5.2 Methoden der Technical Intelligence Collection

Die Informationsbeschaffung mit technischen Hilfsmitteln hat im Bereich der Wirtschafts- und Industriespionage vom Anbruch des Informationszeitalters massiv profitiert. Zum einen hat die weitgehende Digitalisierung kommerzieller Informationen deren Entwendung in Form von *Angriffen auf IT-Systeme* größtenteils von logistischen Problemen befreit, zum anderen erlaubt die stetig fortschreitende Miniaturisierung elektronischer Geräte immer ausgeklügeltere *Lausch- und Spähangriffe*. Diese drei Kategorien stellen zugleich die gebräuchlichsten Formen der Technical Intelligence Collection dar (Corporate Trust 2007: 18). Die im militärischen Wirkungsbereich der Nachrichtendienste verbreiteten Beschaffungsformen des Abfangens und Entschlüsselns von Funksignalen sowie die Echtzeit-Satelliten-Fotografie verfügen im wirtschaftlichen Kontext über eine nur geringe Relevanz und sind somit von der Betrachtung ausgeschlossen. Ebenso entziehen sich den Umständen angepasste Spezialmethoden einer aussagekräftigen Kategorisierung.[80]

Angriffe auf IT-Systeme

Angriffe, welche sich die Digitalisierung kommerzieller Informationen zu Nutze machen wollen, zählen mit fast 15% zu den häufigsten Spionageangriffen gegen privatwirtschaftliche Institutionen (Corporate Trust 2007: 18). Der größte Vorteil dieser Angriffe besteht darin, dass zu ihrer Ausführung keine physische Präsenz des potentiellen Täters am Tatort, und somit auch keine zwischenmenschlichen Kontakte notwendig sind. Weiterhin entstehen beim „Abtransport" der Daten keinerlei Probleme logistischer Art, wie etwa die Notwendigkeit mehrere Kubikmeter Blaupausen oder Prozessakten unauffällig transportieren zu müssen.

Die Schwierigkeit dieser Angriffe liegt jedoch darin, die von der betroffenen Institution implementierten IT-bezogenen Sicherheitsmaßnahmen überwinden zu

80 Ein Beispiel für eine solche exotische Methode wäre das Aufbringen von speziellen Adhäsivstoffen auf die Schuhsohlen einer sowjetischen Delegation, welche 1972 ein Boeing-Werk besichtigte. Der Zweck des Unterfangens lag im Sammeln von Metallproben, die Rückschlüsse auf die im US-Amerikanischen Flugzeugbau verwendeten Werkstoffe ermöglichen sollten (Weiss 1996: 122).

müssen. Zu deren häufigsten zählen Scan-Programme, die eingehende Daten und Anfragen auf Malware[81] untersuchen und Firewalls, welche den Datenaustausch zwischen Rechnernetzen und dem Internet nur unter vordefinierten Bedingungen zulassen (Corporate Trust 2007: 34). Weiterhin besteht auch die Möglichkeit sensible Daten zu verschlüsseln, so dass diese nach ihrer Entwendung durch den Täter erst entschlüsselt werden müssen und andernfalls wertlos sind.

Dem versierten Angreifer steht jedoch eine derartige Fülle von Eindringmöglichkeiten zur Verfügung, dass sie an dieser Stelle nicht in ihrer ganzen technischen Bandbreite erschlossen werden kann. Zur Illustration sei hier die Beobachtung des Geschäftsführers eines Herstellers chirurgischer Präzisionsinstrumente angeführt: Dieser suchte von seinem Büroarbeitsplatz aus im Internet nach Beschaffungsquellen neuartiger Kompositmaterialien. Auf der Homepage eines mit diesen Materialien befassten deutschen Einkaufsverbandes wurde er auf das Werbebanner eines entsprechenden chinesischen Herstellers aufmerksam und klickte dieses an, um sich einen Überblick über dessen Angebotspalette zu verschaffen. Beim Betreten der dahinter liegenden fremden Website, versuchte diese umgehend einen Trojaner auf seinem Rechner zu installieren. Dieser wurde zwar von der installierten Antivirensoftware erkannt, konnte aber nicht beseitigt werden, so dass der IT-Abteilung des Unternehmens keine andere Wahl blieb, als die Festplatten des Rechners zu formatieren und das Betriebssystem neu aufzusetzen.

Eine oftmals übersehene Komponente von IT-Sicherheit ist, dass diese nicht nur aus Schutzsoftware besteht, sondern auch Elemente der Personalsensibilisierung mit einbeziehen muss. Weiterhin kann eine grundlegende Objektsicherheit hier einen wertvollen Beitrag leisten. Was nützt die beste Abwehrsoftware, wenn eine Reinigungskraft nach Dienstschluss die Hardware-Variante des oben erläuterten *Keyloggers* installiert: Ein daumengroßes Gerät, welches zwischen Tastaturkabel und PC gesteckt wird (Bigalke 2007).

81 Wortschöpfung aus „Malicious“ und „Software“, darunter fallen im Wesentlichen Viren, d.h. Infektionen einer ausführbaren Datei, welche das System im Moment der Ausführung befallen und Würmer, welche sich auch ohne das Zutun des Users aktiv verbreiten.

Lauschangriffe

Eine mit einem Anteil von mehr als 10% der bekannten Fälle ebenfalls häufige TECHINT-Form ist das Abhören von Besprechungen und Telefonaten (Corporate Trust 2007: 18). Die hierzu notwendigen, miniaturisierten Geräte sind in einfachster Ausführung bereits für wenige hundert Euro in einschlägigen Internet-„Spyshops" erhältlich (HTCS-Löbl GbR o.J.a). Dort werden unter anderem Funksender von der Größe eines Fingernagels beworben und vertrieben, sofern der Besteller eine Lieferadresse außerhalb des Geltungsbereichs deutscher Gesetzgebung angeben kann (HTCS-Löbl GbR o.J.b). Die Schwierigkeit in der Anwendung dieser Geräte liegt in einer dauerhaften Platzierung am Einsatzort. Diese ist zum Beispiel mittels eines Zufallsfund-Köders oder der Schenkung eines präparierten Gegenstandes möglich. Das Problem dieser Methoden ist allerdings, dass man nach Auslegen des Köders oder erfolgter Schenkung keinerlei Kontrolle mehr über die genaue Platzierung des Gegenstandes hat, und die Schenkung im Falle der Entdeckung des Senders den Täter offenbart (Rustmann 2002: 56).

Erheblich vereinfacht werden derartige Angriffe, wenn der Täter Zutritt zu den Räumlichkeiten des Zielobjektes hat. Dies kann im Rahmen einer Führung oder einer Konferenz einmalig der Fall sein oder auch regelmäßig erfolgen, wenn es jenem Täter zum Beispiel gelingt, durch die Mitarbeit in einer der Servicefirmen des Unternehmens Zutritt zu erlangen. Egal ob Reinigungskräfte, Klimaanlagentechniker, Kopiergerät- und Faxwartungsdienste oder gar Bürogärtner, alle diese Personen haben Zutritt zu den Geschäftsräumlichkeiten eines Unternehmens, häufig sogar unbeaufsichtigt. Verschiedentlich werden sie, zum Beispiel Reinigungskräfte, sogar regelmäßig in sicherheitstechnisch sensiblen Bereichen eingesetzt, da die wenigstens Führungskräfte oder Produktentwickler ihre Fußböden selber wischen. Dieser ungehinderte Zutritt offenbart eine Fülle von Möglichkeiten Abhöreinrichtungen zu platzieren: Zum Beispiel im Telefonhörer, unter der Fußleiste, in der Steckdose, im Kabelschacht oder in der Lehne eines Bürosessels.

Sind diese Geräte erst einmal fachgerecht installiert, bedarf es meist der Hilfe von Spezialisten, sie zu finden und zu beseitigen. Unterstützung bietet hier der bereits in Kapitel 4.2.1 erwähnte Service des BSI. Die Spezialistenteams des Amtes stehen der Wirtschaft gegen Entgelt zur Verfügung, um die Abhörsicherheit von Geschäftsräumen zu prüfen. Aufgrund der Möglichkeit hochentwickelter Abhöreinrichtungen, ihre Sendetätigkeit per Fernbefehl einzustellen, müssen potentiell gefährdete Räumlichkeiten in einem zeitraubendem Prozess einer visuellen Inspektion unterzogen werden (Bundesamt für Sicherheit in der Informationstechnik 2006: 69). Aber auch private Unternehmen stehen für solche Dienste zur Verfügung. Jedoch agieren unter dem Deckmantel der Abhörschutzbranche auch so genannte „Regentänzer", die Räume oft mit antennengespickten vorgeblichen Messgeräten „durchsuchen" und dabei eigene Wanzen hinterlassen. Zum Teil gehen die „Regentänzer" sogar soweit, diese beim nächsten Auftrag wieder zu „finden" (Rustmann 2002: 75). Die Einforderung mehrjähriger, staatlicher Referenzen wird daher vor der Auftragsvergabe empfohlen (ebd.: 76).

Weitere Abhörtechniken entstehen in der Kombination mit Angriffen auf die IT-Systeme eines Unternehmens. So ist es bei digitalen Telefonanlagen mitunter möglich, Telefonendgeräte als „Babyfon", d.h. zur akustischen Raumüberwachung, auch bei aufgelegtem Hörer zu missbrauchen (Bundesamt für Sicherheit in der Informationstechnik 2006: 70). Auch das Abhören eines Raumes von außen ist mittels ausgeklügelter Technik mittlerweile möglich: Mittels eines Lasermikrofons lässt sich die von den Schallwellen menschlicher Sprache verursachte Bewegung von Fensterscheiben in verständliche Sprache zurückverwandeln (Muscatell 1983).

Die deutschen Unternehmen sind auf diese Bedrohung nur mangelhaft vorbereitet: Lediglich 5,8% aller Unternehmen verfügen über einen abhörgeschützten Konferenzraum (Corporate Trust 2007: 33). In fast 60% aller Fälle gibt es innerhalb des Unternehmens keinen Verantwortlichen für die zentralen Belange des Abhörschutzes (ebd.: 32).

Spähangriffe

Im Gegensatz zu den Lauschangriffen, welche auf die akustische Überwachung eines Zielobjektes ausgerichtet sind, liegt die Intention von Spähangriffen in dessen visueller Überwachung. Obwohl Spähangriffe selten thematisiert werden, und weitaus seltener vorkommen als Lauschangriffe, stellen sie doch eine nicht zu unterschätzende Gefahr dar. Ein Beispiel für einen einfachen Spähangriff wäre zum Beispiel die Fernüberwachung eines von einem Fenster aus einsehbaren Monitors mittels einer leistungsstarken Kameraausrüstung.

Konkrete Fälle sind jedoch seltener zu finden als Fälle aus dem Bereich der Lauschangriffe. Ein interessanter Fall war dennoch dem Gespräch mit einem Vertreter eines großen deutschen Industriekonzerns während der NanoSolutions 2007 zu entnehmen: „Während einer Routinewartung entdeckte ein Servicetechniker eine Manipulation des Zuführungsschachtes an einem Shredder für sensible Dokumente: Jemand hatte vor das Schneidewerk das Shredders einen Durchlaufscanner gesetzt, der den Inhalt der Dokumente vor dem Shreddern digitalisierte und über einen mit dem Gerät verbundenen UMTS-Sender auf direktem Wege in die Außenwelt funkte." Diese und ähnliche Manipulationen sind im Übrigen auch bei den in vielen Büros verbreiteten kombinierten Fax- und Kopiergeräten denkbar, da diese bereits serienmäßig eine Scanvorrichtung enthalten und lediglich um einen mit dem Datenspeicher des Gerätes verbundenen Sender erweitert werden müssten.

Eine weitaus exotischere Methode ist das so genannte Van-Eck-Phreaking. Mit Hilfe dieser 1985 vom niederländischen Wissenschaftler Wim van Eck erstmals wissenschaftlich beschriebenen Methode lässt sich, anhand der elektromagnetischen Abstrahlungen eines CRT-Computerbildschirms[82] das auf diesem Schirm gezeigte Bild unter optimalen Bedingungen in Entfernungen von bis zu einem Kilometer auf einem anderen Bildschirm in Echtzeit darstellen (Eck 1985: 276). Dass diese Technik nicht nur unter Modellbedingungen und mit CRT-Geräten funktioniert, ist auf der CEBIT 2006 vom deutschen Cambrigde-Dozenten Dr. Markus Kuhn demonstriert

82 Herkömmlicher Röhrenbildschirm, CRT steht für *Cathode Ray Tube*, wörtlich: Kathodenstrahlröhre, auch Braun'sche Röhre genannt.

worden: In einer Halle mit buchstäblich hunderten von Computerbildschirmen aller Arten gelang es ihm, das Signal eines 25m vom eigenen Stand gelegenen, fremden TFT-Bildschirms[83] zu isolieren und auf dem eigenen Bildschirm anzuzeigen (Kuhn 2006).

Dr. Kuhn hat sich auch mit einer weiteren Form optischer Aufklärung beschäftigt: Aufgrund bestimmter technischer Eigenheiten[84] von Computerbildschirmen ist es unter bestimmten Umständen möglich, deren Anzeige aus dem von einer Wand vor dem Schirm reflektierten diffusen Streulicht zu interpolieren (Kuhn 2002: 17). Eine ähnliche Entdeckung konnte unlängst ein Forscherteam der Universität Saarbrücken für sich verbuchen: Ihnen gelang es mit ähnlichen Verfahren, Reflektionen von in Bildschirmnähe aufgestellten Teekannen, Brillengläsern und sogar den Augenoberflächen der vor dem Bildschirm sitzenden Personen einzufangen und in Bilder umzuwandeln. Auf diesen war – mit Ausnahme der von den Augen stammenden Bilder – eine 12-Punkt-Schriftart noch klar zu lesen[85] (Saar-Uni-Presseteam 2008).

Der Einsatz derart esoterischer Techniken für die Belange von Wirtschafts- und Industriespionage ist der Literatur bislang nicht bekannt. Dennoch können solche Mittel nicht vollständig ausgeschlossen werden und sollten auch zukünftig bei der Planung von Sicherheitskonzepten bedacht werden; ein Faktum, dem das Bundesamt für Sicherheit in der Informationstechnik mit seiner technischen Leitlinie TL-03305 über abstrahlsichere Hardware bereits Rechnung trägt (Bundesamt für Sicherheit in der Informationstechnik 2008).

83 Flachbildschirm, TFT steht für *Thin-Film Transistor.*

84 Kuhn stellte einen besonderen, kurzfristigen Leuchtintensitäts-Peak im ersten Moment der Anregung der in einer Bildschirmmaske gelegen Leuchtelemente fest. Zu Details siehe Kuhn (2002: 4f. und 7 (Fig. 2 a)).

85 Im Falle der Augenreflektionen musste man sich mit dem Lesen größeren Überschriften zufrieden geben.

5.3 Zwischenfazit

Die zuletzt aufgezeigte Methodenauswahl ist exemplarisch und erhebt keinerlei Anspruch auf eine vollständige Abbildung der im Bereich der Wirtschafts- und Industriespionage gängigen Erfassungsmethoden. Sie dient vielmehr einer Kategorisierung in Methodenfelder jenseits des üblicherweise technikorientierten nachrichtendienstlichen Jargons sowie deren beispielhafter Illustration durch ausgewählte Anwendungsfälle.

Gerade die gegen Ende des letzten Kapitels genannten Vorgehensweisen (wie etwa das Van-Eck-Phreaking oder das Umwandeln diffuser Lichtreflexe in verwertbare Bilder) machen deutlich, dass das Spektrum *anwendbarer* Methoden lediglich durch den menschlichen Erfindungsgeist und die Grenzen der Physik beschränkt sind. Was das Spektrum der tatsächlich *angewendeten* Methoden betrifft, so ist dieses durch eine Abwägung des mit den einzelnen Methoden verbundenen Zeit- und Kostenaufwandes, sowie des für die jeweilige Methode erforderlichen Know-Hows wesentlich engeren Beschränkungen unterworfen.[86]

Dennoch ist eine besorgniserregende Verbreitung originär nachrichtendienstlicher Methoden im Bereich der Wirtschafts- und Industriespionage festzustellen, deren Einsatz von den folgenden Faktoren begünstigt wird:

- Offene Kontaktnetzwerke wie Xing/openBC, Myspace, StudiVZ oder Facebook erleichtern das Finden und Erschließen geeigneter Zielpersonen für die Methoden der Human Intelligence Collection. Gleichermaßen erleichtert wird die Aufnahme persönlicher Kontakte zwischen Selbstanbietern und deren potentiellen Abnehmern.
- Die Unternehmen des deutschen Wirtschaftsraums nehmen Abwerbeversuche der Konkurrenz als „business as usual“ hin, da sich der juristische

86 Eine hier treffende Branchenanekdote handelt von drei TECHINT-Spezialisten, die in einer Bar unter Ersinnen unmöglichster IMINT-, SIGINT- & MASINT-Methoden herauszufinden versuchen, was die drei jungen Frauen am anderen Ende des Tresens bereden. Sie sind sehr verblüfft, als diese schließlich auf sie zutreten und sagen: „Ihr versucht also jetzt seit zwei Stunden herauszufinden, was wir bereden? Wir wissen das bei Euch schon lange. Dem Barkeeper 10$ in die Hand zu drücken nennt man übrigens HUMINT.“ (Rustmann 2002: 36f).

Nachweis eines Geheimnisverrats oftmals schwierig gestaltet und Konkurrenzverbote nur in Ausnahmefällen praktikabel sind.

- IT-Sicherheit besteht nicht nur aus Softwareprodukten, sondern muss Aspekte der Objektsicherheit, der Prozesssicherheit und der Personalpolitik mit einbeziehen. So ist zum Beispiel eine flächendeckende Aufklärung über Methoden wie die des Social Engineering nicht gegeben.
- Lauschangriffe sind sogar schon mit einfach erhältlichen und kostengünstigen Mitteln durchzuführen. Professionell installierte Abhöreinrichtungen lassen sich jedoch nur mit Hilfe ausgebildeter Spezialisten nachweisen.
- Wissenschaftliche Grundlagen für wirkungsvolle Spähangriffe existieren zuhauf, eine Verbreitung in der Praxis bleibt abzuwarten und ist am ehesten im nachrichtendienstlichen Umfeld zu vermuten.

Die Empirie macht schließlich deutlich, dass auch wenig esoterischen Methoden im deutschen Wirtschaftsraum gute Erfolgsaussichten beschieden sind: Nur ein Fünftel aller Unternehmen verfügen über eine interne Sicherheitsorganisation (Corporate Trust 2007: 31). Dementsprechend lückenhaft muten die gegen die Methoden der Wirtschafts- und Industriespionage praktizierten Abwehrmaßnahmen an.

6 Fazit

Bereits die ersten im Rahmen dieser Arbeit unternommenen empirischen Forschungen deuteten auf ein hohes Sicherheitsdefizit des deutschen Wirtschaftsraums gegenüber der Wirtschafts- und Industriespionage hin. Dieser Eindruck hat sich im Laufe weiterer Nachforschungen bestätigt. Dies erklärt sich zum einen dadurch, dass Deutschland Teil eines *besonderen Gefahrenraumes* ist und zum anderen durch das im Wirtschaftsraum vorherrschende *mangelnde institutionelle Sicherheitsbewusstsein* und den daraus folgenden Mangel an Initiative zum Selbstschutz.

Die Kennzeichnung des deutschen Wirtschaftsraums als *besonderer Gefahrenraum* der Wirtschafts- und Industriespionage liegt zum einen in einer Reihe *allge-*

meiner Veränderungen der internationalen Rahmenbedingungen begründet, deren wichtigste die Neuausrichtung nachrichtendienstlicher Prioritäten nach dem Ende des Kalten Krieges, ein weltweit steigender Konkurrenzdruck durch die diversen ökonomischen Erscheinungsformen des Globalisierungsphänomens sowie der Eintritt der industrialisierten Welt in das sogenannte Informationszeitalter sind.

Zum anderen ist hierfür eine Reihe von für den deutschen Wirtschaftsraum *spezifischen* Faktoren verantwortlich. Zu nennen sind hier im Wesentlichen die besondere Innovativität des durch seine florierende Exportwirtschaft global verknüpften Forschungsstandortes Deutschland, die diesen zu einem attraktiven Ziel machen, sowie dessen besondere, durch eine nur ungenügende Abschreckungswirkung gekennzeichnete Rechtslage im Bezug auf ökonomisch motivierte Spionagedelikte.

Staat, Industrie und Verbände begegnen diesen Risiken jedoch nicht mit der notwendigen Aufmerksamkeit. Die Unternehmen bringen den zuständigen Ermittlungsbehörden nur wenig Vertrauen entgegen, zeigen aber selbst im Kampf gegen Wirtschafts- und Industriespionage eine Mischung aus Selbsttäuschung und Verdrängungsverhalten. Die Kriminalbehörden zählen den Kampf gegen Industriespionage nicht zu ihren prioritären Herausforderungen, während der Verfassungsschutz nur einen Teil des Problems, nämlich die Bekämpfung systematischer Wirtschaftsspionage durch nicht befreundete Staaten, angeht. Aufgrund der vorherrschenden Schweige- und Stillhaltekultur muss dem deutschen Wirtschaftsraum hier ein *mangelndes institutionelles Sicherheitsbewusstsein* attestiert werden.

Die Konsequenzen dieses Mangels zeigen sich an den von den Unternehmen praktizierten Sicherheitsmaßnahmen, die mangels einer zentralen Planung ganzheitlicher, d.h. sowohl IT-Sicherheit, als auch Objektsicherheit, Prozesssicherheit und Personalsensibilisierung einbeziehender Sicherheitskonzepte, oft eklatante Lücken aufweisen. Neben dem fehlenden Sicherheitsbewusstsein können die Gründe dafür auch in den unkalkulierbaren Rückflüssen einer professionellen Sicherheitsberatung liegen.

Diesem Trend stehen jedoch inzwischen einige mit Landesmitteln finanzierte Beratungsangebote mit thematisch begrenztem Fokus entgegen. So bietet zum Beispiel eine Initiative, die vom Landesministerium für Innovation, Wissenschaft und Forschung NRW in Zusammenarbeit mit dem Verband für Sicherheit in der Wirtschaft NRW getragen wird, seit Ende 2007 eine kostenlose Vor-Ort-Prüfung der IT-Sicherheit nordrhein-westfälischer Unternehmen an und hilft bei der Vermittlung geeigneter Dienstleister zur Erarbeitung von IT-Schutzkonzepten (Landesinitiative secure-it.nrw 2007). Des Weiteren bemühen sich sowohl die Verfassungsschutzbehörden als auch das Bundesamt für Sicherheit in der Informationstechnik mit vertraulichen Beratungs- und Zertifizierungsangeboten um das Vertrauen der Bürger (Bundesamt für den Verfassungsschutz 2006: 22; Bundesamt für Sicherheit in der Informationstechnik 2006: 2). Auch bilden sich derzeit vermehrt private Sicherheitsberatungs- und Risikomanagementunternehmen (Reppesgaard 2007). Mehr als 30% der deutschen Unternehmen zogen in Fällen nicht-autorisierter Informationsabflüsse private Spezialisten hinzu (Corporate Trust 2007: 29). Ob diese Entwicklung jedoch den Beginn einer Trendwende im Sicherheitsbewusstsein des deutschen Wirtschaftsraumes markiert bleibt abzuwarten.

7 Literaturverzeichnis

7.1 Wissenschaftliche Beiträge

Alberts, David S./Papp, Daniel S. (Hg.) (1997): *The Information Age: An Anthology on its Impact and Consequences*, CCRP Publication Series http://www.dodccrp. org/files/ Alberts_Anthology_I.pdf (20.02.2008).

Center for International Development at Harvard University (o.J.): „Readiness for the Networked World: Glossary of Terms“, http://cyber.law.harvard.edu/ readinessguide/glossary.html (20.02.2008).

Cornish, Derek B./Clarke, Ronald V. (1986): *The Reasoning Criminal – Rational Choice Perspectives on Offending*, New York: Springer.

Corporate Trust (2007): „Studie: Industriespionage – Die Schäden durch Spionage in der deutschen Wirtschaft“, http://bc1.handelsblatt.com/news/loadbin/Show Image.aspx? img=1567932 (10.01.2008).

d'Aveni, Richard A. (1994): *The Art of Hypercompetition*, New York: The Free Press.

Deppe, Jens Johannes (2000): „Über Pressefreiheit und Zensurverbot in der Rußländischen Föderation: Eine Untersuchung über die gesetzliche und tatsächliche Ausgestaltung der verfassungsrechtlichen Freiheitsgarantie“, http://www. sub.uni-hamburg.de/ opus/volltexte/2000/215/html/vi6.htm (24.04.2008).

Eck, Wim van (1985): „Electromagnetic Radiation from Video Display Units: an Eavesdropping Risk?“, *Computers & Security*, 4 (4), 269-286.

Encyclopædia Britannica (o.J.): „Espionage“, www.britannica.com/eb/article-9033028/ espionage (11.02.2008).

Fan, Ying (2002): „Questioning Guanxi: Definition, Classification and Implications“, *International Business Review*, 11 (5), 543-561.

Federation of American Scientists (o.J.): „The Intelligence Cycle“, http://www.fas.org/irp/ cia/product/facttell/intcycle.htm (07.04.2008).

Gregory, Sean (1997): „Economic Intelligence in the Post-Cold War Era: Issues for Reform“, http://www.fas.org/irp/eprint/snyder/economic.htm (20.03.2008).

Gutenberg, Erich (1983[24]): *Grundlagen der Betriebswirtschaftslehre, Erster Band: Die Produktion*, Berlin: Springer.

Harbich, Peter (2006): *Die wachsende Bedeutung privater Akteure im Bereich der Intelligence. Private Akteure als Quellen, Abnehmer, Konkurrenten und Kooperationspartner staatlicher Nachrichtendienste* (AIPA 3/2006), http://www.politik.uni-koeln.de/jaeger/ downloads/aipa0306.pdf (26.03.2008).

Henderson, Robert D'A. (2003): *Brassey's International Intelligence Yearbook: 2003 Edition,* New York: Brassey's.

Homann, Frank/Karabulut, Yücel/Voss, Marco/Fraikin, Falk (2005): *Security and Trust in Public eProcurement* (Technical Report No. TUD-CS-2005-4), http://www. ito.tu-darmstadt.de/publs/pdf/Security%20and%20Trust%20in%20public% 20eProcurement.pdf (19.03.2008).

Jäger, Thomas und Beckmann, Rasmus (2007): „Die internationalen Rahmenbedingungen deutscher Außenpolitik“, in: Thomas Jäger/Alexander Höse/Kai Oppermann (Hg.): *Deutsche Außenpolitik – Sicherheit, Wohlfahrt, Institutionen und Normen*, Wiesbaden: VS Verlag.

Jehle, Egon/Müller, Klaus/Michael, Horst (1994): *Produktionswirtschaft*, Heidelberg: Verlag Recht und Wirtschaft.

Keohane, Robert O./Nye, Joseph S. (1998): „Power and Interdependence in the Information Age“, *Foreign Affairs*, 77 (5), 81-94.

Kober, Stanley (1992): *The CIA as Economic Spy: The Misuse of U.S. Intelligence after the Cold War* (Cato Policy Analysis No. 185), http://www.cato.org/pubs/pas/pa-185.html (18.03.2008).

Kononczuk, Wojciech (2006): *The 'Yukos Affair', its Motives and Implications* (Prace OSW / CES Studies August 2006) http://www.osw.waw.pl/files/PRACE_25.pdf (13.03.2008).

KPMG (2006): *Studie 2006 zur Wirtschaftskriminalität in Deutschland*, http://www.kpmg.de/ docs/060626 _ Studie_ 2006_ Wirtschaftskriminalitaet _de.pdf (31.03.2008).

Kuhn, Markus (2002): *Optical Time-Domain Eavesdropping Risks of CRT-Displays* (IEEE Symposium on Security and Privacy), http://www.cl.cam.ac.uk/~mgk25/ieee02-optical.pdf (11.04.2008).

Lallana, Emmanuel C./Uy, Margaret N. (2003): *The Information Age* (e-Asean Task Force UNDP-APDIP Mai 2003), http://www.apdip.net/publications/iespprimers/eprimer-infoage.pdf (20.02.2008).

Lowenthal, Mark M. (2003²): *Intelligence: From Secrets to Policy*, Washington, DC: CQ Press.

Lux, Christian/Peske, Thorsten (2002a): *Competitive Intelligence und Wirtschaftsspionage*, Wiesbaden: Betriebswirtschaftlicher Verlag Dr. Th. Gabler.

Lux, Christian/Peske, Thorsten (2002b) „Competitive Intelligence“, *Zeitschrift für Sicherheit der Wirtschaft*, 2002/1, 15-17.

Mellon, Jérôme (2001): *Assessment of KGB's Intelligence-Gathering Successfulness in the West During the Period of 1954 to 1991*, http://cv.jmellon.com/kgb.pdf (09.04.2008).

Michaeli, Rainer (2004): „Competitive Intelligence in Germany", *Journal of Competitive Intelligence and Management*, 2 (4), 1-6.

Michaeli, Rainer (2006): *Competitive Intelligence: Strategische Wettbewerbsvorteile erzielen durch systematische Konkurrenz-, Markt- und Technologieanalysen*, Berlin: Springer.

Mitnick, Kevin D./Simon, William L. (2002): *The Art of Deception – Controlling the Human Element of Security*, Indianapolis, IN: Wiley Publishing.

Muscatell, Ralph P. (1983): "Laser Microphone – United States Patent 4412105", http://www.freepatentsonline.com/4412105.html (11.04.2008).

Nagaraja, Shishir/Anderson, Ross (2009): *The Snooping Dragon: Social-Malware Surveillance of the Tibetan Movement* (Technical Report Number 746), Cambridge: University of Cambridge http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf (29.03.2008).

Pfaff, Dietmar (2005): *Competitive Intelligence in der Praxis*, Frankfurt a. M.: Campus.

Robins, Nick (2006): *The Corporation that Changed the World: How the East India Company Shaped the Modern Multinational*, London: Pluto Press.

Rustmann, Frank W., (2002): *CIA, Inc. – Espionage and the Craft of Business Intelligence*, Washington, DC: Brassey's.

Sagdeev, Roald Z. (1994): *The making of a Soviet Scientist*, Hoboken, NY: John Wiley & Sons.

Schmidt-Eenboom (1996): *Die schmutzigen Geschäfte der Wirtschaftsspione*, Leipzig: Admos Media.

Seidenberg, Ulrich (1998): *Ist Information als eigenständiger Produktionsfaktor aufzufassen?*, http://www.uni-siegen.de/fb5/wiwi/prod/downloads/pfaktinf.pdf (20.02.08)

Shulsky, Abram N./Schmitt, Gary (2002[3]): *Silent Warfare: Understanding the World of Intelligence*, New York: Brassey's.

Strong, Thompson J. (1994): „Tilting with Machiavelli: Fighting Competitive Espionage in the 1990s", *International Journal of Intelligence and Counterintelligence*, 7 (2), 161-174.

Sule, Satish (2006): *Spionage - Völkerrechtliche, nationalrechtliche und europarechtliche Bewertung staatlicher Spionagehandlungen unter besonderer Berücksichtigung der Wirtschaftsspionage*, Baden-Baden: Nomos.

Többens, Hans W. (2000): „Wirtschaftsspionage und Konkurrenzausspähung in Deutschland", *Neue Zeitschrift für Strafrecht*, 10, 505-512.

Toffler, Alvin (1980): *The Third Wave*, New York: Morrow.

Weiss, Gus W. (1996): „The Farewell Dossier", *Studies in Intelligence*, 39 (5), 121-126.

Westerfield, H. Bradford (1996): "America and the World of Intelligence Liaison", *Intelligence and National Security*, 11 (3), 523-560.

7.2 Journalistische Beiträge

Bigalke, Silke (2007): „Tricks der Wirtschaftsspione: Die Putzfrau hat leichtes Spiel", *Spiegel Online*, 01.10.2007, http://www.spiegel.de/wirtschaft/0,1518,507972,00.html (11.04.2008).

Dahlkamp, Jürgen / Rosenbach, Marcel / Schmitt, Jörg / Stark, Holger / Wagner, Wieland (2007): „Prinzip Sandkorn“, Spiegel, 35/2007, 18-34.

Dunsch, Jürgen (2007): „Luftnummer“, Frankfurter Allgemeine Zeitung , 16.01.2007, 18, http://www.faz.net/s/RubEC1ACFE1EE274C81BCD3621EF555C83C/Doc~ED3EB4882CD94427CAE87BB5A7F366093~ATpl~Ecommon~Scontent.html (28.04.2008).

Ellwart, Timm (2000): „Wenn Freunde spionieren: Amerikanischer Geheimdienst in Deutschland aktiv“, ZDF Frontal, 17.05.2007, http://hp.kairaven.de/miniwahr/echelon-frontal17052000.html (22.03.2008).

Heimbrecht, Jörg/Schultze, H. C. (1998): „Plusminus - Wirtschaftsspionage“, Sendemanuskript zum Beitrag „Lauschangriff“ aus dem Jahr 1998, http://hp.kairaven.de/miniwahr/enercon.html (20.03.2008).

Kramer, Andrew E. (2007): “Former Russian Spies Are Now Prominent in Business”, The New York Times, 18.12.2007, http://www.nytimes.com/2007/12/18/business/worldbusiness/18kgb.html?_r=2&oref=slogin&oref=slogin (07.04.2008).

Kuhn, Markus (2006): “Video eavesdropping demo at CEBIT 2006”, 09.03.2006, http://www.lightbluetouchpaper.org/2006/03/09/video-eavesdropping-demo-at-cebit-2006/ (11.04.2008).

o.V. (1996): „Der lautlose Krieg: Abgehört“, Berliner Zeitung, 22.01.1996, http://www.berlinonline.de/berliner-zeitung/archiv/.bin/dump.fcgi/1996/0122/chefredaktion/0142/index.html (19.03.2008).

o.V. (2007): „Chinesische Akademiker erstatten Anzeige gegen Spiegel-Autoren“, Spiegel, 23.11.2007, http://spiegelkritik.de/2007/11/23/chinesische-akademiker-erstatten-anzeige-gegen-spiegel-autoren/ (19.03.2008).

o.V. (2008a): „Verfassungsschutz will Industriespionage bekämpfen“, EpochTimes Online, 06.01.2008, http://www.epochtimes.de/articles/2008/01/06/220023.html (04.04.2008).

o.V. (2008b): „Wirtschaft fürchtet Anstieg von Industriespionage“, der Tagesspiegel, 11.03.2008, http://www.tagesspiegel.de/wirtschaft/Industriespionage;art271,2492469 (15.04.2008).

Reppesgaard, Lars (2007): „Wissen Sie, mit wem Sie’s zu tun haben?“, http://www.corporate-trust.de/pm-070511.pdf (23.04.2008).

Rifkin, Glenn (1996): „The Art of Hypercompetition“, Strategy + Buisness, http://www.strategy-business.com/press/16635507/14886 (16.01.2008).

Saffire, William (2004): „The Farewell Dossier“, http://www.ranum.com/security/homeland_security/editorials/Farewell_Dossier/nyt_article.html (13.03.2008).

Sontheimer, Michael (1999): „Das Ende einer Legende“, http://www.stasiopfer.de/content/view/104/191/ (07.04.2008).

Tsuruoka, Doug (1997): „Asian Perceptions of What is and is not Legal in Economic Intelligence Collection“, http://www.oss.net/dynamaster/file_archive/040319/13f69584f1e73bcb6abdf06fd196d2bc/OSS1997-04-06.pdf (18.03.2008).

Ulfkotte, Udo (1999): *Marktplatz der Diebe – Wie die Wirtschaftsspionage deutsche Unternehmen ausplündert und ruiniert*, München: Bertelsmann.

Whittacker, Jason (2003): *The Cyperspace Handbook*, New York: Routledge.

Woolsey, R. James (2000): „Why We Spy on our Allies“, The Wall Street Journal, 17.03.2000, http://cryptome.org/echelon-cia2.htm (23.04.2008).

Ya, Luo (2005): „Exklusiv-Interview mit dem chinesischen Diplomaten und Überläufer Chen Yonglin“, EpochTimes Online, 19.06.2005, http://www.epochtimes.de/articles/ 2005/06/19/3500.html (19.03.2008).

7.3 Literarische Beiträge

Forster, Edward Morgan (1909): *The Machine Stops*, http://c-wd.net/machine/ (20.02.2008).

7.4 Mitteilungen staatlicher Stellen

Bundesamt für Sicherheit in der Informationstechnik (o.J.): „IT-Grundschutz-Kataloge“, http://www.bsi.bund.de/gshb/deutsch/index.htm (15.04.2008).

Bundesamt für Sicherheit in der Informationstechnik (2006): „Jahresbericht 2005“, http://www.bsi.bund.de/literat/jahresbericht/jahresbericht2005/bsi_jahresbericht2005.pdf (31.03.2008).

Bundesamt für Sicherheit in der Informationstechnik (2007): „Bericht zur Lage der IT-Sicherheit in Deutschland 2007“, http://www.bsi.de/literat/lagebericht/lagebericht2007.pdf (31.03.2008).

Bundesamt für Sicherheit in der Informationstechnik (2008): „BSI TL-03305 – Für staatliche VS zugelassene abstrahlsichere /-arme Hardware“, http://www.bsi.bund.de/literat/ doc/vshardw/TL_03305.pdf (11.04.2008).

Bundesamt für Verfassungsschutz (2006): „Wirtschaftsspionage - Information und Prävention“, http://www.verfassungsschutz.de/download/SAVE/broschuere_0312_wirtschaftsspionage.pdf (24.04.2008).

Bundesamt für Verfassungsschutz (2007): „Verfassungsschutzbericht 2006“, http://www.verfassungsschutz.de/download/SAVE/vsbericht_2006.pdf (24.04.2008).

Bundesamt für Verfassungsschutz (2008): „Verfassungsschutz - Was wir für sie tun“, http://www.verfassungsschutz.de/download/SHOW/broschuere_0803_was_wir_tun.pdf (27.03.2008).

Bundesanstalt für Arbeitsschutz (2007): „Verbraucherleitfaden: Schutz vor Produkt- und Markenpiraterie“, http://www.baua.de/nn_21604/de/Publikationen/Broschueren/A58,xv=vt.pdf (08.02.2008).

Bundeskriminalamt (2005): „Bundeslagebild Wirtschaftskriminalität 2004“, http://www.bka.de/lageberichte/wi/wikri_2004.pdf (31.03.2008).

Bundeskriminalamt (2007): „Polizeiliche Kriminalstatistik 2006“, http://www.bka.de/ pks/pks2006/download/pks-jb_2006_bka.pdf (28.04.2008).

Bundeskriminalamt (2008): „Aktuelle Herausforderungen in der Kriminalitätsbekämpfung - Strategien des Bundeskriminalamtes“, http://www.bka.de/pressemitteilungen/ 2008/pm080328.html (31.03.2008).

Bundesministerium des Innern (2005): „Bundesgesetzblatt 2005, Teil 1, Nr. 15“, http://217.160.60.235/BGBL/bgbl1f/bgbl105s0519.pdf (15.04.2008).

Bundesministerium des Innern (2007): „Asiatische Spionage kostet Deutschland 20 Milliarden Euro“, http://www.bmi.bund.de/nn_122688/Internet/Content/Nachrichten/Medienspiegel/2007/10/Hanning__BZ__am__Sonntag.html (07.04.2008).

Bundesministerium für Wirtschaft und Technologie (2007): „Welthandel 2007: Deutschland bleibt Exportweltmeister“, http://www.bmwi.de/BMWi/Navigation/Presse/pressemitteilungen, did=227964.html (28.04.2008).

Bundeszollverwaltung (2006): „Jahresbericht Gewerblicher Rechtschutz 2006“, http://www.zoll.de/e0_downloads/d0_veroeffentlichungen/v4_gwr_jahresbericht_2006.pdf (09.02.2008).

Europäisches Parlament (2001): „Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))“, http://www.au.af.mil/au/awc/ awcgate/echelon/ echelon_eur_parliament.pdf (24.04.2008).

Europäisches Patentamt (2006): „European patents granted in 2006“, http://documents.epo. org/projects/babylon/eponet.nsf/0/ 5C6F692D32BB94D4C1257314004A7BA0/$File/European_patents_granted_2006_applicants_residence.pdf 06.03.2008).

Innenministerium des Landes Nordrhein-Westfalen (2001): „Gemeinsame Erklärung über die Bildung einer Sicherheitspartnerschaft gegen Wirtschaftsspionage / Wirtschaftskriminalität“ http://www.im.nrw.de/sch/620.htm (30.03.2008).

Innenministerium des Landes Nordrhein-Westfalen (o.J.): „Ferner Osten“ http://www.im. nrw.de/sch/615.htm (18.03.2008).

Office of the National Counterintelligence Executive (o.J.): CI Reader: „An american revolution into a new millenium“, Volume 4, Chapter 3, http://www.ncix. gov/ issues/CI_Reader/Vol4/Vol4Chap3.pdf (19.03.2008).

Statistisches Bundesamt (2007a): „Inlandsproduktsberechnung – Wichtige gesamtwirtschaftliche Größen“, http://www.destatis.de/jetspeed/portal/cms/Sites/

destatis/Internet/DE/Content/Statistiken/VolkswirtschaftlicheGesamtrechnungen/Inlandsprodukt/Tabellen/Content75/Gesamtwirtschaft,templateId=renderPrint.psml (20.01.2008).

Statistisches Bundesamt (2007b): „Wirtschaftswachstum - Bruttoinlandsprodukt preisbereinigt, verkettet“, http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Grafiken/VolkswirtschaftlicheGesamtrechnungen/Diagramme/Wachstum,templateId=renderPrint.psml (20.01.2008).

Statistisches Bundesamt (2007c): „Konjunkturmotor Export“, http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Content/Publikationen/Querschnittsveroeffentlichungen/WirtschaftStatistik/Aussenhandel/KonjunkturmotorExport,property=file.pdf (28.04.2008).

The White House (1995): „A National Security Strategy of Engagement and Enlargement“, http://www.maxwell.af.mil/au/awc/awcgate/nss/nss-95.pdf (28.04.2008).

US-Intelligence Community (o.J.a): „The Intelligence Process“, http://www.intelligence.gov/2-business.shtml (11.02.2008).

US-Intelligence Community (o.J.b): „Collection“, http://www.intelligence.gov/2-business_cycle2.shtml (11.02.2008).

US-Joint Chiefs of Staff (2000): “Joint Intelligence”, http://www.fas.org/irp/doddir/dod/jp2_0.pdf (08.04.2008).

7.5 Mitteilungen von Unternehmen und Verbänden

Aktion Plagiarius (o.J.): „Innovation vs. Imitation“, http://www.plagiarius.com/d_index.html (09.02.2008).

Arbeitsgemeinschaft für Sicherheit der Wirtschaft (2005): „Anmerkungen zur Sicherheitslage der deutschen Wirtschaft 2004 / 2005“, http://www.asw-online.de/ downloads/Anmerkungen-zur-Sicherheitslage-der-deutschen-Wirtschaft20043.pdf (01.03.2008).

ATTAC (2006): „Globalisierung - Eine andere Welt ist möglich“, http://www.attac.de/ themen/globalisierung/Globalisierung.php (27.04.2008).

Corsair (2008): „Flash Voyager“, http://www.corsair.com/products/voyager.aspx (21.02.2008).

CTC International Group (o.J.a): „Chairman and Founder“ sowie „Principal Associates“, http://www.ctcintl.com/executive.shtml (26.03.2008).

CTC International Group (o.J.b): „Corporate Profile - Our Company“, http://www. ctcintl. com/ourcompany.shtml (26.03.2008).

GeoEye (2007): „GeoEye Imagery Products: GEOEYE-1“, http://www.geoeye.com/ products/imagery/geoeye1/default.htm (28.04.2008).

Global Security (o.J.): „Ministry of State Security [MSS] - Guojia Aquan Bu [Guoanbu]“ http://www.globalsecurity.org/intell/world/china/mss.htm (18.03.2008).

HTCS Löbl GbR (o.J.a): „Raumüberwachung“, http://www.spiontechnik.de/ ?lang=DEU, anschließend Klick auf Audioüberwachung, dann auf Raumüberwachung, (11.04.2008).

HTCS Löbl GbR (o.J.b): „Exportbedingungen“, http://www.spiontechnik.de/ ?lang=DEU, anschließend Klick auf Exportbedingungen (11.04.2008)

Intel (o.J.): „Moore's Law“, http://www.intel.com/technology/mooreslaw/index.htm (15.04.2008).

Landesinitiative secure-it.nrw (2007): “Neue Allianz gegen Wirtschaftsspionage und Datenklau bietet Mittelstand kostenloses Sicherheitspaket”, http://openpr.de/ news/167993/Neue-Allianz-gegen-Wirtschaftsspionage-und-Datenklau-bietet-Mittelstand-kostenloses-Sicherheitspaket.html (19.12.2007).

LGT Gruppe (2008): “Information an unsere Kunden und Interessierte”, http://www.lgt.com/de/wir_ueber_uns/datendiebstahl_2002/index.html (01.03.2008).

Microsoft Technet (2002): “Danger: Remote Access Trojans”, http://www.microsoft.com/technet/security/alerts/info/virusrat.mspx (10.04.2008).

Mitnick Security Consulting (2003): „Kevin Mitnick - Testimony Before the House Financial Services Commitee“, http://www.kevinmitnick.com/media/HFSC-Testimony-20030403.pdf

Saar-Uni-Presseteam (2008): “Pressemitteilung - Verräterische Reflexionen: Wie eine Teekanne Geheimnisse preisgeben kann”, http://idw-online.de/pages/de/news246690%20 (11.04.2008).

Western Digital (2008): „My Book Premium Edition II“, http://www.wdc.com/de/products/ Products.asp?DriveID=342 (21.02.2008).

Wikimedia Foundation (2008): „Wikipedia-Statistik: Gesamtgröße aller Artikel“, http://stats.wikimedia.org/DE/TablesDatabaseSize.htm (21.02.2008).

7.6 Gesetze und Abkommen

Aktiengesetz (AktG)

§404 Verletzung der Geheimhaltungspflicht

http://www.gesetze-im-internet.de/aktg/__404.html (24.04.2008).

Betriebsverfassungsgesetz (BetrVG)

§120 Verletzung von Geheimnissen

http://www.gesetze-im-internet.de/betrvg/__120.html (24.04.2008).

Economic Espionage Act (EEA 1996)

§1831 Economic Espionage

http://www.law.cornell.edu/uscode/18/usc_sec_18_00001831----000-.html

§1832 Theft of trade secrets

http://www.law.cornell.edu/uscode/18/usc_sec_18_00001832----000-.html

(24.04.2008).

Gesetz betreffend die Erwerbs- und Wirtschaftsgenossenschaften (GenG)

§151 Verletzung der Geheimhaltungspflicht

http://www.gesetze-im-internet.de/geng/__151.html (24.04.2008).

Gesetz betreffend die Gesellschaften mit beschränkter Haftung (GmbHG)

§85

http://www.gesetze-im-internet.de/gmbhg/__85.html (24.04.2008).

Gesetz gegen den unlauteren Wettbewerb (UWG)

§17 Verrat von Geschäfts- und Betriebsgeheimnissen

http://www.gesetze-im-internet.de/uwg_2004/__17.html

§18 Verwertung von Vorlagen

http://www.gesetze-im-internet.de/uwg_2004/__18.html

§19 Verleiten und Erbieten zum Verrat

http://www.gesetze-im-internet.de/uwg_2004/__19.html

(24.04.2008).

Gesetz über den Bundesnachrichtendienst (BNDG)

§1 Organisation und Aufgaben

http://www.gesetze-im-internet.de/bndg/__1.html (24.04.2008).

Gesetz über den militärischen Abschirmdienst (MADG)

§1 Aufgaben

http://bundesrecht.juris.de/madg/__1.html

§2 Zuständigkeit in besonderen Fällen

http://bundesrecht.juris.de/madg/__2.html

(24.04.2008).

Gesetz über die Beaufsichtigung der Versicherungsunternehmen (VAG)

§138 Verletzung der Geheimhaltungspflicht

http://www.gesetze-im-internet.de/vag/__138.html (24.04.2008).

Gesetz über die Rechnungslegung von bestimmten Unternehmen und Konzernen (PublG)

§19 Verletzung der Geheimhaltungspflicht

http://www.gesetze-im-internet.de/publg/__19.html (24.04.2008).

Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (BVerfSchG)

§3 Aufgaben der Verfassungsschutzbehörden

http://www.gesetze-im-internet.de/bverfschg/__3.html (24.04.2008).

Grundgesetz für die Bundesrepublik Deutschland (GG)

Artikel 87

http://www.gesetze-im-internet.de/gg/art_87.html (24.04.2008).

Handelsgesetzbuch (HGB)

§333 Verletzung der Geheimhaltungspflicht

http://www.gesetze-im-internet.de/hgb/__333.html (24.04.2008).

Strafgesetzbuch (StGB)

§5 Auslandstaten gegen inländische Rechtsgüter

http://www.gesetze-im-internet.de/stgb/__5.html

§93 Begriff des Staatsgeheimnisses

http://www.gesetze-im-internet.de/stgb/__93.html

§94 Landesverrat

http://www.gesetze-im-internet.de/stgb/__94.html

§95 Offenbaren von Staatsgeheimnissen

http://www.gesetze-im-internet.de/stgb/__95.html

§96 Landesverräterische Ausspähung, Auskundschaften von Staatsgeheimnissen

http://www.gesetze-im-internet.de/stgb/__96.html

§97 Preisgabe von Staatsgeheimnissen

http://www.gesetze-im-internet.de/stgb/__97.html

§97a Verrat illegaler Geheimnisse

http://www.gesetze-im-internet.de/stgb/__97a.html

§97b Verrat in irriger Annahme eines illegalen Geheimnisses

http://www.gesetze-im-internet.de/stgb/__97b.html

§98 Landesverräterische Agententätigkeit

http://www.gesetze-im-internet.de/stgb/__98.html

§99 Geheimdienstliche Agententätigkeit

http://www.gesetze-im-internet.de/stgb/__99.html

(24.04.2008).

Sozialgesetzbuch (SGB), Neuntes Buch (IX)

§130 Geheimhaltungspflicht

http://bundesrecht.juris.de/sgb_9/index.html (24.04.2008).

Wiener Übereinkommen vom 24. April 1963 über konsularische Beziehungen

http://www.datenbanken.justiz.nrw.de/ir_htm/wuek_24-04-1963.htm

(24.04.2008).

7.7 Eigene empirische Untersuchungen

Interviewreihe im Rahmen der Messe Medica in Düsseldorf am 16. November 2007

Fachbereich der Messe:	Medizintechnik
Methode:	Strukturiertes Interview
Anzahl befragter Aussteller:	17

Interviewreihe im Rahmen der Messe NanoSolutions in Frankfurt am 23. November 2007

Fachbereich der Messe:	Nanotechnologie
Methode:	Strukturiertes Interview
Anzahl befragter Aussteller:	18

Interviewreihe im Rahmen der Messe Euromold in Frankfurt am 7. Dezember 2007

Fachbereich der Messe:	Werkzeugmaschinen- und Prototypenbau
Methode:	Strukturiertes Interview
Anzahl befragter Aussteller:	15

Alle Befragungen wurden – unter Zusicherung der vertraulichen Behandlung aller gemachten Angaben – im persönlichen Gespräch mit ausgewählten Unternehmensvertretern durchgeführt. Zur Protokollierung der Ergebnisse wurden Fragebögen analog zu dem im Anhang gezeigten Musterfragebogen verwendet.

8 Anhang

8.1 Anhang 1: Auswertung der Interviewdaten

Im Verlaufe des strukturierten Interviews gestellte Kernfragen	Gesamtergebnis			Ergebnisse der einzelnen Befragungen									
				Medica 2007			nanoSolutions 2007			Euromold			
	Ja	Nein	n	Ja	Nein	n	Ja	Nein	n	Ja	Nein	n	
"Fühlen Sie sich durch Industriespionage gefährdet?"	58%	42%	50	41%	59%	17	67%	33%	18	67%	33%	15	
"Werden neue Mitarbeiter bei Eintritt in das Unternehmen über die Risiken durch Industriespionage aufgeklärt?"	47%	53%	43	47%	53%	15	53%	47%	17	36%	64%	11	
"Wird Ihr Messepersonal über die Risiken einer solchen Veranstaltung aufgeklärt?"	32%	68%	47	38%	62%	16	33%	67%	18	23%	77%	13	
"Besteht in Ihrem Unternehmen ein System schriftlich festgelegter Sicherheitsmaßnahmen zur Abwehr von Industriespionage?"	50%	50%	40	54%	46%	13	47%	53%	17	50%	50%	10	
"Besteht eine Zutrittskontrolle zu Ihrem Firmengelände / Firmengebäude?"	86%	15%	48	87%	13%	15	78%	22%	18	93%	7%	15	
"Bestehen innerhalb ihres Geländes / Gebäudes gesondert gesicherte Bereiche?"	59%	41%	47	93%	7%	15	35%	65%	17	53%	47%	15	
"Besteht eine Kennzeichnungspflicht für vertrauliche Dokumente?"	72%	28%	42	83%	17%	12	87%	13%	15	47%	53%	15	
"Findet bei Einstellungen für gehobene Positionen eine Sicherheitsüberprüfung statt?"	44%	56%	34	67%	33%	12	38%	62%	13	22%	78%	9	
"Achten Sie auf die Sicherheitsstandards Ihrer Zulieferbetriebe?"	43%	57%	30	58%	42%	12	33%	67%	9	33%	67%	9	
"Enthalten Ihre Arbeitsverträge Geheimhaltungsvereinbarungen?"	95%	5%	47	93%	7%	15	94%	6%	18	100%	0%	14	
"Enthalten Ihre Arbeitsverträge ein Wettbewerbsverbot nach Beendigung des Beschäftigungsverhältnisses?"	51%	49%	45	50%	50%	14	50%	50%	16	53%	47%	15	
"War Ihr Unternehmen schon einmal von Industriespionage betroffen?"	32%	68%	50	41%	59%	17	22%	78%	18	33%	67%	15	

n - Spalte: Anzahl der auf die Frage erhaltenen Antworten

8.2 Anhang 2: Mutmaßliche Fälle von Industriespionage

Die im Rahmen der Interviewreihen befragten Unternehmensvertreter führten als Beispiele für mutmaßliche Fälle von Industriespionage die folgenden Begebenheiten an:

- Ein Mitarbeiter hatte erfolgreich Kundenlisten an interessierte Mitbewerber verkauft, in mehreren Fällen kam es zu Kundenverlust
- Die Homepage eines chinesischen Herstellers von Kompositmaterialien versucht einen Trojaner auf dem Rechner eines Mitarbeiters zu installieren
- Versuch der Bestechung von Mitarbeitern eines Messtechnikunternehmens mit dem Ziel, an im Auftrag eines Kunden erstellte Messreihen zu gelangen
- Im Zuführungsschacht eines Dokumentenshredders wurde ein mit einem UMTS-Sender verbundener Scanner gefunden
- Auf einem Kongress infizierte das Laptop, das einen zu Vortragszwecken aufgestellten Beamer steuerte, den USB-Stick eines Vortragenden mit Spyware
- Ein Mitarbeiter bot inländischen Mitbewerbern seines Unternehmens (von seinem Firmenrechner aus) chemische Rezepturen zum Kauf an
- Im Rahmen einer öffentlichen Ausschreibung durch eine französische Regierungsstelle reichte ein Unternehmen ein in technischer Hinsicht sehr detailliertes Angebot ein, erhält den Zuschlag jedoch nicht. Wenige Monate später brachte ein französischer Mitbewerber ein technologisches gleichartiges Produkt auf den Markt.
- Mehrere Unternehmen mussten sich einer Reihe auffällig gezielter Abwerbeversuche erwehren.
- Weiterhin wurde von mehreren Aufsehen erregenden Diebstahlsfällen berichtet, die ähnlich der Wirtschafts- und Industriespionage als Vorbereitung von Produktpiraterie gedient haben könnten: Im ersten Fall wurde eine technische Weltneuheit in der Nacht vor ihrer erstmaligen Präsentation auf der Medica 1994 von dem Messestand des ausstellenden Unternehmens

entwendet. Im zweiten Fall wurde einem Unternehmen innerhalb eines Jahres auf drei unterschiedlichen Messen und Kongressen je ein baugleiches Exemplar eines bestimmten Kernspintomographen gestohlen.

8.3 Anhang 3: Beispiel eines Interviewbogens

Fragebogen zum Thema

„Analyse der Bedrohung des deutschen Wirtschaftsraums durch Wirtschafts- und Industriespionage“

durchgeführt auf der „NanoSolutions“ in Frankfurt a. M. am 23. November 2007
im Rahmen der Diplomarbeit von Daniel Wolff an der Universität Köln

Angaben zu Person und Unternehmen:

Name: .....

Position im Unternehmen: .....

Unternehmen: .....

Mitarbeiter: ..... Umsatz: .....

Einschätzung der Sicherheitslage des Unternehmens:	**Ja**	**Nein**
Sehen Sie Ihr Unternehmen als durch Industriespionage gefährdet?	○	○

Wenn ja, warum? .....

.....

Gibt jemanden in ihrem Unternehmen, der allgemeine Sicherheitsmaßnahmen konzipiert?
(z. B.: Niemand, Sicherheitsbeauftragter, Sicherheitsabteilung, Fremdfirma)

.....

Wem ist dieser Instanz in der Firmenhierarchie direkt untergeordnet?
(z. B.: Vorstand, Geschäftsführer, Produktionsleiter, Werksleiter, außerhalb der Hierarchie)

.....

Wurden Sie bei Ihrem Firmeneintritt über die Gefahr durch Spionage aufgeklärt?	○	○

Wenn ja: Durch wen und in welcher Form? .....

.....

Wurden Sie vor dieser Veranstaltung über deren spezifische Gefahren aufgeklärt?	○	○

Gibt es in Ihrem Unternehmen ein System schriftlich festgelegter Sicherheitsmaßnahmen zur Abwehr von Industriespionage? ○ ○

Wenn ja: Welche der folgenden Maßnahmen sind im Einsatz?

- Zutrittskontrolle Firmengelände / -gebäude ○ ○
- Zutrittskontrolle gesicherter Bereiche auf dem Firmengelände? ○ ○
- Kennzeichnungspflicht vertraulicher Dokumente? ○ ○
- Sicherheitsüberprüfung vor Einstellung? ○ ○
- Routineüberprüfung von Zulieferern und Kooperationspartnern? ○ ○
- Vertragliche Geheimhaltungsvereinbarungen für Mitarbeiter? ○ ○
- Konkurrenzverbot für Mitarbeiter bei Firmenaustritt? ○ ○

Stehen Ihnen folgende Kommunikationsmittel auch kryptografisch gesichert zur Verfügung?

- Email ○ ○
- Telefon ○ ○
- Fax ○ ○

War Ihr Unternehmen schon einmal von Spionage betroffen? ○ ○

Wenn ja, wer waren die Täter? .....
(Falls bekannt, z.B. eigene Mitarbeiter, Konkurrenz, ausländischer Nachrichtendienst)

Wie wurde spioniert? .....
(Falls bekannt, z.B. Diebstahl, Abhöraktion, Abwerben von Mitarbeitern, Hacking-Angriff)

Falls Schaden entstanden ist, welcher Art war dieser? .....
(Z. B. Finanzielle Schäden, Imageschäden, verlorene Patentrechte, geschmälerte Marktzutrittschancen)

.....

Wurde Strafanzeige erstattet, und wenn ja mit welchem Ergebnis? .....

.....

Stehen Sie evtl. für weitere Rückfragen im Verlauf der Arbeit zur Verfügung? ○ ○

Möchten Sie nach Fertigstellung der Diplomarbeit ein Exemplar erhalten? ○ ○

Vielen Dank für Ihr Interesse!

In dieser Reihe sind bisher erschienen:

AIPA 2/2009 Daria W. Dylla: Die Theorie des doppelten Überlebensprinzips. Vom Machterhalt via rational choice zur Außenpolitik

AIPA 1/2009 Joachim Betz: Die Interaktion interner und externer Faktoren beim Wandel der indischen Außenpolitik

AIPA 4/2008 Jeannine Hausmann: Brasilien als neues Land in der Entwicklungszusammenarbeit

AIPA 3/2008 Rasmus Beckmann: Clausewitz, Terrorismus und die NATO-Antiterrorstrategie: Ein Modell strategischen Handelns

AIPA 2/2008 Martin Malek: Russland nach den Wahlen: Erste Amtszeit Medwedjews oder„dritte Amtszeit" Putins?

AIPA 1/2008 Corinna Walter: Bedrohungsperzeptionen und regionale Sicherheitskooperation in Südamerika am Fallbeispiel Cono Sur

AIPA 3/2007 Tillmann Höntzsch: Das Konzept der Zivil-Militärischen Kooperation (CIMIC) – Der Afghanistaneinsatz der Bundeswehr

AIPA 2/2007 Daria W. Dylla: Rational-Choice und das politische Issue Management: Die Gestaltung der politischen Agenda und ihre Rolle bei der Stimmenmaximierung

AIPA 1/2007 Mischa Hansel: '(Although) it's not Rocket Science': A Theoretical Concept for Assessing National Space Policies in Europe

AIPA 4/2006 Thomas Jäger/Kai Oppermann/Alexander Höse/Henrike Viehrig: Die Salienz außenpolitischer Themen im Bundestag. Ergebnisse einer Befragung der Mitglieder des 16. Deutschen Bundestages

AIPA 3/2006 Peter Harbich: Die wachsende Bedeutung privater Akteure im Bereich der Intelligence. Private Akteure als Quellen, Abnehmer,

Konkurrenten und Kooperationspartner staatlicher Nachrichtendienste

AIPA 2/2006 Anatol Adam: Die sicherheits- und verteidigungspolitischen Initiativen Brasiliens im Amazonasgebiet am Beispiel des SIPAM/SIVAM-Projekts

AIPA 1/2006 John Emeka Akude: Historical Imperatives for the Emergence of Development and Democracy: A Perspective for the Analysis of Poor Governance Quality and State Collapse in Africa

AIPA 4/2005: Lisa Sieger: International Mediation in Northern Ireland. An Analysis of the Influence of International Intermediaries on the Process and the Outcome of the Northern Irish Peace Process from 1994 to mid-2004

AIPA 3/2005: Thomas Jäger/Henrike Viehrig: Internationale Ordnung und transatlantische Wahrnehmungen: Die medial vermittelte Interpretation der Darfur-Krise in den USA, Deutschland, Frankreich und Großbritannien

AIPA 2/2005: Gunther Hauser: The Mediterranean Dialogue: A Transatlantic Approach

AIPA 1/2005: Thomas Jäger/Henrike Viehrig: Gesellschaftliche Bedrohungswahrnehmung und Elitenkonsens. Eine Analyse der europäischen Haltungen zum Irakkrieg 2003

AIPA 4/2004: Stephan Klingebiel/Katja Roehder: Militär und Entwicklungspolitik in Post-Konflikt-Situationen

AIPA 3/2004: Conrad Schetter: Kriegsfürstentum und Bürgerkriegsökonomien in Afghanistan

AIPA 2/2004: Andrea K. Riemer/Gunther Hauser: Die Nationale Sicherheitsstrategie der USA und die Europäische Sicherheitsstrategie: Ein Vergleich des Unvergleichbaren

AIPA 1/2004: Kai Oppermann: Blair's U-turn – Das britische Referendum über eine europäische Verfassung

AIPA 4/2003: Andrea Szukala (Hrsg.): Anti-Terror-Politik in Deutschland

AIPA 3/2003: Andrea Szukala (Hrsg.): Krieg im Irak – Krieg gegen den Terror?

AIPA 2/2003: Kai Oppermann: New Labour und der Euro – Die Imperative des innerstaatlichen politischen Wettbewerbs

AIPA 1/2003: Elke Krahmann: The Privatization of Security Governance: Developments, Problems, Solutions