Die wachsende Bedeutung privater Akteure im Bereich der Intelligence: private Akteure als Quellen, Abnehmer, Konkurrenten und Kooperationspartner staatlicher Nachrichtendienste

Harbich, Peter

Arbeitspapier / working paper

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

AIPA 3/2006

Arbeitspapiere zur Internationalen Politik
und Außenpolitik

Peter Harbich

Die wachsende Bedeutung privater Akteure im Bereich der Intelligence. Private Akteure als Quellen, Abnehmer, Konkurrenten und Kooperationspartner staatlicher Nachrichtendienste

Lehrstuhl für Internationale Politik
Universität zu Köln

ISSN 1611-0072

AIPA 3/2006

Arbeitspapiere zur Internationalen Politik
und Außenpolitik

Peter Harbich

Die wachsende Bedeutung privater Akteure im Bereich der Intelligence. Private Akteure als Quellen, Abnehmer, Konkurrenten und Kooperationspartner staatlicher Nachrichtendienste

ISSN 1611-0072

Herausgeber:

Lehrstuhl für Internationale Politik

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

Druck:

Hausdruckerei der Universität zu Köln

Redaktionelle Bearbeitung:

Anna Daun, Sabine Janatschek

Köln 2006

ABSTRACT

Das Heraufkommen des Informationszeitalters und das Endes des Kalten Krieges haben die westliche Welt in den vergangenen zwei Jahrzehnten stark geprägt. Auch für die staatlichen Nachrichtendienste veränderten sich dadurch die Grundlage und der Inhalt ihrer Arbeit von Grund auf.

Eine neue Entwicklung ist in diesem Zusammenhang die Tatsache, dass die Nachrichtendienste zunehmend Beziehungen zu Akteuren der Privatwirtschaft ausbilden, während sie zuvor praktisch autarke Organisationen waren. Insbesondere in den vier Bereichen Wirtschaftsspionage, private Aufklärungssatelliten, Information Warfare und Private Intelligence Services werden private Akteure für die staatlichen Dienste immer bedeutender.

Im Folgenden werden diese Bereiche zunächst charakterisiert. Dies geht einher mit einer Bestandsaufnahme privater Intelligence-Institutionen, die zuvor ausschließlich dem Staat vorbehaltene nachrichtendienstliche Kernaufgaben übernehmen. Anschließend werden die Beziehungen zwischen staatlichen Nachrichtendiensten und privaten Akteuren analysiert und schließlich kategorisiert.

Peter Harbich

Jahrgang 1979, ist geboren und aufgewachsen in München und studierte Betriebswirtschaftslehre mit politikwissenschaftlichem Teil in Wien, Paris und Köln.

Kontakt:
peter.harbich@gmx.net

INHALT

Abbildungs- und Tabellenverzeichnis

Abkürzungsverzeichnis

ASISI	American Society for Industrial Security International
ASW	Arbeitsgemeinschaft für Sicherheit in der Wirtschaft e.V.
BBC	British Broadcasting Corporation
BMI	Bundesministerium des Inneren
BND	Bundesnachrichtendienst
BSI	Bundesamt für Sicherheit in der Informationstechnik
C^3I	Command, Control, Communications and Intelligence
CIA	Central Intelligence Agency
COMINT	Communications Intelligence
COMPINT	Computer Intelligence
COTS	Commercial Off The Shelf
DARPA	Defense Advanced Research Projects Agency
DAX	Deutscher Aktienindex
DCI	Director of Central Intelligence
DGSE	Direction Générale de la Sécurité Exterieure
DHS	Department of Homeland Security
DNI	Director of National Intelligence
ELINT	Electronic Intelligence

FBI	Federal Bureau of Investigation
FTSE	Financial Times Stock Exchange Index
HSPD	Homeland Security Presidential Directive
HUMINT	Human Intelligence
IAO	Information Awareness Office
IMINT	Imagery Intelligence
JETRO	Japan External Trade Organisation
MAD	Militärischer Aufklärungsdienst
MASINT	Measurements and Signatures Intelligence
MI6	Steht für Military Investigation, Abteilung sechs; britischer Auslandsgeheimdienst, auch bekannt unter dem Namen SIS (Secret Intelligence Service)
MITI	Ministry of International Trade and Industry
NASA	National Aeronautics and Space Administration
NGO	Non-Governmental Organisation
NOAA	National Oceanic and Atmospheric Administration
NSA	National Security Agency
NTIS	National Technical Information Service
OECD	Organisation for Economic Cooperation and Development
OSAC	Overseas Security Advisory Council
OSINT	Open Source Intelligence
PCCIP	President's Commission on Critical Infrastructure Protection
PDD	Presidential Decision Directive
SCIP	Society of Competitive Intelligence Professionals
SIGINT	Signals Intelligence
TECHINT	Technical Intelligence
TIA	Terrorism Information Awareness
UNITA	União Nacional para a Independência Total de Angola (Nationale Union für die völlige Unabhängigkeit Angolas)
USAF	United States Air Force

Die wachsende Bedeutung privater Akteure im Bereich der Intelligence. Private Akteure als Quellen, Abnehmer, Konkurrenten und Kooperationspartner staatlicher Nachrichtendienste

In der alten, vertrauten Welt, der geopolitischen Welt, beschäftigte sich militärische Intelligence mit militärischen Angelegenheiten, politische Intelligence mit Politik und wirtschaftliche Intelligence mit Wirtschaft. In einer neuen Welt der Geo-Ökonomien muss sich diese Aufteilung ändern, da Regierungen und Regierungsinstitutionen nicht mehr die selbstverständlichen Schlüsselakteure und Überwacher der weltweiten Ereignisse sind.[1]

1 Einleitung

Die seit den 90er Jahren geführte Diskussion über die zunehmende Privatisierung vormals staatlicher Tätigkeitsbereiche hat inzwischen auch das Feld der ehemals praktisch autarken Nachrichtendienste erreicht. Auch auf diesem Gebiet bilden sich immer differenziertere Beziehungen zwischen Staat und privatem Sektor heraus.

Die wachsende Bedeutung privater Akteure für staatliche Nachrichtendienste steht in einem engen Zusammenhang mit dem seit den 80er Jahren hereinbre-

1 Agrell, Wilhelm: Global Watch – world events and business intelligence, in: Sigurdson, Jon/Tagerud, Yael: The Intelligent Corporation, London: Taylor Graham Publishers, 1992, S. 99 (eigene Übersetzung)

chenden Informationszeitalter. Dieses kennzeichnet sich vor allem durch die Explosion frei verfügbarer Informationen sowie durch die weltweite Vernetzung von Informationsinfrastrukturen. Die zentrale Rolle hierbei spielt das Internet, welches beliebigen Personen weltweit Zugang zu einer nahezu unendlichen Fülle von Daten und Informationen sowie zu räumlich entfernten lokalen Netzwerken ermöglicht.

Aber auch die veränderte Sicherheitslage nach dem Kalten Krieg war für diese Entwicklung von großer Bedeutung. Denn der Zusammenbruch der Sowjetunion und der damit einhergehende Wegfall der hohen Bedrohung führte zu einer Lockerung von gesetzlichen Beschränkungen, wodurch den Privaten ein breiterer Zugang zu dem zuvor fast ausschließlich dem Staat vorbehaltenen nachrichtendienstlichen Bereich eröffnet wurde. Zudem wurden nach 1990 bei den Nachrichtendiensten Ressourcen frei, die zuvor an den Ostblock gebunden gewesen waren. Nun standen nachrichtendienstliche Kapazitäten für andere Zwecke zur Verfügung und konnten auf andere, auch nicht militärische Ziele gerichtet werden. Gerade in den 90er Jahren konkurrierten zumindest die hoch entwickelten Staaten primär in wirtschaftlicher Hinsicht. Entsprechend wurden auch die Nachrichtendienste für die Erlangung der nun im Zentrum stehenden *ökonomischen Sicherheit* eingesetzt. Damit richteten sich die nachrichtendienstlichen Mittel der mächtigen westlichen Staaten nicht mehr nur auf staatliche Institutionen wie Militär und Regierung, sondern zu einem erheblichen Teil auch auf wirtschaftliche Akteure. Daraus ergab sich eine neue Dimension des Verhältnisses zwischen staatlichen Nachrichtendiensten und privatem Sektor.

Die vorliegende Analyse verfolgt im groben und ganzen drei Hauptanliegen: Erstens eine Charakterisierung der verschiedenen nachrichtendienstlichen Bereiche, in denen Private Akteure eine wachsende Bedeutung erhalten. Zweitens eine differenzierte Betrachtung der damit verbundenen unterschiedlichen Beziehungen zwischen staatlichen Nachrichtendiensten und Privaten Akteuren. Und drittens eine Bestandsaufnahme privater Intelligence-Institutionen, die tatsächlich zuvor aus-

schließlich dem Staat vorbehaltenen nachrichtendienstliche Kernaufgaben übernehmen.

Bevor die Rolle privater Akteure in vier Bereichen nachrichtendienstlicher Tätigkeit beschrieben und deren Bedeutung für die Dienste analysiert wird sollen jedoch einige grundlegende Begriffe und Kategorien eingeführt werden, die für das Verständnis der weiteren Ausführungen zentral sind.

2 Grundlagen

2.1 Begriffsbestimmung von Intelligence

Für den Begriff „Intelligence“ gibt es im Deutschen keine Übersetzung, die alle Aspekte der englischen Bezeichnung einschließt. Am ehesten lässt sich Intelligence mit „nachrichtendienstlicher Tätigkeit“ übersetzen, wobei Intelligence jedoch auch das Endprodukt dieser Tätigkeit einschließt. Für die den Prozess erbringende Organisation werden die Begriffe „Nachrichtendienst“, „Geheimdienst“ oder schlicht „Dienst“ synonym verwendet.

In erster Linie beschäftigt sich Intelligence mit militärischen, politischen und wirtschaftlichen Fragen. Militärisch wird auf die potentielle Bedrohung durch andere Staaten abgestellt, also auf die Fähigkeiten möglicher Gegner oder Konkurrenten, politisch sind dagegen die Intentionen der Akteure von Bedeutung. Unter wirtschaftlicher Intelligence wird eine Vielzahl von Begriffen zusammengefasst, die weiter unten voneinander abgegrenzt werden. Daneben gewinnen Informationen aus dem ökologischen und gesundheitlichen Bereich an Bedeutung, da diese für die nationale Sicherheit zunehmend relevant sind.

Ein zentrales Kennzeichen von Intelligence ist die Klandestinität. Die aus offenen und verdeckten Quellen gesammelten Informationen, die Tätigkeiten und zur Verfügung stehenden Mittel und Methoden der Nachrichtendienste sowie deren Organisation werden, wenn auch in unterschiedlichem Maße, vor der Öffentlichkeit

geheim gehalten. Zweck der Geheimhaltung ist es, andere Akteuren über den eigenen Informations- und Wissensstand im Unklaren zu lassen und dadurch einen Informationsvorsprung zu erzielen und zu sichern.

Diesem Ziel dient neben der Klassifizierung von gewonnenen Informationen in Geheimhaltungsstufen unter anderem der Quellenschutz. Um die Informationsgewinnung selbst nicht zu gefährden, werden die Quellen nachrichtendienstlicher Informationsgewinnung nur einer möglichst kleinen Anzahl von Personen bekannt gemacht. Dies soll sicherstellen, dass das Ziel der Aufklärung nichts von der Spionage erfährt, was dieses nämlich augenblicklich zu Gegenmaßnahmen veranlassen würde. Im Falle menschlicher Spionage wäre die Sicherheit des Agenten dadurch gefährdet, im Fall technischer Spionage wäre die Quelle entwertet.

Adressaten von staatlicher Intelligence sind immer die politischen Entscheidungsträger, für die Geheimdienstinformationen deswegen wertvoll sind, weil sie möglichst objektive Informationen zur Verfügung stellen sollen.

In erster Linie haben die Dienste die Aufgabe, strategische Überraschungen zu vermeiden. Im militärischen Bereich ist damit ein Überraschungsangriff gemeint, wie beispielsweise der Angriff der Japaner auf Pearl Harbor 1941. Der Schock darüber führte überhaupt erst zum Aufbau der amerikanischen Intelligence Community und wirkt in den USA immer noch nach, so dass der Fokus amerikanischer Geheimdienstaufgaben auch heute noch in der Vermeidung von solchen Überraschungsangriffen liegt. Strategische Überraschungen können aber auch politischer oder wirtschaftlicher Natur sein, wie zum Beispiel die Ölkrise 1973 oder der unvorhergesehene Sturz des Schahs im Iran 1978.

Daneben soll Intelligence langfristige Expertise liefern. Politische Entscheidungsträger wechseln ihre Positionen und können damit nicht Experten auf allen Gebieten sein, mit denen sie konfrontiert sind. Dies soll durch Geheimdienste gesichert werden, die langfristig Informationen zu verschiedensten Gebieten sammeln und archivieren.

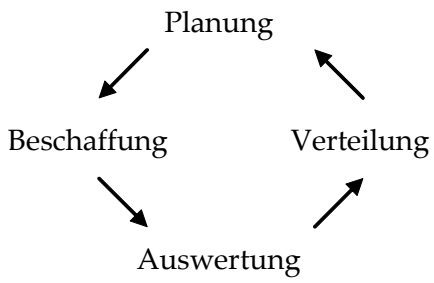
Schließlich soll Intelligence den politischen Prozess unterstützen. Politiker haben ein konstantes Bedürfnis nach maßgeschneiderter Information über Hintergründe, Kontext, Risiken, Nutzen und den wahrscheinlichen Ausgang unterschiedlichster Ereignisse.[2] Da Nachrichtendienste einen institutionalisierten Zugang zu den politischen Entscheidungsträgern haben, übernehmen sie oft die Zusammenfassung tagesaktueller Nachrichten. Insgesamt dient Intelligence der nationalen Sicherheit. Geheimdienste sind diejenigen staatlichen Einrichtungen, die vor aktuellen und potenziellen Bedrohungen warnen und der nationalen Politik einen Informationsvorsprung sichern.

2.2 Aufgaben staatlicher Nachrichtendienste

Die Aufgaben staatlicher Nachrichtendienste können grundsätzlich in die vier Bereiche Beschaffung, Auswertung, Counterintelligence und verdeckte Handlungen unterteilt werden. Das Sammeln von Informationen (Beschaffung) und deren Auswertung sind die Hauptbestandteile des so genannten Intelligence-Prozesses oder Intelligence-Zyklus (siehe Abbildung 1). Ob dieser auch nur annähernd der Geheimdienstpraxis entspricht, wird in der Literatur bereits seit Jahrzehnten diskutiert, jedoch ist er ein sehr anschauliches Instrument für die theoretische Behandlung des Themas und findet daher auch in neuen Publikationen immer wieder Verwendung.

2 Lowenthal, Mark M.: Intelligence: From Secrets to Policy, Washington: CQ Press, 2003, S. 2-4

Abb. 1: Intelligence-Zyklus



Quelle: Hulnick[3]

Bei verschiedenen anderen Autoren wird jeweils die eine oder andere Stufe durch eine detaillierte Untergliederung besonders hervorgehoben[4], teilweise wird zwischen der Beschaffung und der Analyse auch als weiterer Schritt die Aufbereitung der Rohdaten geschoben. Hier werden aus Anschaulichkeitsgründen nur die vier Hauptschritte angeführt.

Der idealtypische Zyklus beginnt mit der Planung, d.h. mit der Bestimmung des Ziels durch den politischen Entscheidungsträger. Der Endabnehmer des Produktes soll also bestimmen was beobachtet wird und steuert damit den Prozess. Nachdem die Ziele vorgegeben worden sind, wird die Vorgehensweise von einem hochrangigen Mitarbeiter des Nachrichtendienstes festgelegt, der die Organisation übernimmt. Die tatsächliche Arbeit am Produkt beginnt anschließend mit der Beschaffung der nötigen Daten und Informationen, die im dritten Schritt dann ausgewertet werden. Der fertige Bericht wird schließlich in mündlicher oder schriftlicher Form an die politischen Entscheidungsträger verteilt.

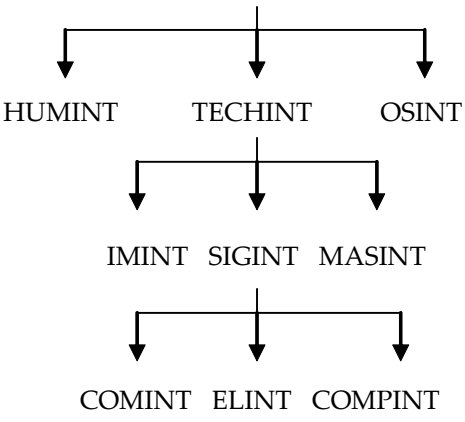
2.2.1 Beschaffung

Nachrichtendienstliche Beschaffungsquellen werden üblicherweise wie in Abb. 2 dargestellt unterteilt. Die bedeutendsten dabei sind HUMINT (HUMan INTelligence), OSINT (Open Source INTelligence), IMINT (IMagery INTelligence), SIGINT (SIGnals INTelligence) und MASINT (Measurements and SIgnatures INTelligence),

3 Hulnick (2004), S. 63
4 so z.B. Berkowitz/Goodman (2000), S. 68 oder Lowenthal (2003), 4. Kapitel

wobei die letzten drei oft unter dem Oberbegriff TECHINT (TECHnical INTelligence) zusammengefasst werden.

Abb. 2: Nachrichtendienstliche Beschaffungsquellen



HUMINT sind menschliche Quellen, dazu zählen Spione und V-Männer (Verbindungs-Männer), aber auch Personen mit relevanten Informationen bzw. relevantem Wissen, denen unter Umständen gar nicht bewusst ist, dass sie dem Geheimdienst Informationen offenbaren. Die wichtigste Kategorie, V-Männer, sind lokale angeheuerte oder freiwillige Quellen, die bereit sind, ausländischen Geheimdiensten Informationen weiterzugeben. Der Kontakt erfolgt dabei über Geheimdienstangehörige mit offiziellem (Diplomat) oder inoffiziellem Cover (Geschäftstätiger, Tourist, Immigrant).

OSINT sind offen zugängliche Quellen, also beispielsweise Nachrichten, die über Massenmedien verbreitet werden oder Informationen, die über das Internet zugänglich sind.

IMINT sind Bild-Aufklärungsquellen, also von Satelliten oder Aufklärungsflugzeugen gewonnene Photos. Unter SIGINT fallen das „Mithören“ bei Kommunikationsverbindungen wie Telefongesprächen, Email-, Funk-, Fax- oder Telegrammverkehr (COMINT), das Abfangen elektromagnetischer Wellen, die als Beiprodukt durch den Betrieb von elektronischen Geräten wie Radarsystemen entstehen (E-LINT) sowie das Eindringen in Computersysteme (COMPINT). Bei MASINT handelt es sich um die Messung verschiedenster physikalisch und chemisch messbarer

Phänomene, um beispielsweise nukleare Explosionen zu registrieren und charakterisieren oder Unterwasserfahrzeuge zu entdecken (Sonar).

Zunächst scheint es ein Widerspruch zu sein, dass offene Quellen (OSINT) überhaupt Teil nachrichtendienstlicher Arbeit sind, da ihnen das Merkmal der Klandestinität fehlt. Der geheime Charakter von Intelligence bezieht sich jedoch nicht in erster Linie auf die Methode der Informationsbeschaffung, sondern auf das Produkt. Schon durch die Kombination verschiedener Informationen aus offenen Quellen kann schützenswertes Wissen entstehen, vor allem aber wenn im Rahmen der „All-Source-Intelligence" zusätzlich zu den offenen Quellen auch geheime in das Produkt einfließen. Daher ist Information aus offenen Quellen dann Intelligence, wenn sie in entsprechender Weise ausgewertet und verteilt wird.[5]

Die Tatsache, dass die Geheimhaltung und der Quellenschutz bei OSINT eine geringere Rolle spielen, erhöht in vielen Fällen sogar den Wert von auf diesem Wege gewonnener Information für die Abnehmer des Produktes. Dies liegt zum einen darin begründet, dass offen gewonnene Informationen von politischen Entscheidungsträgern auch an die Öffentlichkeit weitergegeben werden können. Zum anderen können Nachrichtendienste untereinander mittels OSINT gewonnene Informationen leichter austauschen, was die nationale und internationaler Kooperation vereinfacht.

2.2.2 Auswertung

Die aus den verschiedenen Quellen gewonnenen Informationen werden anschließend von Analysten, die normalerweise organisatorisch unabhängig von den Stellen sind, die Informationen sammeln, ausgewertet. Dabei werden Informationen miteinbezogen, die bereits aus längerer Beobachtung vorhanden sind oder die ihm aus anderen Quellen zur Verfügung stehen.

Es gibt vier Kategorien von Intelligence-Analyse: 1) Warnungen, die politische Entscheidungsträger auf eine herannahende oder aufgetretene Krise aufmerk-

5 Mercado, Stephen C.: Sailing the Sea of OSINT in the Information Age, Studies in Intelligence, Vol. 48, Nr. 3, 2004, S. 51/52

sam machen, 2) aktuelle Intelligence, die den Empfänger über tägliche Entwicklungen unterrichtet, 3) fundamentale Intelligence, die als tiefer gehende Studie oder Schaffung einer Datenbank für spätere Bedürfnisse angelegt ist, und 4) Voraussagen über zukünftige Entwicklungen.[6] Das fertige Produkt wird schließlich in Form eines schriftlichen oder mündlichen Berichtes an den politischen Entscheidungsträger übergeben, dessen Informationslage dadurch verbessert werden soll.

2.2.3 Counterintelligence

Der Prozess der Erkenntnisgewinnung muss geschützt werden. Dies geschieht mit Hilfe der so genannten Counterintelligence. Darunter werden alle Tätigkeiten verstanden, die einen Staat vor den Aktivitäten fremder Geheimdienste schützen sollen. Diesem Ziel dient die Klassifikation von Informationen, also die Einstufung in verschiedene Geheimhaltungsstufen, die sich nach der Größe des Schadens richtet, den die Erlangung der Information durch Fremde anrichten kann. Counterintelligence kann in aktive und passive Maßnahmen eingeteilt werden.

Die passiven Maßnahmen können unter dem deutschen Begriff der Spionageabwehr zusammengefasst werden. Dazu gehören erstens die Überprüfung der Personen, die Zugang zu klassifizierten Informationen haben. Dadurch soll gewährleistet werden, dass diese sie nicht missbrauchen und beispielsweise an eine fremde Macht weitergeben. Zweitens gehört dazu die Gewährleistung der physischen Sicherheit von Informationen, also deren Schutz durch ausreichende physische Zugangsbarrieren. Drittens zählt zu den passiven Maßnahmen die Kommunikationssicherheit. Die Verbindungen sollen dabei so gut wie möglich gegen ein etwaiges „Anzapfen“ gesichert sein. Dort, wo dies nicht möglich ist, müssen die Nachrichten so gut wie möglich verschlüsselt werden. Eine vierte Maßnahme sind die Bemühungen, die Abstrahlung elektromagnetischer Wellen von technischem Gerät so gering wie möglich zu halten, da sich darüber auf die Art und Eigenschaften des Gerätes schließen lässt.

6 Hulnick (2004), S. 89

Dagegen fällt unter die aktiven Maßnahmen zunächst die Überwachung fremder Geheimdienstmitarbeiter, die beispielsweise unter dem Cover eines Diplomaten arbeiten. Zuerst müssen diese erkannt werden, um durch Beschattung mehr über deren Tätigkeiten zu erfahren.

Zur Verfolgung fremder Spione in Deutschland ist im letzten Verfassungsschutzbericht zu lesen: „Im Jahr 2004 wurden durch den Generalbundesanwalt 25 Ermittlungsverfahren wegen des Verdachts geheimdienstlicher Agententätigkeit bzw. wegen Landesverrats eingeleitet. Gegen 10 Personen wurde Haftbefehl erlassen. Im gleichen Zeitraum verurteilten Gerichte in der Bundesrepublik vier Angeklagte wegen Straftaten im Bereich „Landesverrat und Gefährdung der äußeren Sicherheit" (§§ 93 – 101a StGB)".[7] Die genannten Zahlen scheinen angesichts der vermuteten Spionageaktivitäten fremder Dienste in Deutschland wenig, jedoch muss dabei berücksichtigt werden, dass es stets schwierig ist, bei Spionagefällen überhaupt rechtliche Verfahren einzuleiten. Denn diese erfordern als Beweise das Aufdecken geheimer Informationen, was in der Folge Rückschlüsse auf die Quellen und die Arbeit der betroffenen Nachrichtendienste selber zulässt. Daher werden oft gar keine Verfahren eingeleitet, sondern Beschwerde bei der Botschaft des Herkunftslandes des Spions eingelegt, um die Spione des Landes zu verweisen.

Neben der Überwachung fremder Agenten sind Selbstanbieter, Überläufer und Doppelagenten wichtige Quellen um an Informationen über die Aktivitäten fremder Dienste zu gelangen. Selbstanbieter sind Personen fremder Geheimdienste, die von sich aus bereit sind, Informationen an einen fremden Staat zu liefern. Sie bleiben im Gegensatz zu Überläufern weiter für ihren ursprünglichen Dienst tätig. Überläufer spielen vor allem zu Kriegszeiten eine bedeutende Rolle, offenbaren aber auch in Friedenszeiten wichtige Informationen über die Spionagetätigkeit ihrer ehemaligen Auftraggeber. Doppelagenten sind Mitarbeiter eines fremden Geheimdienstes, die aufgedeckt und in der Folge für einen anderen Dienst tätig werden,

7 Bundesministerium des Inneren: Verfassungsschutzbericht 2004, Berlin, 2005, S. 266, http://www.bmi.bund.de/nn_122688/Internet/Content/Broschueren/2005/Verfassungsschutzbericht__2004__de.html

ohne dass der ursprüngliche Auftraggeber davon informiert ist. Gelingt es, so genannte Maulwürfe, d.h. ranghohe Agenten fremder Nachrichtendienste im eigenen Dienst zu enttarnen und zu „drehen“, können dadurch nicht nur Spione enttarnt, sondern auch Einsicht in alle weiteren Bereiche der nachrichtendienstlichen Aktivitäten des fremden Staates genommen werden. In einigen berühmt gewordenen Fällen gaben Maulwürfe jahrelang Informationen weiter, bevor sie schließlich aufgedeckt wurden. Beispiele aus der jüngeren Vergangenheit sind der CIA-Mitarbeiter Aldrich Ames, dessen zehnjährige Tätigkeit für den russischen KGB erst 1994 aufgedeckt wurde, oder der FBI-Agent Robert Hanssen, der 15 Jahre lang geheime Unterlagen an die Sowjetunion weiterreichte, was erst im Jahr 2001 aufflog.

Zuletzt gehört zu den aktiven Maßnahmen die Täuschung, womit das Füttern des Gegners mit falschen Informationen gemeint ist. Eine solche Desinformationskampagne kann beispielsweise zum Ziel haben, dass die eigene Stärke von einem fremden Geheimdienst über- oder unterschätzt wird. Als Transmitter können dabei Doppelagenten wirken, häufiger werden solche Nachrichten jedoch über solche Informationskanäle gesendet, von denen man weiß, dass sie von einem fremden Nachrichtendienst abgehört werden.

2.2.4 Verdeckte Handlungen

Die Planung und Ausführung von verdeckten Tätigkeiten sind der dritte Aufgabenbereich von Geheimdiensten. Dazu gehören Eingriffe verschiedenster Art, angefangen von geheim gehaltener technischer Unterstützung oder der Weitergabe selbst gewonnener Intelligence über die gezielte Streuung falscher Information (Propaganda) bis hin zum Sturz eines gegnerischen Regimes (paramilitärische Aktionen). Ziele können dabei nicht nur Regierungen von Staaten sein, sondern auch die gesamte Gesellschaft eines Staates oder Teile davon.

Im Sinne der zuvor genannten Definition gehört der Bereich der verdeckten Handlungen nicht zur Intelligence, da es dabei nicht um das Sammeln und Auswerten von Informationen oder die Abwehr von Aktivitäten fremder Nachrichtendienste geht. Verdeckte Handlungen sind somit ein Instrument zur Umsetzung von Au-

ßenpolitik, das zwischen Diplomatie einerseits und kriegerischen Aktivitäten andererseits anzusiedeln ist. Dass eine solche Aufgabe in vielen Staaten den Geheimdiensten zufällt, liegt daran, dass sich diese aufgrund von drei Merkmalen besonders dafür eignen: Erstens operieren sie im Geheimen, zweitens haben sie die dafür nötige Organisation und Repräsentanz vor Ort und drittens sind sie nicht an das Legalitätsprinzip gebunden.

2.3 Kategorien von Intelligence

2.3.1 Innerstaatliche versus außerstaatliche Intelligence

Das Hauptaktionsfeld westlicher Geheimdienste liegt generell jenseits der nationalen Grenzen. Das Ziel sind fremde Staaten bzw. nichtstaatliche Akteure im Ausland. Inlandsgeheimdienste befassen sich dagegen mit den Bedrohungen innerhalb der nationalen Grenzen. Sie sind in verschiedenen Staaten unterschiedlich stark ausgeprägt und beschäftigen sich vorwiegend mit Bedrohungen durch nationalen Terrorismus sowie mit Sabotage, verfassungsfeindlichen Elementen und der Abwehr von Intelligence-Tätigkeiten anderer Staaten (Counterintelligence).

Die Trennung zwischen innen und außen spiegelt sich in der Organisation der Geheimdienste wider. In Deutschland ist der Auslandsgeheimdienst der BND, der dem Bundeskanzleramt untersteht. Die Aufgaben des Inlandsgeheimdienstes übernehmen der Verfassungsschutz des Bundes, der dem Bundesministerium des Inneren zugeordnet ist sowie die Verfassungsschutzämter der Länder, deren Präsidenten an die jeweiligen Innenminister der Länder berichten. In den USA gibt es dagegen eine Vielzahl von Behörden, die mit nachrichtendienstlichen Aufgaben betraut sind. Die bekannteste unter ihnen, die CIA, ist ein Auslandsgeheimdienst. Das Federal Bureau of Investigation (FBI) nimmt Aufgaben eines Inlandsgeheimdienstes wahr, ist aber in erster Linie eine polizeiliche Vollstreckungsbehörde.

Die Trennung zwischen Auslands- und Inlandsgeheimdiensten ist ein Problem in Bezug auf neuere Bedrohungen wie den internationalen Terrorismus, der in weltweiten Netzwerken organisiert ist. Ein Anschlag kann im Inland ausgeführt

werden, aber vom Ausland aus geplant und gesteuert sein, daher stellt eine solche Art von Bedrohung die Nachrichtendienste vor große Herausforderungen.

2.3.2 Strategische versus taktische Intelligence

Mit strategischer Intelligence ist die langfristige Analyse von Bedrohungen gemeint, also das, womit Geheimdienste in Friedenszeiten hauptsächlich beschäftigt sind. Taktische Intelligence ist dagegen im militärischen Bereich angesiedelt. Sie umfasst Informationen über den Verlauf der gegnerischen und eigenen Handlungen im Kriegsfall, die naturgemäß für einen wesentlich kürzeren Zeitraum relevant sind. In den USA gibt es aktuell im Bereich der taktischen Intelligence bedeutende Entwicklungen, die mit der Vernetzung sämtlicher Teile des Militärs und der Intelligence sowie dem zunehmenden Einsatz von Präzisionswaffen einhergehen. Diese werden hier jedoch nur am Rande gestreift, die vorliegende Arbeit ist vornehmlich auf strategische Intelligence ausgerichtet.

2.3.3 Zivile versus militärische Intelligence

Militärische Geheimdienste konzentrieren sich auf militärische Bedrohungen durch andere Staaten und unterstützen im Kriegsfall die Streitkräfte sowohl mit strategischer als auch mit taktischer Intelligence. In Deutschland ist hierfür vor allem der Militärische Aufklärungsdienst (MAD) zuständig, der dem Verteidigungsministerium untersteht.

Zivile Intelligence erstreckt sich über mehrere Aufgabengebiete. In erster Linie ist der politische Bereich relevant und hier speziell die Sicherheitspolitik, die naturgemäß wiederum eng mit militärischen Fragen verknüpft ist. Daneben versorgen Geheimdienste die Politik aber auch mit relevanten wirtschaftlichen, ökologischen, gesundheitlichen und sonstigen Informationen, die die Entscheidungsträger im politischen Prozess unterstützen. Im Zusammenhang mit der Bedeutung privater Akteure in der Intelligence, die hier untersucht werden soll, sind militärische Aspekte bei den privaten Satellitenbetreibern (Kap. 3.2) und dem Bereich Information Warfare (Kap. 3.3) relevant.

2.3.4 Kategorien ökonomischer Intelligence

Vor allem mit Bezug auf die ökonomische Intelligence sind sprachliche Bezeichnungen vorzufinden, die in der Literatur oft unterschiedlich gebraucht bzw. verwechselt werden. Dies trifft auf die Begriffe Business Intelligence, Competitive Intelligence, Konkurrenzspionage, Wirtschaftsspionage sowie Wirtschaftsaufklärung zu. Diese werden im Folgenden zunächst definiert, bevor sie anhand der Kriterien privat/staatlich sowie Legalität voneinander abgegrenzt werden.

2.3.4.1 Business Intelligence

Unter Business Intelligence versteht man das legale Sammeln und Auswerten von unternehmensinternen und –externen Informationen durch ein Unternehmen. Dazu gehören Informationen über das Umfeld des Unternehmens im weitesten Sinne, also über aktuelle und zukünftige Aktivitäten von Konkurrenten, das Entstehen und die Entwicklung von Trends im technischen und gesellschaftlichen Umfeld, Veränderungen im rechtlichen und regulatorischen Rahmen sowie relevante Entwicklungen in den Bereichen Umwelt und Gesellschaft. Diese Informationen sollen die Grundlage sein für alle Arten von Managemententscheidungen, vor allem aber für solche, die die strategische Planung betreffen, verbessern und dazu beitragen, Überraschungen vermeiden.

2.3.4.2 Competitive Intelligence

Competitive Intelligence ist ein Unterbegriff von Business Intelligence. Sie betrifft jedoch im Gegensatz zu der weiter gefassten Business Intelligence nur die direkten Konkurrenten des Unternehmens. Die Society of Competitive Intelligence Professionals (SCIP) definiert Competitive Intelligence als Prozess der Überwachung des kompetitiven Umfelds eines Unternehmens, der es dem Management ermöglicht, informierte Entscheidungen in allen Bereichen ihrer Arbeit zu treffen.[8] Die Informationsbeschaffung und –auswertung erfolgt dabei kontinuierlich, legal und ethisch.[9]

8 Quelle: www.scip.org (eigene Übersetzung)
9 ebd.

2.3.4.3 Konkurrenzspionage

Im Gegensatz zur Competitive Intelligence bezeichnet das deutsche Wort der Konkurrenzspionage die illegale Gewinnung von Informationen über konkurrierende Unternehmen. Dabei geht es nicht nur um die Gewinnung von technischem Wissen und Forschungs- und Entwicklungsergebnissen, sondern um Geschäfts- und Betriebsgeheimnisse aller Art. Synonym wird in der Literatur oft der Begriff der Industriespionage verwendet.

2.3.4.4 Wirtschaftsspionage

Als Wirtschaftsspionage bezeichnet man die illegale Beschaffung und Verwertung von internen Informationen ausländischer Unternehmen durch staatliche Geheimdienste eines Landes. Mit Verwertung ist vor allem die Weitergabe der erlangten Informationen an Unternehmen der heimischen Industrie gemeint, die zum Ziel hat, diese gegenüber der internationalen Konkurrenz zu stärken.

2.3.4.5 Wirtschaftsaufklärung

Davon zu unterscheiden ist die (makroökonomische) Wirtschaftsaufklärung. Dies ist die Gewinnung von Informationen über die Leistungsfähigkeit einer Volkswirtschaft insgesamt bzw. einzelner Sektoren. Der Zusammenhang zu nationalen Sicherheitsbelangen ist direkter als bei Wirtschaftsspionage, da solche Informationen im Fall einer Krise von Bedeutung sind. Ein typisches Aufgabenfeld der Wirtschaftsaufklärung sind ökonomische Potentialanalysen.

2.3.4.6 Merkmale staatlicher und privater Aufklärung im wirtschaftlichen Bereich

Grundsätzlich zu unterscheiden ist also, ob die Spionage von staatlichen Nachrichtendiensten oder privaten Akteuren ausgeht und ob die Informationsbeschaffung legal oder illegal erfolgt. In Tabelle 1 werden die erläuterten Begriffe nach diesen Kriterien eingeordnet.

Tabelle 1: Klassifizierung von Begriffen der wirtschaftlichen Intelligence			
		Informationsbeschaffung	
		legal	**illegal**
Ausführender Akteur	**staatlich**	Wirtschaftsaufklärung	Wirtschaftsspionage
	privat	Business Intelligence/ Competitive Intelligence	Konkurrenzspionage

Nicht ganz eindeutig ist die Zuordnung von Wirtschaftsaufklärung zu legaler oder illegaler Informationsbeschaffung. Für die Analysen von marktwirtschaftlich organisierten Volkswirtschaften liegen die meisten Informationen offen vor und können daher legal beschafft werden. Besonders in Bezug auf geschlossene Gesellschaften wie beispielsweise Nordkorea trifft dies jedoch nicht zu, und es muss auf geheime Quellen zurückgegriffen werden. Damit ist die Informationsbeschaffung in solchen Fällen zumeist illegal.

Der Begriff Intelligence wird sowohl im privaten wie auch im staatlichen Bereich benutzt. In beiden Fällen ist es das Ziel, Überraschungen zu vermeiden, zur strategischen Planung beizutragen und aktuelle Entwicklungen zu beobachten.[10] Letzten Endes dient staatliche Intelligence jedoch der Sicherheit des jeweiligen Staates, wogegen Intelligence im privaten Sektor auf die Erhöhung des Profits des jeweiligen Unternehmens ausgerichtet ist. Der zweite große Unterschied besteht im unterschiedlichen rechtlichen Rahmen, in dem agiert wird. Privat betriebene Intelligence muss sich immer im jeweiligen gesetzlichen Rahmen bewegen, wogegen staatliche Nachrichtendienste so gut wie möglich von den dahinter stehenden Staaten geschützt werden, auch wenn sie Gesetze im Ausland überschreiten. Agenten staatlicher Geheimdienste stehen daher im Gegensatz zu Intelligence-Beschäftigten im privaten Bereich unter besonderem Schutz. Dies schränkt die Möglichkeiten privater Intelligence ein, sowohl was das Sammeln von Informationen, als auch was die Counterintelligence-Maßnahmen angeht. Das Sammeln von Informationen ist für den privaten Sektor gesetzlich auf den Open-Source-Bereich (OSINT) beschränkt.

10 Hulnick (2002), S. 69

3 Die Bedeutung privater Akteure für staatliche Nachrichtendienste in vier Bereichen

Im folgenden Hauptteil der Arbeit werden vier unabhängige Bereiche betrachtet, in denen staatliche Nachrichtendienste in unterschiedlicher Beziehung zu privaten Akteuren stehen.

3.1 Wirtschaftsspionage

Insbesondere nach dem Ende des Kalten Krieges gab es eine große Diskussion um die Rolle der Nachrichtendienste im so genannten „Wirtschaftskampf" („Battle of Economies"). In diesem Kapitel werden zunächst die Methoden der Wirtschaftsspionage vorgestellt und das Ausmaß beschrieben, in dem westliche Geheimdienste diese betreiben. Anschließend soll auf andere Formen eingegangen werden, wie staatliche Nachrichtendienste private Unternehmen zur Stärkung der nationalen Konkurrenzfähigkeit unterstützen können, bevor die Rolle der Dienste in der Abwehr fremder Wirtschafts- und Konkurrenzspionage beleuchtet wird. Schließlich wird die Diskussion um Wirtschaftsspionage, die vor allem in den 90er Jahren in den USA stattfand, nachvollzogen und auf Probleme eingegangen, die beim Betreiben von Wirtschaftsspionage entstehen.

Zum Thema Wirtschaftsspionage gibt es auch in Deutschland einige Publikationen, wobei diese zum größten Teil populärwissenschaftliche Ausarbeitungen sind. Die bekanntesten Autoren sind Peter Schweizer, Udo Ulfkotte und Erich Schmidt-Eenboom.[11] Sie unterscheiden allerdings häufig nicht klar zwischen Wirtschafts- und Konkurrenzspionage und liefern in ihren Arbeiten nur in den wenigsten Fällen stichhaltige Beweise, vor allem was die Verwicklung von Geheimdiensten, also Wirtschaftsspionage, angeht. Zu unterscheiden ist die aktive Wirtschafts-

11 Schweizer, Peter: Diebstahl unter Freunden, Reinbek: Rowohlt, 1993; Ulfkotte, Udo: Verschlusssache BND, München: Koehler & Amelang, 1997; Ulfkotte, Udo: Marktplatz der Diebe, München: Bertelsmann, 1999; Schmidt-Eenboom, Erich/Angerer, Jo: Die schmutzigen Geschäfte der Wirtschaftsspione, München: Econ TB Vlg., 1994

spionage einerseits sowie Maßnahmen zur Abwehr fremder Wirtschaftsspionage andererseits.

3.1.1 Aktive Wirtschaftsspionage

3.1.1.1 Methoden der Wirtschaftsspionage

Angesichts der Bandbreite der Aktivitäten, die im wirtschaftlichen Bereich von Interesse sind, ist es unmöglich, eine erschöpfende Darstellung der Methoden zu geben. Das Vorgehen ist sehr stark abhängig von der Art der Aktivität des Unternehmens, das ausspioniert werden soll, hier erfolgt daher nur eine sehr grobe Beschreibung der vornehmlich genutzten Methoden.

Im Bereich HUMINT kommt der „Quelle im Objekt" gegenüber dem Entsenden eines Agenten in das Unternehmen die weitaus größere Bedeutung zu. Im Gegensatz zum militärisch-politischen Bereich handelt es sich dabei meistens um Selbstanbieter, die nicht speziell angeworben werden müssen. Deren Motive sind laut einer Untersuchung der American Society for Industrial Security International (ASISI) neben Geld hauptsächlich Unzufriedenheit und Verärgerung über den eigenen Arbeitgeber.[12] Nur selten werden Verräter unter einer Legende in das Unternehmen eingeschleust, die dann über einen längeren Zeitraum interne Informationen weiterleiten.

Im Bereich TECHINT können Nachrichtendienste auf eine große Palette von Instrumenten zurückgreifen, die allerdings hauptsächlich für politisch-militärische Spionage konzipiert sind. Dort ermöglichen sie es, auf große Entfernung Informationen zu gewinnen wodurch sie nur zum Teil für das Ausspionieren von Unternehmen geeignet sind, denn hier ist das Abfangen von Daten aus unmittelbarer Nähe von größerer Bedeutung. Innerhalb des Bereichs TECHINT ist SIGINT die bedeutendste Quelle für Wirtschaftsspionage, IMINT und MASINT liefern für Wirtschaftsspione nur in wenigen Fällen bedeutende Informationen. Hauptsächlich werden Kommunikationsverbindungen angezapft (COMINT), Daten aufgrund der

12 Lux/Peske (2002), S. 87

elektromagnetischen Abstrahlung von Geräten „mitgeschnitten“ (ELINT), Wanzen zum Abhören von Gesprächen installiert und Einbrüche in unternehmensinterne Computernetzwerke getätigt (COMPINT). Die Datengewinnung mittels Eindringen in das IT-System des Zielunternehmens ist dabei neben den menschlichen „Quellen im Objekt“ die häufigste und ergiebigste Methode. Eine Diskussion über systematisches, breites und ungefiltertes Abhören von Telefon-, Email- und sonstiger Verbindungen wird weiter unten beispielhaft anhand des ECHELON-Systems geführt.

Die Hauptquelle für Wirtschaftsspionage ist jedoch auch für die Geheimdienste die OSINT. Unternehmen gehen meist sehr offen mit Daten um, auch wenn es sich dabei um sensible Informationen handelt. Dies liegt zum einen daran, dass das Gefahrenbewusstsein sehr oft nicht vorhanden ist, und zum anderen daran, dass die Mittel für eine Geheimhaltung nicht zur Verfügung stehen. In vielen Fällen genügt daher eine umfassende Sammlung der frei zugänglichen Informationen, um an die gewollten Informationen zu gelangen.

3.1.1.2 Die westlichen Staaten als Betreiber von Wirtschaftsspionage

Im Bereich der Wirtschaftsspionage nimmt die Spionage, die auf ausländische Rüstungsunternehmen zielt, eine besondere Stellung ein. Sie muss als legitimes Interesse von Nachrichtendiensten gelten, da hiervon unmittelbar die nationale Sicherheit betroffen ist. Darüber hinaus verschwimmen im Rüstungsbereich Wirtschaftsspionage und „normale“ Spionage, denn Rüstungsunternehmen befinden sich selbst in einer Grauzone zwischen öffentlichem und privatem Sektor. Auch wenn die öffentliche Hand nicht direkt Anteile an solchen Unternehmen hält, was in vielen Fällen noch der Fall ist, hat sie doch weitreichende gesetzliche Kontrollmöglichkeiten über ihre Aktivitäten und übt als deren Hauptkunde großen Einfluss auf sie aus. Der private Rüstungsbereich fremder Staaten ist daher mit Sicherheit Ziel der Nachrichtendienste, was durch in der Vergangenheit bekannt gewordene Fälle belegt wird. Insgesamt kann hier von einer mehr oder minder akzeptierten Praxis gesprochen werden, genauso wie bei politisch-militärischer Spionage. Das trifft zum Teil auch zu, wenn Geheimdienste Rüstungskonzerne in Ausschreibungen zur Beschaffung

militärischen Geräts durch fremde Länder unterstützen. Dabei geht es darum, über die Verhandlungsposition der Mitbieter informiert zu sein. Denn es ist mit Hinblick auf die eigene nationale Sicherheit vorzuziehen, dass das importierende Land über Waffensysteme verfügt, die aus heimischer Produktion stammen, denn dadurch kann eine gewisse Kontrolle ausgeübt werden.

Das Ausmaß von Wirtschaftsspionage in den übrigen weniger sicherheitssensitiven Bereichen variiert von Land zu Land und ist aus drei Gründen schwer abzuschätzen. Erstens aufgrund des Merkmals der Klandestinität geheimdienstlicher Arbeit im Allgemeinen. Zweitens aufgrund der Tatsache, dass durch betroffene Unternehmen festgestellte Wirtschaftsspionage meist nicht öffentlich wird, da negative Konsequenzen für den eigenen Ruf befürchtet werden.[13] Und drittens, weil in vielen Fällen nicht zu unterscheiden ist, wer hinter der Spionage steht: ein staatlicher Geheimdienst oder ein Konkurrenzunternehmen. Im ersten Fall handelt es sich um Wirtschaftsspionage, im zweiten Fall jedoch um Konkurrenzspionage. Zahlen über das Ausmaß von Wirtschaftsspionage oder dadurch entstandene Schäden, die in der Literatur oder in Medienberichten zu dem Thema gehandelt werden, dürften aus diesen Gründen höchst fraglich sein. Jedoch lässt sich mit Sicherheit feststellen, dass die Nachrichtendienste unterschiedlicher Länder unterschiedlich stark mit Wirtschaftsspionage betraut sind.

USA

Seit dem Bekanntwerden der Existenz des ECHELON-Abhörsystems im Jahre 1988 ist klar, dass die USA und ihre UKUSA[14]-Verbündeten Großbritannien, Neuseeland, Australien und Kanada, die das System gemeinsam betreiben, die Möglichkeit haben, an jegliche Art von internen Informationen fremder Unternehmen zu gelangen und damit Wirtschaftsspionage zu betreiben. Inwieweit dieses Potential jedoch ausgenutzt wird, ist umstritten. Offiziell wird von amerikanischer Seite betont, dass

13 Ulfkotte (1999), S. 59

14 Zwischen Großbritannien (UK) und den USA 1947 geschlossene Verträge zur Zusammenarbeit der Geheimdienste beider Länder: dem Government Communications Headquarters (GCHQ) und der National Security Agency (NSA). Als weitere Staaten schlossen sich dem Abkommen Australien, Kanada und Neuseeland an.

erlangte Informationen nur dann an amerikanische Unternehmen weitergegeben werden, wenn aus ihnen hervorgeht, dass die abgehörten Unternehmen Wettbewerbsregeln, Exportbeschränkungen oder ähnliches verletzen, so beispielsweise auch in der Presidential Decision Directive (PDD) 35 von Bill Clinton im Jahr 1995.[15] Allerdings setzen die USA damit im Prinzip ihren eigenen Foreign Corrupt Practices Act durch.[16] Die Informationsweitergabe in solchen Fällen erfolgt dabei nicht direkt zwischen Nachrichtendienst und Unternehmen, sondern über das Handels- und Außenministerium. Den begünstigten amerikanischen Unternehmen wird damit bereits ein Wettbewerbsvorteil gegenüber ihren Konkurrenten verschafft, die keine Möglichkeiten haben, über Wettbewerbsverstöße ihrer amerikanischen Konkurrenten Informationen zu erlangen. Damit dürften in diesen Fällen die Merkmale der Wirtschaftsspionage erfüllt sein.

Das Betreiben klassischer Wirtschaftsspionage, also das Stehlen von technologischen Geheimnissen wie Forschungs- und Entwicklungsergebnissen, wird in den USA von offizieller Seite stets vehement bestritten, und Anschuldigungen solcher Art werden zum Teil auch mit juristischen Mitteln bekämpft. Mit Ausnahme von Stansfield Turner haben sich alle Directors of Central Intelligence (DCI) gegen Wirtschaftsspionage durch amerikanische Geheimdienste ausgesprochen, obwohl bekannt ist, dass amerikanische Unternehmen von fremden Nachrichtendiensten zum Teil massiv ausspioniert werden. Angesichts dessen und angesichts der Tatsache, dass sich auch beim Studium der amerikanischen Literatur zu dem Thema die Hinweise für solche Wirtschaftsspionage nicht verdichten lassen, kann davon ausgegangen werden, dass die USA im großen und ganzen keine systematische Spionage in diese Richtung betreiben und die oftmals in der Presse oder in Publikationen des investigativen Journalismus gegen sie erhobenen Anschuldigungen übertrieben sind.

15 Treverton, Gregory F.: Reshaping National Intelligence for an Age of Information, RAND Studies in Policy Analysis, Cambridge: Cambridge University Press, 2003, S. 157
16 ebd. S. 111

Auch einem vom europäischen Parlament beauftragten Ausschuss über ECHELON gelang kein Nachweis dafür. In dem Untersuchungsbericht wird Wirtschaftsspionage im klassischen Sinn von Seiten der USA zwar vermutet:

> „(...) in der Erwägung, dass die Nachrichtendienste der USA nicht nur allgemeine wirtschaftliche Sachverhalte aufklären, sondern Kommunikation von Unternehmen gerade bei Auftragsvergabe auch im Detail abhören und dies mit der Bekämpfung von Bestechungsversuchen begründen; dass bei detailliertem Abhören das Risiko besteht, dass die Informationen nicht zur Bekämpfung der Bestechung, sondern zur Konkurrenzspionage verwendet werden, auch wenn die USA und das Vereinigte Königreich erklären, dass sie das nicht tun", jedoch muss zugegeben werden, „dass es allerdings keinen belegten Fall dafür gibt, dass das globale Abhörsystem dafür eingesetzt wurde, auch wenn dies vielfach behauptet wurde".[17]

Ein einziger Fall klassischer Wirtschaftsspionage durch die USA ist in Deutschland bekannt geworden, der in die Zeit von 1993 bis 1996 fällt. Bill Clinton machte in dieser Zeit die Verbesserung der Konkurrenzfähigkeit der amerikanischen Wirtschaft zu einem Hauptanliegen, wobei auch von offizieller Seite einige Aussagen publik wurden, die den Einsatz von Wirtschaftsspionage über das oben beschriebene Maß vermuten lassen. In diesem Fall wurde das deutsche Unternehmen Enercon, das zu dieser Zeit eine innovative Windkraftanlage entworfen hatte, Opfer von Spionagetätigkeit zugunsten eines amerikanischen Konkurrenten. Auch wenn nie zweifelsfrei bewiesen werden konnte, dass dabei die National Security Agency (NSA) beteiligt war, bleiben sehr dichte Hinweise darauf bestehen.

Großbritannien

In Großbritannien wurde mit dem Intelligence Service Act von 1994 explizit ein ökonomischer Aufklärungsauftrag formuliert, welcher über das herkömmliche Verständnis von Wirtschaftsaufklärung hinausgeht. Dieses war daran orientiert, im Rahmen einer Potentialanalyse die ökonomischen Aspekte der Sicherheitspolitik zu

17 EU Parlament, Nichtständiger Ausschuss über das Abhörsystem Echelon: Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)), Sitzungsdokument A5-0264/2001, Teil 1, 11.7.2001, http://kai.iks-jena.de/miniwahr/echelon-index.html

untersuchen wie etwa die Kriegsfähigkeit der Wirtschaft oder die Sicherheit der Rohstofflieferungen von wichtigen Metallen und Energieträgern. Für das nun erweiterte Aufgabenverständnis wurde der Begriff „economic well-being" geschaffen.[18] Man kann damit davon ausgehen, dass Großbritanniens Geheimdienste Wirtschaftsspionage betreiben, welche auch über den Rüstungssektor hinausgeht.

Frankreich

Der französische Auslandsgeheimdienst DGSE betrieb Wirtschaftsspionage in den 80er und 90er Jahren nachgewiesenermaßen relativ aggressiv. Mehrere Fälle sind bekannt geworden, darunter das Bespitzeln von Geschäftsleuten auf Air France-Flügen sowie Einbrüche in deren Hotels, das Abhören der Telekommunikationsverbindungen von ausländischen Konzernzentralen mit ihren französischen Niederlassungen sowie das Infiltrieren der französischen Gesellschaften von Unternehmen wie IBM, Boeing und mehreren anderen.[19]

1993 drohte Bill Clinton, die Zusammenarbeit der amerikanischen Geheimdienste mit den französischen Partnern aufzukündigen, sollte der DGSE weiterhin amerikanische Unternehmen in diesem Maße ausspionieren. Ob Frankreich seither keinerlei Wirtschaftsspionage mehr betreibt, darf bezweifelt werden, jedoch dürfte das Ausmaß solcher Aktivitäten, wenigstens in den USA, zurückgegangen sein. Diese Vermutung ist auch deswegen plausibel, da seither viele ehemalige Staatsunternehmen privatisiert worden sind, was die Zusammenarbeit zwischen ihnen und den Geheimdiensten erschwert.

Deutschland

Dem BND ist es aufgrund der gesetzlichen Lage durchaus erlaubt, auch Wirtschaftsspionage zu betreiben, offiziell werden solche Tätigkeiten jedoch stets abgestritten. Dass er in systematischer Weise Informationen über fremde Firmen an deutsche Unternehmen weitergibt ist nicht anzunehmen, weder dem amerikani-

18 Jakob (1999), S. 217

19 Richelson, Jeffrey T.: A Century of Spies, New York/Oxford: Oxford University Press, 1997, S. 426/427

schen Autor Peter Schweizer, noch den Deutschen Erich Schmidt-Eenboom und Udo Ulfkotte gelingen hierfür in ihren Publikationen Nachweise. Die in der Vergangenheit bekannt gewordenen Fälle von Wirtschaftsspionage durch den BND betreffen allesamt Unternehmen aus dem Rüstungsbereich. Damit dürfte das primäre Motiv ein sicherheitspolitisches sein, und nicht in erster Linie die Profiterhöhung deutscher Unternehmen auf Kosten ausländischer sein.

Ähnlich wie die CIA unterstützt der BND dagegen deutsche Unternehmen vor illegalen Handelspraktiken von ausländischen Konkurrenzunternehmen. Er gibt solche Informationen an das Bundesausfuhramt weiter, das anschließend sogenannte „Red Flags" an die Unternehmen weitergibt. Darunter versteht man Warnungen über Personen und Organisationen, die versuchen, die Exportkontrolle zu unterlaufen.

Japan

Japan gilt unter den hoch entwickelten Staaten als derjenige, der Wirtschaftsspionage im größten Umfang betreibt. Bis zum Beginn der 90er Jahre war sogar der größte Teil nachrichtendienstlicher Aufklärung auf die Gewinnung von wirtschaftlichen Informationen gerichtet. Die übrige zivile Intelligence, vor allem politischer Art, wurde entweder von den US-Geheimdiensten bezogen oder aber ganz auf sie verzichtet. So umfassten die zivilen Kapazitäten zur Auslandsaufklärung zu Beginn der neunziger Jahre nur etwa 250 Mitarbeiter.[20] Die Gewinnung von Intelligence im wirtschaftlichen Bereich erfolgt nicht durch die staatlichen Geheimdienste selbst, sondern durch halbstaatliche Organisationen und die großen japanischen Konzerne. Daneben sind auch japanische Medienanstalten eingebunden, die schon unter dem Vorwand Reportagen zu erstellen versucht haben, an interne Unternehmensinformationen zu gelangen.[21]

Kennzeichnend für die japanischen Aktivitäten ist die Offenheit der verwendeten Quellen. Die Informationen kommen laut John Sigurdson zu 90 Prozent

20 Schmidt-Eenboom/Angerer (1994), S. 28

21 Fink, Steven: Sticky Fingers, Chicago: Dearborn Trade Publishing, 2002, S. 49

aus offenen, zu neun Prozent aus grauen[22], sowie nur zu einem Prozent aus wirklich geheimen Quellen.[23] Aufgrund dieser Tatsache könnte man zunächst auf praktisch vollkommen legale Konkurrenzspionage schließen. Das Besondere am japanischen System ist jedoch, dass die Aktivitäten von staatlich unterstützten Organisationen koordiniert und die gesammelten Daten dort zentralisiert und ausgewertet werden. Die zwei hauptsächlich mit dieser Aufgabe betrauten Stellen sind das Ministry of International Trade and Industry (MITI) und die ihm unterstehende Japan External Trade Organisation (JETRO). Letztere besitzt außerhalb Japans 76 Büros in 57 Ländern[24], die neben ihrem offiziellen Auftrag, der Förderung des Imports ausländischer Güter nach Japan, der Informationsbeschaffung über die jeweiligen Märkte, Unternehmen und Produkte dienen. Die Tätigkeit der ins Ausland entsandten Experten, nämlich interessante Produkte für den japanischen Markt auszumachen und potentielle Exporteure in die Richtlinien des Exports nach Japan einzuweisen, bietet dabei eine gute Tarnung. Auf diese Weise betreibt JETRO die weltweit führende Datenbank über Wirtschaftsunternehmen und Produktlinien.

Der Verband von Wirtschaftsunternehmen im MITI benutzt JETRO-Informationen darüber hinaus auch, um hochwertige Aufklärungsziele von nationalem Interesse auszumachen und daraufhin teilweise auch illegale nachrichtendienstliche Operationen durchzuführen. Offiziere der Nachrichtendienste, die von JETRO-Büros eingesetzt werden, sind bei ihren Auslandseinsätzen so auch häufig über japanische Konzerne abgedeckt.

Es ist also schwer, die japanischen Spionageaktivitäten von Firmen und staatlichen Geheimdiensten zu trennen. Die JETRO, die sich mit der offenen und verdeckten Beschaffung wirtschaftlicher Informationen aus dem Ausland befasst, ist zwar eine von Industrieunternehmen getragene Agentur, wird jedoch von der Re-

22 Als graue Materialien werden weder geheimgehaltene noch für die Öffentlichkeit bestimmte Informationen bezeichnet

23 Sigurdson, Jon/Nelson, Patricia: Intelligence gathering and Japan. The elusive role of grey intelligence, International Journal of Intelligence and Counterintelligence, Vol. 5, Nr. 1, 1991, S. 17

24 Quelle: www.jetro.de

gierung subventioniert. Deren Aktivitäten fallen daher durchaus unter den Bereich der Wirtschaftsspionage.

3.1.2 Nachrichtendienstliche Unterstützung von Unternehmen im Ausland

Während Wirtschaftsspionage als nachrichtendienstliche Aufgabe sehr umstritten ist[25], unterstützen Geheimdienste Unternehmen auf zwei weitere Arten: aktiv bei Auslandsoperationen heimischer Unternehmen und passiv in der Abwehr von Wirtschaftsspionage. Zunächst zum ersten Punkt.

Seit dem Ende des Kalten Krieges und der damit einhergehenden Kritik an der umfassenden Geheimhaltungspraxis der Dienste wurden viele geheimdienstlich gewonnene Informationen und daraus entstandene Berichte von der Geheimhaltungsstufe befreit („declassified"). Die amerikanische Intelligence Community hat viele ihrer in den Archiven gelagerten Berichte über ein System namens National Technical Information Service (NTIS) der Öffentlichkeit über das Internet zugänglich gemacht. Daneben wird viel Material über das Department of State und das Department of Commerce veröffentlicht, die sich mittlerweile als Stellen zur Weitergabe von Informationen der Intelligence Community an den privaten Sektor etabliert haben.[26] Daneben gibt es die schon immer öffentlich zugänglichen Länderberichte sowie Berichte über Veränderungen bzw. Lageeinschätzungen der geopolitischen Landkarte, so zum Beispiel das von der CIA herausgegebene World Factbook.[27] Diese Materialien enthalten vor allem für Unternehmen, die Auslandsaktivitäten außerhalb der ersten Welt betreiben, sehr nützliche Informationen.

Darüber hinaus gibt es für im Ausland operierende US-amerikanische Unternehmen eine vom State Department ins Leben gerufene Institution, den Overseas Security Advisory Council (OSAC), der in erster Linie Unternehmen betreut, die in Bereichen der Hochtechnologie sowie der Sicherheit und Verteidigung operieren.

25 siehe auch Kapitel 3.1.5

26 Hulnick, Arthur S.: The Uneasy Relationship Between Intelligence and Private Industry, International Journal of Intelligence and Counterintelligence, Vol. 9, Nr. 1, 1996, S. 22

27 zugänglich unter http://www.cia.gov/cia/publications/factbook

Dessen ausführliche Informationen unterstützen solche Firmen dabei, Informationen und Personen in Auslandsgesellschaften vor Kriminalität und fremden Geheimdiensten zu schützen.

Eine noch aktivere Rolle von Geheimdiensten in der Unterstützung amerikanischer Unternehmen im Ausland wird angesichts des Problems der organisierten Kriminalität diskutiert. Da die Rechtssysteme in vielen Ländern den Unternehmen bei der Verfolgung von kriminellen Handlungen nicht behilflich sind, wird gefordert, dass Geheimdienste diese Lücke schließen. Der Vorschlag wird von den Geheimdiensten jedoch wiederum mit dem Hinweis des fehlenden Zusammenhangs zur nationalen Sicherheit zurückgewiesen. Solange der Schaden durch organisierte Kriminalität also kein noch größeres Ausmaß annimmt, werden solche Unternehmen weiterhin nur auf private Sicherheitsdienste zurückgreifen können.[28]

3.1.3 Abwehr von Wirtschafts- und Konkurrenzspionage

Die Abwehr von Wirtschafts- und Konkurrenzspionage wird hier gemeinsam behandelt, da meist nicht erkennbar ist, ob die Spionage von einem fremden Nachrichtendienst oder einem Konkurrenzunternehmen ausgeht. Aufgrund der Freisetzung einer großen Zahl von Mitarbeitern von Geheimdiensten der ehemaligen Ostblockländer steht eine große Zahl hoch qualifizierter Personen zur Verfügung, die sich auf dem so genannten schwarzen Intelligence-Markt anbieten.[29] Sie helfen mit ihren Kenntnissen nicht nur kommerziellen Anbietern methodisch auf den aktuellen Stand zu kommen, sondern haben teilweise auch auf dem „kleinen Dienstweg“ Verbindungen zu ihren alten Arbeitgebern und somit auch Rückgriff auf deren Ressourcen, die sich eventuell für die Konkurrenzspionage nutzen lassen.[30] Gerade letzteres lässt die Grenzen zwischen Wirtschafts- und Konkurrenzspionage verschwimmen.

28 Hulnick (1996), S. 24
29 Lux/Peske (2002), S. 49
30 ebd.

3.1.3.1 Die westlichen Mächte als Ziel der Wirtschaftsspionage

Bei den Angriffen auf westliche Unternehmen sind zwei Kategorien zu unterscheiden: solche, die von den Nachrichtendiensten anderer Westmächte durchgeführt werden, und solche, die von Nachrichtendiensten von Schwellenländer ausgehen. Letztere richtet sich meist auf die Gewinnung technologischer Erkenntnisse, erstere meist auf die direkte Konkurrenz um Aufträge und Marktanteile. Hier geht es um Geschäftsgeheimnisse wie Kundenlisten, Preisinformationen, Forschungsergebnisse, Vertriebsinformationen, Produktionsinformationen, strategische Pläne und Kosteninformationen.[31] Vor allem bei der Vergabe von Großaufträgen mittels Ausschreibung wird mit unlauteren Mitteln versucht, sich einen Vorteil zu verschaffen. In der Literatur zitierte Beispiele sind beispielsweise ein Sechs-Milliarden-Dollar-Auftrag der staatlichen saudi-arabischen Fluglinie, der aufgrund von mit ECHELON gesammelten Informationen 1994 an Boeing und McDonald Douglas ging[32] oder der Verkauf eines Radarsystems an Brasilien, der an das US-Rüstungsunternehmen Raytheon ging, nachdem die CIA Bestechung durch den französischen Konkurrenten nachgewiesen hatte.[33]

Spionage durch Schwellenländer ist in der Regel sehr aggressiv. Der Verfassungsschutzbericht 2004 stellt fest, dass die größten Wirtschaftsspionageaktivitäten derzeit von Russland und den GUS-Verbündeten[34] sowie China und Nordkorea ausgehen.[35] Deren Ziel es ist, die technologische Lücke zu den westlichen Mächten zu verkleinern. In den letzten Jahren wurden einige Fälle chinesischer und russischer Spionage bekannt, hauptsächlich in den USA.[36] Die am meisten gefährdeten Branchen neben dem Rüstungsbereich und Dual-Use-Gütern sind forschungsinten-

31 Fink (2002), S. 266

32 siehe u.a. ebd., S. 53; Ulfkotte (1997), S. 125; Hirschmann, Kai: Geheimdienste, Hamburg: Europäische Verlagsanstalt, 2004, S. 50

33 Treverton (2003), S. 111

34 dazu gehören Armenien, Aserbaidschan, Georgien, Kasachstan, Kirgisistan, Moldawien, Tadschikistan, Ukraine, Usbekistan und Weißrussland

35 Bundesministerium des Inneren: Verfassungsschutzbericht 2004, S. 252

36 vgl. Burger, Timothy J./Bennett, Brian/Calabresi, Massimo/Duffy, Michael/Shannon, Elaine: The Russians Are Coming, Time Canada, Vol. 165, Ausgabe 6 vom 7.2.2005 und Bennett, Brian/Burger, Timothy J./Shannon, Elaine: China's big exports, Time Canada, Vol. 165, Ausgabe 8 vom 21.2.2005

sive Sektoren wie Pharma, Chemie, Nahrungsmittel, Computer Software, Luftfahrt und Automobil.[37]

3.1.3.2 Staatliche Spionageabwehr in Deutschland

In Deutschland sind die Verfassungsschutzbehörden des Bundes und der Länder sowie die Polizei mit der Abwehr von Spionagetätigkeiten betraut.

Gemäß Bundesverfassungsschutzgesetz bzw. Landesverfassungsschutzgesetzen beschränkt sich die Aufgabe der Verfassungsschutzbehörden eigentlich auf die Abwehr von Spionage durch fremde Mächte, was Wirtschaftsspionage im hier gebrauchten Sinne mit einschließt, Konkurrenzspionage aber nicht. Ob es sich jedoch bei einem Fall um Wirtschafts- oder Konkurrenzspionage handelt, lässt sich zunächst meist nicht feststellen, weshalb der Verfassungsschutz oft bis zur endgültigen Feststellung dieser Tatsache ermittelt.[38] Aufgrund des Trennungsgebotes ist der Verfassungsschutz dabei zur Zusammenarbeit mit der Polizei angewiesen, da nur sie Festnahmen und Durchsuchungen durchführen kann. Daneben sind das Bundesministerium des Inneren, das Bundeskriminalamt, das Bundesamt für Sicherheit in der Informationstechnik, das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, das Zollkriminalamt, das Bundesministerium für Wirtschaft und Arbeit, das Bundesamt für Wirtschaft und Ausfuhrkontrolle, das Auswärtige Amt und der Bundesnachrichtendienst in die Abwehr von Wirtschafts- und Konkurrenzspionage eingebunden.

Besonders schützenswerte Unternehmen können unter staatlichen Geheimschutz gestellt werden. Darunter fallen Unternehmen, Einzelpersonen, Institute oder andere Einrichtungen, die Aufträge von Bundes- oder Landesbehörden wahrnehmen und zu deren Ausführung Verschlusssachen bearbeiten, entwickeln oder

37 Fink (2002), S. 266
38 Lux/Peske (2002), S. 57

die aus anderen Gründen geschützt werden müssen.[39] In Deutschland standen im Jahre 2004 ca. 1400 Unternehmen unter staatlichem Geheimschutz.[40]

Das Bindeglied zwischen Wirtschaft und Staat in der Spionageabwehr ist der Arbeitskreis für Sicherheit in der Wirtschaft e.V., der von den Spitzenorganisationen der deutschen Wirtschaft[41], allen deutschen regionalen Sicherheitsverbänden[42] sowie mehreren Branchenverbänden getragen wird. Er fungiert als Zentralorganisation der Wirtschaft in Sicherheitsfragen, als Interessenvertretung gegenüber Regierung, Politik und Verwaltung, als zentrale Koordinierungsstelle zur Weitergabe von Sicherheitsinformationen zwischen Staat und Wirtschaft und als Netzwerk und Forum für Unternehmenssicherheit.[43] Besonders hervorzuheben ist seine Rolle als Intermediär auf dem Intelligence-Markt. Verschiedene sicherheitsbezogene Informationen von staatlichen Organisationen werden gesammelt, analysiert und falls nötig mit Handlungsempfehlungen ergänzt und den Mitgliedern zur Verfügung gestellt.[44]

3.1.3.3 Private Spionageabwehr

Es gibt Anhaltspunkte, dass Erkenntnisse über Wirtschaftsspionage anderer Westmächte, die den Behörden bekannt waren, absichtlich nicht an die betroffenen Unternehmen weitergeleitet wurden. So untersagte Helmut Kohl laut Aussage eines Verfassungsschutzmitarbeiters im Jahre 1999 die Weitergabe von Informationen über die Tätigkeit amerikanischer Wirtschaftsspione auf deutschem Boden an die Wirtschaft, um die deutsch-amerikanische Freundschaft nicht zu gefährden.[45] Aber

39 ebd., S. 162

40 Arbeitsgemeinschaft für Sicherheit in der Wirtschaft e.V. (ASW): Anmerkungen zur Sicherheitslage der deutschen Wirtschaft, Berlin, Oktober 2005, S. 56, http://www.asw-online.de/Anmerkungen-zur-Sicherheitslage-der-deutschen-Wirtschaft20043.pdf

41 dazu zählen: Deutsche Industrie- und Handelskammer, Bundesverband der Deutschen Industrie, Bundesverband der Deutschen Arbeitgeberverbände

42 das sind: Bayerischer Verband für Sicherheit in der Wirtschaft e.V., Sächsischer Verband für Sicherheit in der Wirtschaft e.V., Verband für Sicherheit der Wirtschaft Mitteldeutschland e.V., Verband für Sicherheit in der Wirtschaft Baden-Württemberg e.V., Verband für Sicherheit in der Wirtschaft Niedersachsen e.V., Verband für Sicherheit in der Wirtschaft Norddeutschland e.V., Verband für Sicherheit in der Wirtschaft Nordrhein-Westfalen e.V., Vereinigung für die Sicherheit der Wirtschaft e.V. Hessen – Rheinland – Pfalz – Saarland, Arbeitskreis für Unternehmenssicherheit Berlin-Brandenburg

43 Quelle: www.asw-online.de

44 Lux/Peske (2002), S. 52

45 Ulfkotte (1999), S. 20

auch wenn sie wollten, können staatliche Behörden nur in geringem Maße zur Abwehr von Konkurrenz- und Wirtschaftsspionage beitragen, in erster Linie müssen sich Unternehmen selbst schützen, was sie mit verschiedenen Mitteln tun.

Als erstes ist hier der betriebliche Werkschutz bzw. die Sicherheitsabteilung zu nennen. Deren Aufgabe ist der Schutz des materiellen sowie immateriellen Unternehmensbesitzes sowie von Personen, soweit dies erforderlich ist.[46] Teilweise gehören auch der Informationsschutz bzw. die IT-Sicherheit dazu, die aber in vielen Unternehmen auch von eigenen Abteilungen wahrgenommen werden.

Daneben sind unternehmensexterne Dienstleister von immer größerer Bedeutung. Eine erste Gruppe bietet ähnliche Aufgaben wie der Werkschutz an, also Dienstleistungen im Wach- und Sicherheitsdienst. Aus Kostengründen werden diese immer häufiger an externe Subunternehmen ausgelagert. Weitergehende Dienstleistungen bieten die so genannten Intelligence-Trader an.[47] Damit sind verschiedenste Unternehmen bezeichnet, die spezialisierte Leistungen im Bereich Competitive Intelligence und Spionageabwehr anbieten.[48] Da sie meist sowohl aktiv Informationen beschaffen, als auch Beratung zur Spionageabwehr leisten, ist es schwer, diese getrennt darzustellen. Auf dem Weg der Counterintelligence erlangen Unternehmen natürlicherweise auch offensive Konkurrenzspionagekenntnisse, denn es ist nicht möglich, Spionageabwehr zu betreiben, ohne zu wissen, wie aktive Spionage betrieben wird.[49] Auf dem privaten Sektor hat sich dadurch ein eigener Sicherheitssektor herausgebildet, auf den im Kapitel 3.4 noch genauer eingegangen wird.

3.1.4 Probleme von Wirtschaftsspionage

In den 1990er Jahren wurde der Einsatz der Geheimdienste für Wirtschaftsspionage sowohl in der Intelligence-Praxis, als auch in der Literatur intensiv und kontrovers diskutiert. Die wirtschaftliche Stärke eines Staates gewann an Bedeutung für die

46 Lux/Peske (2002), S. 51/52
47 ebd.
48 ebd.
49 Fink (2002), S. XVII

Machtverteilung im internationalen Rahmen, was als Begründung dafür herangezogen wurde, dass die Wettbewerbsfähigkeit der eigenen Wirtschaft in direktem Zusammenhang zur nationalen Sicherheit steht. Daher wurde von den Nachrichtendiensten gefordert, die heimische Industrie im „Wirtschaftskrieg" zu unterstützen.

Die Vorstellung, dass ein Unternehmen durch gezielte Spionage von staatlichen Geheimdiensten an Informationen kommt, die seine Wettbewerbsfähigkeit gegenüber ausländischen Konzernen erhöht, schien und scheint für viele Autoren und politische Entscheidungsträger verlockend, jedoch werden dabei die Probleme, die im Zusammenhang mit Wirtschaftsspionage entstehen, oft nicht berücksichtigt. Dabei können zwei Felder unterschieden werden: das erste betrifft die Abnehmerseite, also die Wirtschaft bzw. Unternehmen, das zweite die Natur der Geheimdienstarbeit.

Bei den die Wirtschaft betreffenden Problemen ist zunächst die heutige Verflechtung der Volkswirtschaften untereinander für etwaige staatliche Eingriffe, wozu die Begünstigung bestimmter Unternehmen oder Branchen gehört, problematisch. Wird beispielsweise die Konkurrenzfähigkeit eines deutschen Unternehmens auf Kosten eines ausländischen erhöht, bedeutet das Nachteile für diejenigen Beschäftigten des ausländischen Unternehmens, die im Inland tätig sind oder auch für eventuelle inländische Zulieferer. Es ist somit schwierig, den volkswirtschaftlichen Nutzen abzuschätzen.

Ein zweites Problem, das ebenfalls mit der zunehmenden internationalen Verschränkung der Wirtschaft zusammenhängt, ist der transnationale Charakter der heutigen Großunternehmen. Diese lassen sich oft nicht mehr nationalstaatlich zuordnen, was bei der Auswahl der zu fördernden Unternehmen ein Problem darstellt. Bevor die heimische Industrie gefördert werden soll, muss geklärt werden, was ein heimisches Unternehmen ausmacht, wobei weiterhin berücksichtigt werden muss, dass sich die Eignerstruktur börsennotierter Konzerne schnell ändern kann.

Als drittes besteht das Problem der Auswahl des begünstigten Unternehmens innerhalb einer Branche. Es müssen nicht nur Branchen definiert werden, die durch geheimdienstliche Arbeit unterstützt werden sollen, sondern innerhalb dieser Branchen auch bestimmte Unternehmen. Damit wiederum werden jedoch andere heimische Unternehmen der gleichen Branche benachteiligt, was Störungen der Marktmechanismen hervorruft. Vor allem würden höchstwahrscheinlich große Konzerne für eine solche Förderung infrage kommen, was kleinere Unternehmen benachteiligt und dadurch einen uneindeutigen volkswirtschaftlichen Gesamteffekt nach sich zieht.

Zu guter Letzt ist kritisch anzumerken, dass die unmittelbare Verwendung der von den Nachrichtendiensten erhaltenen Informationen durch die Unternehmen nicht unbedingt gegeben ist. Werden zum Beispiel Forschungs- und Entwicklungsergebnisse auf solchem Wege erlangt, heißt das noch nicht, dass diese sofort in die Arbeit eines anderen Unternehmens integriert werden können, denn dies ist auch abhängig von dessen Entwicklungsstand. Nur bei einer sehr engen Kooperation von Unternehmen und Geheimdiensten, bei der die Unternehmen konkrete Objekte zur Beschaffung benennen könnten, ist ein entscheidender Nutzen zu erwarten.

Neben diesen Problemen treten bei der Wirtschaftsspionage Probleme zutage, die mit der Funktion von Geheimdiensten zu tun haben. Hierunter fällt zunächst der Quellenschutz. Die Weitergabe der Informationen erfordert stets eine Gratwanderung zwischen zu allgemeinen und damit wertlosen Hinweisen und zu genauen Informationen, deren Nutzung Rückschlüsse auf die Quellen erlauben würde. Eine Gefährdung selbiger besteht sowohl für die menschlichen Quellen, als auch für die technischen Aufklärungsmöglichkeiten, die durch das Bekannt werden entwertet würden.

Des Weiteren müssen vor der Sammlung der Informationen die Bedürfnisse der Aufklärung festgelegt werden. Die Steuerung der nachrichtendienstlichen Tätigkeit müsste, um gute Ergebnisse zu erzielen, von den späteren Abnehmern vorgenommen werden, was bei den Diensten auf Widerstand stoßen dürfte.

Außerdem ist auch eine mögliche Abwehrhaltung der Geheimdienste gegenüber solchen Tätigkeiten an sich zu erwarten. Diese verstehen sich als kritische Instrumente für den Erhalt der nationalen Sicherheit und sind daher bereit, hohe Risiken bei der Beschaffung von Informationen einzugehen. Da keine direkte Verbindung zwischen Wirtschaftsspionage und nationaler Sicherheit besteht, ist die Motivation dafür eventuell schwer herzustellen. Prägnant ausgedrückt wurde der Sachverhalt von Robert Gates während seiner Zeit als DCI der US-Geheimdienste: kein Agent sei „willing to die for General Motors".[50]

Nicht zuletzt würde die Zusammenarbeit von befreundeten Geheimdiensten gefährdet. Da Wirtschaftsspionage oft zwischen politisch verbündeten Staaten stattfindet, kooperieren deren Nachrichtendienste teilweise sehr eng. Das ein- oder gegenseitige Ausspionieren von Unternehmen würde Misstrauen erwecken und damit die Zusammenarbeit verschlechtern.

Es ist also festzuhalten, dass die Kosten von Wirtschaftsspionage leicht den Nutzen überwiegen können. Schon rein monetär gesehen könnten infolge der Aufdeckung von Wirtschaftsspionageaktivitäten erhebliche Regressansprüche gegen die Geheimdienste bzw. die Regierung gestellt werden. Vor allem gilt dies aber hinsichtlich des diplomatischen Schadens. In den internationalen Beziehungen sind politische und militärische Spionagetätigkeiten zwar illegal, werden aber von den Staaten als gängige Praxis akzeptiert. Anders sieht es dagegen bei Wirtschaftsspionage aus, da diese nicht unmittelbar mit der nationalen Sicherheit in Zusammenhang steht.

Abgesehen von solchen mittelbaren Kosten ist die Vorteilhaftigkeit von Wirtschaftsspionage aber auch bei einer direkten kostenrechnerischen Analyse nicht unbedingt gegeben. Nachrichtendienstliche Arbeit ist sehr kostenintensiv, und so kann der Rückgriff auf diese Ressourcen leicht den Vorteil kompensieren, der durch die Erlangung der Informationen erreicht werden kann.

50 Wolf, Jim: Industrial Spying Comes in From the Cold, Reuters News Service, 3.8.1991

3.1.5 Fazit: Die Beziehungen zwischen staatlichen Nachrichtendiensten und privaten Akteuren im Bereich der Wirtschaftsspionage

Die organisatorische Voraussetzung für das effiziente Betreiben von Wirtschaftsspionage ist eine staatliche Stelle, die eine nationale Industriepolitik definiert und im Anschluss daran die Spionageaktivitäten steuert.

Aus der Analyse des Betreibens von Wirtschaftsspionage der oben genannten Länder lässt sich folgende Tendenz erkennen: Systematische Wirtschaftsspionage wird von einem Land desto eher betrieben, je mehr Staat und Wirtschaft dieses Landes ineinander verwoben sind. In der Fachliteratur, die sich mit Gesellschaften und der Beziehung zwischen Staat und Wirtschaft beschäftigt, wird häufig von zwei ideologischen Paradigmen, nämlich der individualistischen und der gemeinschaftlichen Gesellschaft gesprochen.[51] Auf einem Kontinuum würde unter den hoch entwickelten Mächten die USA als individualistische Gesellschaft an dem einen Extrempunkt stehen, Japan als gemeinschaftliche Gesellschaft am anderen. In Japan ist es damit einfacher, direkte und dauerhafte Verbindungen zwischen Nachrichtendiensten und privaten Unternehmen aufzubauen, so dass Wirtschaftsspionage effizient betrieben werden kann. Denn nur so können aufgrund eines geäußerten Bedürfnisses eines Unternehmens gezielt benötigte Informationen beschafft werden. Die Kommunikation zwischen Unternehmen und Nachrichtendiensten muss für einen systematischen Betrieb von Wirtschaftsspionage in beide Richtungen erfolgen, sowohl von den Diensten zu den Unternehmen, als auch anders herum. In den USA erscheint vor allem letzteres zweifelhaft. Mit Ausnahme des Rüstungssektors, der, wie erläutert, eine besondere Rolle spielt, kann davon ausgegangen werden, dass es solche Verbindungen nicht gibt und damit auch keine systematische Wirtschaftsspionage betrieben wird.

Insgesamt lässt sich die Beziehung zwischen privaten Akteuren und staatlichen Nachrichtendiensten im Bereich der Wirtschaftsspionage wie folgt charakterisieren: In der Wirtschaftsspionage werden von Nachrichtendiensten gesammelte

51 Lux/Peske (2002), S. 37

Informationen an Unternehmen des eigenen Landes weitergegeben, um sie im Wettbewerb gegenüber der internationalen Konkurrenz zu stärken. Dabei ist ein wechselseitiger Austausch zwischen Unternehmen und den Diensten zum effizienten Betrieb nötig. In erster Linie profitieren von der Austauschbeziehung jedoch die privaten Akteure der heimischen Wirtschaft, weshalb diese hier als *Abnehmer* staatlicher Intelligence klassifiziert werden können.

3.2 Private Satellitenaufklärung

Während in der Wirtschaftsspionage per Definition schon ein Zusammenhang zwischen privaten Akteuren und staatlichen Nachrichtendiensten besteht, haben erstere im Bereich der Satellitenaufklärung erst in den letzten Jahren eine Bedeutung für die Dienste gewonnen.

3.2.1 Aufklärungssatelliten als staatliche Domäne?

Aufklärungssatelliten sind seit über 40 Jahren eine klassische Domäne der Geheimdienste. Diese Quelle ist für sie deswegen so bedeutsam, da durch sie überall auf der Welt Bilder legal und meist unbemerkt aufgenommen werden können. Über Jahrzehnte waren die USA und Russland die einzigen Staaten, die über entsprechende Kapazitäten verfügten. Im Jahre 1999 hatten jedoch bereits 21 Staaten und private Organisationen Aufklärungssatelliten im All stationiert, darunter Frankreich, Japan, Südkorea, China, Indien und Kanada.[52] Mit der Inbetriebnahme des Internet-Services „Google Earth“ sind Satellitenbilder jedermann zugänglich geworden. Die dort angebotenen Bilder mit einer Auflösung zwischen 15 Zentimetern und 15 Metern[53] sind zwar nicht aktuell, dafür aber kostenlos zugänglich.

Ein Großteil des amerikanischen Intelligence-Budgets floss und fließt auch heute in den Bau, die Stationierung und den Unterhalt der Satelliten. Dafür liefert IMINT stets bedeutende Informationen für die Politik der Vereinigten Staaten. Bei-

52 Florini, Ann M./Dehqanzada, Yahya A.: Secrets for Sale: How Commercial Satellite Imagery will change the World, Washington D.C.: Carnegie Endowment for International Peace, 2000, S. 15
53 Quelle: http://de.wikipedia.org/wiki/Google_Earth

spielsweise wurde so in den 60er Jahren erkannt, dass der vermutete Missile Gap zur Sowjetunion nicht bestand. Auch entdeckten die USA auf diese Weise russische Raketen auf Kuba. Insgesamt war und ist das Satellitenprogramm der Grundstein für das amerikanische Verteidigungsprogramm, die amerikanische Sicherheitspolitik und Abrüstungsverhandlungen.

Während Satellitenbilder im Kalten Krieg ausschließlich zur Aufklärung verwendet wurden, bekommen sie mit der verstärkten Nutzung von Präzisionswaffen eine neue Bedeutung.[54] Nahezu-Echtzeit-Satellitenbilder dienen in Kriegshandlungen heute vor allem auch der Zielbestimmung.[55] Zum ersten Mal spielten sie diese Rolle während der Operation „Desert Storm" 1991, seither wurde die Satellitenaufklärung umfassend in die Kriegsplanung und –durchführung eingebunden.

3.2.2 Der private Satellitenmarkt

Auf dem privaten Satellitenmarkt ist zwischen solchen Anbietern zu unterscheiden, die Bilder staatlicher Satelliten kommerziell vermarkten, und solchen, die auch die Satelliten privat betreiben.

3.2.2.1 Kommerzielle Vermarktung von Bildern staatlicher Satelliten

Die ersten kommerziellen Satellitenbilder waren 1972 von der National Aeronautics and Space Administration (NASA) im Rahmen des Landsat-Programmes erhältlich. In den USA gab es damit schon relativ früh Versuche, Satellitenbilder dem privaten Sektor zugänglich zu machen, auch wenn die Auflösung der Bilder deutlich schlechter war als die, die dem Militär und der Intelligence Community zur Verfügung stand. Dadurch waren die Bilder für die allermeisten Anwendungen, an denen der private Sektor interessiert war, zunächst nicht tauglich.[56] Die Rohdaten der Bilder wurden jedoch beinahe umsonst weitergegeben, womit ein erster Sektor für die

54 Dupont, Alan: Intelligence for the Twenty-First Century, Intelligence and National Security, Vol. 18, Nr. 4, 2003, S. 18

55 vgl. Best, Richard A. Jr.: Imagery Intelligence: Issues for Congress, CRS Report for Congress, April 12, 2002, http://www.fas.org/irp/crs/IB10012.pdf,

56 Florini, Ann M./Dehqanzada, Yahya A.: No more secrets? Policy Implications of Commercial Remote Sensing Satellites, Washington D.C.: Carnegie Paper No. 1, 1999, http://www.carnegieendowment.org/publications/index.cfm?fa=view&id=150

Verarbeitung der Rohdaten entstand.[57] In der Hoffnung, die Kosten für die extrem teuren Satelliten zu senken, wurde das Landsat-Programm 1979 in das Department of Commerce verschoben. Man versprach sich darüber hinaus auch eine Ausweitung der kommerziellen Nutzung und, im Anschluss daran, die Entwicklung eigener Aufklärungssatelliten durch den privaten Sektor.[58] Im Jahr 1985 wurde der Betrieb der Landsat-Satelliten gänzlich in den privaten Sektor verschoben, indem es einem Joint Venture der Firmen RCA Corporation und Hughes Aircraft Company mit dem Namen EOSAT übertragen wurde. Jedoch erwiesen sich die Schätzungen über die Größe des privaten Marktes als zu optimistisch, was ein mehrmaliges Beinahe-Scheitern und weitere umfangreiche Regierungssubventionen zur Folge hatte. In den frühen 1990er Jahren war die Privatisierung des Landsat-Programmes schließlich endgültig gescheitert, und es drohte ganz eingestellt zu werden. Zum Scheitern trug vor allem auch bei, dass mit dem Ende des Kalten Kriegs drei weitere Länder Bilder von staatlichen Aufklärungssatelliten kommerziell vermarkteten. Neben Frankreich (SPOT-Satelliten) waren dies Indien (IRS-1C und -1D) und Russland (SPIN-2). Diese neuen Anbieter boten darüber hinaus Bilder höherer Auflösung und mit kürzerer Wiederkehrzeit über dem gleichen Objekt als die Landsat-Satelliten. Da sich Landsat allerdings während des Golfkriegs 1990/91 als sehr nützlich erwiesen hatte, wurde es 1992 an die NASA und das Department of Defense rückübertragen.

3.2.2.2 Das Aufkommen privater Betreiber

Die gesetzliche Möglichkeit zur Gründung privater Satellitenbetreiber bestand bereits seit dem Inkrafttreten des Land Remote Sensing Commercialization Acts von 1984, jedoch beantragte in den ersten acht Jahren seiner Geltung aufgrund der starken Regulierung kein privates Unternehmen eine Lizenz.

57 Williamson, Ray A.: Remote Sensing Policy and the Development of Commercial Remote Sensing, in: Baker, John C./O'Connell, Kevin M./Williamson, Ray A. (Hrsg.): Commercial Observation Satellites: At the Leading Edge of Global Transparency, Santa Monica: RAND Corporation, 2001, S. 40

58 ebd., S. 41

Dies änderte sich mit dem Land Remote Policy Act von 1992, der neben der Rückübertragung des Landsat-Programmes an die öffentliche Hand Anreize für private Initiativen in der Satellitenaufklärung schuf. Vor 1992 waren die Beschränkungen vor allem für den Verkauf von Bildern an nicht-amerikanische Kunden sehr streng, weshalb diese das Angebot nur in seltenen Fällen nutzen konnten oder wollten. Das Gesetz erlaubte es privaten Satellitenbetreibern nun, Bilder auch exklusiv und ohne gesetzliche Preisvorgaben an Kunden im In- und Ausland zu verkaufen.[59] In der Folge beantragten bis zum heutigen Zeitpunkt 21 Firmen eine Lizenz zum kommerziellen Betrieb von Aufklärungssatelliten, die in Tabelle 2 aufgeführt sind.

59 Florini/Dehqanzada (2000), S. 18

Tabelle 2: Vergebene Lizenzen an private Aufklärungssatellitenbetreiber in den USA		
Firma	**Datum der Ausstellung**	**Homepage**
DigitalGlobe (ursprünglich WorldView)	04.01.1993	www.digitalglobe.com
Space Imaging (ursprünglich EOSAT)	17.06.1993	www.spaceimaging.com
Space Imaging (ursprünglich Lockheed)	22.04.1994	www.spaceimaging.com
OrbImage (ursprünglich Orbital Sciences)	05.05.1994	www.orbimage.com
OrbImage (ursprünglich Orbital Sciences)	01.07.1994	www.orbimage.com
DigitalGlobe	02.09.1994	www.digitalglobe.com
AstroVision	23.01.1995	www.astrovision.com
GDE Systems Imaging*	14.07.1995	www.gdesystems.com
Motorola*	01.08.1995	http://mcg.motorola.com
Boeing Commercial Space*	16.05.1996	www.boeing.com/defense-space/space
CTA Corporation*	09.01.1997	-
RDL Corporation*	16.01.1998	www.rdl.com/space_corp/space_corp.html
STDC	26.03.1999	www.earthsearch.com
Ball Aerospace/Technologies	21.11.2000	www.ball.com/aerospace/batchp.html
DigitalGlobe	06.12.2000	www.digitalglobe.com
Space Imaging	06.12.2000	www.spaceimaging.com
DigitalGlobe	14.12.2000	www.digitalglobe.com
TransOrbital	06.03.2002	www.transorbital.net
DigitalGlobe	29.09.2003	www.digitalglobe.com
Space Imaging	14.10.2003	www.spaceimaging.com
Northrop Grumman	20.02.2004	www.northropgrumman.com
* Lizenz beendet		

Quelle: NOAA Satellite and Information Service[60]

Über beinahe 30 Jahre hielten die USA damit zivile und militärische Aufklärung strikt getrennt, wobei Bilder mit einer Auflösung von besser als 10m für Sicherheitsbelange reserviert blieben. Diese Trennung wurde erst durch das Aufkommen

60 National Oceanic and Atmospheric Administration (NOAA), http://www.licensing.noaa.gov/licensees.html

nicht-amerikanischer Satelliten aufgebrochen.[61] Anfang der 90er Jahre traten gleich mehrere solche Anbieter auf, und die amerikanischen Betreiber befürchteten auf dem Markt für private Satellitenaufklärung ins Hintertreffen zu geraten. Eine starke Lobby sorgte schließlich dafür, dass die Beschränkungen mit der Presidential Decision Directive 23 (PDD-23) im Jahr 1994 weiter gelockert wurden.

Zu den neuen Akteuren gehörten neben der französischen SPOT Image die indischen Satelliten IRS-1C und –1D, die Bilder mit einer Auflösung von unter 10m boten. Daneben waren Bilder von russischen militärischen Spionagesatelliten zu haben, die in den USA von amerikanischen Firmen vermarktet wurden. Diese boten Bilder mit einer hohen Auflösung sowie eine große Zahl historischer Bilder, die in den Jahrzehnten gesammelt wurden, in denen sie auf amerikanisches Territorium ausgerichtet waren. 1997 gelang es einem amerikanisch-russischem Joint-Venture zwischen Aerial Images und Sovinformsputnik einen russischen Satelliten ins All zu schießen, der 45 Tage lang Tausende von Bildern machte.[62] Diese wurden anschließend über die von Microsoft, Compaq und Kodak betriebene Datenbank „Terraserver" über das Internet zum Verkauf angeboten.[63]

Obwohl bei all diesen Initiativen private Firmen die Vermarktung der Bilder übernahmen, wurde der Betrieb der Systeme von staatlicher Seite übernommen oder stark subventioniert. Private Investoren schreckten lange vor den hohen Kosten zurück, die für den Bau und die Stationierung des Satelliten und der zugehörigen Basisstation zwischen geschätzten 100 und 500 Millionen Dollar betragen.[64]

Der erste rein kommerzielle Aufklärungssatellit war Ikonos 2 der amerikanischen Firma Space Imaging, der im September 1999 seinen Betrieb aufnahm und eine Auflösung von 1m bietet.[65] Kurz darauf folgte der Start des QuickBird-

61 Baker, John C./Williamson, Ray A./Johnson, Bret: U.S. Security Interests and Dual-Purpose Satellite Technologies: Framing the Policy, in: Williamson, Ray A. (Hrsg.): Dual-Purpose Space Technologies, Washington D.C.: Space Policy Institute, 2001, S. 19

62 Amato, Ivan: God's Eyes for Sale, Technology Review Vol. 102, Nr. 2, 1999

63 ebd.

64 Florini/Dehqanzada (1999), S. 22

65 Smith, Marcia S.: U.S. Space Programs: Civilian, Military and Commercial, Issue Brief for Congress, Updated Version of April 22, 2003, S. 4/5, http://usinfo.state.gov/usa/infousa/tech/space/programs.pdf

Satelliten der Firma DigitalGlobe, der sogar Objekte von einer Größe bis zu 60cm „sehen" kann.[66] Einen Überblick über kommerzielle Anbieter von Satellitenbildern gibt Tabelle 3. Sie erfasst sowohl rein privat betriebene Satelliten als auch private Anbieter von Bildern, die von staatlichen Satelliten stammen.

Tabelle 3: Kommerzielle Anbieter von Satellitenbildern

Firma	Land	Satellit	Privat/ Staatl.	max. Auflösung (schwarz-weiß)	Satelliten-start
Landsat	USA	Landsat 3-7	staatlich	14 m (Landsat 7)	1978 - 1999
Space Imaging (2006 von OrbImage übernommen)	USA	Ikonos 2	privat	0,8 m	1999
OrbImage	USA	OrbView 2, 3	privat	1 m	1997/2003
DigitalGlobe (vormals Earth Watch, davor World View)	USA	QuickBird 1, 2	privat	0,6 m	2001
MDA	Kanada	Radarsat-1	staatlich	8 m	1995
Spot Image S.A.	Frankreich	SPOT 1-5	staatlich	2,5 m (SPOT 5)	1986-2002
Sovinformsputnik	Russland	SPIN-2	staatlich	2 m	regelmäßig, Lebensdauer 45 Tage
National Remote Sensing Agency	Indien	IRS-1C und -1D	staatlich	5 m	1995/1997
ImageSat International	Israel	EROS-A	privat	1,8 m	2000
Staatlich	Südkorea	Kompsat-1	staatlich	10 m	1999

3.2.2.3 Die Ursachen für das Aufkommen privater Betreiber

Das Aufkommen privater Satellitenbetreiber in den 90er Jahren ist nach Florini/Dehqanzada[67] insgesamt auf vier Ursachen zurückzuführen.

Erstens fielen mit dem Ende des Kalten Krieges viele Beschränkungen und Auflagen für private Satellitenbetreiber weg, da kommerzielle Interessen nun nicht mehr der Politik untergeordnet waren. Amerikanischen Satellitenbauern wurde es dadurch beispielsweise erlaubt, ihre technische Expertise auch für den Bau privater Satelliten zu verwenden.

66 ebd.

67 vgl. Florini/Dehqanzada(1999) sowie Florini/Dehqanzada (2000)

Zweitens bestand nun die Aussicht auf einen breiten Markt für private Satellitenbilder. Aufgrund von Marktstudien waren mehrere Investoren zuversichtlich, dass sich eine Nachfrage entwickeln würde, sobald die Systeme zur Verfügung stünden. Dabei wurde unter anderem an Farmer, Städteplaner, Kartographen, Umwelt-Aktivisten, Notfallrettungsteams, Nachrichtendienste/Medien, Landvermesser, Geologen, Bergbau- und Ölunternehmen und die Holzindustrie als mögliche Nutzer gedacht. Daneben entdeckten auch Regierungen von Staaten, die über keine eigenen Satellitenaufklärungskapazitäten verfügten mehr und mehr nützliche Anwendungen.[68]

Drittens schufen technologische Fortschritte die Voraussetzungen für eine kommerzielle Vermarktung. Neben den Weiterentwicklungen im optischen Satellitenbaubereich wurde vor allem die Verarbeitung und Weitergabe von Bildern aufgrund der Entwicklungen im informationstechnischen Bereich einfacher, beispielsweise durch die Weitergabe von Bildern auf CD-ROM.

Viertens unterstützte die amerikanische Regierung private Initiativen, weil sie weiterhin auf Kostensenkungen hoffte und die Innovationsfähigkeit des privaten Sektors nutzen wollte. Der Markt für private Satellitenbilder sollte dabei nicht anderen Ländern überlassen werden, weshalb privaten Betreibern direkte und indirekte Subventionen geleistet wurden. Weiterhin sorgt die amerikanische Regierung dafür, dass auch von staatlicher Seite Nachfrage entsteht. In der PDD-49 vom September 1996 wurden in der Folge sämtliche Regierungsstellen dazu aufgerufen, kommerzielle Satellitenbilder im größtmöglichen Umfang zu nutzen.[69] Diesen vier Ursachen ist hinzuzufügen, dass durch den Zugriff auf Raketen unterschiedlicher Staaten die Kosten für die Stationierung gesunken sind. Zusammen mit den angesprochenen technologischen Fortschritten können Satellitenbilder zu Preisen verkauft werden, die sie für eine breite Kundenschicht interessant machen (siehe Tabelle 4).

68 O'Connell, Kevin/Lachman, Beth E.: From Space Imagery to Information: Commercial Remote Sensing Market Factors and Trends, in: Baker, John C./O'Connell, Kevin M./Williamson, Ray A. (Hrsg.): Commercial Observation Satellites: At the Leading Edge of Global Transparency, Santa Monica: RAND Corporation, 2001, S. 62

69 Best (2002), S. 16

Tabelle 4: Kosten für ein bearbeitetes Satellitenbild*			
Satellit	**Preis pro Km²**		**minimale Bildgröße**
	Neuanfertigung	**Archiv**	
IKONOS (s/w)	50-57 $	38-48 $	100 Km²
QuickBird (s/w)	52-63 $	36-52 $	64 Km²
SPOT-5 (Farbe)	9 $	k.A.	1600 Km²
* über U.S. Territorium			

Quelle: Satellite Imaging Corporation[70]

3.2.2.4 Erwartete zukünftige Entwicklung

In der Phase des rapiden Wachstums der Weltraumindustrie in den 90er Jahren gab es eine Vielzahl von Projekten von Staaten und privaten Unternehmen mit dem Ziel, Aufklärungssatelliten im All zu stationieren. Schätzungen, die in den frühen 90er Jahren über den Markt für private Satellitenaufklärung gemacht wurden, sagten für die Jahrtausendwende eine Marktgröße zwischen 2 und 20 Milliarden Dollar voraus.[71] Mit dem Platzen der New-Economy-Blase Anfang des neuen Jahrtausends wurde der gesamte Weltraummarkt jedoch schwer getroffen und erholt sich seither nur langsam.[72] Aufgrund dessen wurden auch die meisten Projekte der kommerziellen Fernaufklärung aufgeschoben oder eingestellt. Der Markt für private Satellitenaufklärung im Jahr 2000 betrug 173 Millionen Dollar, also nur etwa zehn Prozent der konservativsten Schätzung zehn Jahre zuvor.[73]

Heute sind die Aussichten für die Entwicklung des Marktes für private Satellitenbilder jedoch wieder besser. In einer OECD-Studie wird der „Downstream"-Markt, also die Vermarktung von Satellitenbildern, im Jahr 2003 auf eine knappe Milliarde Dollar geschätzt und soll bis 2010 auf ca. 2 Milliarden Dollar steigen.[74] Diese Schätzungen basieren auf einer Szenario-Analyse, in der für die private Satellitenaufklärung eine relativ gute Entwicklung vorausgesagt wird.[75] Jedoch herrscht international großer Wettbewerb, da neben den privaten Betreibern mehrere Länder

70 http://www.satimagingcorp.com/pricing.html
71 O'Connell/Lachman (2001), S. 68
72 Andrieu, Michel: Space 2030: Exploring the Future of Space Applications, OECD-Studie, Paris: OECD, 2005 S. 13
73 O'Connell/Lachman (2001), S. 70
74 Andrieu (2005), S. 15
75 ebd., S. 117-119

Bilder ihrer staatlich betriebenen Satelliten vermarkten und in vielen Fällen die Bildaufklärung mittels Flugzeugen kommerzielle Bedürfnisse ebenso erfüllt.[76]

3.2.3 Bedeutung privater Satellitenaufklärung für staatliche Nachrichtendienste

Bei der Analyse der Bedeutung von privat betriebenen Aufklärungssatelliten muss zwischen Staaten unterschieden werden, die über eigene derartige Kapazitäten verfügen, und solchen, die zuvor keinen eigenen Zugang zu Satellitenbildern hatten.

3.2.3.1 Bedeutung für internationale Akteure ohne eigene Satellitenaufklärungskapazitäten

Das Aufkommen privater Akteure im Bereich IMINT eröffnet Akteuren im internationalen und transnationalen Raum vollkommen neue Möglichkeiten. Diskutiert wird dies in der Literatur unter dem Stichwort der „globalen Tranzparenz".

Nationalstaaten, die bisher über keine eigenen Satellitenaufklärungskapazitäten verfügen, können nun Entwicklungen auf der ganzen Welt verfolgen. Zu diesen Staaten gehörte bis vor kurzem unter anderem auch Deutschland. Gegenwärtig baut die Bundeswehr ihr eigenes nationales Beobachtungssystem „SAR LUPE" auf, um nicht mehr ausschließlich auf die amerikanischen Nachrichtendienste oder private Betreiber als Quelle für IMINT angewiesen zu sein. Dass der BND aber schon seit langem auf kommerziell vermarktete Satellitenbilder zurückgreift, ist spätestens seit 1987 klar. Damals benutzte er SPOT-Bilder, um die Konstruktion einer Chemiewaffenfabrik in der Nähe von Rabta in Lybien öffentlich zu belegen.[77]

Internationale Organisationen, allen voran die UN, profitieren, da sie mit privaten Satellitenbetreibern unabhängig von der Weitergabe von Bildern der Geheimdienste ihrer Mitgliedsstaaten werden.[78] Bei den nichtstaatlichen Akteuren schließlich profitieren beispielsweise NGOs von dieser Entwicklung, indem sie mit

76 ebd., S. 48

77 Florini/Dehqanzada (2000), S. 4

78 Lynch, Colum: Private Firms Aid U.N. On Sanctions; Wider Intelligence Capability Sought, The Washington Post vom 21.4.2001

Satellitenbildern schlagkräftige Argumente sammeln um Nationalstaaten zum Handeln in ihren Anliegen zu bewegen.[79]

3.2.3.2 Bedeutung für internationale Akteure mit eigenen Satellitenaufklärungskapazitäten

In einer anderen Situation befinden sich Länder, die über eigene Spionagesatelliten verfügen. Für sie gehen einerseits angesichts des Dual-Use-Charakters große Gefahren von der weltweiten Verbreitung von privaten Satellitenbildern aus, andererseits können auch sie von den Entwicklungen auf dem privaten Sektor profitieren. In erster Linie sind bei den westlichen Nachrichtendiensten hiervon die USA betroffen, die auf dem Gebiet der militärischen wie zivilen Fernaufklärung führend sind. Hier wird daher eine US-amerikanische Perspektive eingenommen, wobei die Aussagen auf Länder wie Frankreich in ähnlicher Weise zutreffen.

Risiken

Die Gefahren, die von der globalen Verfügbarkeit aktueller Satellitenbilder ausgehen, können nach Baker/Johnson in vier Bereiche unterteilt werden.[80]

Erstens erhöht sich das Risiko durch den Zugriff aggressiver Staaten auf diese Informationsquelle. Es wird befürchtet, dass feindliches Militär im Konfliktfall durch Satellitenaufklärung einen besseren Situationsüberblick („Situational Awareness“) erreichen kann. Des Weiteren könnten hoch auflösende Bilder von feindlichen Mächten zur Zielbestimmung genutzt werden. Vor allem in Kombination mit satellitengestützten Ortungssystemen wie GPS könnten größere Truppenansammlungen damit ein leichtes Ziel für gegnerische Raketenangriffe werden.

Zweitens geht eine erhöhte Gefahr von nichtstaatlichen Akteuren aus, die Zugang zu Satellitenbildern haben. In erster Linie ist hierbei an Terroristen zu denken, die somit an bisher unzugängliche Informationen kommen können. Daneben

79 vgl. Litfin, Karen T.: The Globalization of Transparency: The Use of Commercial Satellite Imagery by Nongovernmental Organizations, in: Baker, John C./O'Connell, Kevin M./Williamson, Ray A. (Hrsg.): Commercial Observation Satellites: At the Leading Edge of Global Transparency, Santa Monica: RAND Corporation, 2001

80 vgl. Baker, John C./Johnson, Dana J.: Security Implications of Commercial Satellite Imagery, in: Baker, John C./O'Connell, Kevin M./Williamson, Ray A. (Hrsg.): Commercial Observation Satellites: At the Leading Edge of Global Transparency, Santa Monica: RAND Corporation, 2001, S. 110

besteht für Nationalstaaten aber auch die Gefahr zu Handlungen gedrängt zu werden, die nicht ursprünglich in ihrem Interesse lagen. NGOs könnten mit Satellitenbildern Ereignisse wie humanitäre Katastrophen aufdecken, die durch mediale Verbreitung in der Folge die Öffentlichkeit sensibilisieren. Ist die öffentliche Meinung stark genug, könnten politische Entscheidungsträger dadurch durchaus zum Handeln gezwungen werden.

Drittens entsteht eine Gefahr dadurch, dass Aktivitäten des eigenen Militärs in Friedens- wie in Kriegszeiten ständig überwacht werden können. Operationelle Überraschungen, wie sie beispielsweise während der Operation Desert Storm („left hook") gelangen, sind dadurch nicht mehr möglich.[81]

Schließlich besteht die Gefahr, dass bisher geheime Intelligence-Quellen und -Methoden offen gelegt werden. Damit könnten sich Akteure, die sich ihrer Beobachtung nicht bewusst waren, vor Spionage schützen, was solche Quellen entwerten würde.

So bedrohlich diese Gefahren sind, muss jedoch kritisch angemerkt werden, dass vor allem für komplexe Anwendungen Fähigkeiten vorhanden sein müssen, über die die meisten der angesprochenen Akteure nicht verfügen. Die Interpretation von Satellitenbildern ist schwierig[82], wobei die Fehlerquellen bei der Datenerfassung, Dateninterpretation und Analyse der Bilder liegen können.[83] Im staatlichen Sektor liegt die Fehlerrate der Analysten während den ersten drei Jahren ihrer Arbeit bei ca. 90 Prozent[84] und einige Fehlinterpretationen von Medien, die Satellitenbilder bei der Berichterstattung nutzten, belegen diese Schwierigkeit.[85] Die Bildana-

81 Fabian, Robert A.: Force Protection in an Era of Commercially Available Satellite Imagery: Space Blockade as a Possible Solution, Newport: Naval War College, 2002, S. 3

82 vgl. Osterhout, Robert: Transcript des Vortrages auf der Konferenz „No more secrets? Policy implications of commercial remote sensing satellites" veranstaltet vom Carnegie Endowment for International Peace, 26.5.1999, zugänglich unter http://www.ceip.org/files/projects/tcs/remotesensingconf/OsterhoutTranscript.htm

83 Baker, John C.: New Users and Established Experts: Bridging the Knowledge Gap in Interpreting Commercial Satellite Imagery, in: Baker, John C./O'Connell, Kevin M./Williamson, Ray A. (Hrsg.): Commercial Observation Satellites: At the Leading Edge of Global Transparency, Santa Monica: RAND Corporation, 2001, S. 538

84 Florini/Dehqanzada (2000), S. 25

85 ebd., S. 24

lyse erfordert daher Experten mit jahrelanger Erfahrung, die nur in relativ geringer Zahl zur Verfügung stehen. Darüber hinaus ist selbst bei einer korrekten Auswertung der Bilder noch nicht gewährleistet, dass die Satellitenbilder in Kampfkraft umgewandelt werden können.[86] Dazu erforderlich ist eine umfassende Einbindung solcher Informationsquellen in das Kriegsführungskonzept.

Chancen

Insgesamt kann der Zugang zu privater Satellitenaufklärung die militärische Stärke von potentiellen Gegnern also entscheidend erhöhen. Die Frage ist, ob die Staaten, die über eigene Satellitenaufklärung verfügen, nicht ebenso davon profitieren können, indem sie ihre eigenen Kapazitäten teilweise abbauen und ihre klassifizierten Quellen in sinnvoller Weise ergänzen. Denn während die Qualität der Bilder stetig steigt, verkürzt sich die Verzögerung zwischen Aufnahme und Lieferung, wodurch inzwischen viele nachrichtendienstliche und militärische Bedürfnisse befriedigt werden können.[87]

Für Intelligence-Überwachungsmissionen mit hoher Priorität sind private Kapazitäten zumindest in naher Zukunft zwar kaum nutzbar, jedoch dürften sie für Aufgaben, die weniger dringend und weniger komplex sind, gut geeignet sein.[88] Darunter fallen unter anderem die weitläufige Überwachung von Regionen zur Entdeckung neuer Aktivitäten oder Bautätigkeiten, sowie die Überwachung von Waffentests und -fabriken, Militärbewegungen und Abrüstungsvereinbarungen.[89]

Ein grundsätzlicher Vorteil privater Produkte besteht darin, dass sie keine Geheimhaltungsstufe erfordern und somit an Verbündete oder die Öffentlichkeit weitergegeben werden können. Vor allem für politische Entscheidungsträger als Abnehmer von Intelligence steigt der Wert der Information damit. Aber auch die Nachrichtendienste selber können solche Bilder an andere Nachrichtendienste weitergeben, was die Zusammenarbeit vereinfacht.

86 Grundhauser, Lt. Col. Larry K., USAF: Sentinels Rising: Commercial High-Resolution Satellite Imagery and Its Implications for US National Security, Airpower Journal, Vol. 12, Nr. 4, 1998, S. 67.
87 Baker/Johnson (2001), S. 110.
88 ebd.
89 ebd., S. 110/111.

Ein weiteres Argument für die verstärkte Nutzung privater Anbieter durch staatliche Dienste ist die erwartete Kostensenkung, die schon bei der Privatisierung des Landsat-Programmes ein Motiv war. Es kann davon ausgegangen werden, dass private Satellitenbilder durch bessere Marktausrichtung und höhere Effizienz um ein Vielfaches billiger sind. Angesichts der Tatsache, dass die mit Satelliten betriebene Fernaufklärung ein sehr bedeutender Posten innerhalb des Intelligence-Budgets ist, besteht ein Anreiz, dieses durch Zukauf privater Kapazitäten zu entlasten.

Schließlich könnten Nachrichtendienste von der Innovationsfähigkeit des privaten Sektors profitieren. Aufgrund des wachsenden Marktes für Satellitenbilder wird die technische Entwicklung vorangetrieben, was sowohl den Bau von Satelliten, beispielsweise im Bereich elektro-optischen Sensoren, Computer und Massenspeicher[90], als auch die wertsteigernde Verarbeitung der Rohdaten („Back-End“) angeht. Diese wurde im öffentlichen Sektor stets vernachlässigt, während sich der private Sektor den Bedürfnissen der Kunden schnell angepasst hat.

Einige Reformer gehen so weit, dass sie mit dem Aufkommen privater Betreiber von Aufklärungssatelliten komplette Arbeitsbereiche aus der nachrichtendienstlichen Tätigkeit ausgliedern wollen. Angesichts der Tatsache, dass Nachrichtendienste aufgrund der Breite der Themenpalette nicht in der Lage sind, alle Aufgaben in der nötigen Tiefe zu bearbeiten, könnten auf die jeweiligen Themen spezialisierte NGOs oder supranationale Organisationen eingesetzt werden. Gedacht wird dabei vor allem an die Überwachung von Abrüstungsverträgen[91], aber auch andere internationale Verträge, beispielsweise im Umweltbereich.

Regulierungspolitik

Während des ersten Golfkrieges, in dem Satelliten überhaupt zum ersten Mal als operative Werkzeuge eingesetzt wurden, benutzten die USA neben den eigenen militärischen Aufklärungssatelliten auch private Satelliten. Um bessere Karten für

90 Grundhauser (1998), S. 72
91 ebd., S. 70

die Missionsplanung zeichnen zu können wurden französische SPOT-Satellitenbilder zugekauft.[92] Gleichzeitig wurde mit diplomatischen Mitteln verhindert, dass der Irak, der Satellitenbilder nachgewiesenermaßen für die Invasion von Kuwait benutzte[93], Zugriff auf SPOT-Kapazitäten bekommt.[94] Die Verhandlungen um das UN-Embargo, das den Handel mit Satellitenbildern einschloss, dauerten jedoch relativ lange, weshalb während des Afghanistan-Krieges eine andere Strategie angewandt wurde: hier kauften die USA die Exklusivrechte für die Ikonos-Satellitenbilder der Region.[95]

Neben diesen diplomatischen und ökonomischen Mitteln betreiben die USA eine Politik des „Shutter Control", die einerseits ermöglichen soll, von den Entwicklungen im privaten Sektor zu profitieren, während andererseits die potentiellen Gefahren so klein wie möglich gehalten werden sollen. Mit der PDD-23 vom März 1994 wurden die meisten Beschränkungen für den Verkauf von kommerziellen Satellitenbildern amerikanischer Betreiber beseitigt, jedoch sind mit der Erteilung einer Lizenz einige Bedingungen verbunden. Diese erlauben es der Regierung, den Anbietern das Sammeln und den Verkauf von Bildern zu verbieten, wenn sie dies aufgrund internationaler Verpflichtungen, nationaler Sicherheitsaufgaben und außenpolitischer Angelegenheiten für notwendig erachtet. Mit Israel existiert darüber hinaus ein Abkommen, das amerikanischen Betreibern die Vermarktung nur solcher Bilder von israelischem Territorium erlaubt, die von der Auflösung her nicht besser sind als die besten, die auf dem internationalen Markt erhältlich sind.

Obwohl amerikanische Unternehmen auf dem privaten Markt führend sind, gibt es mehr und mehr nicht-amerikanische Betreiber, die nicht unter diese Beschränkungen fallen. In Militärkreisen werden daher schon seit längerem andere Methoden entwickelt, um ungewünschte Satelliten „abzuschalten" oder im Weltraum zu zerstören.

92 Fabian (2002), S. 3
93 Baker/Johnson (2001), S. 104
94 ebd., S. 7
95 Smith (2003), S. 5

Insgesamt ist es jedoch vor allem in Friedenszeiten unmöglich geworden, den Markt staatlicherseits zu regulieren. Dies liegt einerseits an der Tatsache, dass die USA und andere Länder den privaten Betrieb von Aufklärungssatelliten selber aktiv unterstützen um eine führende Stellung der eigenen Industrie auf dem Markt zu erlangen oder zu behalten. Andererseits sind die Betreiber der Satelliten zunehmend multinationale Unternehmen. Die hohen Investitionen, die in diesem Geschäft nötig sind, sind oftmals nur im Zusammenschluss finanzstarker Akteure mehrere Länder aufzubringen. Zu den Investoren der Firma Space Imaging zählen beispielsweise Mitsubishi (Japan), Van Der Horst Ltd. (Singapur), Hyundai Space & Aircraft (Südkorea), Swedish Space Corporation (Schweden) und Loxley Public Company Ltd. (Thailand). Den staatlichen Nachrichtendiensten bleibt daher nichts anderes übrig, als sich auf die veränderte Lage, in der sie nicht mehr das Monopol der Satellitenaufklärung haben, einzustellen.

3.2.4 Fazit: Die Beziehungen zwischen privaten Akteuren und staatlichen Nachrichtendiensten im Bereich der Satellitenaufklärung

Damit ergeben sich auf dem Feld der privaten Satellitenaufklärung zwei unterschiedliche Beziehungen zwischen den privaten Betreibern von Aufklärungssatelliten und den Diensten. Einerseits sind die kommerziell erhältlichen Satellitenbilder für staatliche Nachrichtendienste, die über keine eigenen Fernaufklärungskapazitäten verfügen, eine neue Beschaffungsquelle. Dagegen werden private Satellitenbetreiber von Staaten, die selbst Satelliten unterhalten, in erster Linie als Konkurrenz wahrgenommen.

3.3 Information Warfare

3.3.1 Definition

Information Warfare ist ein in Literatur und Praxis sehr uneinheitlich verwendeter Begriff. Grundsätzlich zu unterscheiden ist zwischen dem militärischen Verständnis, das sich in erster Linie mit der Informationssphäre im Zuge von Kriegshand-

lungen beschäftigt[96] und dem sicherheitspolitischen Verständnis, das Information Warfare vor allem auf (den Schutz vor) Cyberattacken auf kritische Infrastrukturen bezieht.

Im militärischen Bereich wird unter Information Warfare eine neue Art der Kriegsführung um und mit Informationen gesehen. Ziel ist es, die Informationshoheit zu gewinnen, wozu sowohl Low-Tech-, als auch High-Tech-Instrumente eingesetzt werden. Zu den Low-Tech-Instrumenten zählen unter anderem eine geeignete Propagandastrategie sowie der Einsatz konventioneller Waffen zur physischen Zerstörung von Infrastrukturen. High-Tech-Instrumente kommen vor allem bei der informationstechnischen Unterstützung der eigenen Streitkräfte zum Einsatz. Letzteres wird auch unter dem Stichwort „C^3I“ (Command, Control, Communications and Intelligence) diskutiert.

In der sicherheitspolitischen Information-Warfare-Diskussion werden vor allem Cyberangriffe auf kritische Infrastrukturen thematisiert, die in Kriegs- wie in Friedenzeiten von staatlichen und nichtstaatlichen Akteuren ausgehen können. Dabei kommen ausschließlich High-Tech-Instrumente zum Einsatz, deren Ziel vor allem die Funktionsunfähigkeit von Kommunikations- und Informationssystemen ist, nicht aber deren physische Zerstörung. Ziele solcher Angriffe sind in erster Linie Staaten, jedoch kann das Konzept auch auf nichtstaatliche Organisationen wie transnationale Unternehmen angewendet werden.

In dieser Arbeit wird eine an Dietrich Cerny angelehnte Definition benutzt[97], die sich in das sicherheitspolitische Verständnis von Information Warfare einordnen lässt. Information Warfare ist danach die Austragung von Konflikten zwischen Parteien, wobei für die Durchsetzung der jeweiligen Absichten Mittel der Informationstechnik zur Störung, Lähmung oder Zerstörung der Informationsversorgung des Kontrahenten und seiner kritischen Infrastrukturen eingesetzt werden. Kritische Infrastrukturen sind dabei „Organisationen und Einrichtungen mit wichtiger Be-

96 Diesem Thema gewidmet ist u.a. Eckert, Dirk, Theorie und Praxis der Information Warfare in den USA, Kölner Arbeitspapiere zur internationalen Politik Nr.1 2001

97 vgl. Cerny, Dietrich: Information Warfare – Eine neue Bedrohung für Staat und Wirtschaft?, in: Tagungsband 5. Deutscher IT-Sicherheitskongress des BSI 1997, Ingelheim: SecuMedia Verlag, 1997

deutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden".[98] In Deutschland werden vom Bundesamt für Sicherheit in der Informationstechnik (BSI), der zentralen und koordinierenden Stelle für den Schutz der kritischen Infrastrukturen, dazu die Sektoren Transport und Verkehr, Energie, Gefahrenstoffe, Informationstechnik und Telekommunikation, Finanz-, Geld- und Versicherungswesen, Versorgung, Behörden sowie Verwaltung und Justiz gezählt.[99]

Es erscheint darüber hinaus sinnvoll, kritische Infrastrukturen nach Dietrich Cerny in sektorale Infrastrukturen einerseits und die Informationsinfrastruktur andererseits zu unterteilen. Unter sektoralen Infrastrukturen werden „technische Infrastrukturen verstanden, die bestimmte, klar umrissene Aufgaben in einem bestimmten Anwendungssektor erfüllen und den Anwendern dort definierte Dienstleistungen und Nutzungsmöglichkeiten zur Verfügung stellen".[100] Dazu gehören zum Beispiel die nationalen und internationalen Verbundsysteme der Energieversorgung oder Verkehrsinfrastrukturen wie das Steuerungssystem des internationalen Flugverkehrs.[101]

Dagegen unterscheidet sich die Informationsinfrastruktur, die alle modernen Informations- und Kommunikationssysteme umfasst, von den sektoralen Infrastrukturen dadurch, dass sie eine Querschnittsfunktion der Unterstützung der Informationsversorgung wahrnimmt. „Sie stellt das Nervensystem der modernen Informationsgesellschaft dar und ist somit die notwendige Voraussetzung für einen reibungslosen und zuverlässigen Informationsaustausch in allen Bereichen des täglichen Lebens und damit auch der sektoralen Infrastrukturen."[102] Im Folgenden soll

98 Bundesamt für Sicherheit in der Informationstechnik: Einführung in den Schutz kritischer IT-Infrastrukturen, Bonn, 2005, http://www.bsi.bund.de/fachthem/kritis/KRITIS_Einfuehrung.pdf
99 ebd.
100 Cerny, Dietrich: Schutz kritischer Infrastrukturen in Wirtschaft und Verwaltung, in: Geiger, Gebhard (Hrsg.): Sicherheit in der Informationsgesellschaft: Gefährdung und Schutz informationsabhängiger Infrastrukturen, Aktuelle Materialien zur Internationalen Politik, herausgegeben von der Stiftung Wissenschaft und Politik, Baden-Baden: Nomos Verlagsgesellschaft, 2000, S. 22/23
101 ebd.
102 ebd., S. 25

unter kritischen Infrastrukturen daher in erster Linie die Informationsinfrastruktur verstanden werden.

3.3.2 Bedrohungen durch Information Warfare

Organisationen des öffentlichen wie privaten Sektors stützen sich zunehmend auf Kommunikations- und Informationsnetze wie das Telefonnetz oder das Internet und sind in hohem Maße von deren Funktionieren abhängig. Informationsinfrastrukturen gehören heute neben Straßen, Wasser- und Stromleitungen zu den nationalen Infrastrukturen, ohne die das private wie das berufliche Leben zum Stillstand käme.[103]

Aber auch das Militär ist in hohem Maße vom Funktionieren kritischer Infrastrukturen abhängig. Für die Bundeswehr trifft dies vor allem auf Kommunikationsverbindungen, Energieversorgung und Logistik zu.[104] Etwa 70 bis 95 Prozent der militärischen Kommunikationsverbindungen laufen über das private Netz der Deutschen Telekom AG[105], und die militärische Stromversorgung ist beim Ausfall ziviler Kraftwerke zum allergrößten Teil nicht gewährleistet. Weil ein großer Teil der militärischen Datenkommunikation über zivile Infrastrukturen läuft, bedrohen zivile Risiken durch Hacker und anderen Eindringlinge gleichzeitig auch die militärische Sicherheit.[106]

Aufgrund der hohen Abhängigkeit moderner Gesellschaften von Informationsinfrastrukturen entsteht eine Gefahr, die Vordenker in den USA schon in den frühen 90er Jahren von einem möglichen „electronic Pearl Harbor" sprechen ließen. Befürchtet werden mit informationstechnischen Mitteln geführte Angriffe, die kritische Infrastrukturen wie das Internet, das Telefonnetz oder das Energieversor-

103 Bundesministerium des Inneren: Nationaler Plan zum Schutz der Informationsinfrastrukturen, Berlin, Kabinettsbeschluss vom 13.7.2005, S. 3, http://www.bmi.bund.de/cln_028/nn_708198/Internet/Content/Themen/Informationsgesellschaft/Sicherheit/NPSI.html

104 Siebel, Jan: Information Warfare: Das Gefechtsfeld der Zukunft?, in: Zoller, Manfred: Der Faktor „Intelligence": Das nachrichtendienstliche Metier in neuer sicherheitspolitischer Verantwortung, Brühl/Rheinland: Fachhochschule des Bundes für öffentliche Verwaltung, 2003, S. 125/126

105 Bendrath, Jochen: Computerkriminalität: Zivile Politik trotz militärischer Rhetorik, in: Daase, Christopher/Feske, Susanne/Peters, Ingo (Hrsg.): Internationale Risikopolitik: Der Umgang mit neuen Gefahren in den internationalen Beziehungen, Baden-Baden: Nomos Verlagsgesellschaft, 2002, S. 146

106 ebd.

gungsnetz lahm legen und die Nation somit handlungsunfähig machen. Cyberattacken sind deutlich unterhalb der Schwelle klassischer militärischer Auseinandersetzungen zu verorten, denn Information-Warfare-Operationen lassen sich wirksam durchführen ohne „offiziell“ Krieg zu führen.[107]

Zwar lassen die weltweite Vernetzung, die leichte Verfügbarkeit von Instrumenten zur Durchführung von Angriffen mit Mitteln der Informationstechnik und deren verhältnismäßig einfache Anwendung keinen Zweifel daran, dass solche Angriffe auch tatsächlich durchführbar sind[108], jedoch ist das herausragende Kennzeichen der gesamten Diskussion um die Verwundbarkeit der elektronischen Infrastrukturen ihre fehlende Erfahrungssättigung. Bisher ist noch kein solcher Angriff erfolgreich durchgeführt worden, wobei allerdings angemerkt werden muss, dass von den Nachrichtendiensten erfolgreich abgewehrte Attacken wahrscheinlich nicht öffentlich würden.[109]

Verbindet man jedoch die Bedrohungspotentiale bisher isoliert voneinander aufgetretener Fälle wie gezielter Hackerangriffe, Ausfälle durch Computerviren und Zusammenbrüche des Energieversorgungs- oder Telefonnetzes, so entsteht das bereits häufig diskutierte Szenario eines Cyberangriffs auf kritische Infrastrukturen. In Deutschland wurde 2001 für eine Übung der Bundeswehr ein solches Szenario erstellt:

> „eine mafiose Gruppe legt die Computer eines Berliner Stromversorgungsunternehmens lahm. Während eine Eingreiftruppe aus Polizei, Telekom und Innenministerium versucht, den Schaden zu beheben, sabotieren die Angreifer weiter Teile des Telefonnetzes. Speziell programmierte PCs blockieren durch Dauerwahl die Telefone, und ein eingeschleuster Täter setzt letztendlich noch das Rechenzentrum einer Großbank außer Betrieb. Die Folgen dieses Angriffes lösten in der

107 Steibl, Ralf E./Ansorge, Peter: Information Warfare: die Mythenmaschine im virtuellen Gefechtsfeld, in: Schneider, Thomas: Kriegserlebnis und Legendenbildung = The experience of war and the creation of myths: das Bild des "modernen" Krieges in Literatur, Theater, Photographie und Film, Bd. 3: "Postmoderne" Kriege? Krieg auf der Bühne. Krieg auf Leinwand = "Postmodern" wars? War on stage. War on the screen, Osnabrück: Rasch Universitätsverlag, 1999, S. 861

108 Cerny (2000), S. 37

109 vgl. Bosch, Olivia: Cyber Terrorism and Private Sector Efforts for Information Infrastructure Protection, Konferenzpapier im Rahmen des Workshop of the ITU Strategy and Policy Unit, Seoul, 20.-22.5.2002, http://www.itu.int/osg/spu/ni/security/workshop/presentations/cniBosch%20paper.pdf

> Simulation über Folgewirkungen den vorübergehenden Zusammenbruch des wirtschaftlichen und öffentlichen Lebens aus.“ [110]

In der Realität ist es bisher nur einmal zu einem derartigen Zusammenbruch gekommen, und zwar bei einem Terrorangriff auf das Verwaltungsgebäude von Oklahoma im April 1995. Der Angriff wurde in diesem Fall allerdings nicht mit informationstechnischen Mitteln geführt sondern mit konventionellen Bomben.

Insgesamt tragen mehrere Aspekte zur Gefährlichkeit eines solchen Cyberangriffs bei. Erstens hängen die sektoralen kritischen Infrastrukturen zunehmend von der Steuerung durch Computer und Datennetze ab, die untereinander immer mehr vernetzt werden. Solange Einrichtungen nur in lokale Netze eingebunden sind, sorgt eine Störung nur für den lokalen Ausfall. Da vor allem Energie- und Kommunikationsnetze zunehmend national und international verflochten werden, werden großflächige Störungen und Ausfälle wahrscheinlicher.[111] In diesem Zusammenhang wird oft von der „Globalen Informationsinfrastruktur“ gesprochen, die sich unter anderem aus den nationalen Informationsinfrastrukturen, also dem öffentlichen und privaten Telekommunikationssystem, Rundfunk und Fernsehen, Rechenzentren und elektronischen Datenbanken sowie den Netzwerken und Informationsverbundsystemen, die auf dem Territorium eines Staates betrieben werden, zusammensetzt.[112]

Zweitens erhöht sich die Gefahr durch die weit verbreitete Verwendung von Standardsoftware („Commercial Off The Shelf (COTS) Software“). Diese ist meistens ohne expliziten Sicherheitsauftrag konzipiert, wodurch mögliche Angriffspunkte in einem System relativ leicht zu finden oder allgemein bekannt sind. Automatisierte Angriffe, die auf Sicherheitslücken in diesen Programmen zielen, rich-

110 vgl. Siebel (2003), S. 132/133

111 vgl. Bundesamt für Sicherheit in der Informationstechnik (2005): Einführung in den Schutz kritischer IT-Infrastrukturen

112 Geiger, Gebhard (Hrsg.): Sicherheit in der Informationsgesellschaft: Gefährdung und Schutz informationsabhängiger Infrastrukturen, Aktuelle Materialien zur Internationalen Politik, herausgegeben von der Stiftung Wissenschaft und Politik, Baden-Baden: Nomos Verlagsgesellschaft, 2000, S. 146

ten durch die große Verbreitung gleichzeitig in vielen Systemen enormen Schaden an, bevor Gegenmaßnahmen ergriffen und die Fehler behoben werden können.[113]

Drittens liegt der größte Teil der kritischen Infrastrukturen in privater Hand, wo die Risikowahrnehmung relativ gering ist.[114] In die Sicherheit der Systeme wird von den Betreibern daher nur soviel investiert, wie eigene wirtschaftliche Interessen oder Vorschriften dies rechtfertigen. Vor allem im Bereich der Informationssysteme gibt es darüber hinaus bisher keine oder nur sehr unzureichende verbindliche Sicherheitsstandards.

Viertens erfordert ein informationstechnisch geführter Angriff nicht die physische Präsenz des Angreifers. Vor allem über das Internet kann weltweit Zugang zu angeschlossenen lokalen Netzwerken gewonnen werden, was die Zahl der möglichen Angreifer stark erhöht. Deren Identifizierung und damit Erkenntnisgewinnung über Intentionen und Fähigkeiten sind kaum möglich.[115] Vor allem im Vorhinein sind Angreifer praktisch nicht auszumachen, da es keine Anzeichen oder Warnungen für einen bevorstehenden Angriff gibt.[116]

Schließlich, und damit verbunden, ist oftmals gar nicht erkennbar, dass ein solcher Angriff überhaupt geführt wird bzw. wurde.[117] Dies kann zum einen daran liegen, dass IT-Nutzer an Ausfälle und Störungen gewöhnt sind und somit nicht erkannt wird, dass eine Störung absichtlich herbeigeführt wurde.[118] Zum zweiten hinterlassen Angreifer bei solchen Attacken keine oder äußerst unauffällige Spuren, wodurch nicht auszumachen ist, ob der Angreifer von außen oder von innen heraus handelt. Dies zusammen genommen sind vor allem koordinierte Angriffe an verschiedenen Stellen innerhalb der Informationsinfrastruktur besonders gefährlich.

Die klassischen Verteidigungsmethoden der Aufklärung und Frühwarnung, der Abschreckung und Vergeltung sind im Fall von Information Warfare wenig

113 Bundesministerium des Inneren (2005): Verfassungsschutzbericht 2004, S. 5
114 Bendrath (2002), S. 151
115 ebd., S. 145
116 Cerny (2000), S. 31
117 Geiger (2000), S.160
118 ebd., S. 161

wirksam.[119] Entsprechend müssen sich geeignete Sicherheitsstrategien weitgehend auf defensive Maßnahmen der Prävention, des Schutzes und der Abwehr von Cyberangriffen konzentrieren.[120]

3.3.3 Öffentlich-private Zusammenarbeit beim Schutz kritischer Infrastrukturen im Fall der USA und Deutschlands

Die Bedrohung durch Cyberangriffe auf kritische Infrastrukturen betrifft die Nation als Ganzes, wodurch es Aufgabe des Staates ist, ihr entgegenzutreten. Die kritischen Infrastrukturen befinden sich jedoch überwiegend in privater Hand, in Deutschland zu über 90 Prozent[121], in den USA dürfte die Zahl sogar noch darüber liegen. Die Umsetzung von Sicherheitsmaßnahmen in diesem Bereich kann jedoch nur von den Betreibern ausgehen. In den Strategiepapieren zum Thema Information Warfare wird daher durchgängig eine enge Zusammenarbeit zwischen öffentlichem und privatem Sektor gefordert, die jedoch dadurch erschwert wird, dass die Zuständigkeiten im öffentlichen Bereich auf viele Stellen verteilt sind.

Den staatlichen Nachrichtendiensten kommt dabei eine Schlüsselrolle zu, allerdings stößt das Thema auf große organisatorische und rechtliche Herausforderungen. Insbesondere die organisatorische Trennung zwischen Auslands- und Inlandsgeheimdiensten ist ein Problem, da, ähnlich wie bei der Terrorismusbekämpfung, schwer zwischen innerer und äußerer Sicherheit unterschieden werden kann. Ob ein Angriff aus dem In- oder Ausland kommt, ist zunächst bzw. gar nicht erkennbar, und der Schaden kann sowohl im Inland als auch bei einem militärischen Auslandseinsatz entstehen.

Im Folgenden soll die Organisation des Schutzes kritischer Infrastrukturen in Deutschland und in den USA dargestellt werden, wobei im Besonderen auf die Zusammenarbeit der Nachrichtendienste mit den privaten Betreibern eingegangen wird.

---

119 ebd., S. 154

120 ebd.

121 Abele-Wigert, Isabelle/Dunn, Myriam: International CIIP Handbook 2006, Vol. 1: An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies, Center for Security Studies, ETH Zürich, 2005, S. 118

3.3.3.1 Deutschland

In Deutschland hat die Regierung auf die Bedrohung durch Information Warfare zuerst 1997 mit der Gründung der ressortübergreifenden Arbeitsgruppe KRITIS (AG KRITIS) reagiert. Der Anstoß dazu erfolgte durch die Veröffentlichung der President's Commission on Critical Infrastructure Protection (PCCIP) in den USA. Ein Jahr später wurde im BSI ein eigenes Referat „Schutz kritischer Infrastrukturen" eingerichtet, dessen Mittel seit den Terroranschlägen des 11. Septembers im Zusammenhang mit den Anti-Terror-Paketen bzw. dem Anti-Terror-Gesetz deutlich erhöht wurden. Im Jahre 2002 wurde im Bundesinnenministerium als Nachfolgerin der AG KRITIS die Projektgruppe KRITIS (PG KRITIS) eingerichtet, die Behörden aus den Bereichen Terrorismusbekämpfung (Bundeskriminalamt), des Zivil- und Bevölkerungsschutzes (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe) und dem Schutz in der Informationstechnik (BSI) vereint. Diese arbeitete schließlich den „Nationalen Plan zum Schutz der Informationsinfrastrukturen" aus, der im Juli 2005 vom Kabinett verabschiedet wurde.[122] Auf Grundlage dessen wird seither auf freiwilliger Basis ein nationaler Plan „Umsetzungsplan KRITIS" mit den privaten Betreibern kritischer Infrastrukturen erarbeitet, wodurch gesetzliche Verpflichtungen vermieden werden sollen.

Insgesamt sind in in den Schutz kritischer Infrastrukturen verschiedenste Regierungsstellen eingebunden. Dazu zählen neben dem BSI das Bundeskriminalamt, das Bundesamt für Verfassungsschutz und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, die jeweils dem Bundesministerium des Inneren untergeordnete sind; Außerdem der BND, der dem Bundeskanzleramt untersteht, die Bundesnetzagentur des Bundesministeriums für Wirtschaft und Arbeit sowie die Bundesministerien der Justiz und Verteidigung.[123] Das BSI ist beim Schutz kritischer Infrastrukturen die zentrale Stelle, die in einem engen Dialog mit den privaten Betreibern kritischer Infrastrukturen steht. Das BSI war bis 1991 unter dem Namen

122 vgl. Bundesministerium des Inneren (2005): Nationaler Plan zum Schutz der Informationsinfrastrukturen

123 Bundesamt für Sicherheit in der Informationstechnik: Der Schutz Kritischer Infrastrukturen in Deutschland, Bonn, 2005, http://www.bsi.bund.de/fachthem/kritis/KRITIS_in_Deutschland.pdf

„Zentralstelle für das Chiffrierwesen“ Teil des BND. Offiziell ist es damit zwar heute nicht mehr der Intelligence Community zuzurechnen, es darf jedoch vermutet werden, dass weiterhin enge Kontakte bestehen.

Ob und inwieweit die deutschen Nachrichtendienste direkt mit privaten Infrastrukturbetreibern interagieren, ist nicht bekannt. Der BND und der Verfassungsschutz sind laut einer Broschüre des BSI vor allem beratend beim Schutz kritischer Infrastrukturen tätig. Die Hauptaufgabe des BND liege darin, „im Vorfeld wichtige Erkenntnisse über die gegenwärtige Bedrohungssituation und über mögliche Ziele für Angriffe auf kritische Infrastrukturen im Inland“ zu erkennen.[124] Dazu beobachtet und analysiert er Aktivitäten relevanter Länder, Gruppierungen und Organisationen unter dem Gesichtspunkt der Information-Warfare-Fähigkeiten.[125]

3.3.3.2 USA

Die US-Regierung sieht den Schutz der Informationsinfrastruktur als ein Element ihrer Homeland-Security-Strategie. Ziele sind die Vermeidung von Cyberattacken gegen kritische Infrastrukturen, die Reduzierung der Verwundbarkeit gegen solche Angriffe und die Minimierung des möglichen entstehenden Schadens sowie der Wiederherstellungszeit nach einem Angriff.[126]

Die zentrale Stelle innerhalb des Department of Homeland Security (DHS) ist das Information Analysis and Infrastructure Protection Directorate (IAIPD), das sowohl für die Cyber-Sicherheit, als auch für den Telekommunikations- und IT-Sektor zuständig ist. 2004 betrug dessen Budget fast 850 Millionen Dollar, was den hohen Stellenwert dieses Bereichs unterstreicht. Ein weiterer Beleg für die hohe Bedeutung des Themas ist die Schaffung eines „Assistant Secretary for Cyber-Security and Telecommunications“ innerhalb des DHS im Frühjahr 2005.[127]

---

124 Bundesamt für Sicherheit in der Informationstechnik: Schutz Kritischer Infrastrukturen: Aktivitäten in Deutschland, Bonn, o.J., S. 3, http://www.bsi.bund.de/fachthem/kritis/schutz_infrastr.pdf

125 vgl. Hanning, August: Rede zur Eröffnung des Symposiums „IW – Kampf um und mit Information“, Pullach, 2.11.2000

126 White House: The National Strategy to Secure Cyberspace, Washington, Februar 2003, http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

127 Gross, Grant: DHS reorganization creates new cybersecurity position. The move could mean more focus on cybersecurity issues, IDG News Service, 13.7.2005,

Auch in den USA sieht man den Schlüssel zum Erfolg in der Zusammenarbeit zwischen öffentlichem und privatem Sektor. Bereits in Clintons PCCIP, die 1995 gegründet wurde und 1997 ihren Bericht vorlegte, war die Empfehlung einer umfassenden Public-Private Partnership der Kernpunkt. Im Jahr 2000 veröffentlichte Clinton die erste Strategie zum Schutz der Informationsinfrastruktur unter dem Namen „Defending America's Cyberspace. National Plan for Information Systems Protection – An Invitation to Dialogue Version 1.0".[128] In der Folge des 11. Septembers wurde dann der Schutz kritischer Infrastrukturen zu einem der sechs „Critical Mission Areas" der National Strategy for Homeland Security erklärt, wobei die Zuständigkeit komplett dem neuen DHS übertragen wurde.

Im Februar 2003 wurde die zusammen mit dem privaten Sektor erarbeitete „National Strategy to Secure Cyberspace" veröffentlicht[129], die mit der im Dezember 2003 veröffentlichten "Homeland Security Presidential Directive/HSPD-7 umgesetzt wurde.[130] Sie ersetzt alle vorherigen präsidentiellen Direktiven und definiert Organisationen und Aufgaben.

Schließlich wurde der Öffentlichkeit im November 2005 der erste Entwurf des neuen „National Infrastructure Protection Plan" vorgelegt.[131] Dieser folgt der HSPD-7 und beschreibt die Rollen und Verantwortlichkeiten betroffener Regierungsstellen, des privaten Sektors sowie bundesstaatlichen und lokalen Regierungen.

Die Geheimdienste sind in den Schutz kritischer Infrastrukturen von Anfang an mit eingebunden worden. Bei allen genannten Initiativen seit der Einrichtung der

---

http://www.computerworld.com/governmenttopics/government/story/0,10801,103174,00.html?source=NLT_SEC2&nid=103174

128 White House: Defending America´s Cyberspace. National Plan for Information Systems Protection, Version 1.0. An Invitation to a Dialogue, Washington, 7.1.2000, http://www.whitehouse.gov/pcipb/

129 White House (2003): The National Strategy to Secure Cyberspace

130 White House: Homeland Security Presidential Directive/HSPD-7, Washington, 17.12.2003, http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html

131 White House: National Infrastructure Protection Plan, Draft NIPP v1.0, Washington, 2.11.2005, www.fas.org/irp/agency/dhs/nipp110205.pdf

PCCIP im Jahr 1995 spielen die Nachrichtendienste eine zentrale Rolle[132], vor allem was die Verhinderung und Warnung vor möglicher Cyberattacken angeht.[133] Dazu versorgen sie die mittlerweile im DHS zusammengefassten Gremien mit Informationen, die diese dann an den privaten Sektor weiterleiten. Auffallend in den offiziellen Dokumenten ist, dass die Dienste ihre extrem restriktive Haltung, was die Weitergabe gewonnener Informationen angeht, in diesem Bereich gelockert zu haben scheinen.[134]

3.3.4 Fazit: Die Beziehungen zwischen Privaten und staatlichen Behörden im Bereich des Schutzes kritischer Infrastrukturen

Der Schutz kritischer Infrastrukturen ist eine Aufgabe der nationalen Sicherheit und somit Aufgabe der Nachrichtendienste, wobei die Eigentümer solcher Infrastrukturen, wie dargestellt, meist private Akteure sind. Bei der *defensiven* Information Warfare sind Geheimdienste daher gezwungen, mit den privaten Betreibern kritischer Infrastrukturen zu kooperieren. Im Gegensatz zu den in den zwei vorangegangenen Kapiteln beschriebenen Bereichen, in denen private Akteure als Abnehmer und Quellen (Wirtschaftsspionage) bzw. Konkurrenten (Satellitenaufklärung) klassifiziert wurden, sind die Dienste hier also auf die Kooperation mit den privaten Betreibern angewiesen, ohne die sie ihre Aufgaben nicht erfüllen könnten. Das impliziert, dass gerade in diesem Bereich die Nachrichtendienste gezwungen sind, relativ viele Informationen weiterzugeben, zunächst an andere beteiligte Regierungsstellen, aber auch an den privaten Sektor.

Jedoch gibt es auch im Falle dieser notwendigen Kooperation ebenso wie bei jeder Public-Private-Partnership eine Vielzahl von Problemen, da die Risikowahrnehmung in den beiden Sektoren unterschiedlich ist und bei den Betreibern kritischer Infrastrukturen meist große Skepsis gegen eine Einmischung des Staates

132 im National Plan for Information Systems Protection kommt das Wort „Intelligence“ auf knapp 200 Seiten genau 100 mal vor

133 White House (2000): Defending America´s Cyberspace. National Plan for Information Systems Protection, Version 1.0. An Invitation to a Dialogue, S. 88

134 vgl. ebd.

herrscht. Viele Autoren meinen daher, dass erst ein „elektronisches Pearl Harbor“ eintreten muss, damit die Kooperation funktioniert.

Neben diesen defensiven Aufgaben sind die Nachrichtendienste auch zuständig für die Ausbildung *offensiver* Information-Warfare-Fähigkeiten, womit ihnen ein neues Aufgabengebiet im Bereich verdeckter Handlungen zugekommen ist. Gerade dies sichert ihnen aber auch eine Expertenrolle in der Abwehr möglicher Information Warfare Attacken.

3.4 Business Intelligence

In diesem Kapitel werden drei voneinander unabhängige Entwicklungen im privaten Sektor angesprochen, die jeweils eine große, wenn auch unterschiedliche Bedeutung für die Arbeit staatlicher Nachrichtendienste haben. Erstens haben in der Wirtschaftsaufklärung mächtige private Akteure staatliche Geheimdienste fast vollkommen verdrängt bzw. einen großen Teil ihrer Arbeit überflüssig gemacht (Kap. 3.4.1). Zweitens sind auf dem Feld der Competitive Intelligence im privatwirtschaftlichen Bereich extrem leistungsfähige Instrumente zur Analyse großer Mengen von Daten entwickelt worden, die von Nachrichtendiensten insbesondere bei der Terrorismusbekämpfung schnell absorbiert wurden (Kap. 3.4.2). Schließlich sind, bedingt durch die stark steigende Zahl von Risiken für transnationale Unternehmen, private Dienstleister entstanden, die eigene Intelligence-Aktivitäten betreiben. Diese Private Intelligence Services bedrohen staatliche Dienste einerseits durch Kopie von deren Methoden, andererseits könnten sie eine Chance darstellen, mit der Flut öffentlich verfügbarer Informationen des Informationszeitalters fertig zu werden (Kap. 3.4.3).

3.4.1 Wirtschaftsaufklärung

Zur Zeit des Kalten Krieges war es eine bedeutende Aufgabe staatlicher Nachrichtendienste, Informationen über die Leistungsfähigkeit der Wirtschaft gegnerischer Staaten im allgemeinen und von Schlüsselbranchen jener im Speziellen zu gewinnen, um daraus Rückschlüsse auf die Fähigkeiten und Intentionen eines Landes ziehen.

Solche Informationen waren in den geschlossenen Gesellschaften des Ostblocks nicht frei zugänglich. So waren viele ökonomische Informationen, wie zum Beispiel Preise, nicht wie in Marktwirtschaften, offen verfügbar. Zur Datenbeschaffung waren daher geheime Quellen nötig, weswegen diese Aufgabe den Nachrichtendiensten zufiel. Diese beschäftigten darüber hinaus führende Volkswirte, die aus den Daten ökonomische Analysen erstellten.

Die wirtschaftliche Leistungsfähigkeit von Staaten und das Wissen darüber hat in der internationalen Sphäre seit dem Ende des Kalten Krieges an Bedeutung gewonnen. Heute gibt es jedoch bis auf wenige Ausnahmen, wie etwa Nordkorea oder Kuba, keine geschlossenen Gesellschaften mehr. Deshalb ist es nun auch anderen Akteuren möglich, Wirtschaftsaufklärung zu betreiben. Dazu zählen beispielsweise die Nationalbanken oder volkswirtschaftliche Forschungsinstitute, vor allem aber werden solche Analysen aufgrund der Globalisierung der Finanzmärkte zunehmend auch von privaten Akteuren wie Dow Jones, McGraw-Hill oder Dun & Bratstreet oder von den großen Banken und Fondsgesellschaften durchgeführt. In deren Arbeit spielen volkswirtschaftliche Länder- und Marktanalysen eine große Rolle, weshalb sie bedeutende Fähigkeiten darin ausgebildet haben. Bei solchen Unternehmen sind aufgrund der bezahlten Gehälter heute auch die besten Ökonomen zu finden. Berkowitz und Goodman illustrieren dies: „George Sorros hat mit seiner Fähigkeit, Wechselkurse zu analysieren, Milliarden Dollar verdient. Können wir wirklich von einem Beamten oder einer Beamtin einer Geheimdienst-Bürokratie erwarten, besser zu sein? Und wenn ja, wieso arbeitet er oder sie dann bei der Regierung?“[135]

Große Teile der ökonomischen Abteilungen staatlicher Nachrichtendienste, die sich vor allem intensiv mit der Leistungsfähigkeit der Sowjetunion beschäftigt hatten, sind damit überflüssig geworden. Vor allem ist zweifelhaft, ob die Geheimdienste tatsächlich über die Informationen und Einschätzungen hinausgehen können, die von den viel beachteten Berichten über Wirtschaftsfragen beispielsweise

135 Berkowitz/Goodman (2000), S. 109 (eigene Übersetzung)

der New York Times, dem Wall Street Journal und dem Economist veröffentlicht werden.[136]

3.4.2 Competitive Intelligence

Während der private Sektor die staatlichen Nachrichtendienste im Bereich volkswirtschaftlicher Analysen vollkommen verdrängt hat, konnten sie von den Entwicklungen im Bereich der Competitive Intelligence profitieren. Parallel zum explodierenden Einsatz von Datenbanken in allen Bereichen der Wirtschaft sind auf dem privaten IT-Sektor leistungsfähige Instrumente des Data Mining entwickelt worden, die bei Nachrichtendiensten auf großes Interesse stoßen.

3.4.2.1 Das Konzept der Competitive Intelligence

Mit Hilfe der Competitive Intelligence sammeln Unternehmen relevante Informationen aus dem Wettbewerbsumfeld. Auch wenn dabei eine rechtliche Grauzone existiert, handelt es sich bei Competitive Intelligence um legale Informationsbeschaffung. Hervorgegangen ist das Konzept aus der Competitor Intelligence von Michael Porter, der in den 80er Jahren ein revolutionäres Strategiekonzept innerhalb der Betriebswirtschaft entwickelt hat.

> "Intelligence, until the end of the 80s, was a subject dealt with by governments and nations. It brought with it connotations of military and state security issues. Companies and private people dealt with information - not with intelligence. During the 90s, more and more corporations developed the concept of business and industrial intelligence as a competitive tool."[137]

In den letzten zehn Jahren ist der Markt für Competitive Intelligence geradezu explodiert.

136 Johnson (2002), S. 67

137 ATHENA GS3 Security Implementations Ltd.: Intelligence from Open Sources: Real Time Intelligence from Unstructured Text in Multiple Languages, Herzliya Pituach, Mai 2003, S. 3, http://www.athenaiss.com/documents/real_time_intelligence.pdf

3.4.2.2 Data Mining

Innerhalb des Feldes der Competitive Intelligence hat der private Sektor im Bereich der informationstechnischen Verarbeitung einer großen Menge an Daten bedeutende Fertigkeiten ausgebildet, die als Methode des Data Mining bekannt sind. Darunter versteht man nach Pieter Adriaans und Dolf Zantinge eine Methode, die sich Datenanalyse-Werkzeugen wie statistischer Methoden, mathematischer Algorithmen und selbstlernender Programme bedient, um vorher nicht bekannte Muster und Beziehungen in großen Datensätzen zu entdecken. Daten können dabei in quantitativer, textualer oder sogar multimedialer Form vorliegen.[138] Verglichen mit anderen Datenanalyseanwendungen wie strukturierten Anfragen oder statistischen Analyseprogrammen besteht der Unterschied in der Induktivität der Methode. Es müssen nicht im Vorhinein Hypothesen aufgestellt werden, die anschließend überprüft werden, sondern es können mit Data Mining Zusammenhänge in Daten „entdeckt" werden. Allerdings wird dem Benutzer dabei nichts über den Wert oder die Signifikanz dieser Muster mitgeteilt. Auch handelt es sich bei gefundenen Beziehungen nicht unbedingt um Kausalzusammenhänge, weshalb immer noch technisch und analytisch geschulte Spezialisten gebraucht werden, die Struktur in die Analyse bringen und die Ergebnisse interpretieren. Die Grenzen von Data Mining sind daher nicht technischer Natur, sondern liegen vielmehr in der Qualität der Daten und im Interpretationsvermögen der auswertenden Personen.

Laut einer vom amerikanischen Kongress angeforderten Studie wird Data Mining im privaten Bereich für verschiedenste Zwecke verwendet.[139] Banken und Versicherungen benutzen die Methode beim Risikomanagement und beim Aufdecken von Betrug; Pharmaunternehmen nutzen Data Mining forschungsleitend, indem sie es auf genetisches Material und chemische Bestandteile anwenden. Telefonanbieter und andere Subskriptionsdienste können damit Prognosen aufstellen, welche der Neukunden in Zukunft wahrscheinlich wieder den Anbieter wechseln. Und

138 Adriaans, Pieter/Zantinge, Dolf: Data Mining, New York: Addison Wesley, 1996

139 vgl. Seifert, Jeffrey W.: Data Mining: An Overview, CRS Report for Congress, Updated January 27, 2006, www.fas.org/sgp/crs/intel/RL31798.pdf

generell können Unternehmen aller Branchen mittels Data Mining aus ihren Kundendatenbanken Erkenntnisse über das Verhalten ihrer Abnehmer gewinnen. Im öffentlich Bereich kommt Data Mining heute in großem Stile bei der Verbrechensbekämpfung zum Einsatz.

3.4.2.3 Bedeutung von Data Mining für staatliche Nachrichtendienste

Welche Bedeutung Data Mining als Methode für die Analyse großer Mengen von Daten für die Nachrichtendienste hat, erschließt sich leicht in Anbetracht der Masse an Informationen, die täglich mittels globaler Abhörsysteme wie ECHELON gewonnen werden. Eine Schlüsselrolle kommt dieser Methode vor allem bei der Terrorbekämpfung zu, bei der Terroristen durch Abgleich verschiedener Datenbanken und abgehörter Kommunikation aufgedeckt werden sollen.

Um die Fähigkeiten des privaten Sektors zu nutzen und weiterzuentwickeln, wurde in den USA im Januar 2002 an der Defense Advanced Research Projects Agency (DARPA), die sich mit Grundlagen- und angewandter Forschung und Technologie in Bereichen beschäftigt, in denen „Risiken und Payoffs sehr hoch sind und in denen Erfolge dramatische Fortschritte für traditionelle militärische Rollen und Missionen ermöglichen“,[140] ein Programm mit dem Namen „Terrorism Information Awareness Program“ (TIA) aufgelegt. Das DARPA ist die zentrale Forschungs- und Entwicklungsorganisation für das Department of Defense, innerhalb dessen das TIA von dem nach dem 11. September 2001 eingerichteten Information Awareness Office (IAO) geleitet wird. Das Ziel des IAO war es “[to] counter asymmetric threats by achieving total information awareness useful for preemption, national security warning, and national security decision making.”[141] Man erhoffte sich dadurch insbesondere die Aufdeckung von terroristischen Schläferzellen. Im Verlauf des Projektes kam es jedoch seitens des Kongresses und der breiten Öffentlichkeit zu Bedenken bezüglich des Datenschutzes, was zur Einstellung des Programms im September 2003 führte. Trotzdem kann mit Sicherheit davon ausgegangen werden, dass

140 Quelle: http://www.darpa.mil.

141 Department of Defense: Report to Congress Regarding the Terrorism Information Awareness Program, o.O., 20.5.2003, S. 1, http://www.iwar.org.uk/news-archive/tia/darpa-tia-report.htm

auf diesem Gebiet weiterhin mit Hochdruck gearbeitet und mit privaten Unternehmen kooperiert wird.

Die CIA ist einen anderen Weg gegangen, um die Innovationsfähigkeit des privaten Sektors für sich nutzbar zu machen. Sie hat einen organisatorisch außerhalb des Dienstes liegenden Venture Capital Fond mit dem Namen In-Q-Tel gegründet, der jungen Unternehmen Mittel bereitstellen soll.[142] Die CIA weist öffentlich darauf hin, dass sie mit In-Q-Tel gerade auch im Bereich Data Mining Hilfe vom privaten Sektor bekommen hat und weiterhin sucht.[143] Von 48 auf der Homepage vorgestellten Unternehmen sind nach eigenen Recherchen 17 in diesem Bereich aktiv, namentlich Attensity, Convera, Decru, Endeca, FMS, Initiate Systems, Intelliseek, Inxight, Kofax, NovoDynamics, piXlogic, Soflinx, Spotfire, Stratify, SRD, Thetus und Visual Sciences.

3.4.3 Private Intelligence Services

Competitive Intelligence wird oft von den Unternehmen selbst betrieben, allerdings gibt es auch immer mehr spezialisierte Dienstleister, die solche Services übernehmen. Davon zu unterscheiden sind die so genannten Private Intelligence Services, die sich oft auch als Risikoberatungsgesellschaften bezeichnen. Sie „handeln“ ebenfalls mit Informationen, allerdings liegt ihr Fokus nicht auf Wettbewerbsunternehmen, sondern auf sicherheitsrelevanten Bereichen - vor allem dem politisch-militärischen.

3.4.3.1 Die Entstehung von Private Intelligence Services

Unternehmen besonders in den Branchen Finanzen, Handel und Öl haben schon immer eigene Intelligence betrieben, da sie seit jeher in einem komplexen Umfeld agieren. Beste Beispiele sind Banken, die großen japanischen Handelshäuser und Ölkonzerne.[144] Transnationale Konzerne aller Branchen haben heute jedoch ein Informationsbedürfnis, das weit über den wirtschaftlichen Bereich und damit über

142 Hulnick (2004), S. 64

143 vgl. www.in-q-tel.com

144 Herring, Jan P.: The unique role of the future in intelligence, in: Sigurdson, Jon/Tagerud, Yael: The Intelligent Corporation, London: Taylor Graham Publishers, 1992, S. 161

das, was Competitive Intelligence liefert, hinausgeht. Informationen werden für Unternehmen zu einer immer bedeutenderen Ressource im Leistungserstellungsprozess und für den Erhalt der Wettbewerbsfähigkeit. Zudem agieren transnationale Unternehmen vielfach in Staaten, die ihre Sicherheit nicht mehr garantieren können. Das führt dazu, dass sie sowohl qualitativ wie auch quantitativ stark erhöhten Risiken ausgesetzt sind, für deren Einschätzung (und Abwehr) sie selbst sorgen müssen.

Spätestens mit den Terroranschlägen vom 11. September 2001 ist dafür ein breites Bewusstsein entstanden und damit das Bedürfnis nach privater Intelligence. In einer Broschüre des israelischen Private Intelligence Service ATHENA GS3 Security Implementations Ltd. ist dies folgendermaßen ausgedrückt:

> „The terror attacks of 9.11.2001 brought about a new consciousness in the world. It is now understood that future wars will be targeted primarily against civilian targets—not against military establishments—and will be perpetrated by civilians. As a result, more and more civil organizations, both public and private, began to perceive their responsibility to protect themselves, on top of whatever security their governments can, and will be able to, provide. Private and public civil organizations that wish to cost effectively protect themselves, without interrupting their day-to-day business and activities, need access to real intelligence, awareness, and knowledge, not just unprocessed information."[145]

Parallel zu den Entwicklungen im Bereich Competitive Intelligence ist daher ein Markt für private Informationsbroker entstanden, die kommerzielle Intelligence in sicherheitsrelevanten Bereichen vertreiben. Neu ist dabei vor allem die Professionalisierung und Institutionalisierung von Intelligence-Aktivitäten innerhalb des Entscheidungs-Unterstützungs-Systems verschiedener Organisationen im privaten Bereich.[146]

145 ATHENA GS3 Security Implementations Ltd., S. 3
146 Agrell (1992), S. 101

3.4.3.2 Die Tätigkeit von Private Intelligence Services

Private Intelligence Services nehmen Unternehmen und anderen Organisationen die aufwändige Sammlung und Auswertung von Informationen mit Risikopotential ab, welche diese in den meisten Fällen aus mehreren Gründen nicht selbst leisten können oder wollen. Zu diesen Gründen zählen das dynamische Wachstum von Daten, Informationen und Wissen, die Zeit- und Kostenintensivität des Auffindens relevanter Informationen, deren eingeschränkter Zugang zu Informations- und Wissensquellen, das aufwändige Herausfiltern von Informationen und die schwierige und ineffiziente Transformation von Information in Wissen.[147] Die Aufgabe der Private Intelligence Services besteht somit in der Aggregation von Daten, dem Filtern und Verdichten von Informationen, der Analyse von Wissen und dem Generieren von neuem Wissen.[148] Private Intelligence Services sind somit als Intermediäre zwischen Wissens- und Informationsquellen und Wissenskonsumenten zu verstehen. Wissens- und Informationsquellen können dabei in drei Kategorien eingeteilt werden: Experten; Printmedien wie Bücher, Geschäftsberichte, Fachpublikationen, Lexika, Zeitungen etc.; und elektronische Träger von Informationen wie das Internet und elektronische Datenbanken. Wissenskonsumenten sind private, halböffentliche und öffentliche Organisationen wie Unternehmen, Verbände, NGOs und Regierungsstellen.

3.4.3.3 Akteure

In Tabelle 5 sind etablierte Private Intelligence Services aufgezählt. Neben den großen Anbietern wurden solche aufgenommen, die aufgrund der Beschäftigung bedeutender ehemalige Mitarbeiter von staatlichen Geheimdiensten auffallen (gekennzeichnet mit „+“ oder „++“).[149]

147 Lux/Peske (2002), S. 40

148 ebd.

149 Weitere Unternehmen, die Dienstleistungen im Intelligence- und Sicherheitsbereich erbringen, können beispielsweise einer Überblickstabelle in Avant, Deborah D.: The Market for Force: The Consequences of Privatizing Security, Cambridge: Cambridge University Press, 2005, S. 10-15 entnommen werden

Tabelle 5: Überblick über Private Intelligence Services						
Name	**Anzahl Büros weltweit**	**Mitarbeiter m. nachrichtendienstl. Hintergrund**	**Kunden**		**Sitz**	**Homepage**
			priv.	**staatl.**		
Control Risks	23	+	x	x	London, UK	www.control-risks.com
Stratfor	2	+	x	x	Austin, TX, USA	www.stratfor.com
Kroll & Associates	65	+	x	x	New York, NY, USA	www.krollworldwide.com
Diligence	8	++	x		Washington D.C., USA	www.diligencellc.com
Economist Intelligence Unit	40	-	x	x	London, UK	www.eiu.com
Oxford Analytica	4	-	x	x	Oxford, UK	www.oxan.com
Crises Group	20	-		x	Brüssel, Belgien	www.crisisgroup.org
International Risk	6	+	x		Hong Kong, China	www.intl-risk.com
CTC International Group Inc.	1	++	x		West Palm Beach, FL, USA	www.ctcintl.com
Global Options	10	++	x	x	Washington D.C., USA	www.globaloptions.com
International Intelligence Limited	4	+	x		Cotswold, UK	www.int-int.co.uk
Infosphere	1	-	x	x	Stockholm, Schweden	www.infosphere.se
ATHENA GS3 Security Implementations Ltd.	3	++	x	x	Herzliya Pituach, Israel	www.athenaiss.com
Global Source LLC.	3	++	x		Fairfax, VA, USA	www.globalsourcellc.com
Global Risk Assessments	1	++	x	x	Riverside, CA, USA	www.grai.com
Smith Brandon International	1	++	x		Washington D.C., USA	www.smithbrandon.com
Eurasia Group	3	-	x	x	New York, NY, USA	www.eurasiagroup.net
Exclusive Analysis	1	+	x	x	London, UK	www.exclusive-analysis.com
Sentigence, Inc.	1	++	x		?, USA	www.sentigence.com
The Scowcroft Group	1	++	x		Washington D.C., USA	www.scowcroft.com

Die Anzahl der Büros soll als Indikator für die Größe der Unternehmen dienen, da Mitarbeiter- oder Umsatzzahlen in den meisten Fällen nicht zugänglich sind. Da diese Unternehmen jedoch häufig auf eine große Anzahl von Experten zurückgreifen, die nicht fest angestellt sind, können Unternehmen auch mit geringer Anzahl von Büros durchaus relativ groß sein, zu den Marktführern zählt beispielsweise Stratfor mit nur 2 Büros in den USA. Die Angaben zur Kategorie der Kunden (privat und/oder staatlich) sind, wie die übrigen Informationen auch, Selbstauskünfte der Firmen auf ihren Homepages.

Zu den bekanntesten Anbietern gehören Control Risks, Stratfor und Kroll & Associates, die neben reinen Informationsdiensten auch weitere Dienstleistungen im Sicherheitsmanagement anbieten. Die britische Firma Control Risks, 1975 von ehemaligen britischen Agenten und Anti-Terror-Spezialisten gegründet[150], hat, ergänzt durch etwa 1000 freie Mitarbeiter, weltweit etwa 500 Angestellte und besitzt in Berlin ein Büro mit 25 Mitarbeitern.[151] Der Umsatz ist von 20 Millionen Pfund im Jahre 2001 auf 140 Millionen Pfund im Jahr 2005 gestiegen, wobei das Unternehmen nach eigenen Angaben heute in Deutschland mehr als die Hälfte der DAX-Unternehmen zu seinen Kunden zählt.[152] Das Regelgeschäft von Control Risks sei über die Länder zu informieren, in denen ein Unternehmen Geschäfte machen will, wozu es in der Firma ganze Stäbe gibt, die im Stile von Wissenschaftlern nichts anders machen als Informationen über bestimmte Länder zu sammeln.[153] Jedoch bietet Control Risks auch Sicherheitsdienstleistungen wie Transportschutz an und war bei über 1400 Entführungsfällen in der ganzen Welt als Berater tätig.[154] Neben Control Risks haben von den aufgeführten Unternehmen nur Kroll & Associates sowie Diligence eine Vertretung in Deutschland.

150 Asmuth, Tobias: Unser Mann in Treptow; Von RAF bis Sayyaf: Die Firma Control Risks berät weltweit Manager in Sicherheitsfragen - ein Standort ist Berlin, Süddeutsche Zeitung vom 22.5.2002
151 Büschemann, Karl-Heinz: Geheimnisvolle Geschäfte mit der Sicherheit, Süddeutsche Zeitung vom 25./26.3.2006
152 ebd.
153 ebd.
154 ebd.

Private Intelligence Services zählen mittlerweile auch staatliche Stellen sowie supranationale Organisationen zu ihren Kunden. Ein Komitee des UN-Sicherheitsrates, das Sanktionsverletzungen in Angola überwachte, engagierte im Jahr 2001 beispielsweise Kroll & Associates für 100.000 Dollar, um die Geldanlagen von UNITA-Rebellenführer Jonas Savimbi zu verfolgen.[155] Begründet wurde die Wahl eines Private Intelligence Service damit, dass die UN so unabhängiger von den staatlichen Geheimdiensten der Mitgliedsstaaten sei. Ob auch staatliche Geheimdienste zu den Auftraggebern ihrer privaten Pendants gehören, kann nur vermutet werden.[156] Eine Aussage hierzu wurde auf Anfragen des Autors von Control Risks und Kroll & Associates verweigert.

3.4.3.4 Bedeutung von Private Intelligence Services für staatliche Nachrichtendienste

Mit dem Aufkommen von Private Intelligence Services sind staatliche Nachrichtendienste mit einem Phänomen neuer Qualität konfrontiert, da sich deren Tätigkeiten mit denen der Dienste in hohem Maße überschneiden. Dies ist für staatliche Nachrichtendienste einerseits problematisch, andererseits können letztere davon auch profitieren.

Negative Auswirkungen

Problematisch für sie ist zunächst, dass Wissen um die Methoden und Arbeitsweise der staatlichen Geheimdienste an den privaten Sektor abfließt. Dort unterliegt es keinerlei Kontrolle mehr, und dies umso weniger, da die Arbeitsmethoden und Quellen geheim sind. Diese Gefahr entsteht hauptsächlich aus der Tatsache heraus, dass viele, zum Teil sehr ranghohe Geheimdienstmitarbeiter in den privaten Sektor übergewechselt sind und dort selbst Private Intelligence Services gegründet haben oder von solchen beschäftigt werden. Beispiele sind Shabtai Shavit, der von 1989 bis 1996 Direktor des israelischen Geheimdienstes Mossad war und nun Chairman der

155 Lynch, Colum: Private Firms Aid U.N. on Sanctions; Wider Intelligence Capability Sought, The Washington Post vom 21.4.2001

156 vgl. Kupchinsky, Roman: Information Revolution Feeds Alternative Intelligence Market, Washington D.C.: Radio Free Europe/Radio Liberty, 23.5.2005, http://www.globalsecurity.org/intell/library/news/2005/intell-050523-rferl01.htm

israelisch-amerikanischen ATHENA GS3 Security Implementations Ltd. ist, Frederick W. Rustmann, Jr., der 1990 nach 24jähriger Beschäftigung bei der CIA ausschied und nun Chairman des Executive Committee der amerikanischen CTC International Group Inc. ist, James Woolsey (Direktor des CIA von 1993 bis 1995), William H. Webster (Direktor des CIA von 1987-1991 und Direktor des FBI von 1978-1987) und William S. Sessions (Direktor des FBI von 1987-1993), die heute Berater für die amerikanische GlobalOptions Inc. sind, sowie Gerard Burke, früherer Assistant Director der NSA und Executive Director des Foreign Intelligence Advisory Board von Präsident Nixon, der nach Gründung eines eigenen Private Intelligence Service mit dem Namen Parvus nun Direktor von Global Source LLC ist.

Durch diese Entwicklung wird nachrichtendienstliches Wissen kommerziell erhältlich und daher verschiedensten Personen und Unternehmen im In- und Ausland zugänglich. Transnationale Unternehmen gewinnen durch ihre Dienste an Unabhängigkeit und können ihre Rolle als eigenständige Akteure im internationalen Raum festigen. Im schlimmsten Fall könnten auch kriminelle Gruppen, insbesondere aus dem Feld der organisierten Kriminalität, oder sogar Terroristen auf diesem Weg an gefährliches Wissen gelangen.

Problematisch ist weiterhin, dass staatliche Nachrichtendienste Private Intelligence Services für Aktivitäten engagieren könnten, die außerhalb ihrer definierten Aufgaben liegen. Zwei solcher Fälle sind bisher bekannt geworden. Der erste mutmaßliche Fall ereignete sich im Juni 2001, bei dem der britische Private Intelligence Service Hakluyt, der enge Verbindungen zum britischen Auslandsgeheimdienst MI6 hat, NGOs im Umweltbereich für BP und Shell ausspionierte. Eine mögliche Verbindung könnte dabei BPs Director of Government and Public Affairs John Gerson sein, der zuvor ein Kandidat für die Nachfolge von Sir David Spedding als Chef des MI6 war.[157] Die Anschuldigungen stützen sich vor allem auf die Tatsache, dass die Gründer von Hakluyt ehemalige Mitarbeiter des MI6 waren. Die Firma wurde 1995 gegründet und hatte nach eigenen Angaben im Jahre 2001 ein Viertel aller

157 Chittenden, Maurice/Rufford, Nicholas: How agent Camus sank Greenpeace oil protests, Sunday Times vom 17.6.2001

FTSE[158]-100-Unternehmen unter Vertrag. Von britischen Parlamentsabgeordneten wurde Hakluyt als Front des MI6 bezeichnet, um gegen Umweltaktivisten zu spionieren.[159] Die Anschuldigung mündete in eine Anfrage an den damaligen Außenminister Jack Straw über die Firma.

In die Schlagzeilen geraten ist in dieser Affäre vor allem auch der Deutsche Manfred Schlickenrieder, der sich über Jahre unter dem Cover eines Sympathisanten und Filmemachers in der linken Szene bewegte, während er nebenbei für Hakluyt arbeitete. Aus damals sichergestellten Dokumenten geht hervor, dass er zur gleichen Zeit auch vom deutschen Verfassungsschutz und vom BND bezahlt wurde. Schlickenrieder arbeitete dabei als „freiberuflicher" Spion direkt für die deutschen Dienste, Hakluyt war nicht verwickelt. Der Fall wurde in Deutschland im Parlamentarischen Kontrollgremium diskutiert, dessen Ergebnisse jedoch nicht veröffentlicht werden.

Im zweiten bisher bekannt gewordenen Fall steht ebenfalls eine britische Firma im Zentrum. Am 5. Oktober 2003 berichtet die Sunday Times über das Sicherheitsunternehmen Group 4, zu dessen Klienten in Großbritannien unter anderem Gefängnisse, die königliche Familie sowie die Regierung gehören.[160] In diesem Fall wurde Group 4 von der britischen Regierung mit dem Schutz von umstrittenen Straßenbauarbeiten beauftragt. Group 4 kaufte im Zuge dessen vom Private Intelligence Service R&CA Publications geheim gewonnene Informationen über Protestanten. R&CA Publications wird von Evelyn Le Chene geleitet, die enge Kontakte zu den Geheimdiensten hat. Die Firma besitzt ein Netzwerk von Agenten um eine Datenbank zu unterhalten, die mittlerweile 148.000 Personen, die linken Aktivistengruppen zugerechnet werden, enthält. Diese Namen werden von Le Chene für 2,25 Pfund pro Stück an große Unternehmen verkauft.

158 Der Financial Times Stock Exchange Index, kurz FTSE, ist ein Aktienindex, der die 100 wichtigsten Aktien umfasst, die an der Börse in London gehandelt werden.

159 Lubbers, Eveline: Corporate Intelligence, in: Lubbers, Eveline (Hrsg.): Battling Big Business, Totnes: Green Books Ldt., 2002, S. 126

160 ebd., S. 127

Angesichts dieser Gefahren gibt es in mehreren Staaten Bemühungen, die Aktivitäten von Private Intelligence Services zu kontrollieren. In Brasilien ist dazu ein Gesetzesentwurf in Zusammenhang mit einem Rechtsstreit gegen Kroll & Associates eingebracht worden[161], in Südafrika zielt ein Entwurf auf die Verletzung der Privatsphäre durch Private Intelligence Services ab.[162] Auch in den USA machen sich einige Kongressmitglieder Sorgen über das unregulierte Wachstum in diesem Feld, vor allem was die Verletzung von Persönlichkeitsrechten angeht.[163]

Positive Auswirkungen

Das Aufkommen von privaten Akteuren im Bereich der Intelligence hat aber durchaus auch positive Rückwirkungen auf die Arbeit staatlicher Nachrichtendienste. Es könnte für die Intelligence Community nämlich ein Mittel sein, OSINT besser zu nutzen.

In den letzten Jahren ist der Anteil offener Quellen innerhalb der nachrichtendienstlichen Arbeit aufgrund der Explosion öffentlich zugänglicher Informationen stark gestiegen. Diese Entwicklung hat den Wert geheimer Informationen gemindert[164], doch die Dienste haben es bisher nicht geschafft, angemessen darauf zu reagieren. Offene Quellen dürften heute deutlich mehr als 80 Prozent ausmachen (einige Autoren sprechen von bis zu 95 Prozent), jedoch ist unumstritten, dass das OSINT-Potential bei weitem nicht ausgeschöpft wird.[165]

Zumal OSINT keiner oder nur einer geringen Geheimhaltungsstufe unterliegt, sprechen sich viele Autoren dafür aus, die Sammlung und Auswertung von OSINT hauptsächlich oder ganz dem privaten Sektor zu überlassen. Einer der ersten Autoren, der den Beitrag, den der private Sektor für staatliche Intelligence leisten kann, erkannt hat, ist der slowenisch-schwedische Professor Stevan Dedijer. Sein

161 BBC Monitoring Latin America – Political: Brazilian government looking to control private intelligence agencies, 31.7.2004
162 Hartley, Wyndham: Private intelligence firms face clampdown, in: Business Day (South Africa) vom 18.6.2003
163 vgl. Kupchinsky (2005)
164 Treverton (2005), S. 226
165 siehe beispielsweise Dupont (2003), S. 26

Werk wurde 1992 anlässlich seines 80. Geburtstages mit dem von Jon Sigurdson und Yael Tagerud herausgegebenen Buch „The Intelligent Corporation: The Privatisation of Intelligence“ geehrt.[166] In den USA hat der frühere CIA-Mitarbeiter Robert D. Steele seine Ideen aufgegriffen, weiterentwickelt und auf die amerikanische Intelligence Community übertragen. Er zählt seit den frühen 90er Jahren zu einem der größten Verfechter für eine bedeutendere Rolle von OSINT für die nachrichtendienstliche Arbeit und für eine stärkere Einbindung des privaten Sektors. Nach Steele soll der private Sektor nachrichtendienstliche Aufgaben im Bereich OSINT zunächst als Provisorium übernehmen, da die Dienste aufgrund ihrer historisch gewachsenen Rolle mit der Informationsflut des neuen Zeitalters überfordert sind. Wenn die Dienste sich in diesem Bereich neu aufgestellt haben soll der private Sektor als Benchmark fungieren, gegen den sich geheime nachrichtendienstliche Arbeit messen muss. Letztlich dient der private Sektor damit als Startpunkt für die „Neuerfindung“ der Geheimdienste.[167] Den Nutzen, den die verstärkte Nutzung von offenen Quellen haben kann, wies er in mehreren weiteren Publikationen nach. In der Reformdebatte um die amerikanischen Geheimdienste hat Steele mit seiner Position auch innerhalb der Intelligence Community starken Einfluss gewonnen. Der Analyst des Directorate of Science and Technology Stephen C. Mercado übernimmt beispielsweise in zwei Beiträgen der CIA-internen Zeitschrift Studies in Intelligence nahezu eins zu eins die Argumentation von Steele.[168]

Berkowitz/Goodman sehen den Einsatz von Geheimdiensten überhaupt nur dort gerechtfertigt, wo der private Sektor solche Leistungen nicht erbringen kann. Dies sei dann der Fall, wenn nachrichtendienstliche Arbeit unprofitabel, technisch zu anspruchsvoll oder illegal ist, sowie dann, wenn es um maßgeschneiderte Produkte geht, die spezielle Informationen für offizielle Regierungsvertreter enthal-

166 Sigurdson, Jon/Tagerud, Yael: The Intelligent Corporation: The Privatisation of Intelligence, London: Taylor Graham Publishers, 1992

167 vgl. Steele, Robert D.: Private Enterprise Intelligence: It’s Potential Contribution to National Security, in: Intelligence and National Security, Vol. 10, Nr. 4, 1995

168 vgl. Mercado, Stephen C. (2004) und Mercado, Stephen C.: Reexamining the Distinction Between Open Information and Secrets, Studies in Intelligence, Vol. 49, Nr. 2, 2005

ten.[169] Sie argumentieren, dass jegliches übrige Informationsbedürfnis besser, billiger und schneller vom privaten Sektor erbracht werden kann, was auf Private Intelligence Services durchaus zutreffen könnte.

William J. Lahneman spricht im Zusammenhang mit der Möglichkeit des Outsourcing der verschiedenen „INTs" (HUMINT, TECHINT, OSINT) von „Kernfunktionen" der Nachrichtendienste, die nicht in den privaten Sektor ausgelagert werden können. Zu unterscheiden davon sind „kritische Funktionen", die zwar wichtig für nachrichtendienstliche Analysten sind und daher vor allem von Vertretern der Intelligence Community für nicht ausgliederbar gehalten werden, für ihn aber durchaus Kandidaten für ein mögliches Outsourcing sind. Zu den „Kernfunktionen" zählt er lediglich HUMINT und die Weiterverarbeitung von Informationen, die vom diplomatischen Apparat gesammelt werden. Lahneman sieht sogar die Analysefunktion der Nachrichtendienste als „kritische Funktionen", und nicht als „Kernfunktion", die somit auch von Akteuren außerhalb der Intelligence Community wahrgenommen werden könnte.[170]

Die jüngsten Entwicklungen lassen darauf schließen, dass den Forderungen solcher Autoren mehr und mehr entsprochen wird. So wurde von John Negroponte, der das neu geschaffene Amt des Director of National Intelligence (DNI) innehat, im November 2005 angekündigt, eine eigene, organisatorisch selbständige Einheit für OSINT zu bilden, nämlich das innerhalb der CIA angesiedelte DNI Open Source Center.[171]

3.4.4 Fazit: Die Beziehungen zwischen privaten Akteuren und staatlichen Nachrichtendiensten im Bereich der Business Intelligence

Im Bereich Business Intelligence gibt es an mehreren Stellen Verbindungen zwischen staatlichen Nachrichtendiensten und privaten Akteuren.

169 Berkowitz/Goodman (2000), S. 40ff

170 vgl. Lahneman, William J.: Oursourcing the IC's Stovepipes?, International Journal of Intelligence and Counterintelligence, Vol. 16, Nr. 4

171 vgl. Office of the Director of National Intelligence: News Release No. 6-05, 8.11.2005, http://www.fas.org/irp/news/2005/11/odni110805.html

Auf dem Gebiet der Wirtschaftsaufklärung haben private Akteure die Dienste zurückgedrängt. Vor allem aufgrund der Öffnung ehemals geschlossener Gesellschaften nach 1990 ist ein Großteil der ehemals nur auf illegalem Wege zu beschaffenden Wirtschaftsdaten heute zugänglich. Die ökonomische Aufklärung kann daher zumeist ohne besonderen staatlichen Schutz erfolgen und ist, nicht zuletzt wegen der dort deutlich besseren Bezahlung fast vollständig in den Privatsektor übergegangen. In der Folge wurden die entsprechenden Abteilungen bei den Geheimdiensten abgebaut. Das Verhältnis zwischen Privaten und staatlichen Nachrichtendiensten ist bzw. war also im Bereich der Wirtschaftsaufklärung konkurrierend, wobei es aufgrund der veränderten Wesensmerkmale des Gegenstands klar zugunsten der Privaten entschieden worden ist.

Brisanter und stärker in die Zukunft weisend ist die Konkurrenz der Nachrichtendienste zu den so genannten Private Intelligence Services, deren Dienstleistungen hauptsächlich von transnationalen Unternehmen nachgefragt werden. Denn in diesem Fall verlieren die staatlichen Dienste nicht deshalb an Territorium, weil aufgrund der Veränderung politischer Rahmenbedingungen bestimmte Daten in den Bereich der OSINT gefallen sind. Vielmehr sind den staatlichen Nachrichtendiensten hier zum ersten Mal Konkurrenten erwachsen, die den gleichen Kernaktivitäten nachgehen. Durch die Tatsache, dass bei diesen Unternehmen häufig ehemalige Geheimdienstmitarbeiter tätig sind, ist die Gefahr des unkontrollierten Wissensabflusses groß. Jedoch könnten sie angesichts der hohen Qualität ihrer Arbeit für die Dienste auch als neue Quellen im Bereich OSINT dienen.

Innerhalb der Competitive Intelligence ist die Methode des Data Mining, die stark weiterentwickelt wurde, für Dienste insbesondere bei den „neuen" Bedrohungen wie dem internationalen Terrorismus und der organisierten Kriminalität von großer Bedeutung. Private Akteure fungieren hier als Quellen für die Nachrichtendienste, wenn auch weniger mit Bezug auf spezifische Daten als vielmehr in methodischer Hinsicht.

4 Fazit

Die Bedeutung privater Akteure für staatliche Nachrichtendienste ist seit dem Ende des Kalten Kriegs sowohl quantitativ, als auch qualitativ gewachsen. Quantitativ vor allem deshalb, weil sich das Aufgabengebiet der Dienste stark verbreitert hat und nun in vielen Bereichen in den privaten Sektor hineinreicht. Qualitativ sind die zwei wichtigsten Entwicklungen die wachsende Bedeutung transnationaler Unternehmen als eigenständige Akteure in der internationalen Politik und, damit zusammenhängend, das Aufkommen der Private Intelligence Services als Konkurrenten im Kernfeld nachrichtendienstlicher Aufgaben. Dabei können die transnationalen Unternehmen ein neues Motiv für staatliche Dienste sein, Wirtschaftsspionage zu betreiben. Dies wäre eine neue Art von Wirtschaftsspionage, die nicht darauf zielt, die heimische Wirtschaft zu unterstützen, sondern im Eigeninteresse der Dienste Aufklärung über die Interessen und Aktivitäten solcher Akteure zu gewinnen.

Grundsätzlich ist eine zunehmende Verschränkung von staatlichen und privaten Akteuren im Bereich der Intelligence festzustellen. In einigen Bereichen geschieht dies, da sich die Aufgaben für beide in ähnlicher Weise stellen, beispielsweise im Bereich Business Intelligence für staatliche Nachrichtendienste und Private Intelligence Services oder im Bereich wirtschaftlicher Spionage für Wirtschafts- und Konkurrenzspione. Besonders in den Feldern Information Warfare und Abwehr von Wirtschafts- und Konkurrenzspionage, die zur Counterintelligence gehören, sind die Dienste zur Kooperation mit privaten Unternehmen gezwungen, um wirksame Ergebnisse zu erzielen.

Mit der zunehmenden Herausbildung einer im Privatsektor angesiedelten Intelligence-Branche geht eine steigende Konkurrenz um Personal einher. Waren zu Zeiten des Kalten Krieges noch einige der besten Experten auf ihrem Feld bei den Nachrichtendiensten beschäftigt, so haben diese heute in vielen Bereichen Probleme, qualifizierte Beschäftigte zu finden. Dies liegt zum einen an der sich ändernden

Wahrnehmung der Dienste in der Öffentlichkeit und zum anderen an den Gehältern und Entwicklungsmöglichkeiten, die der private Sektor bietet. Dieses Problem wird von den Nachrichtendienste dadurch zu entschärfen versucht, dass Experten eine relativ lose Zusammenarbeit angeboten wird. Darüber hinaus ist es in zunehmendem Maße möglich, zwischen öffentlichem und privatem Sektor hin- und herzuwechseln.

Insgesamt stehen die Dienste also in unterschiedlichem Verhältnis zu Akteuren des privaten Sektors, in einigen Bereichen sind sie Quellen, in anderen Abnehmer, Konkurrenten oder Kooperationspartner (siehe Tabelle 6).

Tabelle 6: Klassifizierung der Beziehungen zwischen privaten Akteuren und staatlichen Nachrichtendiensten

Quellen	Abnehmer	Konkurrenten	Kooperationspartner
- Private Satellitenaufklärung (Staaten ohne eigene Kapazitäten) - Business Intelligence: Data Mining, Private Intelligence Services	- Wirtschaftsspionage	- Private Satellitenaufklärung (Länder mit eigenen Kapazitäten) - Business Intelligence: - Private Intelligence Services - Personal	- Information Warfare

Die Politik der Geheimdienste hat sich bisher um keine Klarstellung dieses Verhältnisses gekümmert, was dazu führt, dass ihnen private Akteure, die eventuell mehrere dieser Rollen spielen, mit einiger Reserviertheit begegnen. Problematisch ist dies für die Dienste vor allem da, wo sie private Akteure als Kooperationspartner oder Quellen benötigen.

Um Vertrauen aufzubauen setzt die Intelligence Community in den USA vor allem auf eine freiwillige Kooperation mit dem privaten Sektor, um von dessen Kapital, technischer Expertise und Schnelligkeit in der Entwicklung zu profitieren. Die Ansätze reichen dabei von Versuchen, über die CIA-eigene Firma In-Q-Tel Venture Kapital für junge, viel versprechende Unternehmen bereitzustellen, über die Subventionierung von am Markt nicht rentablen, für die Dienste aber interessante Investitionen, wie beispielsweise einer schnelleren Übertragung von aufgenommenen

Satellitenbildern an Erdstationen zur weiteren Verarbeitung, bis hin zu einer freiwilligen Selbstbeschränkung bei der Vermarktung sensibler Techniken und Produkte im Kommunikationsbereich oder wiederum bei den privaten Satellitenaufklärern.[172]

Ein positiver Nebeneffekt des zunehmenden Rückgriffs staatlicher Dienste auf private Akteure ist, dass diese Entwicklung die Zusammenarbeit zwischen den Nachrichtendiensten verschiedener Länder vereinfacht.[173] Neue Bedrohungen wie der internationale Terrorismus oder die organisierte Kriminalität erfordern zur Bekämpfung die Zusammenarbeit der Staaten, jedoch handhaben diese die Weitergabe von Geheimdienstinformationen traditionell sehr restriktiv. Durch die zunehmende Bedeutung von OSINT, die Private Intelligence Services in steigendem Maße auswerten, sowie durch die Verfügbarkeit privater Satellitenbilder ist die Notwendigkeit der strikten Geheimhaltung in vielen Fällen nicht mehr gegeben, wodurch eine Weitergabe von Informationen zwischen verschiedenen Nachrichtendiensten erleichtert wird.

Internationale Institutionen wie die UN bedienen sich bereits dieser neuen Quellen, um von den staatlichen Nachrichtendiensten ihrer Mitgliedsländer unabhängig zu werden. Sie nutzen daher Private Intelligence Services ebenso wie eine Vielzahl staatlicher Behörden. Ob und in welchem Umfang Geheimdienste auf sie zurückgreifen, konnte vom Autor nicht herausgefunden werden. Die Private Intelligence Services sind in der wissenschaftlichen Literatur bisher noch nicht untersucht. Sie stellen jedoch ein Phänomen neuer Qualität dar, dem sich die Intelligence-Forschung in zunehmendem Maße widmen werden muss.

172 Berkowitz/Goodman (2000), S. 51-53

173 vgl. Rathmell, Andrew: The Privatisation of Intelligence: A Way Forward for European Intelligence Co-operation, Cambridge Review of International Affairs, Vol. XI, Nr. 2, 1998, S. 199-211

5 Literaturverzeichnis

Primärquellen:

Arbeitsgemeinschaft für Sicherheit in der Wirtschaft e.V.: Anmerkungen zur Sicherheitslage der deutschen Wirtschaft, Berlin, Oktober 2005, http://www.asw-online.de/Anmerkungen-zur-Sicherheitslage-der-deutschen-Wirtschaft20043.pdf

ATHENA GS3 Security Implementations Ltd.: Intelligence from Open Sources: Real Time Intelligence from Unstructured Text in Multiple Languages, Herzliya Pituach, Mai 2003, http://www.athenaiss.com/documents/real_time_intelligence.pdf

Best, Richard A. Jr.: Imagery Intelligence: Issues for Congress, CRS Report for Congress, April 12, 2002, http://www.fas.org/irp/crs/IB10012.pdf

Bundesministerium des Inneren: Verfassungsschutzbericht 2004, Berlin, 17.5.2005, http://www.bmi.bund.de/nn_122688/Internet/Content/Broschueren/2005/Verfassungsschutzbericht__2004__de.html

Bundesministerium des Inneren: Nationaler Plan zum Schutz der Informationsinfrastrukturen, Berlin, Kabinettsbeschluss vom 13.7.2005, http://www.bmi.bund.de/cln_028/nn_708198/Internet/Content/Themen/Informationsgesellschaft/Sicherheit/NPSI.html

Bundesamt für Sicherheit in der Informationstechnik: Schutz Kritischer Infrastrukturen: Aktivitäten in Deutschland, Bonn, o.J., http://www.bsi.bund.de/fachthem/kritis/schutz_infrastr.pdf

Bundesamt für Sicherheit in der Informationstechnik: Der Schutz Kritischer IT-Infrastrukturen in Deutschland, Bonn, 2005, http://www.bsi.bund.de/fachthem/kritis/KRITIS_in_Deutschland.pdf

Bundesamt für Sicherheit in der Informationstechnik: Einführung in den Schutz kritischer IT-Infrastrukturen, Bonn, 2005, http://www.bsi.bund.de/fachthem/kritis/KRITIS_Einfuehrung.pdf

Department of Defense: Report to Congress Regarding the Terrorism Information Awareness Program, o.O., 20.5.2003, http://www.iwar.org.uk/news-archive/tia/darpa-tia-report.htm

EU Parlament, Nichtständiger Ausschuss über das Abhörsystem Echelon: Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)), Sitzungsdokument A5-0264/2001, Teil 1, 11.7.2001, http://kai.iks-jena.de/miniwahr/echelon-index.html

Hanning, August: Rede zur Eröffnung des Symposiums „IW – Kampf um und mit Information“, Pullach, 2.11.2000

Office of the Director of National Intelligence: News Release No. 6-05, 8.11.2005, http://www.fas.org/irp/news/2005/11/odni110805.html

Seifert, Jeffrey W.: Data Mining: An Overview, CRS Report for Congress, Updated January 27, 2006, www.fas.org/sgp/crs/intel/RL31798.pdf

Smith, Marcia S.: U.S. Space Programs: Civilian, Military and Commercial, Issue Brief for Congress, Updated Version of April 22, 2003, http://usinfo.state.gov/usa/infousa/tech/space/programs.pdf

White House: Defending America´s Cyberspace. National Plan for Information Systems Protection, Version 1.0. An Invitation to a Dialogue, Washington, 7.1.2000, http://www.whitehouse.gov/pcipb/

White House: The National Strategy to Secure Cyberspace, Washington, Februar 2003, http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf
White House: Homeland Security Presidential Directive/HSPD-7, Washington, 17.12.2003, http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html
White House: National Infrastructure Protection Plan, Draft NIPP v1.0, Washington, 2.11.2005, www.fas.org/irp/agency/dhs/nipp110205.pdf

Sekundärquellen:

Abele-Wigert, Isabelle/Dunn, Myriam: International CIIP Handbook 2006, Vol. 1: An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies, ETH Zürich: Center for Security Studies, 2005
Adriaans, Pieter/Zantinge, Dolf: Data Mining, New York: Addison Wesley, 1996
Agrell, Wilhelm: Global Watch – World Events and Business Intelligence, in: Sigurdson, Jon/Tagerud, Yael: The Intelligent Corporation, London: Taylor Graham Publishers, 1992, S. 99-106
Amato, Ivan: God's Eyes for Sale, Technology Review, Vol. 102, Nr. 2, 1999, S. 1-9
Andrieu, Michel (Bearb.): Space 2030: Exploring the Future of Space Applications, OECD-Studie, Paris: OECD Publ., 2005
Asmuth, Tobias: Unser Mann in Treptow; Von RAF bis Sayyaf: Die Firma Control Risks berät weltweit Manager in Sicherheitsfragen - ein Standort ist Berlin, Süddeutsche Zeitung vom 22.5.2002
Avant, Deborah D.: The Market for Force: The Consequences of Privatizing Security, Cambridge: Cambridge University Press, 2005
Baker, John C./Williamson, Ray A./Johnson, Bret: U.S. Security Interests and Dual-Purpose Satellite Technologies: Framing the Policy, in: Williamson, Ray A. (Hrsg.): Dual-Purpose Space Technologies, Washington D.C.: Space Policy Institute, 2001, S. 13-63
Baker, John C./Johnson, Dana J.: Security Implications of Commercial Satellite Imagery, in: Baker, John C./O'Connell, Kevin M./Williamson, Ray A. (Hrsg.): Commercial Observation Satellites: At the Leading Edge of Global Transparency, Santa Monica: RAND Corporation, 2001, S. 101-138
BBC Monitoring Latin America – Political: Brazilian government looking to control private intelligence agencies, 31.7.2004
Bendrath, Jochen: Computerkriminalität: Zivile Politik trotz militärischer Rhetorik, in: Daase, Christopher/Feske, Susanne/Peters, Ingo (Hrsg.): Internationale Risikopolitik: Der Umgang mit neuen Gefahren in den internationalen Beziehungen, Baden-Baden: Nomos Verlagsgesellschaft, 2002, S. 143-166
Bennett, Brian/Burger, Timothy J./Shannon, Elaine: China's big exports, Time Canada, Vol. 165, Ausgabe 8 vom 21.2.2005
Berkowitz, Bruce D./Goodman, Allan E.: Best Truth: Intelligence in the Information Age, New Haven: Yale University Press, 2000
Boren, David: The Intelligence Community: How crucial? Foreign Affairs, Vol. 71, Nr. 3, 1992
Bosch, Olivia: Cyber Terrorism and Private Sector Efforts for Information Infrastructure Protection, Konferenzpapier im Rahmen des Workshop of the ITU Strategy and Policy Unit, Seoul, 20.-22.5.2002, http://www.itu.int/osg/spu/ni/security/workshop/presentations/cniBosch%20paper.pdf
Burger, Timothy J./Bennett, Brian/Calabresi, Massimo/Duffy, Michael/Shannon, Elaine: The Russians Are Coming, Time Canada, Vol. 165, Ausgabe 6 vom 2.7.2005

Büschemann, Karl-Heinz: Geheimnisvolle Geschäfte mit der Sicherheit, Süddeutsche Zeitung vom 25./26.3.2006

Cerny, Dietrich: Information Warfare – Eine neue Bedrohung für Staat und Wirtschaft?, in: Tagungsband 5. Deutscher IT-Sicherheitskongress des BSI 1997, Ingelheim: SecuMedia Verlag, 1997, S. 205-213

Cerny, Dietrich: Schutz kritischer Infrastrukturen in Wirtschaft und Verwaltung, in: Geiger, Gebhard (Hrsg.): Sicherheit in der Informationsgesellschaft: Gefährdung und Schutz informationsabhängiger Infrastrukturen, Aktuelle Materialien zur Internationalen Politik, herausgegeben von der Stiftung Wissenschaft und Politik, Baden-Baden: Nomos Verlagsgesellschaft, 2000, S. 21-42

Chittenden, Maurice/Rufford, Nicholas: How agent Camus sank Greenpeace oil protests, Sunday Times vom 17.6.2001

Dupont, Alan: Intelligence for the Twenty-First Century, in: Intelligence and National Security, Vol. 18, Nr. 4, 2003, S. 15-39

Eckert, Dirk: Theorie und Praxis der Information Warfare in den USA, Kölner Arbeitspapiere zur internationalen Politik, Nr.1 2001

Fabian, Robert A.: Force Protection in an Era of Commercially Available Satellite Imagery: Space Blockade as a Possible Solution, Newport: Naval War College, 2002

Fink, Steven: Sticky Fingers, Chicago: Dearborn Trade Publishing, 2002

Florini, Ann M./Dehqanzada, Yahya A.: No more secrets? Policy Implications of Commercial Remote Sensing Satellites, Washington D.C.: Carnegie Paper No. 1, 1999, http://www.carnegieendowment.org/publications/index.cfm?fa=view&id=150

Florini, Ann M./Dehqanzada, Yahya A.: Secrets for Sale: How Commercial Satellite Imagery will change the World, Washington D.C.: Carnegie Endowment for International Peace, 2000

Geiger, Gebhard (Hrsg.): Sicherheit in der Informationsgesellschaft: Gefährdung und Schutz informationsabhängiger Infrastrukturen, Aktuelle Materialien zur Internationalen Politik, herausgegeben von der Stiftung Wissenschaft und Politik, Baden-Baden: Nomos Verlagsgesellschaft, 2000

Gross, Grant: DHS reorganization creates new cybersecurity position. The move could mean more focus on cybersecurity issues, IDG News Service, 13.7.2005, http://www.computerworld.com/governmenttopics/government/story/0,10801,103174,00.html?source=NLT_SEC2&nid=103174

Grundhauser, Lt. Col. Larry K., USAF: Sentinels Rising: Commercial High-Resolution Satellite Imagery and Its Implications for US National Security, Airpower Journal, Vol. 12, Nr. 4, 1998, S. 61-81

Hartley, Wyndham: Private intelligence firms face clampdown, Business Day (South Africa) vom 18.6.2003

Henze, Saskia/Knigge, Johann: Stets zu Diensten, Hamburg/Münster: rat/Unrast-Verlag, 1997

Herring, Jan P.: The unique role of the future in intelligence, in: Sigurdson, Jon/Tagerud, Yael: The Intelligent Corporation, London: Taylor Graham Publishers, 1992, S. 161-184

Hirschmann, Kai: Geheimdienste, Hamburg: Europäische Verlagsanstalt, 2004

Hulnick, Arthur S.: The Uneasy Relationship Between Intelligence and Private Industry, International Journal of Intelligence and Counterintelligence, Vol. 9, Nr. 1, 1996, S. 17-31

Hulnick, Arthur S.: Risky Business: Private Sector Intelligence in the United States, Harvard International Review, Vol. 24, Nr. 3, 2002, S. 68-72

Hulnick, Arthur S.: Keeping us safe: Secret Intelligence and Homeland Security, Westport: Praeger Publishing, 2004

Jakob, Bernd: Geheime Nachrichtendienste und Globalisierung, Europäische Hochschulschriften Band 380, Frankfurt am Main u.a.: Peter Lang, 1999

Johnson, Loch K.: Bomben, Wanzen und Intrigen: Amerikas Geheimdienste, Düsseldorf: Patmos Verlag, 2002

Kupchinsky, Roman: Information Revolution Feeds Alternative Intelligence Market, Washington D.C.: Radio Free Europe/Radio Liberty, 23.5.2005, http://www.globalsecurity.org/intell/library/news/2005/intell-050523-rferl01.htm

Lahneman, William J.: Oursourcing the IC's Stovepipes?, International Journal of Intelligence and Counterintelligence, Vol. 16, Nr. 4, 2003, S. 573-593

Litfin, Karen T.: The Globalization of Transparency: The Use of Commercial Satellite Imagery by Nongovernmental Organizations, in: Baker, John C./O'Connell, Kevin M./Williamson, Ray A. (Hrsg.): Commercial Observation Satellites: At the Leading Edge of Global Transparency, Santa Monica: RAND Corporation, 2001, S. 463-484

Lowenthal, Mark M.: Intelligence: From Secrets to Policy, Washington: CQ Press, 2003

Lubbers, Eveline: Corporate Intelligence, in: Lubbers, Eveline (Hrsg.): Battling Big Business, Totnes: Green Books Ldt., 2002

Lux, Christian/Peske, Thorsten: Competitive Intelligence und Wirtschaftsspionage, Wiesbaden: Gabler, 2002

Lynch, Colum: Private Firms Aid U.N. on Sanctions; Wider Intelligence Capability Sought, The Washington Post vom 21.4.2001

Mercado, Stephen C.: Sailing the Sea of OSINT in the Information Age, Studies in Intelligence, Vol. 48, Nr. 3, 2004, S. 45-55

Mercado, Stephen C.: Reexamining the Distinction Between Open Information and Secrets, Studies in Intelligence, Vol. 49, Nr. 2, 2005

O'Connell, Kevin/Lachman, Beth E.: From Space Imagery to Information: Commercial Remote Sensing Market Factors and Trends, in: Baker, John C./O'Connell, Kevin M./Williamson, Ray A. (Hrsg.): Commercial Observation Satellites: At the Leading Edge of Global Transparency, Santa Monica: RAND Corporation, 2001, S. 53-78

Osterhout, Robert: Transcript des Vortrages auf der Konferenz „No more secrets? Policy implications of commercial remote sensing satellites", veranstaltet vom Carnegie Endowment for International Peace, 26.5.1999, http://www.ceip.org/files/projects/tcs/remotesensingconf/OsterhoutTranscript.htm

Rathmell, Andrew: The Privatisation of Intelligence: A Way Forward for European Intelligence Co-operation, Cambridge Review of International Affairs, Vol. XI, Nr. 2, 1998, S. 199-211

Richelson, Jeffrey T.: A Century of Spies, New York/Oxford: Oxford University Press, 1997

Schmidt-Eenboom, Erich/Angerer Jo: Die schmutzigen Geschäfte der Wirtschaftsspione, München: Econ TB Vlg., 1994

Schweizer, Peter: Diebstahl unter Freunden, Reinbek: Rowohlt, 1993

Shulsky, Abram N./Schmitt, Gary J.: Silent Warfare: Understanding the World of Intelligence (3rd edition), Washington D.C.: Brassey's Inc., 2002

Siebel, Jan: Information Warfare: Das Gefechtsfeld der Zukunft?, in: Zoller, Manfred: Der Faktor „Intelligence": Das nachrichtendienstliche Metier in neuer sicherheitspolitischer Verantwortung, Brühl/Rheinland: Fachhochschule des Bundes für öffentliche Verwaltung, 2003, S. 113-190

Sigurdson, Jon/Nelson, Patricia: Intelligence gathering and Japan. The elusive role of grey intelligence, in: International Journal of Intelligence and Counterintelligence, Vol. 5, Nr. 1, 1991, S. 17-34

Sigurdson, Jon/Tagerud, Yael: The Intelligent Corporation, London: Taylor Graham Publishers, 1992

Steele, Robert D.: Private Enterprise Intelligence: It's Potential Contribution to National Security, in: Intelligence and National Security, Vol. 10, Nr. 4, 1995, S. 212-228

Steibl, Ralf E./Ansorge, Peter: Information Warfare: die Mythenmaschine im virtuellen Gefechtsfeld, in: Schneider, Thomas: Kriegserlebnis und Legendenbildung = The experience of war and the creation of myths: das Bild des "modernen" Krieges in Literatur, Theater, Photographie und Film, Bd. 3: "Postmoderne" Kriege? Krieg auf der Bühne. Krieg auf Leinwand = "Postmodern" wars? War on stage. War on the screen, Osnabrück: Rasch Universitätsverlag, 1999, S. 849-868

Treverton, Gregory F.: Reshaping National Intelligence for an Age of Information, RAND Studies in Policy Analysis, Cambridge: Cambridge University Press, 2003

Ulfkotte, Udo: Verschlusssache BND (3. Aufl.), München/Berlin: Koehler und Amelang, 1997

Ulfkotte, Udo: Marktplatz der Diebe, München: Bertelsmann, 1999

Williamson, Ray A.: Remote Sensing Policy and the Development of Commercial Remote Sensing, in: Baker, John C./O'Connell, Kevin M./Williamson, Ray A. (Hrsg.): Commercial Observation Satellites: At the Leading Edge of Global Transparency, Santa Monica: RAND Corporation, 2001, S. 37-52

Wolf, Jim: Industrial Spying Comes in From the Cold, Reuters News Service, 3.8.1991

In dieser Reihe sind bisher erschienen:

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 und 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 und Henrike Viehrig: Gesellschaftliche Bedrohungswahrnehmung und Elitenkonsens. Eine Analyse der europäischen Haltungen zum Irakkrieg 2003

AIPA 4/2004: Stephan Klingebiel und 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 und 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