Private Sicherheit im Spannungsfeld globaler Datenströme und konkurrierender Volkswirtschaften

Sicherheitsanalyse für Vorstände und Führungskräfte

http://www.wipn.de

Autor: Kay Golze, sowie Co-Autoren des Think Tanks STRATPROG

2. Aktualisierte Auflage, April 2009
Letzter Druck 28.05.2009

Impressum

Herausgeber und Vertrieb

WIPN Group

Internet: www.wipn.de

E-Mail: mail@wipn.de

Rechtliche Hinweise

Die Studien werden mit größtmöglicher Sorgfalt erstellt. Trotzdem kann die WIPN Group keine Haftung für die Nutzung der Studien übernehmen. Haftungsansprüche gegen die WIPN Group, welche sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der Studien verursacht wurden, sind grundsätzlich ausgeschlossen, sofern seitens des Autors kein nachweislich fahrlässiges oder grob fahrlässiges Verschulden vorliegt.

Alle innerhalb der Studien genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

Inhaltsverzeichnis

Persönlicher Hinweis des Autors

In diesem Band werden Szenarien beschrieben, die wenigen Personen bekannt sind, jedoch real existieren. Der Band beschreibt erstmalig komplexe Zusammenhänge von Informationstechnologie und Interessen von Unternehmen, anderer Staaten und kriminellen Organisationen, die für alle modernen Datennetze gelten, wie Internet, Intelligente Stromnetze, Smart Grids, Objekt to Objekt communication, etc.. Die in diesem Band in den Fokus gestellten Entscheidungsträger, als für eine Volkswirtschaft besonders wichtige und zentrale Personengruppe, wurden stellvertretend für die Auswirkungen von indirekter Informationsbeschaffung ausgewählt. Diese Gruppe steht aber stellvertretend für jede andere Gruppe oder Person. Der hier vorgestellte Band stellt also ein Szenario zur Diskussion, das mit dem Ausbau von Objekt to Objekt-Datennetzen und Smart Grids weiter sich verschärfen wird.

Die hier vorliegende Ausarbeitung stellt erstmals die Konzeptbasis bestehender Sicherheitskonzepte von Unternehmen grundsätzlich in Frage. Nach Ansicht des Autors entsprechen sie einer „mittelalterlichen Burg“ – wie z.B. im Wort Firewall besonders deutlich assoziiert –, die jedoch durch moderne „Missels“ angegriffen wird. Die modernen „Missels“ der Informationstechnologie entsprechen den indirekten Informationsbeschaffungskonzepten wie z.B. Scoring, Dataminging, etc., die als Grundlage einer personenbasierten Datenermittlung heute eingesetzt werden. In der Ausarbeitung werden dazu zahlreiche Beispiele angeführt.

Es ist dringend erforderlich, auf Staatsebene, auf Unternehmensebene und auf der persönlichen Ebene über die bestehenden Sicherheitskonzepte und die „Informelle Selbstbestimmung“ nachzudenken, die bereits heute nur noch rudimentär vorhanden ist. Durch die Weiterentwicklung der Informationstechnologie und der Entwicklung neuer Datennetze entstehen weitere Informationsmedien, die durch die Digitalisierung leicht und kostengünstig von Unbefugten ausgenutzt werden können. Die bekannt gewordenen kriminellen Fälle von „Bootnetzen“ bestätigen die in dieser Ausarbeitung aufgestellten Thesen deutlich. Die Entwicklung neuer Datennetze, wie z.B. die Smart Grids in der Energiewirtschaft, bergen dabei so erhebliche Einflussmöglichkeiten für moderne Angreifer, dass bereits beim Design dieser Netze nicht nur der Datenschutz, sondern auch vollkommen neue gesetzliche Rahmenbedingungen zum Schutz der Netze und damit ganzer Volkswirtschaften geschaffen werden müssen. Andernfalls bergen diese neuen Netze ein erhebliches Angriffspotential im sich verschärfenden Konkurrenzkampf der Volkswirtschaften.

Der Band weist beispielhaft an einer wichtigen Personengruppe auf die Informationslecks hin, die vor allem beim Schutz der nationalen und sich weiter entwickelnden internationalen Mobilität verstärkt beachtet werden müssen.

Vorwort

In dieser Studie werden weitestgehend unbekannte Zusammenhänge, Hintergründe und Szenarien, die bei der Nutzung globaler Kommunikationsmedien vorhanden sind, in ihrem Kontext verarbeitet. Damit werden erstmals Angriffs- und Gefährdungspotentiale von Führungskräften in Unternehmen, Organisationen und anderen Einrichtungen thematisiert, die durch die Nutzung der modernen Kommunikationssysteme entstehen. Die Studie zeigt ein zusammenhängendes Bild der Sicherheitsgefährdungen von Einzelpersonen und ihre Einordnung in unterschiedliche Zielsetzungen von verschiedenen Staaten, Organisationen sowie anderen einzelnen Personen – sogenannte „interessierte Gegenspieler“ – auf. Die Studie ist deshalb vor allem für die Entscheidungseliten in Unternehmen, Instituten und anderen Einrichtungen von besonderer Wichtigkeit.

Gesellschaft, Wirtschaft und Staat benötigen zuverlässige Informationen. Dazu sind sichere Kommunikationswege erforderlich, damit Informationen ihre Adressaten erreichen (Verfügbarkeit), Informationen als „wahr“ anerkannt werden (Integrität) und volle Vertraulichkeit gegeben ist.

In zahlreichen Untersuchungen wurde nachgewiesen, dass Sicherheit in den modernen Kommunikationsmedien nicht nur eine Frage der Technik ist, sondern auch eine Frage des organisatorischen Rahmens und des Kontextes, in dem die Technik eingesetzt wird. In der folgenden Abhandlung wird Top Down analysiert, welche Risiken für bestimmte Zielgruppen durch den Einsatz der modernen Kommunikationstechniken systembedingt gegeben sind und ob es für diese Zielgruppen einen Schutz gibt. Durch die Down-Betrachtung erschließen sich bestimmte Szenarien und ihre Schlüssigkeit wird erkennbar.

Mit dieser Studie werden die neuen Kommunikationsmedien (Internet, Mobilnetze, WLAN, etc.) und ihre Risikopotentiale im Zusammenhang analysiert. Die Instrumentalisierung der umfangreichen Datenkenntnis über einzelne Personen der Entscheidungselite einer Volkswirtschaft ist im Vergleich zur klassischen Kriegsführung das effizientere Mittel, um sich die Ressourcen eines konkurrierenden Industrie- oder Schwellenlandes dienstbar zu machen. Grundlage für diese Überlegungen bilden Strategien wie “Cyberwar“, „Information Warfare“, “Netwar” oder „Full Spectrum Dominance”. Mit der Strategie der „Full Spectrum Dominance“ wird keine klassische Eroberung von Territorien verfolgt, sondern der Machteinfluss in den entsprechenden Volkswirtschaften, der Zugang zu Ressourcen und der Marktzugang für eigene Produkte abgesichert. Die modernen Kommunikationsmedien liefern Geheimdiensten und Unternehmen in anderen Staaten Daten über einzelne Entscheidungsträger frei Haus. Damit sind die Entscheidungseliten, ihre Familien und Kinder einer neuen, hoch brisanten Gefahr bisher schutzlos persönlich ausgesetzt, ohne dass sie davon Kenntnis haben und ohne das es zur Zeit dagegen eine Abwehrmöglichkeit gibt. Dieses Bulletin informiert erstmalig über diese Gefahrenquelle.

Die ansteigende Bedrohung durch Software-Schädlinge (Viren, Würmer, Trojanische Pferde (kurz Trojaner genannt), Spyware, etc.), der Trend zur Kommerzialisierung und Professionalisierung der Internet-

kriminalität, der Trend zu immer detaillierteren (Internet-) Beobachtungen und zur Erstellung von Persönlichkeitsprofilen, der internationale Datenhandel mit personenbezogenen Daten, das geringe Schutzniveau vieler IT-Systeme – all das sind Warnhinweise auf Gefährdungspotentiale, die eine ganzheitliche und nachhaltige IT-Sicherheitsstrategie erforderlich machen. In der folgenden Abhandlung soll ein integrativer ganzheitlicher Ansatz gefunden werden, um der Komplexität im Zusammenspiel von fremden Interessen, Technologie, Angeboten/Produkten und Sicherheitsanforderungen gerecht zu werden. Als Leitbild soll der „Schutz von Persönlichkeitsrechten eines Individuums“ dienen. In diesem Leitbild kumulieren sich die Anforderungen an sichere, zuverlässige, vertrauenswürdige und geschützte Informationswege.

In dieser Studie wird analysiert, woher Gefährdungspotentiale kommen und in welchen Zusammenhängen sie stehen. Die Studie gibt den aktuellen Stand der Gefährdungen in ihrem Zusammenhang wieder, die durch das BSI und den Bundesverfassungsschutzbericht 2008 gestützt werden. Unser Think Tank will mit dieser Studie auch versuchen, die „Gefahrenpunkte“ zu entdecken und durch das Verständnis der Zusammenhänge erste Hilfestellungen für die Entwicklung eigener Abwehrstrategien zu geben. Der Think Tank STRATPROG der WIPN Group hat sich zum Ziel gesetzt, in den folgenden Quartalen der nächsten Jahre weiterführende Bulletins zu veröffentlichen.

In diesem Aufsatz wird die Diskussionslinie aus der Vogelperspektive „Volkswirtschaft“ als oberste Strukturebene entwickelt, so dass über diese Ebene wichtige Zusammenhänge und strategische Fragen erkannt und beantwortet werden können. Nur aus dieser Perspektive können auch integrative strategische Sicherheitsfragen gestellt werden, die aus Sicht international aufgestellter Unternehmen, NGO's und anderer Einrichtungen, von existentieller Bedeutung sind. Diese übergeordneten Zusammenhänge haben jedoch auch einen direkten Einfluss auf Fragen zum persönlichen Schutz der eigenen Daten, Sicherheit, Vertraulichkeit, Anonymität, Zuverlässigkeit, Integrität und Verfügbarkeit von Informationen und der Informationstechnologie selbst. Im Verlauf des Analyseprozesses wird diese „Vogelperspektive“ verlassen und wichtige Einzelaspekte im Detail behandelt. Insgesamt wird das Ziel verfolgt, über mehrere Bulletins einen strategischen Lagebericht der persönlichen Gefährdungspotentiale durch die weltweit vernetzten Kommunikationssysteme zu liefern.

Im Folgenden wird eine komplexe Gefährdungs- und Sicherheitslage beschrieben. Für den Entwurf eines Sicherheitskonzeptes ist jedoch eine möglichst vollständige Analyse über alle Ebenen notwendig, um richtige und wirksame Maßnahmen einleiten zu können. Erst durch die Kenntnis der komplexen Zusammenhänge können sich Entscheidungsträger mit Hilfe dieser Informationen ein vollständiges Bild machen und eigene strategische Überlegungen zu einem ihren Bedürfnissen angepassten Sicherheitskonzept entwerfen. Mit diesem Aufsatz soll diese umfassende Sichtweise und komplexe Kenntnislage vermittelt werden.

Quellen für vertiefende Studien, Analysen, Statistiken

Quellen und Studien wurden vor allem mit dem Ziel umfassender Informationsgewinnung gesichtet. Dabei wurden, unabhängig von politischen Einordnungen, eine möglichst große Brandbreite betrachtet. Grundlage aller Quellen sind die Seriosität, Zuverlässigkeit, Nachvollziehbarkeit der Aussagen ihrer eigenen Quellen. Die Quellenangaben in dieser Studie umfassen nur die wesentlichen Quellen. Der Autor beabsichtigt in einer neuen und erweiterten Auflage eine aktuelle Informationsliste zu diesem Thema herauszugeben. Sie wird mehrere Seiten umfassen.

- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth, Kansas
- Headquarters Department of the Army, Washington
- EPIC Electronic Privacy Information Center, Washington
- Project for the new American Century, Washington: Rebuilding American's Defenses, Strategy, Forces and Resources For a New Century
- American Enterprise Institute, Washington
- Global Network Initiative, Protecting and Advancing Freedom of Expression and Privacy in Information and Communications Technologies
- Xamit Beratungsgesellschaft mbH
- WIPN Group, Studie zur Sicherung der Persönlichkeitsrechte im Internet
- Universität Dresden, Institut für Systemanalyse
- Dr. Ralf Bendrath, Postmoderne Kriegsdiskurse u.a.
- Bundesministerium für Bildung und Forschung (BMBF), Hightechstrategie für Deutschland
- AGOF e.V., Veröffentlichungen und Statistiken
- SAP in Zusammenarbeit mit der Initiative „Deutschland sicher im Netz“; Faktor Mensch: Die Kunst des Hackens oder warum Firewalls nichts nützen
- NATO, Strategisches Konzept von 1999
- NATO Press Kommuniqué - 24. April 1999
- NATO Handbuch 2001
- Weißbuch 2006 der Bundesregierung zur Verteidigungspolitik
- Army Special Operations Forces, Unconventional Warfare, Sept. 2008

- Forschungsgruppe Informationsgesellschaft und Sicherheitspolitik
- Heise Online, Archive
- Telepolis Online
- Spiegel Online, Archiv
- Financial Times Deutschland, Archiv
- Süddeutsche Zeitung, Archiv
- Revolution in Military Affairs, Joint Vision 2010/2020
- Jörg Becker/Mira Beham, Operation Balkan: Werbung für Krieg und Tod
- Kishore Mahbubani: Die Rückkehr Asiens. Das Ende der westlichen Dominanz
- Andre Gunder Frank: ReOrient (Deutsche Ausgabe ab September 2009)
- Internationale Energieagentur der OECD (IEA)
- Association of the Study of Peak Oil (ASPO)
- Infowar-Monitor Organisation

Zusammenfassung

Die Sicherheit der weltweit vernetzten Kommunikationsmedien kann nicht isoliert, z.B. aus IT-technischer Sicht, betrachtet werden. Diese Analyse bietet eine komplexe Sicht auf die Bedeutung von Sicherheit für die global vernetzten Kommunikationsmedien wie Internet, Telefonie, Mobiltelefonie und andere digitale Medien. Dies ist vor allem für global agierende Unternehmen und ihren Führungsmannschaften von besonderer Bedeutung. Die Analyse zeigt auch auf, dass dieser komplexe Ansatz für Organisationen, multinationalen Konzernen, lokal aufgestellte Firmen und andere Entscheidungsträger in anderen Einrichtungen ebenfalls von herausragender Bedeutung ist.

Die Sicherheitsfrage von Kommunikationswegen und den damit übertragenen Informationen hat in den letzten Jahren aufgrund der raschen technologischen Entwicklung erheblich an Bedeutung zugenommen. Das Defizit an Sicherheit hat spiegelbildlich dazu ebenfalls im selben Zeitraum erheblich zugenommen (siehe Grafik). Die Sicherheitsfrage in Kommunikationsmedien muss deshalb in einem neuen Kontext gestellt und beantwortet werden. Vor allem vor dem Hintergrund erheblicher Entwicklungen im Zugriff unterschiedlicher staatlicher und nichtstaatlicher Stellen auf die privaten Daten (z.B. DPI=*Deap Packet Inspection;* GhostNet, etc.).

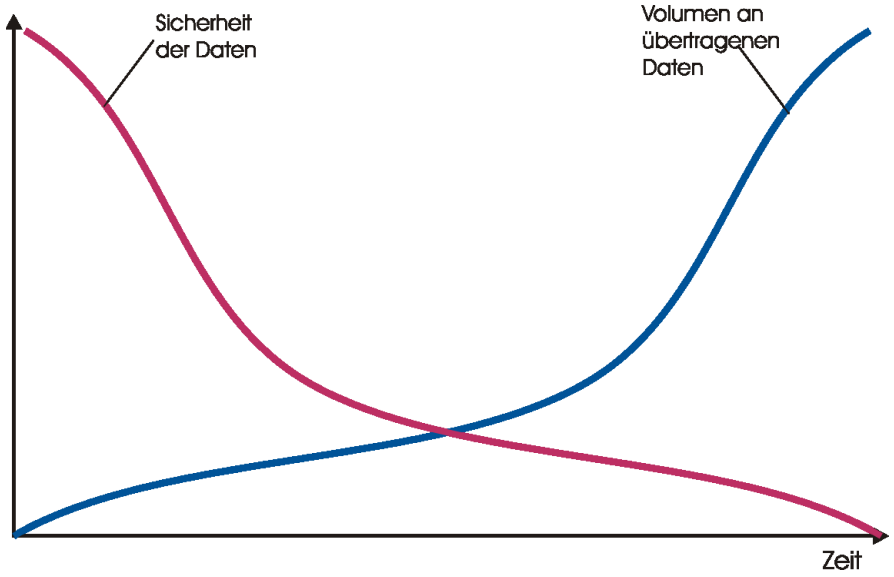

Abbildung 1: Bandbreitenentwicklung versus Daten- und Informationssicherheit

Das *Ghostnet* wirft ein Schlaglicht auf die neue Qualität von Gefahr: Anfang 2009 umfasste das *Ghostnet* handverlesene 1.295 Computer in ca. 103 Ländern (siehe Analyse des Infowar Monitor, Feb. 2009). Die Ziele waren/sind Außenministerien, Botschaften, Regierungsorganisationen, Verbänden, Banken, Nachrichtenorganisationen, Unternehmen und unklassifizierte Computer der NATO. Die Rechner des *Ghostnet* wurden zielgerichtet mit Spionage-Software infiziert, um Dokumente, E-Mails mit Kontaktinformationen, Terminpläne, Einladungslisten, Anwesenheitslisten, Entwürfe und Positionspapiere, Sit-

zungsunterlagen und Protokolle, Budgetplanungen, Geschäftspläne, Besucherlisten die Aufschluss über den Kontakt zu Rivalen und Feinden geben, Dokumente mit anderen Organisationen zu stehlen. Mit diesen Informationen aus verschiedenen Computern werden Absichten, Strategien und Projekte den Angreifern bekannt. Klassische Sicherheitsmaßnahmen wie Virenscanner und Firewalls bieten keinen Schutz vor einem solchen Angriff. Unsere Analyse stellt diese Angriffe in einen Kontext und zeigt die Hintergründe auf.

Wenigen ist eine von Staaten betriebene Internetspionage bekannt, wie sie z.B. von den Vereinigten Staaten, Israel, China, Russland und England, alle führende in diesem Bereich, betrieben wird. Diese Länder gehen in ihren Sicherheitsdoktrin davon aus, dass im strategischen Bereich der Cyberspace ein Äquivalent zu Land, Luft, Sea und Weltraum darstellt. China und andere Staaten betrachten den Cyberspace als einen Eckpfeiler in ihren Sicherheitsstrategien. Chinas „Cyber Warfare Doctrin“ sind weit entwickelt. Zur Zeit werden in Auftrag der chinesischen Regierung mit großem Engagement, Personaleinsatz und Technologie Einsatzzentren entwickelt. Andere Staaten entwickeln ebenfalls entsprechende Aktivitäten.

Neben Staaten führen im Cyberspace Unabhängige, Hacker und organisierte Kriminelle ebenfalls solche Angriffe durch.

Analyserahmen

Die Sicherheit der Daten in global vernetzten Kommunikationswegen ist in das folgende Umfeldszenario und dessen zukünftige Entwicklung eingebunden. Die Konkurrenzkämpfe zwischen den Volkswirtschaften um Energie, Rohstoffe und Märkte werden weiter zunehmen. Sie werden durch die derzeitige globale Finanz- und Wirtschaftskrise verstärkt. Dabei wird der erfolgreiche Konkurrenzkampf um Ressourcen, aber auch um (geographische) Einflussgebiete und Technologien, über das Überleben der Volkswirtschaften entscheiden. Die Intensität der Konkurrenz wird vor allem durch die sich weltweit ändernden Rahmenbedingungen wie Klimawandel, Bevölkerungswachstum, demographischer Wandel in den Industrienationen, Nahrungserzeugung und Versorgung, Verknappung fossiler Energien und Trinkwasser etc. bestimmt werden. Hinzu kommt eine sich abzeichnende Verlagerung des weltwirtschaftlichen Schwerpunktes nach Asien.

Die Fähigkeiten einer Volkswirtschaft zur Anpassung an diese neuen Bedingungen werden über ihre innere Sicherheit, ihren gesellschaftlichen Zusammenhalt und letztlich über ihr Überleben entscheiden. Die notwendige Anpassungsfähigkeit wird zukünftig wesentlich durch die Lösungskompetenzen innerhalb der eigenen Volkswirtschaft bestimmt werden. Die Entwicklung zukünftiger Absichten und die sich anschließende Lösungskompetenz basiert auf den Fähigkeiten von einzelnen Personen, die über moderne Kommunikationsmedien Informationen austauschen. „Lösungskompetenz“ ist bereits jetzt eine moderne Ressource.

Das Individuum als „Angriffsziel“

Die vorliegende Untersuchung analysiert diejenigen Risikopotentiale, die für eine Volkswirtschaft unter Nutzung der „neuen“ Kommunikationstechniken einhergehen. Die zentrale These ist, dass sich durch moderne Datenverarbeitungsanlagen und Kommunikationssysteme öffentliche Institutionen, Unternehmen und letztlich ganze Volkswirtschaften auf der Ebene einzelner natürlicher Personen sich „auflösen“ lassen. Anders formuliert: gelingt es, personenbezogene Daten und Informationen insbesondere über die Eliten einer Volkswirtschaft zu sammeln und auszuwerten, lässt sich hieraus ein aussagekräftiges Bild des gesamten Entwicklungs- und Leistungsstandes einer Volkswirtschaft zeichnen und ggf. für eigene Ziele und Vorteile nutzen. Das gilt vor allem dann, wenn Volkswirtschaften wie z.B. USA/Europa und China bzw. andere Staaten unterschiedlich organisiert sind. Die Konsequenz: sind private und berufliche Informationen in ausreichendem Maße von einzelnen Personen bekannt und sinnvoll zusammengefügt, kann auf die Köpfe und somit auf die Entwicklung des gesamten Systems gezielt Einfluss genommen werden und damit zum eigenen Vorteil ein Markt, öffentliche Meinung oder politische Entwicklung einer Volkswirtschaft erobert oder beherrscht werden. Prinzipiell entspricht dieses Bestreben klassischen Geheimdiensttätigkeiten. Durch die modernen Kommunikationssysteme und der Auslagerung von Geheimdiensttätigkeiten in Geschäftsmodelle entsteht jedoch eine neue Qualität und Quantität in der Informationsgewinnung, Auswertung und Einflussnahme auf die Eliten einer Volkswirtschaft.

Vor diesem Hintergrund verwundert es nicht, dass bereits seit längerem weltweit Szenarien für den „Angriff“ auf einzelne Personen in anderen Volkswirtschaften zum Vorteil der eigenen Volkswirtschaft oder eines Unternehmens entworfen werden. “Cyberwar“, „Information Warfare“, “Netwar” oder „Full Spectrum Dominance“ als Dachstrategie, sind in diesem Zusammenhang nur einige der Strategien, die in den vergangenen Jahren entwickelt wurden. Mit ihren Mitteln ist es möglich, die einzelne Person oder ein Führungsgremium ins Zentrum eines Angriffs durch z.B. einen anderen Staat, Unternehmen oder Organisation zu stellen (siehe Stucksnet, Botnet, etc.). Dies ist ein unmissverständlicher Hinweis darauf, dass der virtuelle Kampf um die Wissensressourcen konkurrierender Volkswirtschaften, also um die Köpfe einzelner Menschen, längst entbrannt ist.

Datenerhebung ab dem Kindesalter

Persönliche Daten der Eliten einer konkurrierenden Volkswirtschaft zu sammeln und zu einem aussagekräftigen Profil zusammenzuführen stellt im Internet-Zeitalter allenfalls ein logistisches, jedoch längst kein technisches Problem mehr dar. Bereits heute ist von einem „natürlichen Individuum aus Daten“ (NID) auszugehen, das als Datenabbild in modernen Kommunikationssystemen gespeichert ist. Über diese Datenbilder lassen sich mit ausgereiften mathematischen Verfah-

ren Persönlichkeitssimulationen durchführen, um Schwachstellen oder Angriffspotentiale zu ermitteln.

Das Datenabbild speist sich aus den unzähligen Informationen, die beinahe täglich – mit und ohne Wissen der Betroffenen, bzw. mit seiner unbewussten Mithilfe – von privatwirtschaftlicher oder staatlicher Seite erhoben werden. Internet-Nutzerprofile, Kunden- und Kreditkartendaten, auf Vorrat gespeicherte Telefonverbindungsdaten, oder auch die jüngst eingeführte eindeutige Steuer-Nummer auf Lebenszeit, bilden dabei lediglich einen kleinen Ausschnitt der hierzulande offiziell und inoffiziell praktizierten Datenerhebung ab.

Besonders beunruhigend: Entscheidungsträger auf allen Ebenen der Gesellschaft und in fast allen Einrichtungen des Staates haben die hieraus resultierende Gefährdung für eine Volkswirtschaft und sich selbst bisher nicht oder noch nicht vollständig erkannt. So ist hierzulande beispielsweise kein einziges datentechnisches Sicherheitskonzept eines Unternehmens oder einer anderen Einrichtung bekannt, dass nicht nur den CEO/Geschäftsführer in einem Unternehmen selbst, sondern auch dessen Ehepartner und Kinder im privaten Bereich datentechnisch schützt. Genau an dieser Stelle setzen die langfristig ausgerichteten Angriffsstrategien der Datensammler jedoch an. Mit Hilfe moderner Werbung – beispielsweise in Form von kostenlosen Services, Produkten und Diensten im Internet – werden vor allem Jugendliche dazu animiert, ihre persönlichen Neigungen und Beziehungen offen zu legen. Was weder die Kinder noch ihre Eltern ahnen: aus Sicht konkurrierender Volkswirtschaften stellen insbesondere die Daten Jugendlicher ein wertvolles Gut dar, da diese in aller Regel die Zukunft einer Volkswirtschaft repräsentieren und zukünftig auch zu den Eilten gehören könnten. Zusätzlich liefern Kinder und Jugendliche durch ihren naiven Umgang mit ihren eigenen Daten und den Daten Anderer (siehe u.a. Facebook und „Freundeslisten“) wichtige private Informationen über ihre Eltern, Einkommen der Eltern, Telefonnummern, private Adressen, Neigungen, Bekanntenkreis und anderer Beziehungen.

Umdenken ist überlebenswichtig

Angesichts dieser Mechanismen einerseits und der hierzulande noch immer vorherrschenden Einstellung andererseits, neue Kommunikationsmedien seien in erster Linie mit Chancen, aber kaum mit Risiken verbunden, ist festzustellen: um die für Deutschland zukunftsweisende Ressource Wissen zu schützen und entsprechende Abwehrmaßnahmen gegenüber konkurrierenden Volkswirtschaften entwickeln zu können, ist ein fundamentales Umdenken in Sachen Datenschutz in allen Ebenen der Gesellschaft unerlässlich. Betroffen hiervon sind alle in der Gesellschaft agierenden Gruppen, mit Schwerpunkt jedoch ihre Führungsmannschaften.

Während der private Bürger die häufig allzu leichtfertige Preisgabe seiner persönlichen Daten im Internet überdenken müsste, sollten multinational arbeitende Unternehmen und Organisationen das eigene Verhalten mit Blick auf ihren Status als potentielles Angriffsziel in einer Volkswirtschaft analysieren. Dazu ist die Entwicklung einer

ganzheitlichen Sicherheitsstrategie notwendig, die die neuen Angriffsmechanismen und somit den Schutz der persönlichen Daten der eigenen Entscheidungsträger berücksichtigen muss. Zudem sollten global aufgestellte Unternehmen die Einbindung in ihre jeweiligen Rechtsräume beachten und gegebenenfalls eine Unterstützung ihrer Interessen durch ihre Regierungen einfordern.

Auf staatlicher Ebene besteht ebenfalls erheblicher Handlungsbedarf. Im Zuge der Entwicklung einer neuen nationalen Datensicherheitsstrategie müsste unter anderem die dringende Frage beantwortet werden, ob und wie die durch Behörden gesammelten Daten vor dem Zugriff anderer Volkswirtschaften, aber auch vor Privatkriminalität, zuverlässig gesichert werden können. Unter dem Deckmantel der nationalen Gefahrenabwehr („Terrorismus“) werden hierzulande immer mehr Daten unbescholtener Bürger gesammelt und teilweise an befreundete, jedoch wirtschaftlich konkurrierende Staaten übermittelt. Als wesentliches Beispiel hierzu sei nur auf die Verträge zwischen den USA und der EU zur Übergabe von Fluggastdaten hingewiesen, mit denen gegen geltendes EU-Recht verstoßen wurde.

Mit der Preisgabe oder dem Verlust der persönlichen Daten in modernen Kommunikationsmedien beginnt der Verlust der persönlichen Souveränität. Der Zusammenhang zwischen den Datensammlungen und den Interessen anderer Volkswirtschaften, anderer Unternehmen oder Organisationen ist häufig nicht bekannt oder er wird unterschätzt. Zusätzlich wird die Dimension der persönlichen Gefährdung in der Regel nicht erkannt, vor allem dann, wenn Geheimdienste anderer Staaten oder von ihnen beauftragte Unternehmen den Aufbau von Datensammlungen betreiben. Ein Schutz des Einzelnen vor diesem Angriffspotential ist zur Zeit nicht vorhanden. Ein Schutz vor dem Verlust der eigenen Daten und dem damit einhergehenden Verlust an persönlicher Souveränität, ist jedoch dringend notwendig.

Die Bedeutung einer sicheren Kommunikation mit modernen Medien und deren Gefährdungspotentiale aus Sicht von Volkswirtschaften

Die Bedeutung von Datenströmen innerhalb und zwischen den Volkswirtschaften hat vor dem Hintergrund einer sich weiter global diversifizierenden Wirtschaft und eines sich global entwickelnden Marktes an Bedeutung für die Stabilität von Staaten und deren ökonomische und politische Modellvarianten zugenommen. Volkswirtschaften konkurrieren. Ihre Konkurrenz wird durch die sich global ändernden Rahmenbedingungen (Klima, Rohstoffe, Energie, Märkte) zunehmen.

Das Organisationsmodell „Staat“ hat sich im Lauf der Geschichte in unterschiedlichen Varianten herausgebildet und unterliegt einem stetem Wandel. Seit dem Ende des 2. Weltkrieges tendieren die Nationalstaaten dazu, sich in größeren Einheiten zu organisieren. Am Beispiel der EU zeigt sich, dass die wirtschaftliche Integration nicht mit der politischen Schritt hält. Die nationale Volkswirtschaft ist in der EU nach wie vor die Konstante, die das Gefüge der einzelnen Mitgliedsstaaten in erster Linie zusammenhält; in Lateinamerika und Asien zeigt sich dies trotz rudimentärer Ansätze zur Etablierung gemeinsamer Wirtschaftsräume noch deutlicher. Da die EU aus 16 Staaten der Eurozone und 11 weiteren Staaten besteht, die noch über ihre eigenen Währungen verfügen, ist sie in Krisenzeiten instabiler (siehe z.B. Finanzkrise 2008-2009 und befürchteter Staatsbankrott von einzelnen EU-Staaten) als der wirtschaftliche und politische Gesamtraum der Vereinigten Staaten von Amerika (USA), der mit dem Dollar nicht nur über eine Einheitswährung verfügt, sondern zusätzlich über die Weltreservewährung. Der EU fehlt eine Wirtschaftsregierung, die diesen strukturellen Nachteil kompensieren könnte. Dies macht sie insgesamt, und die einzelnen Mitgliedsstaaten im besonderen, in der ökonomischen Konkurrenz anfällig für „Angriffe“. Für unsere Thematik bleibt festzuhalten: In Europa bleiben die nationalen Volkswirtschaften bis auf weiteres der Kitt, der die einzelnen Gesellschaften zusammenhält.

Ihre öffentlichen Kenndaten spiegeln die wirtschaftliche Leistungsfähigkeit von Nationalstaaten wieder. Diese Leistungsfähigkeit der Nationalstaaten wird entscheidend mitbestimmt, durch den sicheren Zugang zu Rohstoffen, einschließlich fossiler Energien, und zu Absatzmärkten. Durch die zunehmende Zahl von Staaten, die als Schwellenländer die Entwicklung zum Industriestaat nachholen, kann sich die Konkurrenzsituation ohne eine Moderation im Rahmen einer global anerkannten Regulierungsinstitution (Vorschlag der Bundeskanzlerin Frau Merkel) verschärfen. Dies gilt besonders dann, wenn die ökonomische Gesamtausrichtung der Industriestaaten weiterhin mit einem unaustarierten Schwerpunkt auf den Export gelegt wird.

Für die nähere Zukunft werden die Staaten ihre nationalen Strategien zur Absicherung und zum Ausbau ihrer Positionen folglich an den existierenden Rahmenbedingungen ausrichten. Dies gilt es für den Aufbau eines eigenen wirksamen Sicherheitskonzepts zu berücksichtigen.

Im Folgenden wird analysiert, welche möglichen Strategieansätze eine Volkswirtschaft und deren Eliten für die Sicherung der persönlichen Kommunikation unter den heutigen und zukünftigen Rahmenbedingungen verfolgen müssen, um sich dem Änderungsdruck erfolgreich stellen zu können. Die vorliegende Analyse beschränkt sich auf die Auswirkungen moderner Kommunikationstechniken, mit Schwerpunkt Internet, auf moderne Volkswirtschaften. Strategische Fragen der nationalen und individuellen Sicherheit stehen im Vordergrund. Dabei greifen wir auf offizielle Dokumente aus frei zugänglichen Quellen zurück (siehe Quellenliste).

Ausgangslage

In dem Bericht „Lage der IT-Sicherheit in Deutschland 2007“ des BSI (Bundesamt für Sicherheit in der Informationstechnik, dem Bundesinnenministerium unterstellt) wird davon ausgegangen, dass Wissen und Innovation zukünftig zentrale Wirtschaftsgüter sind. Die Bundesregierungen der letzten Legislaturperioden haben als ein langfristiges Ziel festgelegt, dass Deutschland zu einer Wissensgesellschaft umgebaut werden soll. Der Übergang von der Industrie- hin zur Wissensgesellschaft führt zu einer immer intensiveren, auch weltweiten Vernetzung der Informationsströme. Wissen und Innovation stellen dabei die zentralen Objekte der Wertschöpfung dar. Beides basiert auf Individuen und ihren persönlichen Fähigkeiten. Wissen und Innovation können nur entstehen, wenn sie über moderne Kommunikationssysteme ausgetauscht werden. Sie bedürfen der Sicherheit, dem Schutz und der Vertraulichkeit, vor allem dann, wenn andere Staaten die Kommunikationssysteme als Äquivalent für Land, Luft, See und Weltraum ansehen.

Der Wandel des Sicherheitsbegriffs

Der Sicherheitsbegriff auf staatlicher Ebene unterliegt einem ständigen Wandel. Er ist abhängig von der jeweiligen machtpolitischen und wirtschaftlichen Interessenlage und reflektiert reale, objektive Risiken oder Bedrohungen nur in einem sehr begrenzten Umfang. So wurde im Kalten Krieg von westlicher Seite das militärische Potential der Sowjetunion stets überzeichnet. Derzeit werden die vom Terrorismus ausgehenden Gefahren alarmistisch überzeichnet, um vom Staat erwünschte Eingriffe in die Freiheit und Privatsphäre des Bürgers auszuweiten.

Für das tiefere Verständnis der hier vorgelegten Analyse werden die Hintergründe für den Wandel des Sicherheitsbegriffs kurz zusammengefasst. Dabei ist zu sehen, dass parallel zu diesem Wandel auch die modernen Kommunikationsmedien wie z.B. das Internet entwickelt worden sind. Die Erkenntnisse über die Entwicklung der zwischenstaatlichen Beziehungen, der Märkte und der global vernetzten Kommunikationstechnologie, sowie über ihre jeweiligen Rückkopplungspotentiale eröffnen ein umfassendes Verständnis für die Notwendigkeit, eigene Sicherheitsstrategien zu etablieren (siehe Grafik).

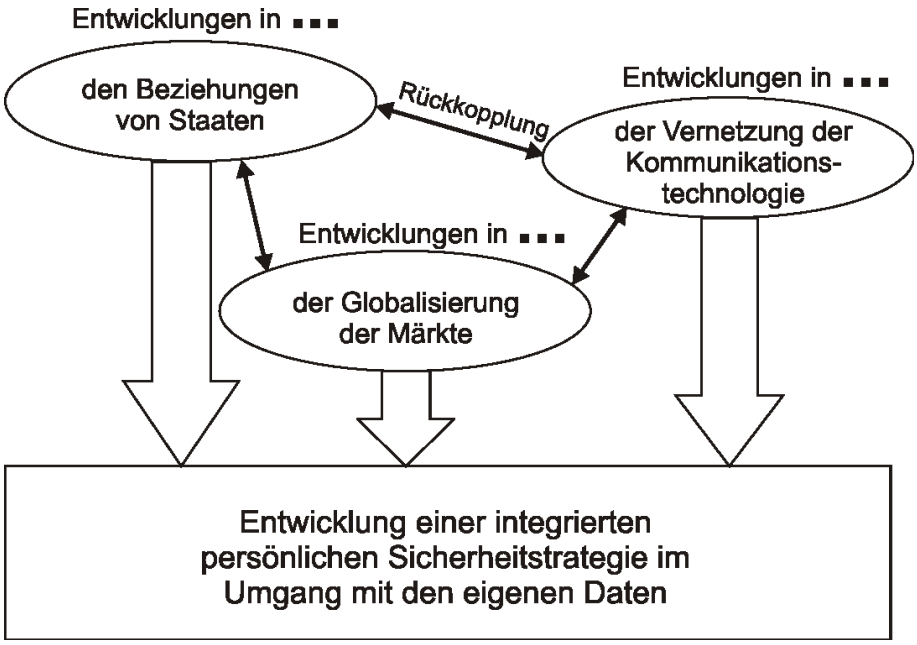

Abbildung 2: Einflussgrößen auf die Entwicklung des Sicherheitsverständnisses

Die äußere Sicherheit eines Staates zu gewährleisten ist Aufgabe seiner Streitkräfte. Alle Sicherheitsbegriffe innerhalb eines Staates ordnen sich direkt oder indirekt in diesen Rahmen ein und beziehen sich auf die für die äußere Sicherheit entwickelten Doktrinen, Strategien und Zielsetzungen. Mit Blick auf die Sicherheit moderner Kommunikationstechnik zeigt sich, dass vor allem in diesem Bereich ein erheblicher Einfluss militärischer Überlegungen vorhanden ist.

Der Wandel des Sicherheitsbegriffs im internationalen Beziehungsgefüge hatte bereits vor der Auflösung des Ostblocks eingesetzt, erhielt aber durch die „Wende“ in Deutschland ein erhebliches Momentum. Er hängt eng zusammen mit der Entwicklung der Weltwirtschaft und ihres Ordnungsrahmens, also dem, was heute als „Globalisierung“ bezeichnet wird. Mit der Erweiterung der nationalen Märkte zu globalen Märkten und der Etablierung einer entsprechenden globalen Wirtschaftsordnung geht ein Wandel der Interessenlage und folglich des Sicherheitsbegriffs einher, begleitet durch die technologische Entwicklung in den Kommunikationsmedien und der Leistungsfähigkeit moderner Datenverarbeitungsanlagen

Auf der militärpolitischen Ebene lässt sich somit der Wandel der Beziehungen zwischen den Staaten auch am Wandel des Sicherheitsbegriffes ablesen.

Früher fand die Erwirtschaftung von nationalem Reichtum vorwiegend innerhalb einer Volkswirtschaft statt. Dabei waren die Staatsgrenzen in der Regel mit den Grenzen der Volkswirtschaften identisch. Mit der massiven Industrialisierung und der Ausweitung des Welthandels seit dem 19. Jahrhundert – unterbrochen von der Zeit zwischen dem 1. Weltkrieg und dem Ende des 2. Weltkrieges – wurden entwickelte Volkswirtschaften im erhöhten Maß von der Versorgung mit Rohstoffen abhängig, über die sie selber nicht verfügten. Die damit verbundenen Gefahren zeigten sich erstmals einer breiten Öffentlichkeit mit der sog. Ölkrise der 1970er Jahre. Die Absicherung von Rohstofflieferungen war für jedermann sichtbar eine existentielle Funktion des wirtschaftlichen Systems der Volkswirtschaften bzw. der Industriestaaten geworden. Die USA entwickelten vor diesem Hintergrund die „Carter-Doktrin“, die den Zugriff auf die Ölvorräte im Nahen Osten zum „nationalen Sicherheitsinteresse“ erklärten. Sie gilt bis heute.

In den 1980er Jahren entwickelten sich die großen nationalen Konzerne im Rahmen der Doktrin des „freien Welthandels“ zu transnationalen „Global Player“, die ihre Produktionsstrukturen auf verschiedene Länder verteilten. Mit dieser Entwicklung setzten sich globale Kapitalverwertungsbedingungen durch. Ein Meilenstein auf diesem Weg war die Gründung der Welthandelsorganisation (WTO) 1995, in der die westlichen Industriestaaten dominieren und die Regeln setzen. Ihre Aufgabe ist es, dem Prinzip des „freien Handels“ weltweit Geltung zu verschaffen. In der Folge bedeutete das, dass die nationalen Märkte der Volkswirtschaften zu Teilen des Weltmarktes wurden und werden und dessen Bedingungen unterliegen, von ihnen selbst jedoch nur begrenzt beeinflussbar sind. Im Rahmen dieser Analyse geht es nicht darum, das Pro oder Kontra dieser Entwicklung zu erörtern, sondern darum, ihre Auswirkungen auf die jeweiligen Sicherheitsstrategien darzulegen, die wiederum von der jeweiligen Konkurrenzsituation und den gesamtpolitischen Zielen der Staaten abhängig sind.

An diese Entwicklung wurden die bisher am Nationalstaat ausgerichteten Sicherheitskonzepte angepasst. Mit der Gründung der WTO wurde die Organisation der Wirtschaft nicht mehr national sondern transnational ausgerichtet. Parallel dazu – durch das WTO-Abkommen befördert – fand die kommunikative Globalisierung, also die der Medien statt (u.a. Unterhaltungsindustrie, CNN, Internet, etc.). Entge-

gen diesen Entwicklungen stehen die Staaten, die nicht der Entwicklung der Globalisierung der Märkte gefolgt sind.

Somit hat der Weltmarkt eine massive Durchsetzungskraft gegenüber den einzelnen Nationalstaaten entwickelt, die politisch territorial organisiert sind. Damit verschärfen sich jedoch auch Ungleichheiten innerhalb und nicht mehr überwiegend nur außerhalb der einzelnen Gesellschaften (Kapital, Arbeitsplätze und Informationen können frei wandern, wie die Güterströme). Die Ausrichtung der Volkswirtschaften auf die Verwertungsinteressen transnational arbeitender Konzerne, zulasten der binnenmarktorientierten Unternehmen und des Faktors Arbeit, ist heute in fast allen Industrienationen umfassend auf den Weg gebracht worden. Hieraus zunehmend entstehende und sich verschärfende Ungleichheiten innerhalb der nationalen Gesellschaften können gravierende Folgen entwickeln und ihre Stabilität gefährden (auf Gesellschaftsteile bezogene Verarmung, Radikalisierung, Abspaltungen, Desintegration, etc.), die bislang ausschließlich mit Entwicklungsländern, nicht jedoch mit demokratisch verfassten Industrienationen assoziiert wurden, wie schwindende Akzeptanz des demokratischen/politischen Systems (siehe Rückgang der Wahlbeteiligung, Rückbesinnung auf nationale Präferenzen in den politischen Parteien, etc.) sowie letztlich gewaltsame Auseinandersetzungen mit bürgerkriegsähnlichem Charakter. Die ersten Vorboten einer solchen Entwicklung zeigen sich bereits in der Folge der aktuellen Finanz- und Wirtschaftskrise in Spanien, Frankreich, Portugal, Griechenland, Litauen und Großbritannien.

Unter diesen Bedingungen und bei Abwesenheit eines staatlichen äußeren Gegners geht es den politischen Eliten nicht mehr um die Sicherung von Territorien oder Volkswirtschaften, sondern um das „Funktionieren“ des Wirtschaftsprozesses/Wirtschaftsmodells insgesamt (siehe Bankenrettungsmaßnahmen; ausschließliche „Systemrelevanz“ von Unternehmen des Kapitalmarktes). In der folgenden Grafik werden die Entwicklungen von Unten nach Oben und von Links nach Rechts zusammengefasst aufgezeigt.

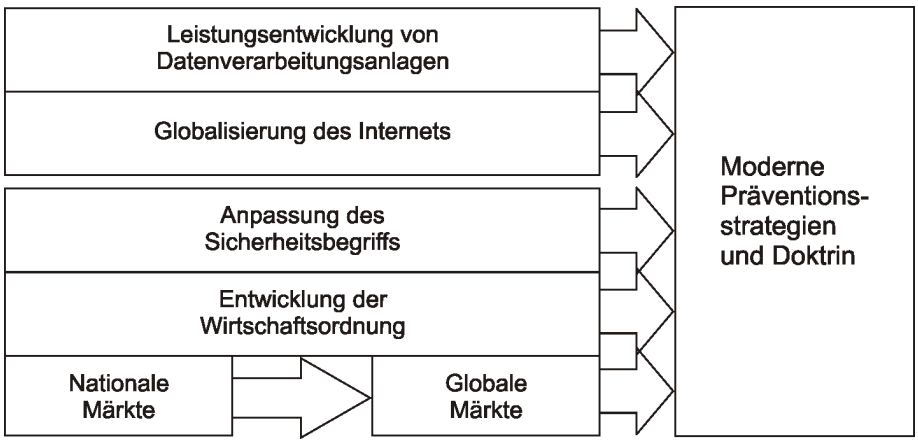

Abbildung 3: Einflüsse auf die Entwicklung moderner Präventionsstrategien und Doktrin

Entsprechend wurden Sicherheitsbegriff und Sicherheitskonzepte in den Staaten angepasst. Der Sicherheitsbegriff wurde um die Siche-

rung der gesellschaftlichen Funktionszusammenhänge – um die Absicherung der Globalisierungsrisiken – erweitert. Dieser Logik folgend sind die Sicherheitsdoktrin auf der militärischen Ebene seit 1990 auf die „Sicherheit vor Risiken“ angepasst worden. Die NATO hat 1991 und 1999 in ihrem jeweils verabschiedeten „Neuen Strategischen Konzept“ (siehe gleichnamige Dokumente) den neuen Sicherheitsbegriff übernommen und legitimiert, und damit ihre Daseinsberechtigung nach dem Ende des Systemkonflikts (Mauerfall bzw. Ende der UDSSR).

Die heutigen „Risiken“ werden auch unter dem Sammelbegriff „Instabilität“ zusammengefasst. Mit dem Begriff der „Sicherheit vor Risiken“ konnten somit auf den Nationalstaat bezogene Sicherheitsanforderungen, die in der Regel einen Gegner von außen annahmen, in exterritoriale oder auch innerstaatliche Szenarien umgewandelt werden (siehe auch die Weiterentwicklung der Strategische Konzepte der NATO). Mit dem neuen Sicherheitsbegriff wurde die frühere nationalstaatliche Sicherheitsstrategie den globalisierten Märkten angepaßt und Einsätze in anderen Staaten wie auch im Innern (des eigenen Territoriums) legitimiert. Die NATO bezeichnet diese Einsätze als „out of area“, weil sie außerhalb des Gebietes stattfinden, das im Nordatlantikvertrag definiert ist.

Die neuen „Risiken“ werden nicht mehr, wie noch bei der früheren „Bedrohung“ an konkreten Akteuren festgemacht. Als Risiken können alle Entwicklungen wahrgenommen werden, deren Ausgang offen ist und aus denen irgendwann eine Störung des globalen Kapitalverwertungsprozesses bzw. eine Störung im Funktionieren des Wirtschaftsmodells entstehen kann. Mit diesem weitgefassten Sicherheitsbegriff ist im Prinzip alles, was in einer Gesellschaft, der Politik und der Ökonomie weltweit passiert, für den Zugriff des Militärs und der Geheimdienste interessant, da die prinzipielle Offenheit aller Veränderungen in einem Staat, zwischen Staaten oder durch allgemeine Entwicklungen hervorgerufen (Klimawandel), ein mögliches Risiko darstellt. In diesem neuen strategischen Ansatz entfällt der Bezug zu einen konkreten Gegner. In der Konsequenz entfällt die Option zu Verhandlungen, die deeskalierend wirken können. Mit einem „abstrakten Risiko“ lassen sich keine Verhandlungen führen, etwa im Rahmen von vertrauensbildenden Maßnahmen oder Abrüstungskonferenzen.

In der Logik dieser Sicherheitsstrategie/Sicherheitspolitik kann gegen „Risiken“ nur eine „Risikovorsorge“ eingesetzt werden. Anders als früher, nimmt das Militär daher nicht mehr die Rolle des letzten Mittels ein, sondern wird als eines von vielen, als „normales“ Instrument zum „Krisenmanagement“ angesehen. Der Einsatz von Militär gegen die eigene Bevölkerung wird wieder salonfähig. Damit dringt aber das militärische Handlungsfeld auch in soziale Bereiche der eigenen Bevölkerung ein, die traditionell nicht als militärischer Handlungskontext angesehen wurden. Im internationalen Kontext wird mit dieser Entwicklung die Krisenprävention mit zivilen Mitteln zurückgedrängt und durch völkerrechtlich nicht gedeckte militärische „Präventivkriegsführungen“ ersetzt.

Im Bereich der inneren Sicherheit geht es nun parallel zur Strafverfolgung um „Sicherheitsvorsorge“, um Präventionsmaßnahmen. Damit erhalten Polizei und Justiz weit im gesellschaftlichen Vorfeld von

eventuellen Straftaten eine erweiterte Zuständigkeit (siehe Gesetzesänderungen seit 2006 eingebracht durch das Innenministerium). Innerhalb Europas wurden auf Basis dieser strategischen Überlegungen auch konkrete Abkommen zwischen den Nationalstaaten, wie z.B. das „Schengener Abkommen“, unterzeichnet. In diesem Abkommen können sogenannte „Sicherheitsschleier“ ausgelegt werden, die Kriminellen ebenso wie auch der eigenen Bevölkerung gelten (unscharfe, im Rahmen der Sicherheitsvorsorge angewandte Maßnahmen ohne konkrete Zielpersonen, sondern zur Abwehr von abstrakten Risiken).

Vor diesem Hintergrund sind auch die aktuellen Entwicklungen (2008 und 2009) in den Gesetzesvorlagen zur Vorratsdatenspeicherung, zur Onlinedurchsuchung, zu den erweiterten BKA-Zuständigkeiten und zu den Bestrebungen zum Einsatz der Bundeswehr im Inneren zu beurteilen.

Entwicklung in den Kommunikationsmedien

Mit dem geänderten Sicherheitsbegriff, vor dem Hintergrund der Globalisierung und der parallel dazu verlaufenden Entwicklung der Kommunikationsmedien entstanden auch vollkommen neue strategische Überlegungen, die zu neuen strategischen Szenarien wie „Cyber war“ oder „Information Warfare“ geführt haben (siehe auch Think Tank RAND Corporation). Die Folge war die Gründung der „School of Information Warfare and Strategy“ an der National Defense University in Washington. Die hier entwickelten Strategien wurden in die Strategiepapiere des US-Generalstabes „Joint Vision 2010“ und „Joint Vision 2020“ aufgenommen. Als Standardwerk wurde das Buch „War and Anti-War“ von Alvin und Heidi Toffler angesehen, in dem eine neue Form des Krieges vorhergesagt wurde, die auf der Beherrschung der Information basiert. In Rahmen dieser Entwicklungen ist auch der Begriff der „Full Spectrum Dominance“ geprägt worden, auf den später in diesem Bulletin eingegangen wird (im strategischen Bereich stellt das Cyberspace ein Äquivalent zu Land, Luft, Sea und Weltraum dar).

Wenn jedoch in den Kriegen der Zukunft nicht mehr die Feuerkraft, sondern die *Informationsvorherrschaft* entscheidend ist, dann zielt die Krisenstrategie nicht mehr auf die „Hardware“ des Gegners – seine Infrastruktur und Produktionskapazitäten, sein Militär – sondern auf den Geist der Menschen in einer anderen Volkswirtschaft. Dabei soll die „*Selbst- und Umweltwahrnehmung des Gegners so strukturiert werden, dass er dem Willen des Angreifers folgt, ohne mit Gewalt gezwungen zu werden“* (George Stein). Zitat: „Das Angriffsziel des Informationskrieges ist dann das menschliche Denken, speziell das Denken derer, die die Schlüsselentscheidungen über Krieg und Frieden treffen.“ (Information Warfare (8), in: Airpower Journal, Nr. 1), so Prof. George Stein, am Army War College. Auf dieser Basis wurden weitere Konzepte für weitergehende Formen der Kriegsführung entwickelt, die unter den Leitbildern „Netwar“ oder „Neocortical War“ zusammengefasst werden. Sie beinhalten eine Ausweitung des Kriegsbegriffs auf alle Konfliktformen in der Gesellschaft, die mit öffentlichen Mitteln ausgetragen werden. Informationen gelten dabei zunehmend als Waffe. Die Vordenker in den Universitäten, Colleges und amerikani-

schen Think Tanks sind der Überzeugung, dass in der gezielten konzertierten Zusammenarbeit zwischen Nichtregierungsorganisationen (NGO's), Journalisten, Medienkonzernen einerseits und diese Zusammenarbeit steuernden staatlichen Informationsstellen eines Landes andererseits, ein gewaltfreies Äquivalent für militärische Macht gefunden wurde. Diese Überzeugungen wurden in fast allen Staaten der EU, besonders in Deutschland und England, übernommen!

Abgeleitete Entwicklungen

Vor dem Hintergrund dieser Entwicklung des Sicherheitsbegriffs und den damit einhergehenden Änderungen in den Sicherheitsdoktrin werden auch die letzten Vorschläge des Bundesinnenministeriums (in 2008) erklärbar und verständlich, mit denen weitreichende Kompetenzen für das BKA und dessen Zusammenarbeit mit dem BND als Superbehörde (2008, Bundesinnenministerium) bzw. der Einsatz von Software zur Durchsuchung von privaten PC (Stichwort „Bundestrojaner“) gefordert wurde. Vorbild ist hier das „Heimatschutzministerium“ der USA, obwohl das Deutsche Grundgesetz eine strikte Trennung von Polizei und Geheimdiensten vorschreibt.

Dabei geht man davon aus, dass ein privater PC in seinem Datenbestand ein „Abbild der Persönlichkeit“ ist und somit hinreichende Informationen über die Tätigkeiten seines Benutzers, deren Neigungen, Bedürfnisse und dessen Überzeugungen liefern kann (siehe dazu auch Bundesverfassungsurteil zur Online-Durchsuchung in 2008).

An dieser Stelle soll lediglich auf die historischen Wurzeln einzelner Entwicklungen im Rahmen der modernen Kommunikationssysteme hingewiesen werden. Eine Interpretation der zusammengetragenen Fakten kann in diesem Rahmen jedoch nicht stattfinden. Hier soll auf entsprechende Dokumente aus den oben erwähnten Universitäten, zahlreiche Bücher zu diesem Thema und öffentlich zugänglichen Dokumenten des Pentagon und der NATO hingewiesen werden.

Konkurrenz der Volkswirtschaften

Wegen der globalen Konkurrenz unter den Volkswirtschaften bestehen besondere Anforderungen an ein Sicherheitskonzept sowohl auf nationaler, wie auch transnationaler Ebene, wenn sich Volkswirtschaften in Staatenbünden wie z.B. der EU zusammenfinden. Dabei ist der staatliche Sicherheitsbegriff der Oberbegriff, in dem die nationale IT-Sicherheit eingebettet sein muss. Einerseits sind die nationalen Volkswirtschaften mit ihren Interessen zu berücksichtigen (einzelne Mitgliedsstaaten der EU), andererseits müssen Entwicklungen zur Harmonisierung ihrer spezifischen Interessen im Staatenverbund stattfinden. Diese Harmonisierungsentwicklungen mildern den Konkurrenzkampf der Volkswirtschaften innerhalb der EU.

Zusätzlich zu diesen Entwicklungsprozessen auf der transnationalen Sicherheitsebene innerhalb der EU ist als „besondere Herausforderung“ an europäische und andere Volkswirtschaften und ihre Sicherheitssysteme – besonders beim Einsatz moderner Kommunikationssysteme wie dem Internet – der umfassende Dominanzanspruch der

Vereinigten Staaten zu sehen, der sich hinter dem Begriff „Full Spectrum Dominance“ verbirgt (siehe auch „Der Wandel des Sicherheitsbegriffs“). Dem eigenen Anspruch, angesichts der von den US-Strategen so bezeichneten Rivalen wie EU, China und Anderen, gerecht zu werden, erfordert einen umfassenden Instrumentenkasten. *Full Spectrum Dominance* wurde folglich von einer militärischen Strategiedefinition des Pentagons zu einem zentralen strategischen Handlungsrahmen zahlreicher amerikanischer Einrichtungen und Unternehmen erweitert. Mit dieser langfristigen Strategie wird das Ziel verfolgt, der amerikanischen Volkswirtschaft auf allen Handlungsfeldern die Interessendurchsetzung zur Herstellung voller Dominanz zu sichern. Sie wurde also aus ihrem ursprünglich nur auf den militärisch bezogenen Überlegenheitsanspruch gelöst und auf alle Bereiche ausgedehnt, die der Absicherung der US-Hegemonie dienen könnte. Für die Anwendung dieser nationalen strategischen Zielsetzung gibt es zahlreiche praktische Beispiele, auf die in den folgenden Absätzen punktuell hingewiesen wird.

Unter dem Begriff „Full Spectrum Dominance“ und „Cyber Warfare“ können zahlreiche öffentlich zugängliche Abhandlungen auf den Webseiten des amerikanischen Militärs und dessen Einrichtungen abgefragt werden (siehe auch „School of Advanced Military Studies“, „United States Army Command“ und „General Staff College“). Unter dem Begriff der „Full Spectrum Dominance“ wird eine Vorherrschaft über wesentliche Bereiche wie Militärausstattung und Einsatz, Technologie, Finanzwirtschaft, Weltwirtschaftssystem (WTO, IWF, Weltbank, Dollar als Weltleitwährung), Energiereserven und ihre Transportströme, Rechtsverständnis/Rechtssystem, Nahrungsmittelproduktion (Gentechnik und damit verbundene Patente, die wesentlich in den USA erteilt worden sind) und Kultur (Way of Live) verstanden.

Seit dem 11. September 2001 wird unter dem Begriff „Krieg gegen den Terror“ (War on Terror) ein globales Ziel definiert und unter Führung der USA eine „Allianz der Willigen“ zusammengestellt. Vor dem Hintergrund der oben beschriebenen Doktrin, ihrer realen Umsetzung und der globalen wirtschaftlichen Verflechtungen kann sich ein Staat diesem Wunsch nach Gemeinsamkeit in einer „Koalition der Willigen“ kaum entziehen. In der global definierten Strategie des „Krieges gegen den Terror“ wurden seit dem Anschlag in New York zahlreiche nationale und internationale Maßnahmen beschlossen. Der Begriff *Krieg gegen den Terror* wurde zu einem Vorwand, Maßnahmen zur Einschränkung der Bürgerrechte in vielen Staaten der EU und den USA gegenüber der Öffentlichkeit zu begründen. “Terrorabwehr“ in seiner präventiven oder „vorsorgenden“ Ausrichtung verdeutlicht den Wandel des Sicherheitsbegriffs, der früher von der Bedrohung durch andere Staaten ausging, hin zur „Sicherheitsvorsorge“ gegen eine unkonkrete, diffuse Terrorgefahr durch nichtstaatliche Akteure (Einführung des Begriffs der „asymetrischen Bedrohung“ bzw. des „asymetrischen Krieges“; Einführung der Begriffe der „Abstrakten Gefahr“ bzw. der „Abstrakten Gefährdung“). “Terrorismus“, gegen den unter der Führung der USA innerstaatlich und global Krieg geführt wird, ist das heutige neue Feindbild.

Dazu beigetragen haben die in Echtzeit von der Welt wahrgenommenen Bilder der Anschläge vom 11. September. „Der“ internationale

Terrorismus als globales Bedrohungsphänomen für alle Staaten der Welt ist jedoch irreführend, weil terroristische Aktivitäten ihren jeweils nationalen/regionalen Bezugspunkt haben (siehe z.B. in Europa: ETA Spanien, IRA Nordirland, RAF Deutschland, Rote Brigaden Italien, PKK Türkei, Kontras in verschiedenen Staaten Südamerikas, Taliban in Pakistan, etc.).

Mit Blick auf den noch bevorstehenden Wandel des Militärs (US-Regierung unter Obama) wurde der Begriff des „asymmetrischen Krieges“ eingeführt. Damit öffnet sich die Tür weiter zu einer verdeckten Kriegsführung mit gezielten Tötungen, Entführungen und Folter in Geheimgefängnissen. Die demokratische Kontrolle eines solchen geheimen Kriegs ist im Vergleich mit einem offenen Krieg kaum möglich. Gleichwohl erwecken die einschlägigen Risikoanalysen den Eindruck, als existiere ein global vernetzter Terrorismus mit einer gemeinsamen Agenda. Die Frage ist daher erlaubt, wie die Sicherheitskonzepte der Industrienationen – bei Abwesenheit eines staatlichen militärischen Bedrohungspotentials – aussähen, gäbe es keinen Terrorismus in der Welt.

„Sicherheit“ ist hierarchisch strukturiert und bildet mit der Sicherheit des Staates die oberste Ebene. Die jeweils angestrebte staatliche Sicherheit definiert sich über Interessen und einen staatlichen Handlungskontext. (siehe auch „Der Wandel des Sicherheitsbegriffs“).

In dieser und den folgenden Analysen wird das Ziel verfolgt, die Grundlagen dafür zu liefern, um eine Sicherheitsstrategie für die persönliche Ebene entwickeln zu können, die den oben beschriebenen staatlichen Kontext berücksichtigt und von der Nutzung moderner Kommunikationstechnik (Vernetzung) ausgeht. Dabei wird vermieden, den bereits besetzten Begriff der IT-Sicherheit zu nutzen, da dieser für das hier verfolgte Ziel nicht ausreichend ist. IT-Sicherheit beschreibt eher den spezifischen Unterbau in der hier angestrebten umfassenden Sicherheitsdefinition. Die neu zu entwickelnde Sicherheitsstrategie wird aber die IT-Sicherheit einschließen.

Generell ist die neue zu entwickelnde Sicherheitsstrategie zur Sicherung der persönlichen Kommunikation und der eigenen Daten in eine Struktur von Sicherheitskonzepten eingebettet, die auf der oberen Ebene durch die Interessen des Staates und die damit – teilweise – identischen Interessen seiner Bürger vorgegeben ist. Im Wesentlichen werden diese Interessen durch Gesetze, jedoch auch durch Zielvorgaben des Staates als Rahmen definiert. Somit steht eine Sicherheitsstrategie für die „*Sicherung der Persönlichkeitsrechte in modernen Kommunikationsmedien*“ (SPIK) immer im Kontext der Sicherheitsstrategie des Staates und ist somit direkt oder indirekt Bestandteil dieser Rahmenbedingungen. Wir gehen davon aus, dass nur mit Kenntnis dieser Rahmenbedingungen eine integrierte, langfristig wirksame Sicherheitsstrategie wie SPIK gefunden werden kann.

Diese und weitere Überlegungen werden bei der Analyse und der Diskussion um IT-Sicherheitskonzepte von uns berücksichtigt. Die Konkurrenzsituation zwischen Volkswirtschaften spielt dabei eine primäre Rolle, da mit den modernen Kommunikationsmedien globale Infrastrukturen für den Datentransfer genutzt werden.

Gefährdungspotentiale

Dem Schutz der Informationsströme, die zunehmend zum Ziel von Angriffen auch in Form organisierter Kriminalität werden, kommt eine steigende Bedeutung zu. Der Lagebericht 2007 des BSI kam zu dem Schluss, dass bis zum Jahr 2008 40 Prozent aller Organisationen Ziel finanziell motivierter krimineller Angriffe wurden. Aus Sicht einer Volkswirtschaft stellt sich jedoch die Frage, welche zusätzlichen Gefährdungspotentiale bestehen, die von wirtschaftlicher Konkurrenz motiviert sind. (siehe auch „Der Wandel des Sicherheitsbegriffs“). Andere Staaten haben Strategien entwickelt, um konkurrierende Volkswirtschaften zielgerichtet zu dominieren (siehe auch Konkurrenz der Volkswirtschaften), um so eine wirtschaftliche und politische Vormacht abzusichern oder zu erreichen. Aus Sicht einer Volkswirtschaft sind derartige Dominanzbestrebungen anderer Volkswirtschaften als eigenes Gefährdungspotential einzustufen. Der Einsatz illegaler Mittel muss im Konkurrenzkampf realistischerweise antizipiert und entsprechende Abwehrstrategien als legitimes Mittel des Schutzes angesehen werden (siehe Spiegel Online: „BND nutzt Bundestrojaner zur Spionage“).

Informationsströme entstehen durch Daten, die durch natürliche Personen abgegeben werden. In diesem Papier geht es ausschließlich um diese Daten. Sie bilden die Grundlage aller Datenströme, auch wenn sie in einer späteren Entwicklungsphase automatisch erzeugt werden sollten. Gehen wir also davon aus, dass die Informationsströme aus personenbezogenen Daten bestehen, die von Individuen selbst, direkt oder indirekt erzeugt und abgegeben werden. Diese natürlichen Personen sind also die Quellen der Daten, Informationen und – besonders wichtig – Innovationen, die über moderne Kommunikationsmedien ausgetauscht werden. Es liegt daher nahe, dass in einer umfassenden Betrachtung zur Sicherung von Persönlichkeitsrechten in modernen Kommunikationsmedien auch die Frage nach dem Schutz der „Informationsquellen“ betrachtet werden muss. Häufig wird bei der Definition von Sicherheitsstrategien nur ein Unternehmen oder eine Institution als Ganzes betrachtet. Wir werden sehen, dass diese Betrachtung genau zu den Sicherheitsmängeln führt, die heute bestehen.

Prävention

Das Sicherstellen der Kontinuität von Geschäftsprozessen (Business Continuity) für den Krisenfall und die Entwicklung präventiver Maßnahmen für den Normalfall zeigt sich deshalb als wesentliche Managementaufgabe – schließlich können durch Betriebsausfälle gewaltige Kosten entstehen. Der Verlust von Kundendaten oder internen Informationen über Geschäftsabläufe kann massive Wettbewerbsnachteile mit sich bringen. Eine 2006 weltweit durchgeführte Studie zeigt bei der Implementierung von Sicherheitsmaßnahmen allerdings große Branchenunterschiede. Während im Finanzdienstleistungssektor 88 Prozent der Unternehmen über unternehmensweite Business

Continuity-Programme und einen *Chief Information Security Officer* verfügten, lag die Vergleichszahl im Bereich der Technologie-, Medien- und Telekommunikationsunternehmen nur bei rund 50 Prozent.

IT-Sicherheit stellt bereits heute einen entscheidenden Faktor in der Wertschöpfungskette dar. Im Lagebericht 2007 des Bundesamtes für Sicherheit in der Informationstechnik wird ein massiver Handlungsbedarf zur Einführung von Sicherheitstechnologie für alle Gesellschaftsschichten diagnostiziert. In dem Bericht wird gefordert, dass die Sicherheitskompetenz aller Nutzer massiv verbessert werden muss. Dabei muss das zentrale Element immer die Eigenverantwortung des Bürgers, also der einzelnen Person, bleiben. In diesem Zusammenhang wird vor allem das geringe Problembewusstsein in deutschen Unternehmen massiv kritisiert.

Bei dieser Forderung fällt auf, dass in der Bundesrepublik ein Milliardenmarkt für Sicherheitssysteme existiert, in dem zahlreiche Lösungen für Privatpersonen, Unternehmen und Behörden angeboten werden. Auf der anderen Seite existiert ein erhebliches Defizit an Sicherheit auf diesem Feld. Offensichtlich besteht eine Diskrepanz zwischen den aktuell vorhandenen Sicherheitslösungen und den tatsächlichen Gefährdungspotentialen. Diesem Mangel wollen wir hier nachgehen.

Strukturierung

Aus ökonomischer Sicht kann weltweit eine oberste Strukturebene, die Volkswirtschaft, erkannt werden. Folgende Unterteilung dieser Struktur wird vorgeschlagen:

1. System von Volkswirtschaften als Staatenverbund wie die EU
2. einzelne Volkswirtschaft
3. volkswirtschaftliche Elemente (Behörden, Institute, Unternehmen, Vereine, etc.)
4. Einzelperson oder Individuum

Der Repräsentant der Ebene 1-3 ist immer das Individuum, ohne Ansehen seines gesellschaftlichen Ranges. So kann mit Hilfe moderner Datenverarbeitungsanlagen die Ebene zwei (einzelne Volkswirtschaft) in seine Basisbestandteile der Ebene vier (Einzelperson oder Individuum) aufgelöst werden. Bei Risiko- und Gefährdungsszenarien können somit immer Betrachtungen auf der Ebene vier (4) erfolgen, sofern eine Zuordnung der Individuen zu den entsprechenden anderen Ebenen möglich ist. Mit der jetzt vorangetriebenen EU-weiten Einführung des „ID-Managements“ wird es zukünftig möglich sein, diese eindeutige Zuordnung auf Grundlage gesetzlicher Vorgaben vornehmen zu können. Damit wird eine systemische/strategische Lücke geschlossen, weil Datenprofile eindeutig natürlichen Personen zugewiesen werden.

Hierdurch ist es möglich, Einfluss auf volkswirtschaftliche Elemente – eine Behörde oder ein Unternehmen – über seine seine Entscheidungsträger, also Individuen, zu nehmen. Somit entstehen vollkom-

men neue Szenarien im Konkurrenzkampf zwischen Volkswirtschaften und vollkommen neue Fragestellungen zur strategischen Ausrichtung von Armeen. Die Missbrauchsmöglichkeiten dieses Ansatzes werden offensichtlich, wenn man von den in den vorherigen Absätzen beschrieben Rahmenbedingungen in den Abschnitten *Gefährdungspotentiale* und *Prävention* ausgeht.

Umfeldanalyse

Die deutsche Volkswirtschaft ist ohne den effizienten Austausch von Daten und Informationen zwischen ihren Funktionselementen in Ebene drei (siehe *Strukturierung*) nicht denkbar. Unter Funktionselementen werden hier alle Einrichtungen des Staates, des Rechts, der Wirtschaft, Bildungseinrichtungen, Organisationen und Institute verstanden. Der Grad der Kommunikation zwischen allen Teilnehmern und die Geschwindigkeit, mit der Informationen in einer Volkswirtschaft ausgetauscht werden, kennzeichnet das Maß des Organisationsgrades einer Volkswirtschaft.

Je höher der Organisationsgrad einer Volkswirtschaft, umso erfolgreicher ist deren Handeln gegenüber anderen Volkswirtschaften. Mit anderen Worten: der Umgang mit der Ressource Information bestimmt den Wohlstand der Menschen in einer modernen Volkswirtschaft entscheidend mit. Dieser Hinweis soll die Bedeutung der Kommunikation über moderne Kommunikationsmedien für das erfolgreiche Funktionieren einer Volkswirtschaft verdeutlichen.

Ein Merkmal von Kommunikation ist, dass die damit ausgetauschten Informationen im Wert zunehmen, je freier sie sich ausbreiten können. Die Bestrebungen der EU, umfassende persönliche Datenprofile über jeden Bürger anzulegen, ist in dieser Hinsicht kontraproduktiv und Wert- „vermindernd“. Wird das Vorhaben verwirklicht, können Informationen nur noch unter Beobachtung des Staates ausgetauscht werden. Damit erhält der Staat frühzeitig Kenntnis von Innovationen, Lösungsansätzen für Problemstellungen, Produktentwicklungen, Patententwicklungen, Interessenbildungen von Menschen und Unternehmen, sowie Absichten/Zielen der Eliten des eigenen Landes bzw. innerhalb des EU-Binnenmarktes. Die Anonymität der Informationen/ Personen ist dann nicht mehr gegeben. Aus Sicht einer einzelnen Person ist ein Angreifer nicht mehr identifizierbar bzw. klassifizierbar. Der eigene Staat bzw. andere Staaten werden damit zum unidentifizierten unsichtbaren „Angreifer“ und die Einzelperson – auch und vor allem Entscheidungsträger – werden zum datentechnischen Spielball intransparenter Interessen. Kommunikation und ihre modernen technischen Systeme sind also janusköpfig: Einerseits unverzichtbar für eine entwickelte Volkswirtschaft, andererseits eine Achillesferse, weil sie Begehrlichkeiten von Anderen wecken.

Da sich die deutsche Volkswirtschaft in wesentlichen Teilen zu einer Exportwirtschaft entwickelt hat (der Export trägt fast 50 Prozent zum BIP bei), ist der Zugang zu anderen Märkten von erheblicher Bedeutung. Deswegen ist auch der Schutz ihrer Produktinnovationen von gleicher Bedeutung. Nur durch Innovation wird es auch zukünftig möglich sein, die von deutschen Unternehmen hergestellten Produkte

in Konkurrenz zu anderen Produkten auf dem Weltmarkt durchzusetzen. Diese Produktinnovationen entstehen jedoch nicht im „stillen Kämmerlein“, sondern in einem Prozess des Informations- und Ideenaustausches, in der Kenntnis der Bedarfswünsche und Nutzungsanforderungen anderer Märkte/Kunden. In diesem komplexen Austausch von Daten werden Innovationen geboren und zu neuen Produktinnovationen entwickelt. Sind die Kommunikationswege und ihre Informationsquellen ungeschützt, gehen Produktinnovation an andere Volkswirtschaften und konkurrierende Unternehmen verloren. Der Verlust an Daten und Informationen an andere Volkswirtschaften verringert aber den Innovationsvorsprung und damit die Wettbewerbsfähigkeit.

Mittelfristig soll in Deutschland individuelles und kollektives Wissen stärker zur Grundlage des gesellschaftlichen und ökonomischen Zusammenlebens werden („Wissensgesellschaft“). Damit gewinnt die Kommunikation mit Hilfe moderner Kommunikationssysteme eine herausragende Bedeutung. Zugleich wird das Schutzerfordernis für Kommunikationssysteme und ihre „Informationsquellen“ wesentlich stärker in das Bewusstsein der Öffentlichkeit allgemein, und der Entscheidungsträger im Besonderen, treten müssen. Dabei ist zu berücksichtigen, dass sich in diesem Prozess die Produktinnovationen von materiellen zu immateriellen Gütern wandeln werden. Die immateriellen Güter einer Wissensgesellschaft sind bei ungeschützten Datenquellen (Individuen, die Daten austauschen) und Kommunikationsmedien ein vielfach höheres Gefährdungspotential für die Stellung der deutschen Wirtschaft in der Welt.

Die deutsche Volkswirtschaft wird diese politisch gewollte Transformation in eine Wissensgesellschaft nur dann meistern können, wenn zuvor sichere Kommunikationssysteme für den Schutz der Wissensprodukte vorhanden sind. Dabei muss der Staat eine Sicherungs- bzw. Schutzfunktion übernehmen. Diese Sicherungsfunktion entspricht dem Schutz von Anlagen und Gütern durch das nationale Militär in einer klassischen Industriegesellschaft. Der Staat hat dabei jedoch darauf zu achten, dass er nicht selbst die Kommunikationssysteme zur Überwachung der Innovationsträger im eigenen Land missbraucht, indem er den Innovationsträgern die Daten und Innovationen wegen einer „Sicherheitsvorsorge“ entwendet und ihren notwendigen Schutz ihrer Anonymität aufgibt. Überspitzt in einem Gleichnis formuliert, würde der Verlust der persönlichen Anonymität und Vertraulichkeit in den Kommunikationsmedien vergleichbar mit dem Einsatz der Armee gegen das eigene Volk entsprechen, in der Absicht, dessen Güter für sich zu requirieren.

Schutz einer Volkswirtschaft

Moderne Volkswirtschaften veröffentlichen ihre wirtschaftlichen Kenndaten in regelmäßigen Abständen. Damit können andere Volkswirtschaften offiziell erkennen, wie groß und erfolgreich ihre Konkurrenten sind, wie viel Material und Güter ein- und ausgeführt worden sind, wie viel Energie eine Volkswirtschaft verbraucht hat und wie viel Kapital eingesetzt worden ist. Vor der Etablierung moderner Kommunikationsmittel konnten sich konkurrierende Volkswirtschaften nur mit einigem Aufwand ein zutreffendes Bild über die Konkurrenz verschaffen. Es war ihnen nicht oder nur eingeschränkt möglich, die offiziellen Daten zu verifizieren. Erst mit den Einsatzmöglichkeiten der modernen digitalen Kommunikationsmedien – und hier vor allem seit dem Siegeszug des Internets und leistungsfähiger Datenverarbeitung – wurde es für konkurrierende Volkswirtschaften möglich, die Frage zu beantworten: „*Wie funktioniert ein anderes Land und welche Ziele verfolgt es*“.

Vor der IT-Revolution veredelten klassische Volkswirtschaften Rohstoffe zu Produkten mit Hilfe der drei klassischen Ressourcen Mensch, Maschine, Material. Daten/Informationen wurden erst durch moderne Kommunikationsmittel und Kommunikationsmedien als Ressource erschlossen. Klassische Volkswirtschaften schützten ihre Güter und ihren Reichtum durch Armeen und Geheimdienste. Dabei wurden ihre internen Daten, Organisationsstrukturen, Ziele und Absichten, die als Informationen auch in klassischen Volkswirtschaften vorhanden waren, implizit mit geschützt.

Viele Staaten haben die Gefährdung ihrer Existenz durch den Verlust von Informationen in ihren Volkswirtschaften noch nicht vollständig erkannt und noch keine „Armee“ für deren Schutz aufgestellt. Die Rand Corp. (USA) prognostiziert, dass die zukünftigen Waffen die Daten sein werden. Nur wenige Staaten haben rechtzeitig nationale Strategien entwickelt, mit denen der Schutz ihrer Bevölkerung/Personen und Güter durch den Schutz ihrer Daten erfolgt. Viele Staaten beschränken ihren Schutz immer noch auf Güter, obwohl die Daten/ Informationen über ihre innovativen Eliten – und damit ihre relevanten Unternehmen – bereits von konkurrierenden Volkswirtschaften „angegriffen“ und in Besitz genommen werden. Zusätzlich ist der Trend zu erkennen, dass Staaten Daten über ihre eigene Bevölkerung auf der Ebene von Einzelpersonen, ihre Unternehmen und Institutionen, ihre Entscheidungsträger, ihre Verwaltungsstrukturen, ihre Ziele und Absichten erfassen und anderen Volkswirtschaften zur Verfügung stellen.

Eine solche Entwicklung versucht die EU-Richtlinie 46/1995 wie auch das Bundesdatenschutzgesetz, das diese Richtlinie in deutsches Recht umsetzt, einzuhegen. Gleichwohl greift der Schutz nur gegenüber Privatunternehmen. Staaten und auch die EU begrenzen durch Gesetze und Richtlinien (EU) den Schutz so, dass der staatlichen Aktivität kaum Grenzen gesetzt sind. Der Anspruch der Richtlinie bleibt meistens unerfüllt:

> “Die Mitgliedsstaaten räumen jeder Person das Recht ein, keiner für sie rechtliche Folgen nach sich ziehenden und keiner sie erheblich beeinträchtigenden

> Entscheidung unterworfen zu werden, die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht, beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens."

Der Politologe Ralf Bendrath kommentiert die Richtlinie mit einem leicht abgewandelten Zitat von Karl Popper:

> „Wie können wir unsere technischen Infrastrukturen so aufbauen, dass unfähige und unredliche Machthaber damit keinen großen Schaden anrichten können?"

Verlust der persönlichen Souveränität

Der einzelne Bürger verliert durch diese staatlich/privaten Datensammlungen sowohl im eigenen Land, wie auch in anderen Ländern an persönlicher Souveränität und individuellem Schutz. Dieser Verlust entsteht vor allem dadurch, dass mit dem Abbilden detaillierter Datenprofile in Form von Persönlichkeitsprofilen zu vorerst nicht konkret bestimmten Zwecken – der Zweck der Datensammlungen ist im einzelnen nicht transparent und divergiert von Datensammlung zu Datensammlung – die Unschuldsvermutung als höchstes Gut eines Rechtsstaates in eine latente Schuldvermutung de facto umgewandelt wird. Eine derartige staatliche Datensammlung ergäbe sonst keinen Sinn (siehe auch Einordnung nationaler Datenerhebungen). Tendenziell verliert damit die eigene Volkswirtschaft an Innovations- und Entwicklungspotentialen gegenüber anderen Volkswirtschaften.

> **Anmerkung:** Die Analyse anderer Länder erfolgt mit Hilfe der Daten über Personen anderer Staaten, die im Rahmen des „Krieges gegen den Terrorismus" erhoben wurden. Diese Strategie hat sich seit dem 11. September 2001 weltweit als eine neue Praxis zur Datenerhebung über einzelne Personen/Bürger entwickelt. Sie ist im Zuge von allgemeinen Gesetzesänderungen auch auf die Eliten einer Volkswirtschaft ausgedehnt worden. Diese Gesetzesänderungen zur allumfassenden Datenerhebung sind von der Bevölkerung stillschweigend akzeptiert worden, weil sie mit der allgegenwärtigen Terrorismusgefahr und damit notwendigen Vorsorgemaßnahmen legitimiert wurden. Gleichwohl leiden auch unschuldige Personen durch staatliche „Anti-Terrorlisten" unter Flugverbote, Entführungen, Ausschluss von jeglicher wirtschaftlicher Tätigkeit usw. Diese Listen unterliegen weder einer gerichtlichen noch einer demokratischen Kontrolle.

Einige Staaten haben noch nicht erkannt, welche Möglichkeiten sich ihnen bieten, mit Hilfe der Daten- und Informationsgewinnung über konkurrierende Volkswirtschaften sich Wettbewerbsvorteile zu verschaffen. Teilweise versorgen sie sogar Konkurrenten mit eigenen internen Daten. Eine Reihe anderer Staaten nutzt jedoch die modernen Medien zur umfassenden Informationsgewinnung über andere Volkswirtschaften auf allen Ebenen (z.B. USA, England, Israel, China, Indien, Russland). In diesem Beitrag soll auf Strategieansätze hingewiesen werden, die vor diesem Hintergrund Wettbewerbsvorteile für die eigene Volkswirtschaft, ihre Unternehmen und Bürger sichern und Wettbewerbsnachteile vermeiden können.

Angriff und Fremdbestimmung

Das Ungleichgewicht zwischen den Volkswirtschaften mit Blick auf die Einschätzung moderner Kommunikationsmedien und ihrer Nutzung für eigene strategische Zwecke birgt Gefahren für die betroffenen, die betroffenen Eliten und die Bevölkerung insgesamt. Vor allem Datenerhebungen und -Auswertungen über andere Volkswirtschaften und deren Eliten werden langfristig zu erheblichen Veränderungen in den Verhältnissen zwischen den Volkswirtschaften und ihren Unternehmen (siehe auch Abbildung 1 „Einflussgrößen auf die Entwicklung des Sicherheitsverständnisses“) sowie der Konkurrenzsituation bei Produkten und dem internationalen Warenverkehr führen. Dies muss durch die Entwicklung effizienter Schutzkonzepte auf Individual-, Unternehmens- und Staatenebene begleitet werden.

Mit dem Anwachsen von Zahl und Qualität detaillierter personenbezogener Daten im Cyberspace werden diese zum Ziel („Target“) anderer Interessen (siehe auch Abbildung 2 „Einflüsse auf die Entwicklung moderner Präventionsstrategien und Doktrin“). Das bedeutet, Datenerhebungen über die Eliten anderer Volkswirtschaften sind als potentieller Angriff auf diese Personen einzustufen. Dies gilt vor allem dann, wenn sie in ein strategisches Konzept einer anderen Volkswirtschaft eingebettet sind, mit dem nationale Ziele verfolgt werden, wie im Fall der US-Strategie der Full Spectrum Dominance oder der neuen chinesischen Verteidigungsdoktrin.

Bei knapper werdenden Rohstoffen und anderen künftig schwierigeren Rahmenbedingungen werden Staaten die verschärfte Konkurrenzsituation nur dann bewältigen können, wenn ihre Innovationskraft ausreicht, um sich an die neuen Verhältnisse anpassen zu können. Die Innovationskraft einer Volkswirtschaft ist abhängig von der Qualität ihrer Eliten in Forschung, Technik und Management. Diese Eliten werden durch einzelne Personen repräsentiert. Sie sind somit der Schlüssel für alle zukünftigen Anpassungsprozesse an sich ändernde Rahmenbedingungen. Dies gilt sowohl hinsichtlich der dynamischen Wirtschaftsentwicklung in Asien als auch mit Blick auf die dem deutschen/kontinentaleuropäischen Wirtschaftsmodell diametral entgegengesetzten angelsächsischen Vorstellungen von „Partnerschaft“. Weitere Einflussfaktoren für das Überleben von Staaten werden in diesem Rahmen nicht thematisiert.

Der Entscheidungsträger im Fadenkreuz

Die Innovationskraft einer Volkswirtschaft und ihre Problemlösungskompetenz angesichts sich ändernder Rahmenbedingungen werden zukünftig für ihr Überleben entscheidend sein, sowie in der Folge den inneren Frieden und den Zusammenhalt der Gesellschaft beeinflussen. Innovationskraft und Lösungskompetenz einer Volkswirtschaft basieren im Wesentlichen – vor allem im Vorfeld von entsprechenden Produktentwicklungen – auf *Informationsaustausch* und den innovativen Fähigkeiten einzelner Handelnder (Die „*Abbildung der „handelnden“ Person erfolgt über Persönlichkeitsprofile, die aus den persönlichen Daten gewonnen werden“*). Für eine konkurrierende

Volkswirtschaft ist somit von hohem Interesse, diese Personen, ihre Abhängigkeiten, ihre Möglichkeiten, ihre Absichten und Vernetzung, ihre Ziele, Fähigkeiten und Motivationen genauer zu kennen, um ggf. Einfluss auf sie nehmen zu können. Eine innovative Person/Gruppe, die sich als Datenprofil abbilden lässt, wird somit über das bereits bestehende Maß hinaus künftig selbst zu einer lukrativen Ressource werden. Das gilt wegen ihrer Stärke in besonderem Maße für die deutsche Volkswirtschaft. Mit dem „Verlust“ (in Gestalt der in Datenprofilen abgebildeten natürlichen Personen = NID) dieser Gruppe gingen auch deren Innovationen zum Schaden der eigenen Wirtschaft verloren. Der „Verlust“ der Datenprofile wird zum „Gewinn“ einer konkurrierenden Volkswirtschaft. Realisiert werden kann er – der Einfluss – durch unterschiedliche Maßnahmen, zum Beispiel durch Verführung, Fehlinformation, Erpressung, uvm.

Zukunftsfelder und Rahmenbedingungen

Das mögliche „Abwerben“ von innovativen Personen aus anderen Volkswirtschaften muss als Teil künftiger Überlebensstrategien und als Angriffspotential der Konkurrenz verstanden werden. Innovationen mit hohem Wettbewerbspotential, wie z.B. Technologien zur effizienten Speicherung und Nutzung von Energie, wecken besondere Begehrlichkeiten.

Kreativität, Innovationskraft, Umsetzungsgeschwindigkeit in Produkte und Lösungskompetenz sind die Eckpfeiler, auf denen der Erfolg im wirtschaftlichen Überlebenskampf ruht. Knapper werdende fossile Energiereserven („Peak Oil“) und andere Rohstoffe, zunehmende Umweltdegration, Klimaveränderungen und knapper werdende Nahrungsmittelreserven (Ausbeutung der Weltmeere; Erosion landwirtschaftlicher Flächen, etc.) bilden den Handlungsrahmen für Anpassungsprozess von Volkswirtschaften. Dieser Anpassungsprozess kann vor allem in den Industriestaaten nur über Innovationen und technologische Kompetenz ihrer Eliten bewältigt werden.

Die Auflösung der Volkswirtschaft auf Individualebene

Wesentliche Teile eines Wirtschaftsraums sind staatliche Akteure (Ministerien, Parlament, Behörden, Streitkräfte, Polizei, Justizwesen etc.), Universitäten und Institute, Unternehmen, Finanzinstitutionen, Presse/Medienunternehmen, Gesundheits- und Sozialdienste.

Sie alle werden durch Individuen repräsentiert und sind generell hierarchisch aufgebaut. Im Wesentlichen bestimmt die Führungsebene, wie eine Einrichtung arbeitet und wie Entscheidungen getroffen werden. Diese Führungsebenen werden als die Eliten einer Volkswirtschaft, eines Staates, angesehen. Erstmalig in der Geschichte der Menschheit ist es mit den modernen digitalen Medien möglich geworden, die Daten/Informationen über Einzelpersonen ganzer Völker im Detail zu ermitteln, zu erfassen, auszuwerten und mit anderen Datenprofilen in Verbindung zu setzen. Hier sind die Führungseliten von be-

sonderem Interesse. Die einfachste Form der Auswertung besteht in sogenannten persönlichen Profilen, in denen spezifische Informationen über eine einzelne Person erfasst sind. Diese Profile existieren heute in modernen Volkswirtschaften nahezu über jeden Menschen. Sie werden von Unternehmen und staatlichen Einrichtungen zusammengestellt und genutzt. Allgemein bekannt ist die Nutzung dieser Profile für den Einsatz persönlicher Werbeangebote oder zur Bewertung der Kaufkraft von Personen, Personengruppen, Stadtteilen, Städten und Landstrichen (scoring).

Die Entwicklung moderner leistungsfähiger Datenverarbeitungstechnologie in Verbindung mit leistungsfähigen Kommunikationsmedien ermöglichte es, die Kommunikation zwischen einzelnen Menschen zu erfassen und im Detail auszuwerten. Durch das organische Wachstum des Internets als Schlüsseltechnologie im Bereich der Kommunikationsmedien werden diese Datenströme über die Landesgrenzen einer Volkswirtschaft hinweg weltweit unkontrolliert transportiert. Selbst staatlichen Einrichtungen ist nicht nachvollziehbar, wer welche Daten von wem und zu welchem Zeitpunkt erfasst. Die Möglichkeit, Daten über Individuen einer Volkswirtschaft via Internet in und durch Länder zu transportieren, wird zunehmend von großen Unternehmen und staatlichen Einrichtungen zur Verfolgung eigener Ziele genutzt.

Das Revolutionäre an dieser Situation ist, dass auf diese Weise Wirtschaftsspionage auf einem bislang nicht gekannten qualitativen und quantitativen Niveau stattfindet. Die Auflösung von Strukturen einer Volkswirtschaft über individuelle Daten und Datenprofile ihrer Repräsentanten, Entscheidungs- und Innovationsträger ist erstmalig in der Geschichte der Menschheit möglich und bietet damit vollkommen neue Möglichkeiten der Einflussnahme auf andere Volkswirtschaften. Die Realität der internationalen Struktur des Internets ermöglicht einen fast ungefilterten Datenstrom zwischen allen Volkswirtschaften. Daraus ziehen Legitimierte, nicht Legitimierte und Kriminelle ihren Nutzen.

Das Abkommen der EU mit den USA zum Austausch personengebundener Fluggastdaten zeugt folglich von einer gefährlichen Naivität auf der EU-Seite, vor der sogar geltendes EU-Recht nicht schützen konnte. Unter Bezugnahme auf die präventive Terrorismusbekämpfung werden mit diesem Abkommen individuelle Daten an die Behörden der USA übermittelt, ohne dass die betroffenen Personen jemals die Verwertung ihrer Daten nachvollziehen oder kontrollieren können. Die Verwendung und der Verbleib der Daten bleiben ebenfalls völlig intransparent. Aus diesen Daten von EU-Bürgern lassen sich Bewegungsprofile erstellen, Beziehungen zwischen Personen erkennen, persönliche Vorlieben und Absichten europäischer Repräsentanten wichtiger Unternehmen und aus anderen Bereichen extrahieren, wie von Journalisten, Ingenieuren und Wissenschaftlern. All diese Daten werden den US-Behörden freiwillig ohne erkennbare Notwendigkeit übermittelt. Dies eröffnet alle Spielarten von Manipulationen einzelner Personen Tür und Tor. Die Staaten der EU haben damit ihre Schutzpflicht gegenüber ihren Bürgern ernsthaft vernachlässigt und zum Zeitpunkt der Vertragsunterzeichnung geltendes EU-Recht gebeugt. Für die USA ist das Abkommen hingegen ein Baustein in der Umsetzung ihrer Strategie der Full Spectrum Dominance.

Um die Strukturen einer Volkswirtschaft auf der Ebene der persönlichen Datenprofile ihrer Bürger aufzulösen, werden insbesondere einfach zugängliche Daten ihrer Eliten benötigt. Da immer mehr Einzelpersonen bzw. wichtige Einrichtungen einer Volkswirtschaft über das Internet kommunizieren und auf diese Weise persönliche Daten produzieren, rückt dieses Medium in den Mittelpunkt des Interesses. In diesem Zusammenhang spielen die Angebote in dem Medium eine herausragende Rolle. Sie basieren vor allem auf Angebots- und Imageverlockungen („kostenlose Nutzung"; „neue Funktionen"; „dazugehören und modern sein wollen": Community-Gefühl, etc.). Nach der Integration von E-Mail in Beobachtungsszenarien wie z.B. Google Mail, also der Auswertung privater Daten einzelner Personen, werden jetzt unter dem Begriff des WEB 2.0 auch die persönlichen Beziehungen und Neigungen einzelner Personen miteinander verbunden. Der Titel des Vortrags von Prof. Marc Drüner beim Kongress „Web 2.0" Ende März 2009 in München spricht für sich: „Web 2.0 – immer mobiler, immer offener, immer persönlicher".

Trends und Gefährdungspotentiale

Analog zum Trend, militärische Aufgaben zu privatisieren, führt der veränderte Sicherheitsbegriffs auch zur Privatisierung geheimdienstlicher Funktionen des Staates. Hier geht es im wesentlichen um die Daten- und Informationsbeschaffung aus Internet, Mobilfunknetzen, Navigationssystemen, Satellitentelefonie, Internettelefonie, Fax und Telefonie (Verbindungsdaten; Voice Finding; etc.). Da viele Unternehmen das Internet für die Kommunikation nutzen, hat die Beschaffung von Informationen mit Hilfe des Internets an Bedeutung gewonnen. Nach der „Information Warfare"-Doktrin (offensiv: *Information Operations*, defensiv: *Information Assurance*) soll der Angegriffene „*dem Willen des Angreifers folgen, ohne mit Gewalt gezwungen zu werden"* (George J. Stein). Viele neuen Dienste im Internet bzw. Entwicklungen im Advertising-Market werden vor allem mit dieser Zielsetzung angeboten.

Ein wesentliches Mittel der Anwerbung, ein bestimmtes Angebot aus dem Internet zu benutzen, ist die „Verführung" (z.B. durch Aufmachung der Internetseite oder Zusatznutzen wie Online-Spiele u.a. bei Smartphones) durch scheinbar kostenlose Nutzung neuer Dienste (siehe u.a. Google Apps), ein Zusammengehörigkeitsgefühl/ Zugehörigkeit (Community) zu erzeugen (z.B. Facebook oder andere Social Networks) oder sogenannte „neue Funktionen" für die „Erleichterung der Arbeit" (kostenloses Cloud Computing, kostenlose E-Mail-Accounts, u.v.m.) anzubieten. Treten diese drei Grundelemente zusammen auf, können sich viele Menschen und vor allem auch Entscheidungsträger diesen Angeboten nicht entziehen. Sie werden sie nutzen, obwohl sie damit ihre und ihrer Mitarbeiter persönlichen Daten kostenlos und freiwillig anderen unbekannten Verwertern zur Verfügung stellen. Das damit ein Verlust an Autonomie der Person einhergeht, dringt bislang offensichtlich nicht ausreichend ins Bewusstsein. Interessant ist in diesem Zusammenhang, dass Systembetreuer für DV-Systeme, Entscheidungsträger und Sicherheitsberater diesen „Verlockungen" ebenfalls unterliegen, sich den Sicherheitsfragen

nicht stellen und den Verlust an Autonomie nicht erkennen oder herunterspielen. Da viele Angebote auch im Bereich professioneller Nutzergruppen platziert werden, sind die Angebote also genau auf die Zielgruppe der Entscheidungsträger ausgerichtet.

Ein besonders gefährliches Beispiel für die Abschöpfung persönlicher Daten ist das Angebot von bestimmten Diensten des Internets, in denen der Nutzer zur öffentlichen Erfassung seiner persönlichen DNA verpflichtet wird (Hinweis: Auf die Mechanismen, die durch die Abhängigkeiten vom Internet entstehen und die dazu indirekt Menschen zwingen, bestimmte persönliche Daten bekannt zu geben, kann hier nicht eingegangen werden, jedoch soll darauf hingewiesen werden. Zu diesem Themenfeld gibt es zahlreiche Studien). Äußerst kritisch und bemerkenswert ist die Einführung einer eindeutigen persönlichen und lebenslang gültigen Steuernummer (oder einer zukünftigen persönlichen ID im Internet) zu bewerten, die jedem Bundesbürger bis zum 31.12.2008 zugeteilt wurde. Mit der eingeführten Steuernummer wird jedermann lebenslang von Gesetzes wegen unkalkulierbaren persönlichen Risiken ausgesetzt, die derzeit noch nicht übersehen werden können. Diese elektronische Steuernummer wird zukünftig als einfaches und eindeutiges Identifikationsmerkmal u.a. für persönliche Datenprofile eingesetzt werden. Sie wird mit Hilfe der Datenprofile zu einer realen „DNA-ähnlichen Sequenz von Zahlen“ einer einzelnen Person in zahlreichen Rechenzentren privater und staatlicher Einrichtungen, die wie die biologische DNA persönliche Eigenschaften, Überzeugungen und andere individuelle Merkmale enthält.

Der Trend geht dahin, dass zukünftig für Dienste im Internet eine eindeutige ID (ähnlich einer Personalausweisnummer) verlangt wird. Zur Zeit können ID’s verwendet werden, die keinen Bezug zu einer realen Person aufweisen (Pseudonym). Für die Zukunft ist denkbar, dass Dienste nur dann genutzt werden können, wenn man seine persönliche ID angibt. Wären transparente, vertrauenswürdige und rechtlich abgesicherte Nutzungsverfahren etabliert, wäre ein „Internetpass“ keine persönliche Bedrohung. Jedoch fehlen dem Einzelnen jegliche Kontrollmöglichkeiten. Damit verliert er die Hoheit über seine persönlichen Daten und verliert sie willkürlich an Staaten, Unternehmen oder kriminelle Organisationen.

Mit Hilfe moderner Werbung – als Beispiel soll hier nur auf die kostenlosen Angebote von Produkten und Diensten im Internet hingewiesen werden – werden vor allem Jugendliche dazu animiert, ihre persönlichen Neigungen und Beziehungen offen zu legen. Dabei ist diese Zielgruppe aus Sicht von konkurrierenden Volkswirtschaften von wesentlicher Bedeutung, da sie in der Regel die Zukunft einer Volkswirtschaft repräsentiert. Mit Hilfe des Internets und seinen Lockangeboten wird die „Naivität im Umgang mit den eigenen Daten“ vollständig ausgenutzt.

> **Hinweis**: Der Benutzer von Internetangeboten verwendet in der Regel Pseudonyme um sich zu schützen. Da ein hohes persönliches Gefährdungspotential in der Benutzung des Internets liegt, ist diese Maßnahme berechtigt. Das Internet ist und gilt de facto immer noch als rechtsfreier Raum. Eine Wahrung der persönlichen Rechte wie auch eine Verfolgung von Straftaten gestaltet sich in der Praxis bereits für Behörden schwierig, vor allem dann, wenn die Firmen im Ausland sitzen. Einzelpersonen stehen der Vielzahl an Rechtsräumen chancenlos ge-

genüber. Durch eine zwangsweise Abschaffung der individuellen Möglichkeit zur Verwendung von Pseudonymen steigt das persönliche Risiko erfolgreich angegriffen zu werden erheblich. Diese Risiken tragen Einzelpersonen; die Auswirkungen tragen Unternehmen.

Das Internet wird weltweit von allen Teilen der Gesellschaft als gewinnbringendes Kommunikations- und Informationsmedium angesehen. Dabei werden vor allem die Chancen hervorgehoben, die durch dieses Medium geboten werden. Diesem Trend können sich auch Entscheidungsträger nur schwer entziehen. So werden heute fast alle Prozesse eines Betriebes oder einer staatlichen Einrichtung über dieses Medium abgewickelt. Dabei werden vor allem die Argumente Kosteneinsparung, Effizienzgewinn etc. angeführt. Häufig werden dabei jedoch die Risikokosten falsch einkalkuliert oder einfach übersehen.

Vielen Entscheidungsträgern sind die bisher geschilderten Zusammenhänge nicht bekannt. In Unkenntnis der Gefährdungspotentiale werden Produkte/Dienstleistungsangebote eingeführt, die zu einer weiteren Gefährdung auf der Ebene des Individuums führen. Zusätzlich entstehen neue Produkte über das Medium Internet, die hohe Interaktionen mit einzelnen Personen als Geschäftsmodell enthalten. Abläufe und persönliche Interaktionen mit anderen Personen in Form von Produkten über das Internet zu organisieren soll im Folgenden als „Trend“ vieler Entscheidungsträger bezeichnet werden.

Als ein wesentliches Beispiel für staatliche Fehleinschätzung von Gefährdungspotentialen und ein geringes Sicherheitsverständnisses soll an dieser Stelle auf den Trend zu eGoverment hingewiesen werden. Mit eGovernment wird von Behörden das Ziel verfolgt, viele Verwaltungsfunktionen eines Staates mit Hilfe des Internets abzuwickeln. Um zu verhindern, dass mit der Einführung der elektronischen Kommunikation zwischen Bürger und den Behörden Daten Dritten einer Volkswirtschaft offen gelegt werden, sind Sicherheitsmaßnahmen wie Verschlüsselungen notwendig. Diese Maßnahmen sind jedoch bisher nicht oder nur sehr selten vorhanden. (Beispiel: teilweise unverschlüsselte Übertragung der Steuerdaten via ELSTER). Mit Hilfe moderner Datenverarbeitungsanlagen ist die Erfassung, Auswertung und Einflussnahme der sich daraus ergebenen Datenprofile nur eine Frage „ob es gemacht werden soll“ und nicht „ob es möglich ist“. eGoverment ist in der heutigen Konzeption ein Sicherheitsrisiko für jeden einzelnen Bürger und strategisch ein Sicherheitsrisiko für die deutsche Volkswirtschaft. Für die Einführung von eGoverment-Produkten, die modernen Qualitäts- und Sicherheitsansprüchen genügen, sind noch keine entsprechenden Voraussetzungen geschaffen worden. Hier besteht noch erheblicher Nachholbedarf in Bezug auf strategische Konzepte und technische Sicherheitssysteme zum Schutz der Bürger und ihrer Daten.

Volkswirtschaften, die diesen „Trends“ im Internet nicht folgen oder in denen sich bei der Umsetzung/Einführung Verzögerungen ergeben, haben einen strategischen Vorteil (Eine Analogie aus dem militärischen Bereich: Der elektromagnetische Puls, EMP, ist als Waffe gegen technologisch einfache Waffensysteme unwirksam). Das gleiche gilt für Volkswirtschaften, die bereits über eine Strategie und entsprechende Schutzprodukte zur Sicherung der persönlichen Daten von In-

dividuen verfügen. Diesen verdeckten Vorteilen stehen jedoch die öffentlichen Trends entgegen, so dass bei den meisten Entscheidungsträgern das Bewusstsein einer Gefährdung der eigenen Person, anderer Entscheidungsträger bzw. längerfristig ihrer eigenen Volkswirtschaft durch die Einführung entsprechender Internetangeboten nicht erkannt wird und die Zusammenhänge bisher nicht transparent sind. Aus einem anderen Blickwinkel wird so die Aussage im Lagebericht 2007 des BSI nochmals verdeutlicht und unterstrichen, dass im Umgang mit den persönlichen Daten trotz einer florierenden Sicherheitswirtschaft ein erhebliches Sicherheitsdefizit existiert.

Hieraus folgt, dass die Eliten in Regierung, Verwaltung und Unternehmen ein Bewusstsein für die modernen Gefährdungspotentiale und strategischen Zusammenhänge mit Blick auf die Absichten anderer Volkswirtschaften und Unternehmen entwickeln müssen! Dies ist zugleich die Voraussetzung dafür, dass sich eine entsprechende Sensibilität im Umgang mit den persönlichen Daten auch auf alle anderen Ebenen der Gesellschaft durchsetzt. Bei einigen Organisationen und kleineren innovativen Unternehmen ist das Schutzerfordernis für die persönlichen Daten im Internet und die Sicherung der Persönlichkeitsrechte bereits erkannt worden. Lediglich die Kenntnis der Zusammenhänge, ihre Auswirkungen und eine entsprechende Präventionsstrategie fehlen.

Informationsgewinnung

Wie oben beschrieben, ist infolge moderner Datenverarbeitungstechnologien und der Internettechnologie als integrierendes weltweites Informationsmedium die Grundlage geschaffen worden, ganze Volkswirtschaften auf der Individualebene ihrer Eliten umfassend als Datenprofile abzubilden. Dabei stellt sich die Frage, wie und welche Mechanismen angewendet werden, um individualisierte Informationen zu erfassen und abzubilden. Mit Hilfe der umfassenden Kenntnis über diese Mechanismen können wirksame Abwehrmaßnahmen und Sicherheitskonzepte erarbeitet und eingesetzt werden.

Das Interesse an persönlichen Datenprofilen besteht weltweit. In der folgenden Abbildung wird versucht, eine erste grobe Kategorisierung von möglichen nationalen und internationalen Interessenten vorzunehmen. Angriff auf eine Person über moderne Kommunikationsmedien durch

- Staaten/Volkswirtschaften
- Unternehmen
- Kriminelle Organisationen
- Kriminelle Personen

Abbildung 4: Interessenten an persönlichen Datenprofilen

Informationen über andere Stämme/Völker waren auch vor der Staatenbildung für die Absicherung der Existenz der eigenen „Gruppe" nötig. Staaten entwickelten zur Informationsgewinnung die staatliche Funktion der Spionage. Sie galt als eine zentrale, in der Regel geheime Einrichtung eines Staates für defensive und offensive Zwecke gegenüber anderen Staaten. Die Abläufe in den Geheimdiensten, zum Teil auch deren Existenz an sich bzw. die Existenz bestimmter Abteilungen waren noch in der jüngsten Vergangenheit geheim. Mit dem Einzug der modernen Kommunikations- und Datenverarbeitungssysteme werden zunehmend Teile von klassischen Geheimdiensttätigkeiten industrialisiert bzw. als Geschäftsmodell in Unternehmen „ausgelagert". Damit folgen die Geheimdienste einem Trend zur Privatisierung von hoheitlichen Aufgaben aus dem militärischen Bereich (siehe den Einsatz von privaten „Sicherheitsunternehmen" im Irak, in Afganistan, Bolivien (Südamerika), etc.) und der Geheimdienste. Ausschlaggebend dafür waren die dadurch mögliche Verschleierung von Kosten und von Verlusten vor den Parlamenten, die geringeren rechtlichen Beschränkungen im Vergleich zu regulären Truppen und die Vermeidung diplomatischer Verwicklungen. Vorreiter dieses „Privatisierungstrends" waren die USA, andere Nationen sind gefolgt. Die freiwillige Preisgabe persönlicher Daten über Tätigkeiten, Beziehungen, Verhalten, Neigungen u.v.m. Einzelner Personen erleichtert Geheimdiensten die Arbeit erheblich und reduziert die Beschaffungskosten. Der Anspruch, den Prof. George Stein formulierte „*dem Willen des Angreifers folgen, ohne mit Gewalt gezwungen zu werden*", konnte und wird weitestgehend in den Gesellschaften u.a. mit Hilfe des Internets implementiert! Der Privatisierungstrend in den Geheimdiensten weitet den Kreis der „Auswerter" und Datensammler nun auch auf Unternehmen aus, deren Auftraggeber für die Öffentlichkeit bzw. einer Privatperson verborgen bleibt.

Ein Teil geheimdienstlicher Aufgaben besteht in der Gewinnung von Informationen aus dem Ausland, wie auch aus dem Inland. Die Erfas-

sung persönlicher Daten durch Beobachtung ist mit der Einführung des Internets für private Unternehmen zum Geschäftsmodell entwickelt worden und wird u.a. als Advertising oder Profiling bezeichnet. Dabei ist von außen nicht zu unterscheiden, ob das Unternehmen diese persönlichen Datenprofile an andere Geheimdienste verkauft oder in einem staatlichen Auftrag handelt. Unternehmen handeln gewinnorientiert. Insofern wäre der Verkauf der durch Beobachtung ermittelten Datenprofile an den Meistbietenden aus Sicht des Unternehmens legitim. Ob ein solcher Verkauf legal ist, hängt von der jeweils gültigen Rechtsordnung ab.

Problematisch ist in diesem Zusammenhang, dass Unternehmen unter dem Vorwand der statistischen Erfassung von Konsumentenverhalten private Datensammlungen aufbauen, die sich jeglicher Kontrolle entziehen. Es ist somit denkbar, dass große Unternehmen, die sich der systematischen Erfassung von personenbezogenen Daten aus unterschiedlichen Volkswirtschaften widmen, mit den Geheimdiensten ihres Staates oder eines anderen Staates zusammenarbeiten. Im Rahmen eines Unternehmens, das z.B. in Deutschland viele Datenströme beobachtet und personenbezogene Datenprofile erfasst, könnte ein ausländischer Geheimdienst legal, über einen entsprechenden Kaufvertrag oder eine Auftragsvergabe, detaillierte Personendaten aus allen Bevölkerungsschichten auf Datenträgern oder Online per Internet erhalten und diese nach seinen eigenen strategischen Zielvorstellungen auswerten und nutzen. Interessant für Geheimdienste sind in diesem Zusammenhang auch Staatsverträge wie das oben erwähnte Abkommen zur Übermittlung von Fluggastdaten zwischen der EU und den USA.

Mit der Privatisierung vormals geheimdienstlicher Tätigkeiten, wie Internetbeobachtung oder Datensammlung im Rahmen von Advertising oder Profiling, die zu Geschäftsmodellen werden, hat dieses Vorgehen gesellschaftliche Akzeptanz erfahren, obwohl seine Risiken für die eigene Volkswirtschaft insgesamt und für den Einzelnen im besonderen nicht überschaubar sind. Hiermit soll kein Unternehmen der Spionage verdächtigt werden, sondern lediglich auf die Möglichkeit hingewiesen werden, umfassende Daten von Personen legal aus Volkswirtschaften zu erwerben und daraus strategische Konzepte jeder Art zu entwickeln, die gegen den „Lieferanten“ der Daten gerichtet sind. Diese Möglichkeit der Beobachtung und Datensammlung ist zusätzlich, also als weitere „sichere Informationsquelle“, zu den anderen geheimdienstlichen Tätigkeiten eines Staates zu verstehen. Nur wer sich dieser strategischen Möglichkeiten der Datensammlung mit Hilfe von Unternehmen/Internetunternehmen bewusst ist, kann entsprechende Gegenstrategien und Sicherheitskonzepte entwickeln.

Für die Auflösung volkswirtschaftlicher Funktionen auf die Individualebene der Eliten mit Hilfe persönlicher detaillierter Datenprofile steht anderen Volkswirtschaften bereits heute eine Fülle von weiteren Informationen zur Verfügung: Fluggastdaten, internetbasierte Buchungssysteme von Reise- oder Transportunternehmen, persönliche E-Mails, Daten von Advertising- oder Profiling- Unternehmen, persönliche Beziehungen durch Social Networks (oder anderen auf WEB 2.0 basierenden Internetangeboten), Wirtschaftsdaten und Verwaltungsdaten durch eGovernment-Produkte, zukünftige elektronische Ge-

sundheitsdienste und andere Angebote internetbasierter Produkte. Mit Hilfe dieser Datenquellen lässt sich das Profil einer Person sehr präzise nachbilden (persönliche Stärken, Schwächen, Neigungen, Schwachstellen, Empfindlichkeiten, Wünsche, persönliche Fitness, Krankheiten, Empfindlichkeiten, etc.). Eine konkurrierende Volkswirtschaft vermag so das Verhalten einzelner Personen aus einer Führungselite sehr genau zu beobachten, die sie beeinflussen oder manipulieren will.

Bereits heute ist vielen Unternehmen bzw. Entscheidungsträger nicht bekannt, das Technologien seit einigen Jahren eingesetzt werden, die eine Online bzw. Echtzeitanalyse von Datenpaketen und ihrem Inhalt ermöglichen, die über das Internet verschickt werden. Diese Technologie wird auch als DPI oder *Deep Packet Inspection* bezeichnet. Diese Technologie wird zur Klassifizierung und subsequenten Filterung bzw. Umleitung einzelner Pakete oder bestimmter Datenströme eingesetzt. DPI repräsentiert in der Tat eine neue Qualität in der Analyse von Datenströmen. Wie bereits darauf hingewiesen wurde, ist heute eine indirekte Netzbeobachtung mit der Identifizierung der Verbindungsdaten eines Sender zu seinem Empfänger (welche Person ruft wann welche Daten ab oder kommuniziert mit einer anderen Person) „State of the Art“. Mit DPI wird nun zusäztlich zu den Verbindungsdaten auch der Datenteil (Inhalt einer Nachricht) erfasst und ausgewertet. Damit ist für einen Beobachter das Wer, Wann, mit Wem und Was kommuniziert wird, zugänglich – auf der Ebene einer einzelnen Person und häufig weltweit zugänglich! Telekommunikationsunternehmen wie Cisco stellen mittlerweile dedizierte Geräte (sog. Appliances) her, die diese Aufgabe vollautomatisch erledigen. Deren Einführung ist zum Zeitpunkt der Erstellung dieses Bulletin noch nicht flächendeckend erfolgt. Jedoch wurde im Deutschen Innenministerium darüber nachgedacht, ob nicht über den Hebel der Gesetzesinitiative zur „Sperrung von Seiten mit kinderpornographischem Inhalt“ diese Technologie generell in Deutschland bei den Providern eingesetzt werden sollte. Die Unkenntnis vieler Entscheidungsträger, Politiker und Richter über dieser Möglichkeit der indirekten Datenauswertung im Internet durch unsichtbare „Beobachter“, führt in vielen Unternehmen, Verbänden und staatlichen Einrichtungen zu eklatanten Fehlentscheidungen in Bezug auf Datensicherheit und Schutz von Individualdaten. Weiterhin sind bei den Führungseliten ebenfalls Projekte und ihre Hintergründe nicht bekannt, wie z.B. das von der Regierung Obama am 30. Januar 2009 gestartete und, nach Angaben des *Biometrics Task Force* des US-Verteidigungsministeriums,

> "Next Generation Automated Biometric Identification System" (ABIS) (NGA) in Betrieb genommen und damit das bisherige "Automated Biometric Information System" (ABIS) abgelöst wurde. Das militärische ABIS NGA für alle US-Streitkräfte und das zivile "Next Generation Identification System" (NGI) für alle Polizei- und Geheimdienstbehörden sind die beiden Multimilliarden-Dollar "Manhattan Projekte" auf dem Gebiet der Biometrie. Dahinter steht jedoch die Erfassung, Speicherung, der Austausch und die Nutzung *aller* biometrischen Merkmale, deren man habhaft werden kann. Denn beide Systeme sollen aufgrund der gleichen Datenbanken, Protokolle und Formate vollständig komplementär zueinander funktionieren. Langfristig sollen die beiden Systeme mit weiteren Datenbanken in einer gigantischen Plattform fu-

sionieren, an die dann in einem weiteren Schritt Biometrie-Datenbanken von Staaten oder Gemeinschaften wie der EU angebunden werden, um so zu einem verteilten, den Globus umspannenden Biometrie Datenbank-Verbund zu mutieren, der sich dann zum Beispiel für Identifizierungs- und Authentifizierungszwecke über biometrische Erkennungssysteme in Videoüberwachungskameras, mit mobilen Überprüfungsgeräten, in Kontrollstellen an Grenzübergängen, Sicherheitsschleusen in Gebäuden und dem Abgleich biometrischer Merkmale, die in elektronischen ID-Dokumenten gespeichert sind, von jedem angeschlossenen Staat und Streitkräften nach der Okkupation eines Landes nutzen ließe. Bedingung und Unterstützung der ehrgeizigen Langzeit-Pläne stellt die Angleichung und Harmonisierung der eingesetzten Datenbankstrukturen, Datenformate und Protokolle in allen Staaten und Staatengemeinschaften dar, die sich eines Tages in der Form zusammenschließen wollen. Ein Prozess, der zum Beispiel in der Europäischen Union mit dem Vertrag von Prüm und bilateralen Austausch-Abkommen eingesetzt hat.

Vor dem Hintergrund der bisherigen Analyse stellen beide Technologien, DPI und NGI, in der nächsten Dekade dieses Jahrhunderts (2010-2020) zusammen einen erheblichen Angriff auf die persönlichen Daten einer Person und ihrer Selbstbestimmung dar. Für eine Volkswirtschaft, ihren Unternehmen und sonstigen Einrichtungen stellen diese Entwicklungen eine ernstzunehmende Herausforderungen für ihre Sicherheitssysteme dar, die bisher noch nicht im öffentlichen oder politischen Fokus angekommen ist, obwohl die Technologien bereits vorhanden sind, eingesetzt werden oder mit massivem Mitteleinsatz weiterentwickelt werden. Zusammenfassend stehen also indirekte Mittel auf der Ebene von Staaten bzw. großen Technologieunternehmen und Internetunternehmen zur Verfügung, jedes andere Unternehmen, Interessenvertretung oder Einrichtungen des anderen Staates, dass über öffentliche Kommunikationsinfrastrukturen kommuniziert, auf Personenebene zu analysieren oder anzugreifen (siehe Ghost-Net, China), ohne dass ihre konventionellen Sicherheitseinrichtungen diese Angriffe erkennen können.

Die Kinder der Eliten sind die Entscheidungsträger der Zukunft, von ihnen hängt die künftige Innovationskraft der Wirtschaft ab. Sie sind mithin ein als „vorrangiges Objekt für die Erstellung von Datenprofilen“ einzustufen. Die ersten öffentlichen Überlegungen zur Erfassung von persönlichen Datenprofilen (siehe „Der Wandel des Sicherheitsbegriffs“) und zu den damit verbundenen Strategien wurden in den 1990er Jahren durchgeführt. Persönliche Datenabbilder und Datenerfassungen sind seit Beginn des neuen Jahrtausends bekannt. Damit könnten die ältesten Profile einer Person bereits heute über 10 Jahre Lebenszeit als Datenabbild umfassen. Auf dieser Datenbasis lassen sich genaue psychologische Profile erstellen und auf wichtige Personen anwenden.

Personenbezogene Daten wurden von jeher durch die unterschiedlichsten Organisationen und Unternehmen gesammelt. Meistens konzentriert man sich auf spezifische Aspekte aus dem Informationsspektrum einer einzelnen Person. Reisebüros planen die Reise, Ärzte dokumentieren und rechnen Krankheiten ab und Buchhändler registrieren die Lesevorlieben ihrer Kunden. Jede Datensammlung für sich genommen sagt wenig über die Person als Ganzes aus. Da diese Datensammlungen ohne ihre Verknüpfungen mit anderen Daten die

Anonymität der Person im Kern nicht einschränkten, wurden sie auch gesellschaftlich akzeptiert. Als diese Daten noch auf Papier vorlagen, wäre die Auswertung und Verknüpfung zu einem integrierten, individuellen Gesamtprofil nur mit einem immensen Aufwand möglich gewesen. Daraus erwuchs dem Einzelnen ein passiver Schutz seiner Person.

> **Hinweis**: Umfassende Datenerhebungen auf personenbezogener Ebene wurden jedoch in der ehemaligen DDR mit der Absicht durchgeführt, den Staat vor „subversiven" Einflüssen zu schützen. Das entsprach einer Präventionsstrategie, mit der rechtzeitig entsprechende Personen ausfindig gemacht werden sollten. Für die heutigen Datensammlungen gilt im Wesentlichen:
>
> - In der Beschaffung privatisiert
> - Dezentralisiert gespeichert
> - Besitzen eine hohe Aussagequalität über ein Individuum
> - Sind elektronisch und in einem digitalen Format schnell über Kommunikationsmedien verfügbar
> - Können selektiv und bis auf Individualebene genutzt werden
> - Zugriffsgeschwindigkeit ist extrem hoch, so dass ganze Bevölkerungen durchsucht werden können (z.B. Rasterfahndung)

Mit der Entwicklung digitaler Kommunikationsmedien als integrale Kommunikationsplattformen und entsprechender Datenverarbeitungskapazitäten entstand jedoch die Möglichkeit, unterschiedliche Datenquellen und Datenbestände personenbezogener/persönlicher Daten ohne großen Aufwand zusammenzuführen. Elektronische Daten lassen sich heute aus verschiedenen digitalen Datenquellen mit Hilfe der modernen Kommunikationsmedien beziehen, schnell zusammenführen und auswerten. Dabei kommt es gar nicht einmal auf die Richtigkeit einzelner Daten an. Durch den ständigen Abgleich von Daten über längere Zeiträume entstehen in den elektronischen Persönlichkeitsprofilen Ähnlichkeiten, die über statistische Verfahren zu aussagekräftigen Bildern einer einzelnen Person zusammengestellt werden können. Zusätzlich können unterschiedliche Auswertungs- und Simulationsverfahren auf die Datenprofile angewendet werden, ohne dass die Ergebnisse und deren Verwendung kontrolliert werden können.

Zu der Gefahr des anonymen Verlustes persönlicher Daten tritt hinzu, dass der „Auswerter" (Profiler) bzw. „Kunde"/Nutzer eher geneigt ist, diese unscharfen Daten für wahr zu halten, unbeschadet ihres objektiven Wahrheitsgehaltes. Entsprechende Mechanismen und Auswirkungen können beim Scoring beobachtet werden. Z.B. bewertet die Schufa – und ähnliche Unternehmen, die Scoringverfahren einsetzen – die Kreditwürdigkeit einer Person mit Scoringverfahren, deren Datenbasis, Verfahren (mathematische Formel) oder Interpretation durch die bewerteten Personen nicht beeinflusst werden können, auch wenn objektiv Fehler in den Simulationsergebnissen vorhanden sind. Damit wird die einzelne Person in ein gesellschaftliches „Ranking" eingeordnet, auf die sie keinen Einfluss hat, unabhängig von ihrer realen Position, ihrer realen Leistung und ihrer Verdienste. Das kann dazu führen, dass z.B. eine Person nach einem Umzug keinen Bankkredit mehr erhält oder bestehende Kredite sofort fällig gestellt

werden (Beispiel 2007 Berlin: Umzug eines Arztes mit seiner Praxis von einem „guten“ Bezirk in einen „schlechten“ Bezirk). Damit ist konkret der Verlust der persönlichen Selbstbestimmung realisiert und ein Äquivalent militärischer Macht gegenüber einer einzelnen Person in einer Volkswirtschaft implementiert. Ein persönlicher Scoringwert wird auch von verschiedenen Versicherungen zur Einstufung von Personen in die Beitragsbemessung verwendet. Die einzelne Person hat weder Einblick in die Verwendung von Scoringwerten noch die Möglichkeit einer Korrektur falscher Scoringwerte. Sie ist der Anwendung und den Ergebnissen dieses „Datenabbilds“ schutzlos ausgeliefert.

Die Basis für Scoringverfahren sind immer Daten aus digitalen Kommunikationsmedien und private digitale Datensammlungen von Unternehmen. Die Gefahr liegt also in der heimlichen und intransparenten Datenerfassung persönlicher Daten durch private Unternehmen oder staatlichen Einrichtungen, deren Auswertung zu Profilen, den daraus abgeleiteten Interpretationen und den auf Basis der Interpretation eingeleiteten Maßnahmen von Dritten wie z.B. Banken, Versicherungen, Ärzten, Krankenkassen, Arbeitgebern, etc., ohne dass der Betroffene über diese Daten oder deren Interpretation jemals informiert wird oder korrigierend auf falsche Daten oder deren Interpretation Einfluss nehmen könnte. Hieran wird deutlich, wie bereits heute einzelne Menschen mit ihren persönlichen Datenprofilen konfrontiert und manipuliert werden. Auf der Ebene von Staaten werden diese Datensammlungen über Eliten anderer Staaten aufgebaut, um jeweils die eigenen Interessen durchzusetzen.

Spekulatives Szenario zur Dominanz einer Volkswirtschaft

Selbstverständlich bedienen sich auch andere Unternehmen und staatliche Einrichtungen der oben beschriebenen Verfahren. Ohne Zweifel können Verfahren des „Data mining“ auch auf Personen anderer Volkswirtschaften angewendet werden. Damit wird die Grundlage für eine „neue“ Angriffsstrategie einer Volkswirtschaft gegen andere gelegt, wie es u.a. von Prof. George Stein und Alvin und Heidi Toffler postuliert wurde. Hinsichtlich der Volkswirtschaft als Ganzes unterscheiden sich nur die Interpretationen der Datenprofile unter anderen Zielsetzungen von den Praktiken in Unternehmen. An dieser Stelle soll lediglich darauf hingewiesen werden, dass die Technologien, Verfahren und Strategien bereits vorhanden sind und in großem Umfang angewendet werden. Es ist also nicht die Frage, ob moderne Kommunikationssysteme, Datenbeobachtungen und Datensammlungen auf der Ebene persönlicher Daten, mathematische Verfahren und Auswertungen persönlicher Daten für Profiling, Scoring und Data Mining eingesetzt werden, sondern nur noch die Frage, welche Ziele mit diesen Datenprofilen verfolgt werden, also in welchen strategischen Kontext sie eingebunden sind.

Unter dem strategischen Aspekt konkurrierender Volkswirtschaften ergeben sich also vollkommen neue Ansätze mit Hilfe weltumspannender moderner Kommunikationsnetze und der Privatisierung militärischer und geheimdienstlicher Tätigkeiten/Funktionen, um das Ziel einer „*Full Spectrum Dominance*“ zu erreichen. Dabei steht die einzelne Person einer anderen Volkswirtschaft als Angriffsziel zur Durchsetzung dieses Ziels im Zentrum. Aus der Sicht eines Angreifers sind die Chancen für die Durchführung einer erfolgreichen „Operation“ besonders hoch, weil mit Mitteln von geheimdienstlichen Tätigkeiten und detaillierten Informationen die Einflussnahme auf einen einzelnen Entscheidungsträger erfolgversprechend erscheint.

Mit der Strategie der „Full Spectrum Dominance“ werden keine klassischen Eroberungen von Territorien verfolgt, sondern der Machteinfluss in den entsprechenden Volkswirtschaften, der Zugang zu Ressourcen und die Absicherung der Marktzugänge für eigene Produkte durchgesetzt (als Beispiel siehe Staatsvertrag zwischen der EU und der USA zum europäischen Satellitennavigationssystem Galileo).

> **Hinweis**: In diesem Zusammenhang ist eine Bemerkung erforderlich. Es geht hier nicht um eine Anklage gegen die USA, nicht um Antiamerikanismus. Die Full Spectrum Dominance-Strategie entspringt nicht der Phantasie der politischen Gegner der Vereinigten Staaten. Sie ist vielmehr die selbsterklärte Planungsgrundlage der strategischen US-Vordenker in offiziellen und parteiungebundenen Instituten. Darauf müssen sich alle anderen Staaten und ihre Führungskräfte einstellen. Ebenfalls bilden diese strategischen Konzepte Vorgaben für andere Staaten, entsprechende Strategien oder Gegenstrategien zu entwickeln, wie sie von z.B. China, Russland, Indien und anderen Staaten massiv entwickelt werden.

Die umfangreichen Erkenntnisse über einzelne Personen der Entscheidungselite einer Volkswirtschaft könnten künftig den klassischen Krieg, der aus wirtschaftlichen Konkurrenzgründen geführt wird, als relativ unattraktiv erscheinen lassen. Wir stellen die These zur Dis-

kussion, dass es für eine konkurrierende Volkswirtschaft künftig sinnvoller ist, eine andere Volkswirtschaft möglichst ohne den „Wertverlust“ zu „übernehmen“, der in einem Krieg üblicherweise mit der Zerstörung großer Teile der gegnerischen Infrastruktur und den eigenen Verlusten einhergeht. Die vollständige Dominanz der Eliten des konkurrierenden Staates kann wesentlich effizienter sein, als die klassische territoriale Besetzung mit anschließendem Wiederaufbau. Das gilt vor allem mit Blick auf Industrie- und Schwellenländer.

Kriege zur Kontrolle der Energie- und Rohstoffversorgung bleiben hingegen weiterhin eine Option, die jedoch militärische Überlegenheit voraussetzt. Zu erwarten ist, dass in den entwickelten Industriestaaten Szenarien für beide Optionen entwickelt werden: die Okkupation mit militärischen Mitteln sowie die virtuelle Okkupation mit Hilfe der Dominanz über die Eliten einer anderen Volkswirtschaft.

Aus der Sicht von transnational tätigen Unternehmen und Organisationen, die u.a. über Schlüsseltechnologien verfügen, sollte die eigene Position in der jeweiligen Volkswirtschaft unter dem Blickwinkel analysiert werden, als potentielles Angriffsziel identifiziert zu werden. Diese Analyse ist dann zur Grundlage einer umfassenden Sicherheitsstrategie zum Schutz der persönlichen Daten der eigenen Entscheidungsträger zu machen. Dabei sollten die Unternehmen auch die Einbindung in die unterschiedlichen Rechtsräume beachten und ggf. die Unterstützung ihrer Interessen hinsichtlich moderner Sicherheitsanforderungen durch gesetzliche Maßnahmen bei ihren Regierungen einfordern. Analog gilt dies auch für alle anderen Einrichtungen in einer Volkswirtschaft.

Da der Angriff auf das Individuum durch eine oder gar mehrere Organisationen erfolgt, befindet sich das Ziel, der einzelne Mensch, in einer strategisch nachteiligen Position, denn seine Verteidigungsfähigkeit sind finanziell, gesetzlich und organisatorisch enge Grenzen gesetzt. Deshalb müssen Analyse und Sicherheitsstrategie berücksichtigen, dass durch die informationstechnische Auflösung der Institutionen und Einrichtungen einer Volkswirtschaft in datenbasierte Individualrepräsentanten (NID) eine gezielte und wirkungsvolle Einflussnahme bereits jetzt möglich ist.

Mögliche Angriffsszenarien können erfolgen durch

- Änderung persönlicher Daten,
- Beeinflussung von Scoringwerten, die für die Bewilligung von Krediten, Versicherungen etc. genutzt werden,
- Nutzung von Internetangeboten und Diensten unter einer anderen Identität mit dem Ziel der Verbreitung falscher Informationen, wirtschaftlichem Schaden, Arbeitsplatzverlust oder Diskriminierung, über Foren oder Social Networks, etc.
- Elektronisches Hijacking von persönlichen Identitäten mit Zugriff auf Personaldaten, persönliche Konten, Foren mit persönlicher Meinung und Preisgabe intimer Daten, etc.,
- öffentliche Diskriminierung im Internet und Verbreitung von falschen Informationen mit Hilfe der Presse oder typischen Pressequellen durch deren Fehlinformation,

- Social Mobbing, Kampagnen,
- persönliche öffentliche Auszeichnungen (z.B. Verleihung von hochrangigen Auszeichnungen ohne erkennbare Leistung jedoch bezogen auf die gesellschaftliche oder betriebliche Stellung um damit öffentlichen moralischen Druck für den Abschluss von Verträgen zu erzeugen) mit öffentlichen Druck durch ausländische Presse zur Annahme der Auszeichnung,
- Vortäuschung von Systemfehlern in komplexen technischen Systemen, durch Änderung von Prozessdaten (Ablaufdaten) in Unternehmen (z.B. Manipulation von Navigationsdaten zum Verlust oder der Fehlleitung von Gütern),
    - Z.B. „zeitlich begrenzte fehlerhafte oder ungenaue“ Positionsdaten für Transporte über Lkw's und Schiffen mit dem Ziel zeitlicher Verzögerungen oder der Verhinderung von Effizienzpotentialen in bestimmten Warenströmen (bringt Kostennachteile gegenüber Konkurrenten),
    - vermeintliche Datenfehler in Netzen, die zu Ausfällen von Systemen führen (siehe Artikel aus der Telepolis, 25.8.2008: Redundanz im Cyberkrieg),
    - Spam-Daten zur Blockierung von Informationskanälen oder deren Bandbreitenverlust; etc.
- Änderungen von persönlichen Daten zur Verhinderung oder schlechteren Klassifizierung bei z.B. Krankenversicherungen,
- Verhinderung des Zugangs zu Krediten, Verträgen, Versicherungen, Bonitäten, etc.
- verdeckte Fälschung von Daten z.B. zur Ausgrenzung von Personen,
- Schädigung der gesellschaftlichen Stellung z.B. mittels Scoring und der Veröffentlichung der dadurch fehlenden Kreditwürdigkeit
- Schädigung von Unternehmen durch den Angriff von Führungseliten (bevorzugt mittleres Management) bzw. deren Familien oder Angehöriger, im besonderen bei Staatsaufträgen in anderen Volkswirtschaften zur öffentlichen Verunglimpfung von Konkurrenten z.B. mit Hilfe von Korruptionsvorwürfen, die mit Hilfe von Internetdaten/Profilen belegt werden können, etc.

und vieles andere mehr.

Abschließend wird nochmals darauf hingewiesen, dass alle Überlegungen in diesem Dokument für die Individualebene gelten. Da jedoch die Führungseliten wichtiger Einrichtungen und Schlüsselunternehmen eines Staates im Fokus virtueller Angriffe im Rahmen eines „*Information Warfare*“ stehen, wirken sie sich auf die Volkswirtschaft als Ganzes aus und führen im Erfolgsfall zu negativen Rückkopplungseffekten wie z.B. der Abgabe von Marktanteilen.

Einordnung nationaler Datenerhebungen und Aufgabe des Prinzips der Unschuldsvermutung

Die Beschlüsse der Innenministerien auf Landes- und Bundesebene haben vor allem einen Rechtsrahmen zur Datenermittlung über die eigenen Bürger geschaffen. Folgende Systeme sind dafür als wesentlich anzusehen:

- Telefonüberwachung: Verbindungsdaten, Gesprächsinhalte über Schlüsselwortinterpreter.
- Mautsystem: Erfassung von LKW und PKW zur Speicherung von Gebühren, Ortsdaten und Erstellung von Bewegungsprofilen.
- Biometrische Datenerfassungen in den Meldeämtern: Erfassung biometrischer Kenndaten wie Fingerabdrücke und Gesichtsgeometrien und Zuordnung zu einem Persönlichkeitsprofil.
- Vergabe einer lebenslang eindeutigen, aussagekräftigen individuellen Steuernummer (entspricht zusammen mit den persönlichen Datenprofilen einer virtuellen DNA). Sie identifiziert ein Individuum sein Leben lang eindeutig und eröffnet die Möglichkeit, datentechnisch eindeutige persönliche Charakteristika zuzuordnen. Durch diese Nummer ist die Verbindung von unterschiedlichen Datenprofilen in unterschiedlichen Systemen möglich! Ein Schutz dieser Nummer kann weder durch die Person noch durch eine Behörde gewährleistet werden.
- Die elektronische Gesundheitskarte (eGK) speichert u.a. Krankengeschichten auf freiwilliger Basis in zentralen Rechenzentren. Die Speicherung erfolgt verschlüsselt in Datenzentren. Laut Spezifikation hat nur der Patient die Möglichkeit, die Daten zu entschlüsseln. Da die Schlüssel – nicht mit der PIN zu verwechseln – staatlich erstellt werden (oder die Erstellung zertifiziert wird), ist ein lebenslanges Vertrauen in den Staat notwendig. Zwar ist laut dem Betreiber *gematik* eine Erzeugung und Speicherung von Schlüsselduplikaten, mit deren Hilfe Dritte die Krankengeschichten lesen könnten, nicht vorgesehen. Eine Praxis, die sich aber jederzeit ändern lässt. – Die Infrastruktur der eGK (Elektronischen Gesundheitskarte) bietet weitreichende Möglichkeiten, ein zentrales Krankenregister virtuel oder real, verdeckt oder öffentlich für die deutsche Bevölkerung zu errichten.
- Zentrale Polizeidateien: In den zentralen Polizeidateien werden alle Verdächtigen, Kriminellen und Zeugen mit ihrer DNA gespeichert.
- Clearingstellen: Europol stellt eine europaweite Clearingstelle für Polizeidaten zur Verfügung. Diese Stelle soll Redundanzen in den Datenbeständen nationaler Datenbanken vermeiden. Um eine Clearingstelle einrichten zu können, werden „virtuelle“ Datenbanken (Register) aufgebaut. Virtuelle Datenbanken basieren auf dem teilweise zeitlich begrenzten Zusammenschluss realer Datenbanken zu einer Superdatenbank, z.B. Clearingstelle.
- eGovernment-Daten für Steuerdaten, KFZ, etc.

- Vorratsdatenspeicherung bei Telefongesellschaften und Internetprovidern: Die Verbindungsdaten aller Telefonate und Internetzugriffe werden bei den Telekommunikationsunternehmen für 6 Monate gespeichert und stehen staatlichen Stellen zur Aufklärung von schweren Straftaten zur Verfügung.

Ministerien und andere staatliche Einrichtungen erfassen über diese Systeme erhebliche Datenmengen über Bürger ihres eigenen Landes. Unter der Regierung Obama wurde am 30. Jan. 2009 das System "Next Generation Automated Biometric Identification System" (ABIS) (NGA) in Betrieb genommen (Information der Biometrics Task Force des US-Verteidigungsministeriums). Im Grunde sind ABIS NGA und NGI nur zwei Seiten eines Systems zur Erfassung, Speicherung, dem Austausch und der Nutzung *aller* biometrischen Merkmale, deren man habhaft werden kann, denn beide System sollen aufgrund der gleichen Datenbanken, Protokolle und Formate vollständig komplementär zueinander funktionieren. Langfristig sollen die beiden Systeme mit weiteren Datenbanken in einer gigantischen Plattform fusionieren, an die dann in einem weiteren Schritt Biometriedatenbanken von Staaten oder Gemeinschaften wie der EU angebunden werden, um so zu einem verteilten, den Globus umspannenden Biometrie Datenbankverbund mutieren, der sich dann zum Beispiel für Identifizierungs- und Authentifizierungszwecke über biometrische Erkennungssysteme in Videoüberwachungskameras, mit mobilen Überprüfungsgeräten, in Kontrollstellen an Grenzübergängen, Sicherheitsschleusen in Gebäuden und dem Abgleich biometrischer Merkmale, die in elektronischen ID-Dokumenten gespeichert sind, von jedem angeschlossenen Staat und Streitkräften nutzen ließe. Bedingung und Unterstützung der ehrgeizigen Langzeitpläne stellt die Angleichung und Harmonisierung der eingesetzten Datenbankstrukturen, Datenformate und Protokolle in allen Staaten und Staatengemeinschaften dar, die sich eines Tages in der beschriebenen Form zusammenschließen wollen. Ein Prozess, der zum Beispiel in der Europäischen Union mit dem Vertrag von Prüm und dem bilateralen Austauschabkommen eingesetzt hat (Realisierung der Doktrin *Full Spectrum Dominance*).

Durch die informationstechnische Auflösung eines Staatengebildes oder einer Volkswirtschaft in seine Atome, den Individuen, ist die Einordnung der oben aufgelisteten Systeme und weiterer Systeme in eine neue nationale Datensicherheitsstrategie notwendig. Dabei ist die Frage zu stellen, ob und wie diese Daten vor dem Zugriff anderer Staaten/Volkswirtschaften gesichert werden können und weiter, ob es Überlegungen gibt, wie ein Angriff auf ein Individuum durch andere Staaten/Volkswirtschaften mit Hilfe dieser Daten erkannt, bekämpft und geahndet werden kann. In diesem Kontext stellt sich auch die wesentliche Frage, ob der Staat dieses Gefährdungspotential bereits erkannt hat und welche Hilfsmittel ein betroffenes Individuum zur Abwehr eines Angriffs nutzen kann. Für konkurrierende Volkswirtschaften sind die zentralen Datensammlungen von erheblichem Interesse. Auch Personen, die in Einrichtungen arbeiten, in denen diese Daten erhoben und verwaltet werden, sind hinsichtlich ihrer persönlichen Datenprofile ein lohnendes Angriffsziel. Dasselbe gilt für das persönliche Umfeld der Führungskräfte wie Familie, Freunde und andere soziale Verbindungen.

Bisher scheint der Staat das Gefährdungspotential nicht erkannt zu haben. Dies ist jedenfalls aus der Absicht des Bundesinnenministers Wolfgang Schäuble zu schließen, die Speicherung weiterer persönlicher Daten der eigenen Bevölkerung zu forcieren, um so „gefährliche" Personen (was und wer gefährlich ist, bleibt diffus im Rahmen einer diffusen Präventionsstrategie; siehe auch Der Wandel des Sicherheitsbegriffs) gezielt aufspüren zu können (siehe heise-Newsticker: EU-Innenpolitiker wollen sämtliche digitalen Nutzerspuren überwachen).

Damit wird eines der Grundprinzipien eines rechtsstaatlichen Strafverfahrens, die Unschuldsvermutung, in Frage gestellt und schrittweise durch den grundsätzlichen Generalverdacht gegenüber jedermann ersetzt! In Deutschland erfolgte dies vor allem durch die aktuellen Gesetzesänderungen (Analysezeitraum von 2007 bis 2008) im Bereich des Datenschutzes, der inneren Sicherheit und der Polizeigesetze. Wenn sich aber der Rechtsstaat schleichend zum Präventionsstaat (siehe auch Hinweis zur Bekämpfung „subversiver" Einflüsse in der Deutschen Geschichte) entwickelt, ergibt sich als logische Folge die Rechtfertigung für eine umfassende Datensammelverpflichtung des Staates.

Das aktuelle Vorgehen des Bundesinnenministeriums steht beispielhaft für die Abkehr vom klassischen Schutz (Abwehr) vor definierten Bedrohungen hin zur „Vorsorge vor Risiken" (Prävention), also zu Maßnahmen, die im Vorfeld einer Straftat oder eines Terroraktes angesiedelt sind (Siehe auch „Der Wandel des Sicherheitsbegriffs"). In der Logik des Bundesministers des Inneren heißt Prävention jedoch, dass jeder Bürger verdächtig ist. Dabei stellt sich der Staat auf die „Generalebene des Unschuldigen" während der Bürger auf die „Generalebene eines Schuldigen" gestellt wird. Der Einzelne verliert durch dieses Vorgehen generell an staatlichem Schutz und persönlicher Souveränität und wird damit vermeidbaren Gefahren ausgesetzt. Konkurrierende Staaten können sich derselben Argumentation bedienen und den durch die Aufgabe der Unschuldsvermutung eintretenden Verlust an individuellem staatlichen Schutz nutzen, um unter dem Vorwand der Prävention das ausgespähte Individuum für eigene Zwecke in Anspruch zu nehmen (angreifen). Einem Angreifer werden auf diese Weise sogar die Rechtfertigungsargumente frei Haus geliefert, er kann für sich in Anspruch nehmen, rechtlich und moralisch richtig zu handeln und einen „Verdächtigen anschuldigen, entführen, foltern, verhören oder töten".

Auch dies muss bei der Entwicklung persönlicher Sicherheitsstrategien als Gefahrenquelle für das Individuum und dem Schutz seiner persönlichen Daten berücksichtigt werden, vor allem vor dem Hintergrund des Entstehungsprozesses von zwei Diktaturen in Deutschland im 20igsten Jahrhundert (Drittes Reich, Deutsche Demokratische Republik) und ihren Überwachungsapparaten. Wegen des vom Bundesinnenminister und seinem Vorgänger eingeschlagenen Tempos befinden sich die Eliten in Deutschland in einer besonders gefährlichen „Datenlage".

Perspektiven

In der Folge der hier präsentierten Analyse besteht eine wesentliche Gefahr in der Entwicklung nationalstaatlicher Strategien, dem methodischen Nationalismus, im Bereich IT-Sicherheit. Eine diesem Trend entgegen wirkende Entwicklung liegt in den Staatenbünden wie z.B. EU oder Mercosur (Lateinamerika). Eine hoffnungsvolle Entwicklung besteht in diesen Staatenbünden, die durch eine übergeordnete Organisation (z.B. EU-Parlament, EU-Kommission) innere Standards setzen können. Mit diesen Standards könnten auch Sicherheitsfragen im IT-Bereich so gefasst werden, dass eine einzelne Person Eigentümer seiner Daten bleibt und nicht zum Spielball unterschiedlicher intransparenter Interessen wird bzw. diesen Gefahren ausgesetzt wird.

Es ist jedoch in den nächsten 10 Jahren davon auszugehen, dass das Gefährdungspotential durch die wesentlichen Kräfte, wie der Privatisierung von militärischen und geheimdienstlichen Funktionen, weiter zunehmen wird. Die datentechnische Sicherheit der eigenen Person muss deshalb ein privates erstrangiges Anliegen sein, dass vor allem durch die Unternehmen, Organisationen und Behörden, in denen die Entscheidungsträger wirken, massiv im Unternehmensinteresse unterstützt wird. Unternehmen sollten dazu eine besondere IT-Sicherheitsstrategie für ihre Entscheidungsträger entwickeln, die diese modernen Risiken berücksichtigen. Dazu ist das Wissen um die Gefährdungen und die Schutzmöglichkeiten, vor allem von Entscheidungsträgern und ihren Kindern, von existentieller Bedeutung.