Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
18(24)89

Fraunhofer SIT

Effektivierung der Kontrolle des Exports von Überwachungs- und Spionagesoftware auf deutscher und europäischer Ebene und öffentliche Auftragsvergabe

Stellungnahme für das öffentliche Fachgespräch des Ausschusses »Digitale Agenda« am 16. Dezember 2015

16. Dezember 2015

Prof. Dr. Michael Waidner
michael.waidner@sit.fraunhofer.de

Institutsleiter des
Fraunhofer-Instituts für Sichere Informationstechnologie (SIT), Darmstadt
www.sit.fraunhofer.de

Professor für Sicherheit in der Informationstechnologie,
Fachbereich Informatik, Technische Universität Darmstadt
www.sit.tu-darmstadt.de

Sprecher der gemeinsamen Forschungszentren CRISP und CASED
von Technischer Universität Darmstadt, Hochschule Darmstadt,
Fraunhofer IGD und Fraunhofer SIT
www.crisp-da.de / *www.cased.de*

Inhalt

Vorwort

Dieser Bericht nimmt Stellung zu den Fragen des Ausschusses »Digitale Agenda« anlässlich eines öffentlichen Fachgesprächs zum Thema »Effektivierung der Kontrolle des Exports von Überwachungs- und Spionagesoftware auf deutscher und europäischer Ebene und öffentliche Auftragsvergabe«.

Kapitel 1 formuliert Leitgedanken zur Exportkontrolle. Die Kapitel 2 bis 10 beziehen sich auf die vom Ausschuss vorgegebenen Fragen, wobei diese jedoch teilweise zu übergeordneten Fragen zusammengefasst wurden.

Dieser Bericht entstand in enger Zusammenarbeit mit Dr. Markus Schneider und Dr. Michael Kreutzer, beide Mitarbeiter des Fraunhofer SIT. Für ihre großzügige Unterstützung und Mitarbeit möchte ich mich sehr herzlich bedanken. Ebenfalls herzlich bedanken möchte ich mich bei Dr. Birgit Baum-Waidner und Dr. Haya Shulman, ebenfalls Fraunhofer SIT.

1 Leitgedanken

Exportkontrolle betrifft heute neben klassischen Gütern wie Kriegswaffen auch die Überwachung geeigneter Güter der Informations- und Kommunikationstechnologie, kurz: IKT-Güter.

Auch die Bewertungskriterien möglicher Bestimmungsländer für Exporte sind in der jüngeren Vergangenheit intensiv diskutiert worden. Ursprüngliche Kriterien waren etwa Sicherheit und Stabilität in einer Region oder die Gefahr der Weitergabe an Dritte, insbesondere an Terrorgruppen. Vielfach vorgeschlagen wurde, diese Kriterien um die Einhaltung von Menschenrechten und die Freiheit von Bürgern in den Bestimmungsländern zu erweitern. Die Bundesregierung hat erklärt, dass sie dem Menschenrechtskriterium eine besondere Bedeutung einräumt und dass dieses bei künftigen Exportentscheidungen Berücksichtigung finden soll.[1,2,3] Vor diesem Hintergrund soll insbesondere auch die Ausfuhr von IKT-Gütern, z.B. Überwachungssoftware, berücksichtigt werden. In autoritären

1 Siehe hierzu *http://www.auswaertiges-amt.de/DE/Aussenpolitik/Aussenwirtschaft/Exportkontrolle/Exportkontrollpolnational_node.html*

2 Georg Mascolo, Frederik Obermaier: Gabriel plant Exportstopp von Späh-Software. Süddeutsche, 20.5.2014, *http://www.sueddeutsche.de/digital/internetueberwachung-gabriel-plant-exportstopp-von-spaeh-software-1.1969189*

3 Axel Kannenberg: Gabriel will Export von Spähsoftware beschränken. Heise Online, 19.5.2014, *http://www.heise.de/newsticker/meldung/Gabriel-will-Export-von-Spaehsoftware-beschraenken-2193268.html*

Staaten wird die Bevölkerung schon lange nicht mehr nur mit Waffen in ihren Rechten eingeschränkt, sondern auch durch den Einsatz von Überwachungstechnologie. Die Bundesregierung hat erklärt, dass der Export von Überwachungstechnologie in solche Länder gestoppt werden soll.

In Deutschland ansässige Unternehmen haben oftmals IKT-Güter wie Trojaner oder Software zur Internet- und Telekommunikationsüberwachung exportiert. Exportziele waren auch Länder, in denen die Menschenrechte missachtet werden.[4,5] Kritik hieran wurde z.B. von der OECD und »Reporter ohne Grenzen« erhoben.[6,7] Deutschland gehört zu den Marktführern auf dem weltweiten Markt für Überwachungstechnologie.

Deshalb ist es wichtig, dass der Export von Überwachungstechnologie kontrolliert und die Ausfuhr in solche Länder verboten wird, in denen unsere Grundwerte nicht ausreichend berücksichtigt werden.

Hierfür werden die folgenden Leitgedanken vorgeschlagen.

1. Technologien gegen Menschenrechte müssen kontrolliert werden

Überwachungstechnologie kann der legitimen Strafverfolgung, aber auch der unrechtmäßigen Verletzung von Persönlichkeits- und Freiheitsrechten dienen. Die Werte des Grundgesetzes müssen auch außerhalb Deutschlands geschützt werden. Der Export von IKT-Gütern, deren *vorrangiges* Ziel gegen die Persönlichkeits- und Freiheitsrechte der Bevölkerung gerichtet ist, muss deshalb bei begründeten Zweifeln an der Menschenrechtslage im Bestimmungsland stets untersagt werden. Bei der Exportentscheidung zu reiner Überwachungstechnologie muss der Schutz der Menschenrechte immer Vorrang haben.

2. Technologien für Menschenrechte müssen exportierbar sein

Viele IKT-Güter unterliegen heute der Exportkontrolle, dienen aber vorrangig nicht der Überwachung, sondern vielmehr dem *Schutz* vor Überwachung und damit dem *Schutz* der Menschenrechte. Beispiele hierfür sind Verschlüsselung, Technologien zur Erkennung von Angriffen und die automatisierte Erkennung von Softwareschwachstellen. Bei solchen Gütern sollte der Schutzgedanke stets Vorrang haben, d.h. sie sollten frei exportierbar sein.

4 Siehe hierzu Fußnote 2.

5 Georg Mascolo, Frederik Obermaier: Deutsche Technik für Despoten. Süddeutsche, 20. Mai 2014, *http://www.sueddeutsche.de/digital/spaehsoftware-werkzeuge-fuer-den-ueberwachungsstaat-1.1969195*

6 Martin Holland: OECD-Beschwerde gegen Hersteller von Überwachungssoftware. Heise Online, 6.2.2013, *http://www.heise.de/newsticker/meldung/OECD-Beschwerde-gegen-Hersteller-von-Ueberwachungssoftware-1798948.html*

7 Axel Kannenberg: Reporter ohne Grenzen: Exporte von Überwachungstechnik kontrollieren. Heise Online, 5.9.2013, *http://www.heise.de/newsticker/meldung/Reporter-ohne-Grenzen-Exporte-von-Ueberwachungstechnik-kontrollieren-1950280.html*

3. Schutz braucht Forschung und internationale Kooperation

Technisch betrachtet sind Überwachungsprodukte oft schlicht Angriffswerkzeuge. Man denke etwa an Spionage-Trojaner, die Schwachstellen in der IT ausnutzen, um Daten vom Zielsystem abzugreifen und an einen Kontrollserver zu übermitteln.

Die Verbesserung der Cybersicherheit ist folglich essenziell für den Schutz vor Überwachung. Je sicherer ein IKT- Produkt ist, desto aufwändiger wird es, in dieses einzudringen und so den Nutzer zu überwachen.

Cybersicherheit ist ein Hochtechnologiethema. Die systematische frühzeitige Erkennung von Angriffsmöglichkeiten und die Entwicklung von Sicherheitsmechanismen und Schutzkonzepten braucht Forschung und Entwicklung auf international höchstem Niveau.

Nur wenn sich die Forschung in Deutschland intensiv mit Angriffs- und Überwachungstechniken auseinandersetzen kann, entwickeln und behalten wir die Fähigkeit, entsprechende Schutzmechanismen zu entwickeln. Überwachstechnologien nutzen sehr oft Fehler, sogenannte Schwachstellen, in IKT-Produkten aus. Ein zentrales Ziel der Cybersicherheitsforschung ist es deshalb, solche Fehler von Anfang an, also »by design«, zu vermeiden. Leider gelingt das aber selbst den besten IKT-Herstellern nur sehr unvollständig. Deshalb ist es wichtig, dass die Forschung Methoden entwickelt, solche Schwachstellen schnell zu finden und diese den Herstellern zu melden. Die »good guys« der Forschung müssen schneller sein als die »bad guys« auf der anderen Seite.

Damit dies in der Praxis gelingt, darf es keine rechtlichen Hemmnisse für die Cybersicherheitsforschung geben, insbesondere nicht für die Erforschung von Schwachstellen in IKT-Produkten.

Ebenso wenig darf es rechtliche Hemmnisse für die internationale Zusammenarbeit und den Informationsaustausch zur Cybersicherheit geben. Deutschland nimmt in der Cybersicherheitsforschung einen Spitzenplatz ein, der weitaus größte Teil der Forschung findet aber im Ausland statt. Die internationale Forschungskooperation muss bei der Erstellung von Regeln zur Exportkontrolle angemessene Berücksichtigung finden.

4. Kontrollkriterien müssen der Technologieentwicklung folgen

Die Digitalisierung ist entscheidend für den Wohlstand unserer Gesellschaft und Erfolg unserer Wirtschaft, vergrößert zugleich aber den Anwendungsbereich von Überwachungstechnologie. Man denke etwa an »Smart Cars« oder »Smart Buildings« mit ihren vielfältigen Möglichkeiten der Überwachung ihrer Nutzer.

Konsequenterweise müssen deshalb die Listen für die Exportkontrolle kritischer Güter kontinuierlich an die neuen Anwendungsgebiete und damit verbundenen

neuen Überwachungstechnologien angepasst werden. Die Geschwindigkeit, mit der dies geschehen muss, wird durch die allgemeine Technologieentwicklung vorgegeben.

5. Marktgetriebene Entwicklung von Überwachungstechnologie

Überwachungstechnologie wird heute praktisch ausschließlich durch kommerzielle Anbieter entwickelt und vertrieben.

Prinzipiell ist es zwar vorstellbar, aber nicht empfehlenswert, in Deutschland die Entwicklung von Überwachungstechnologie für die eigenen hoheitlichen Zwecke staatlichen Stellen zu übertragen. In der IKT ist die Konkurrenz am internationalen Markt einer der Haupttreiber für Innovation und Qualität. Damit ist zu erwarten, dass staatliche Überwachungsprodukte der kommerziellen Konkurrenz letztlich immer qualitativ und funktional unterlegen wären.

Ein weitergehendes, vollständiges Verbot der Entwicklung von Überwachungstechnologie durch kommerzielle Anbieter wäre schwer vorstellbar. Viele Überwachungstechnologien dienen der Strafverfolgung oder völlig unbedenklichen zivilen Zwecken, so dass ein allgemeines Verbot nicht zu rechtfertigen wäre.

6. Abwägung und Abgrenzung bei Dual-Use-Gütern

Die EU-Verordnung 428/2009 bezeichnet als »Dual Use-Güter« oder »Güter mit doppeltem Verwendungszweck« alle Güter, die sowohl für zivile als auch für militärische Zwecke verwendet werden können.[8] Der Begriff des »militärischen Zwecks« wird hier mit »nicht-zivilem Zweck« gleichgesetzt, umfasst also beispielsweise auch die Überwachung durch Sicherheitsbehörden.

Nach dieser Definition haben sehr viele IKT-Produkte einen doppelten Verwendungszweck. Wie schon erwähnt, gilt dies auch für IKT-Produkte, die vorrangig dem Schutz vor Überwachung dienen und deshalb m.E. nicht der Exportkontrolle unterliegen sollten. Die Chancen und Risiken von IKT müssen deshalb bei der Definition von Dual-Use sorgfältig gegeneinander abgewogen werden. Eine zu weit gefasste Definition erfasst viele weniger bedenkliche Güter und behindert damit sinnvolle, zivile Anwendungen und verteuert und behindert den Export durch deutsche Unternehmen.

7. Kontrollentscheidungen können durch Technik durchgesetzt werden

IKT-Güter, z.B. Software, können häufig über das Internet modifiziert werden. Der häufigste Grund sind Updates zur Fehlerbeseitigung oder zum Nachrüsten von Funktionen. Sehr häufig kontaktieren IKT-Güter aber auch den Hersteller

8 Siehe *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:de:PDF*

über das Internet, um sicherzustellen, dass das Produkt korrekt lizensiert wurde. Scheitert eine solche Überprüfung, so deaktiviert sich das Produkt oder modifiziert seine Funktionalität.

Es wäre zu untersuchen, ob und wie sich diese Prinzipien der Durchsetzung von Lizenzen, also des »Digital Rights Managements«, auf Überwachungsprodukte anwenden ließen. Durch eine dynamische Deaktivierung könnte man z.B. zeitlich befristete Ausfuhrgenehmigungen realisieren, oder bei Änderung der Rahmenbedingungen im Bestimmungsland früher, eventuell irrtümlich genehmigte Ausfuhren zurückziehen.

Zumindest für manche Arten von Überwachungsprodukten könnte man die Anwendung solcher Methoden zur Vorbedingung für die Exportgenehmigung machen. Keinesfalls darf die technische Kontrolle aber die eigentliche Prüfung ersetzen oder auch nur absenken.

2 Welche Technologien können zur Überwachung verwendet werden?

Überwachungstechnologie verfolgt den Zweck, Informationen über Organisationen, Personen, Beziehungen, Kommunikationsvorgänge, Kommunikationsinhalte, Dokumenteninhalte und Meta-Daten in Erfahrung zu bringen. Die Überwachung geschieht in der Regel so, dass die überwachten Personen zur Zeit der Überwachung und während der Verarbeitung der dadurch gewonnenen Daten zunächst nichts von der Überwachung mitbekommen. Dies schließt folgende Aspekte ein:

1. Überwachte Personen oder Organisationen nehmen nicht wahr, dass sie überwacht werden. Überwachungstechnologien geben zum Zeitpunkt der Überwachung keine Rückmeldung an die überwachten Personen, so dass diese nicht bemerken können, dass eine Überwachung stattfindet.

2. Überwachte Personen können nicht wahrnehmen, an welchen Stellen, d.h. an welchen Orten bzw. bei der Nutzung welcher informations- und kommunikationstechnischen Systeme, sie überwacht werden. Das gilt selbst dann, wenn überwachte Personen die Vermutung haben, dass sie überwacht werden könnten.

3. Überwachte Personen nehmen nicht wahr, welche Informationen bei der Überwachung erfasst werden. Das gilt selbst dann, wenn über-

wachte Personen die Vermutung haben, dass sie überwacht werden könnten.

Früher war das Spektrum von Überwachungstechnologien relativ überschaubar, deren technische Ausrichtungen im Wesentlichen in den Bereichen Optik, Akustik und Telekommunikation lagen. Mit der Entwicklung von Informations- und Kommunikationstechnologie wie Computer, Internet, Anwendungen und Dienste auf der einen Seite und dem einfachen Zugang zu modernen Informations- und Kommunikationstechnologien und deren intensiver Nutzung auf der anderen Seite sind die technischen Ansatzpunkte und Möglichkeiten zur Überwachung vervielfacht.

Diese technische Weiterentwicklung macht es schwierig, den Begriff »Überwachungstechnologie« klar zu definieren. Die Schwierigkeit einer klaren Definition für Überwachungstechnologie zeigt sich beispielsweise daran, dass es Technologien wie etwa Werkzeuge zur Überwachung von Netzwerkverkehr gibt, die gleichermaßen auch zur Erkennung und Abwehr von Überwachung eingesetzt werden können. Damit wird auch schon deutlich, dass technische Produkte, die für Überwachungszwecke verwendet werden können, sich auch für andere Zwecke einsetzen lassen. Meistens verhält es sich mit dieser Dual-Use-Problematik jedoch genau entgegengesetzt: IT-Produkte, die ursprünglich für andere Zwecke entwickelt worden sind, lassen sich darüber hinaus auch für Überwachungszwecke einsetzen.

Auch wenn wegen der unscharfen Grenzen eine klare Definition von Überwachungstechnologie schwierig ist, so ist es doch möglich, Überwachungstechnologie gegen andere Technologien wie beispielsweise zur Zensur von Informationen abzugrenzen. Technologien zur Überwachung und zur Zensur unterscheiden sich in ihrer Zielsetzung deutlich. Geht es bei Überwachung prinzipiell um Informationsgewinnung, so geht es bei Zensur um Informationsvermeidung, indem einzelnen Personen oder Personengruppen, wie z.B. Bürgern eines Staates, bestimmte Inhalte vorenthalten werden. Technisch geschieht diese Vorenthaltung beispielsweise dadurch, dass Kommunikationsverbindungen zu bestimmten Adressen nicht zustande kommen, so dass Inhalte von diesen Adressen nicht übertragen werden können, oder dadurch, dass Daten bei der Übertragung analysiert werden und gegebenenfalls die Übertragung bestimmter Inhalte blockiert wird. Sowohl mit Technologien zur Überwachung als auch mit Technologien zur Zensur kann die Freiheit von Bürgern stark beeinträchtigt oder verletzt werden. Technologie zur Überwachung und Technologien zur Zensur können beide gegen demokratische Prinzipien verstoßen. Zensur behindert die Pressefreiheit und somit mittelbar den Meinungspluralismus, bei Überwachung ist die freie Meinungsäußerung gefährdet, da Andersdenkende Repressionen zu befürchten haben.

Überwachungstechnologie kann man dahingehend unterscheiden, ob sie sich gegen bestimmte Personen oder Organisationen richtet (gerichtete Überwa-

chung) oder ob sie sich gegen die Masse richtet, um beispielsweise in der Masse Personen identifizieren zu können (ungerichtete Überwachung). Bei der gerichteten Überwachung geht es in der Regel darum, möglichst umfangreiche Informationen zu einer gegebenen Person (z.B. ein bestimmter Journalist oder eine Person, bei der ein bestimmter Verdacht vorliegt) oder einer gegebenen Gruppe von Personen (z.B. Mitglieder einer bestimmten Menschenrechtsorganisation) in Erfahrung zu bringen. Entsprechend werden dann von Überwachungssystemen nur solche Daten erfasst, die in einem direkten Zusammenhang mit den gegebenen Personen oder Organisationen stehen. Bei der ungerichteten Überwachung werden massenweise Daten von Personen erfasst, um dann in diesen Massendaten zu vorgegebenen Merkmalen Daten bzw. die damit in Beziehungen stehenden Personen extrahieren zu können (z.B. zur Identifikation von Personen, die sich telefonisch zu einem bestimmtem Thema austauschen, oder zur Erkennung einer bestimmten Person in den Aufzeichnungen der Videoüberwachungsanlagen öffentlicher Plätze).

Zur Durchführung von gerichteter und ungerichteter Überwachung kann man Güter in drei Technologiebereiche unterscheiden:

1. Güter aus dem Bereich dezidierte Überwachungstechnologie: Dieser Technologiebereich umfasst Produkte, die ausschließlich zum Zweck der Überwachung entwickelt wurden. Auch Produkten aus dem Bereich dezidierter Überwachungstechnologie sind der Dual-Use-Kategorie zuzuordnen, da sie sowohl zur repressiven, freiheits- und demokratieschädlichen Zwecken eingesetzt werden können als auch zu Zwecken der Strafverfolgung, Strafermittlung und Terrorismusbekämpfung im positiven Sinn.

2. Güter mit primär anderem Verwendungszweck: Dieser Kategorie werden alle Güter zugeordnet, deren ursprüngliches Anwendungsziel nicht im Bereich der Überwachung liegt, die jedoch zum Zweck der Überwachung verwendet werden können. Damit ist auch hier die Dual-Use-Charakteristik offensichtlich. Beispiele hierfür sind Produkte zur Durchführung von IT-Sicherheitsanalysen, IT-forensische Produkte, Produkte aus dem Bereich der Datenwiederherstellung, Produkte für Fernzugriff und Fernsteuerung von Computern.

3. Güter aus dem Bereich Basistechnologie: Zu diesem Bereich zählen Produkte zur technischen Grundausstattung, die zwar notwendig zur Durchführung von Überwachungen, jedoch für diesen Zweck bei weitem nicht hinreichend sind. Zu dieser Kategorie zählen Güter wie beispielsweise leistungsfähige Computer. Diese haben als technische Universalwerkzeuge keinen klar bestimmbaren und eingrenzbaren Anwendungszweck.

Die Menge der Güter, die zur Überwachung eingesetzt werden können, umfasst ein breites Spektrum von Produkten, Diensten oder Know-how. Im Folgenden wird exemplarisch dargestellt, wie verschiedene Typen von Gütern für Überwachungen genutzt werden können:

- Güter zur Telekommunikationsüberwachung (TKÜ): Dies umfasst Produkte zum Abhören von Telefongesprächen in Festnetzen und Mobilfunknetzen, dem Mitlesen von E-Mails, Kurznachrichten (SMS) und Telefax und dem Verfolgen von Aufenthaltsorten in Mobilfunknetzen.[9] Eine spezielle Variante dieser Telekommunikationsüberwachung ist die Quellen-Telekommunikationsüberwachung, bei welcher die Information bereits vor ihrer Übertragung am Endgerät der zu überwachenden Person abgefangen wird. Diese Art der Überwachung wird gewählt, wenn nach Verschlüsselung kein Zugriff bei der Übertragung möglich ist. Dies kann beispielsweise durch Trojaner oder Hintertüren in Produkten geschehen.

- Trojaner: Mittels Trojanern kann man Zugriffe auf Computern von Benutzern bekommen. Über diese Zugriffe können beispielsweise Tastatureingaben mitgeschnitten werden. Dies ist insbesondere bei der Eingabe von Passwörtern kritisch, da in Erfahrung gebrachte Passwörter auch den Zugang zu Daten, die bei Diensten gespeichert sind ermöglichen. Darüber hinaus können Trojaner auch den Zugriff zu Daten auf der Festplatte und deren Versendung ermöglichen. Solche Trojaner können für Cyberangriffe von Cyberkriminellen zum Abfangen von Kreditkartendaten oder zur Industriespionage oder von staatlichen Organisationen zu Zwecken der Überwachung genutzt werden.

- IT-forensische Werkzeuge: IT-forensische Werkzeuge dienen primär der Rekonstruktion von Vorgängen und Handlungen beim Einsatz von Informationstechnologie. Dies geschieht meist zur Beweisermittlung in Strafverfolgungsverfahren, in denen Tathergänge aufgeklärt werden müssen. Diese Werkzeuge lassen sich beispielsweise dazu einsetzen, um Zugangskontrollen wie Passwort- oder PIN-Eingabe an Computern und Smartphones zu umgehen und dadurch Zugriff auf alle gespeicherten

9 Unternehmen, die in den vergangenen Jahren in die Schlagzeilen gekommen sind, weil ihre Produkte und Dienstleistungen in anderen Staaten zu repressiven Zwecken zum Einsatz gekommen sind, sind beispielsweise Gamma (*http://www.gammagroup.com*), Syborg (*http://www.syborg.de*) und Trovicor (*http://www.trovicor.com*). Siehe hierzu beispielsweise Georg Mascolo, Frederik Obermaier: Deutsche Technik für Despoten, Süddeutsche, 20. Mai 2014, *http://www.sueddeutsche.de/digital/spaehsoftware-werkzeuge-fuer-den-ueberwachungsstaat-1.1969195* oder Heise Online, OECD-Beschwerde gegen Hersteller von Überwachungssoftware, 6.2.2013, *http://www.heise.de/newsticker/meldung/OECD-Beschwerde-gegen-Hersteller-von-Ueberwachungssoftware-1798948.html*

Daten zu bekommen.[10] IT-forensische Werkzeuge können sowohl zur Ermittlung von Straftaten als auch zur Überwachung verwendet werden.

- Werkzeuge zur Netzwerkanalyse: Mit Werkzeugen zur Netzwerkanalyse kann der Datenverkehr in Computernetzen überwacht werden. Sie ermöglichen den Zugang und die Aufzeichnung von Datenverkehr an einer Netzwerkschnittstelle und den Zugriff auf Datenpakete, die von verschiedenen Nutzern geschickt werden.[11] Werkzeuge zur Netzwerkanalyse wurden eigentlich zur Identifikation von Fehlern oder von IT-Angriffen in Computernetzen entwickelt. Sie lassen sich jedoch auch zur Überwachung verwenden.

- Recovery-Werkzeuge: Es gibt Werkzeuge oder Dienste, welche sich in bestimmten Fällen bei drohendem Verlust von Daten wie z.B. Passwörtern einsetzen lassen. Ist beispielsweise ein Passwort verloren gegangen, mit dem ein Zugriff auf Dateiinhalte z.B. durch Verschlüsselung abgesichert wurde, dann können mit diesen Werkzeugen Passwörter rekonstruiert werden, so dass die Datei wieder geöffnet werden kann. Dies kann sogar gelingen, selbst wenn die Datei mit starken Verfahren verschlüsselt wurde. Die Angebote zur Rekonstruktion von Passwörtern funktionieren ähnlich wie Schlüsseldienste, bei denen Türen trotz verloren gegangener Schlüssel geöffnet werden. Sie werden in Form von Software und als IT-basierte Dienste angeboten.[12]

- Schwachstellen als Güter: Informationen um IT-Schwachstellen in Produkten wie beispielsweise Betriebssystemen oder Anwendungen und das Wissen wie man diese ausnutzen kann, bieten ebenfalls eine Möglichkeit, um Personen oder Organisationen überwachen zu können. Das Wissen um Schwachstellen ist einerseits wichtig, damit die Schwachstellen geschlossen werden können und Anwender somit besser geschützt werden können, andererseits kann man durch Missbrauch dieses Wissens Überwachung durchführen, so lange die Schwachstellen nicht geschlossen sind.

- Werkzeuge zur Schwachstellenerkennung: Mittels spezieller Werkzeuge zur Schwachstellenerkennung können Schwachstellen in IT-Produkten und IT-basierten Diensten gefunden werden. Die Analyseergebnisse dieser Werkzeuge können zur Verbesserung der Sicherheit von Anwendern

10 Beispiele für Unternehmen als Hersteller von solchen Gütern sind Cellebrite (*http://www.cellebrite.com*) oder MSAB (*http://www.msab.com*).

11 Ein Beispiel für ein solches Werkzeug ist Wireshark, siehe Heise Online, Netzwerkschnüffler Wireshark in Version 1.0 erschienen, 31.3.2008, *http://www.heise.de/newsticker/meldung/Netzwerkschnueffler-Wireshark-in-Version-1-0-erschienen-193886.html*

12 Siehe z.B. *http://www.elcomsoft.de/*

dieser Produkte und Dienste verwendet werden, jedoch auch für Überwachungszwecke ausgenutzt werden. Vor diesem Hintergrund kommt Werkzeugen zur Schwachstellenerkennung eine duale Verwertungsmöglichkeit zu.

- Werkzeuge zur Fernsteuerung von Computern: Diese Werkzeuge erlauben es, Computer oder Smartphones als Überwachungsgeräte vergleichbar einer Überwachungskamera oder einer Wanze zu verwenden. Hierfür können per Fernsteuerung Kamera und Mikrofon von Computern oder Smartphones angeschaltet werden und die mitgeschnittenen Inhalte über das Internet direkt übertragen werden. Zur Überwachung ist somit keine vorherige Installation der Überwachungsgeräte erforderlich, für welche man Zugang zu physischen Orten benötigt. Darüber hinaus sind klassische Überwachungsgeräte ortsgebunden, was bei der Nutzung von Aufnahmefunktionen an Smartphone und Computer nicht der Fall ist, weshalb sich diese sehr viel flexibler einsetzen lassen.

- Biometrische Verfahren: Biometrische Verfahren lassen sich sowohl zur Verbesserung der Absicherung von informationstechnischen Systemen wie etwa zur Zugangskontrolle verwenden als auch zur Überwachung wie etwa zur Identifikation bestimmter Personen durch Gesichtserkennungssoftware bei Videoaufnahmen.

- Werkzeuge für Big Data: Mit Big-Data-Analysen wird versucht, durch Analyse von Daten in großen Datenbeständen Zusammenhänge zu erkennen und neue Erkenntnisse abzuleiten. Die Anwendungsfelder solcher Big-Data-Analysen sind sehr vielfältig. Sie lassen sich beispielsweise zur Verbesserung des Marketings von bestimmten Produkten verwenden wie auch zur Gewinnung von Informationen für Überwachungszwecke.

Das große Spektrum der Liste von Gütern, die bereits für Überwachungszwecke eingesetzt werden können, und die rasante Weiterentwicklung neuer Technologien zeigen, dass die Regelungen für die Kontrolle des Exports parallel zum technologischen Fortschritt zeitlich sehr engmaschig kontrolliert und gegebenenfalls angepasst und weiterentwickelt werden müssen.

3 Welche Technologien können zur Abwehr von Überwachung eingesetzt werden?

Um sich gegen Überwachung schützen zu können, gibt es ein breites Spektrum von Möglichkeiten. Allen voran sind hier die Technologien zur sicheren Ende-zu-Ende-Verschlüsselung zu nennen, die auch von wenig technikaffinen Nutzern meistens direkt verwendet werden können. Hierbei kommt es jeweils auf die verwendeten Kommunikationsmedien an.

Der Aufwand zur Nutzung von sicherer Ende-zu-Ende-Verschlüsselung ist für verschiedene Kommunikationsmedien unterschiedlich hoch. Bei wenigen Medien bzw. Programmen ist die sichere Ende-zu-Ende-Verschlüsselung bereits integriert (z.B. die gängigen Browser unterstützen TLS zur sicheren Übertragung von Webseiten oder bei Jabber für Instant Messaging).

Bei E-Mail kommt es auf die verwendeten Dienste und die dabei genutzten technischen Werkzeuge an; bei browser-basierter E-Mail-Kommunikation muss man unterscheiden, ob die Verschlüsselung Ende-zu-Ende geschieht oder nur auf Teilstrecken bei der Übertragung angewendet wird. Bei dieser streckenbezogenen Verschlüsselung gibt es Computer im Internet, bei denen E-Mail-Inhalte unverschlüsselt vorliegen; in der Ende-zu-Ende-Variante bleibt die E-Mail zwischen den Computern des Versenders und des Empfängers geschützt. Bei der Verwendung von installierbaren E-Mail-Programmen sind in der Regel die Komponenten für den Austausch von Ende-zu-Ende-gesicherten E-Mails enthalten.

Die Nutzung von Ende-zu-Ende-gesicherter Telefonie ist sehr kostspielig, sowohl für das Festnetz als auch für Mobilnetze; sie funktioniert nur, wenn beide Kommunikationspartner entsprechende Geräte haben.

Ende-zu-Ende-Sicherheit kann man auch auf Dienste übertragen wie z.B. Cloud-Dienste zur Speicherung und gemeinsamen Nutzung von Daten. Ende-zu-Ende-Verschlüsselung bedeutet dort, dass Daten zwischen dem Hochladevorgang ab dem Computer des hochladenden Nutzers bis zum Computer des Herunterladens durchgängig verschlüsselt sind. Hierfür gibt es noch wenige Angebote wie z.B. OmniCloud.

Neben der Ende-zu-Ende-Verschlüsselung gibt es zur Abwehr von Überwachung Anonymitätsnetze, wie z.B. TOR. Damit können Nutzer gegenüber Organisationen, welche die Kommunikation an einem Knoten im Internet überwachen, verheimlichen, mit welchen anderen Adressen bzw. Parteien sie in Verbindung stehen.

Darüber hinaus gibt es viele weitere Möglichkeiten, die zur Abwehr von Überwachung verwendet werden können, wie z.B. der Einsatz von Werkzeugen zur

Erkennung und Beseitigung von Trojanern, Firewalls zur Abwehr von IT-Angriffen, Schwachstellenscanner, Werkzeuge zur Netzwerkanalyse oder das Wissen um Schwachstellen und wie diese geschlossen werden können.

4 Welche Gefahren entstehen durch den Einsatz von Überwachungstechnologien?

Durch den Einsatz von Überwachungstechnologien können für einzelne Menschen, Gruppen und ganze Gesellschaften große Gefahren entstehen, wenn diese in Staaten im Rahmen von interner Repression beispielsweise gegen Demokratiebewegungen oder gegen Menschenrechte eingesetzt werden. In den vergangenen Jahren sind einige Fälle bekannt geworden, die den Einsatz von Überwachungstechnologie in Staaten für solche Zwecke belegen. Im Folgenden werden einige dieser bekannt gewordenen Fälle als Beleg für reale Gefahren angeführt:

- In Bahrain wurde im Jahr 2010 Abd al-Ghani al-Chandschar festgenommen, für 6 Monate inhaftiert und später für 15 Jahre verurteilt, nachdem er sich für die Rechte von Folteropfern eingesetzt hatte. Zuvor wurde er mit Überwachungstechnologie, die aus Deutschland importiert worden war, überwacht.[13]

- Im Iran wurde im Jahr 2008 mit deutsch-finnischer Technologie ein Kontrollzentrum zur Überwachung von Bürgern aufgebaut.[14]

- Im Jahr 2011 wurde in Ägypten Überwachungssoftware aus Deutschland im Kampf gegen die Demokratiebewegung angewendet, die sich im Rahmen des Arabischen Frühlings gebildet hatte.[15] Durch die Überwachung konnten Anti-Mubarak-Aktivisten identifiziert und verhaftet werden. Es wurde gefoltert, einige dieser Aktivisten starben in Haft.[16]

13 Falk Steiner: Vorarbeit für Folterer. DER SPIEGEL, Nr. 6, 2013
14 Georg Mascolo, Frederik Obermaier: Deutsche Technik für Despoten. Süddeutsche, 20. Mai 2014, *http://www.sueddeutsche.de/digital/spaehsoftware-werkzeuge-fuer-den-ueberwachungsstaat-1.1969195*
15 Siehe Fußnote 14
16 Reinhard Bütikofer: Dual Use: Exportkontrolle ohne Zähne. Blätter für deutsche und internationale Politik, 1/2014, Januar 2014

- Das libysche Regime unter Muammar al-Gaddafi hat ein Programm des Herstellers Amesys namens »Eagle« zur Internetüberwachung von Oppositionellen eingesetzt[17].

- Die Organisation »Reporter ohne Grenzen« setzt Überwachungstechnologie mit Waffen gleich, wenn sie in die Hände eines autoritären Regimes gelangt.[18]

- Mit dem Export von Überwachungssoftware werden Autokraten in der ganzen Welt darin unterstützt, die freie Meinungsäußerung zu unterdrücken und Menschenrechte zu verletzen. Die Ausbreitung der Demokratie wird damit behindert und die nachhaltige Stabilisierung unserer internationalen Umwelt unterminiert.[19]

Diese Einschätzung der Gefahren beruht nicht auf Einzelmeinungen, sie wird von vielen anderen bestätigt, wie durch die folgende Aufzählung belegt wird:

- Entsprechend des Ergebnisses der Konferenz der zuständigen Minister des Europarats[20] vom 8.11.2013 können Technologien zur Massenüberwachung dazu missbraucht werden die Demokratie zu untergraben oder zu zerstören: »Die für die Medien und Informationsgesellschaft zuständigen Minister aus den 47 Mitgliedsstaaten des Europarates haben heute angemessene und wirksame Garantien zum Schutz vor dem Missbrauch der immer größer werdenden Möglichkeiten zur elektronischen Massenüberwachung gefordert. Ein solcher Missbrauch kann die Demokratie untergraben oder gar zerstören.«

- Der Europarat sieht die Menschenrechte durch die Massenüberwachung in Gefahr. Am 26.1.2015 beschloss dieser einstimmig[21]: »The surveillance practices disclosed so far endanger fundamental human rights, including the rights to privacy (Article 8 European Convention on Human Rights (ECHR)), freedom of information and expression (Article 10, ECHR), and the rights to a fair trial (Article 6, ECHR) and freedom of religion (Article 9) - especially when privileged communications of law-

17 Patrick Beuth: Die Ausreden der "Feinde des Internets". ZEIT ONLINE, 13. März, 2013, *http://www.zeit.de/digital/datenschutz/2013-03/feinde-des-internets-staatstrojaner*

18 Siehe Fußnote 17.

19 Annegret Bendieck: Menschliche Sicherheit kommt zu kurz. DER TAGESSPIEGEL, 28.2.2013, *http://www.tagesspiegel.de/meinung/andere-meinung/gastkommentar-zur-eu-cybersicherheitspolitik-menschliche-sicherheitkommt-zu-kurz/7853378.html*

20 Siehe *https://wcd.coe.int/ViewDoc.jsp?Ref=DC-PR140(2013)&Language=lanGerman&Ver=original&BackColorInternet=F5CA75&BackColorIntranet=F5CA75&BackColorLogged=A9BACE*

21 Siehe *http://website-pace.net/documents/19838/1085720/20150126-MassSurveillance-EN.pdf/df5aae25-6cfe-450a-92a6-e903af10b7a2*

yers and religious ministers are intercepted and when digital evidence is manipulated). These rights are cornerstones of democracy. Their infringement without adequate judicial control also jeopardizes the rule of law.«

- Der UN-Sonderberichterstatter[22] stellte am 17.4.2013 fest: »Inadequate legal standards increase the risk of individuals being exposed to violation of their human rights, including the right to privacy and the right to freedom of expression.«

- Nach einer Studie des PEN-Zentrums vom 5.1.2014 führt die Überwachung zur Selbstzensur bei Journalisten: »Surveillance conducted by government authorities induces self-censorship by writers around the world.«[23]

5 Was wurde auf verschiedenen Ebenen unternommen, um zum Schutz gegen Überwachung beizutragen?

In den vergangenen Jahren hat sich die Haltung der Politik zum Export von IuK-Gütern, die in einem Zusammenhang mit Überwachung von Personen stehen, deutlich geändert. Die Exportkontrolle, die früher stärker durch Leitgedanken zum Schutz des Staates bestimmt war, berücksichtigt zunehmend den Schutz von Personen in Ländern, welche als Endbestimmungsländer für Güter in Frage kommen. Die Rahmenbedingungen im Bereich Überwachung lassen sich differenzieren in Steuerung der Exportkontrolle sowie steuerungspolitische Maßnahmen zur Technologie- und Forschungsförderung.

Steuerung der Exportkontrolle

Hier sind verschiedene Ebenen zu betrachten. Es ist jedoch festzustellen, dass die Aktivitäten bzgl. der Einstufung von Überwachungstechnologie auf den verschiedenen Ebenen eine starke Kohärenz zeigen. Auf der Ebene der Staaten, die dem Wassenaar-Abkommen beigetreten sind, besteht durch die Weiterentwicklung der Wassenaar-Listen seit dem Jahr 2013 Einigkeit darüber, dass

22 Siehe *http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf*

23 Siehe PEN: Global Chilling - The Impact of Mass Surveillance on International Writers. January 5, 2015, *http://www.pen.org/sites/default/files/globalchilling_2015.pdf*

Überwachungstechnologie für das Internet und Intrusion Software der Exportkontrolle unterliegen sollte, ähnlich wie Kriegswaffen.[24,25]

Auf europäischer Ebene wurden mit der Verordnung Nr. 428/2009 die ersten Schritte unternommen, die Ausfuhr von Gütern zur Überwachung zu regeln bzw. einzuschränken. Die Güter, für welche solche Exportbeschränkungen gelten, werden in einer Liste erfasst, die fortlaufend aktualisiert werden sollte. Die Liste der Verordnung Nr. 428/2009 kombiniert verschiedene Listen, unter denen auch die Wassenaar-Liste enthalten ist. Die Verordnung Nr. 428/2009 ist EU-weit rechtsverbindlich und gilt somit in Deutschland.

In Deutschland werden die nationalen gesetzlichen Grundlagen der Exportkontrolle hauptsächlich durch das Außenwirtschaftsgesetz (AWG)[26] mit ihrer Außenwirtschaftsverordnung (AWV)[27] und das Kriegswaffenkontrollgesetz (KrWaffKontrG)[28] als Ausführungsgesetz zu Artikel 26 Abs. 2 des Grundgesetzes gebildet. Die Mitte 2015 auf den Weg gebrachte 4. Änderungsverordnung zur Außenwirtschaftsverordnung[29] (AWV) regelt die Kontrolle des Exports von Auswertesystemen für Telefonie und bei Dienstleistungen zu Überwachungstechnik. Damit regelt Deutschland den Export von Überwachungstechnologie strenger, als dies durch die aktuell gültigen Vorgaben der EU notwendig ist. Mit den Änderungen der Außenwirtschaftsverordnung hat Deutschland künftige Änderungen in der EU-Verordnung vorweggenommen, deren Inkrafttreten nicht vor Ende 2017 erwartet wird. In der Begründung[30] heißt es: »… Die vorliegenden Genehmigungs- und Unterrichtungspflichten in Bezug auf bestimmte Güter der Kommunikationsüberwachung dienen dazu, die Ausfuhr und das Erbringen technischer Unterstützung aus Menschenrechtserwägungen untersagen zu können. Die betreffenden Güter weisen ein hohes Missbrauchspotential dafür auf, sie zur Verletzung von Menschenrechten, insbesondere im Rahmen interner Repression, einzusetzen. Dies betrifft namentlich die Ermittlung, Verfolgung und Inhaftierung von Systemkritikern, Oppositionellen und Angehörigen von Minderheiten, das Ausspähen entsprechender Personen und Personengruppen sowie die Nutzung erhobener Informationen zur gezielten Propaganda, Diffamierung und Schwächung politischer Gegner. Durch die neuen Genehmigungs- und Unterrichtungspflichten können für die Menschenrechte

24 Siehe *http://www.wassenaar.org*
25 Mathias Monroy: Erneuertes Wassenaar-Abkommen: Spionagesoftware könnte zukünftig mehr Exportkontrolle unterliegen. Netzpolitik, 13. Dezember, 2013, *https://netzpolitik.org/2013/erneuertes-wassenaar-abkommen-spionagesoftware-koennte-zukuenftig-mehr-exportkontrolle-unterliegen/*
26 Siehe *http://www.gesetze-im-internet.de/awg_2013/*
27 Siehe *http://www.gesetze-im-internet.de/bundesrecht/awv_2013/gesamt.pdf*
28 Siehe *http://www.gesetze-im-internet.de/krwaffkontrg/*
29 Siehe *http://www.bmwi.de/BMWi/Redaktion/PDF/V/vierte-verordnung-zur-aenderung-der-aussenwirtschaftsverordnung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdfl*
30 Siehe *http://www.bmwi.de/BMWi/Redaktion/PDF/V/vierte-verordnung-zur-aenderung-der-aussenwirtschaftsverordnung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf*

im Bestimmungsland kritische Ausfuhren und technische Unterstützungen untersagt werden. …« Mit dieser aktuellen Änderungsverordnung macht Deutschland seine Verantwortung beim Schutz von Menschenrechten durch die Kontrolle beim Export deutlich. Das Bundeswirtschaftsministerium hat angekündigt, mit den nationalen Regelungen zur Exportkontrolle von Überwachungstechnologie über die Anforderungen internationaler Regelungen, wie z.B. den EU-Regelungen hinausgehen zu wollen.[31,32,33]

Technologie- und Forschungsförderung

Zur Stärkung von Menschenrechten dienen nicht nur Regelungen zur Exportkontrolle und deren Durchsetzung. Stattdessen kann man auch Technologien verwenden, mittels derer man Überwachungsversuche abwehren kann. In diesem Zusammenhang sind Technologien aus dem Bereich der IT-Sicherheit und des Privatsphärenschutzes zu nennen.

Die Bundesregierung hat den Schutz von Privatsphäre als wichtiges Ziel in ihre »Digitale Agenda 2014 – 2017«[34] zur Förderung von neuen Technologien aufgenommen: »Wir wollen die Privatsphäre der Menschen und ihre Kommunikation im Internet besser schützen. Wir schaffen die Voraussetzungen dafür, dass jeder Einzelne in der Lage ist, sich selbst und seine Daten im Netz wirksam zu schützen.«

Auf der Seite der Forschungsförderung unterstützt das Bundesforschungsministerium verstärkt Forschung in den Bereichen IT-Sicherheit und Privatsphärenschutz. Als Beispiel ist die im Jahr 2011 erfolgte Einrichtung von Kompetenzzentren für IT-Sicherheit in Darmstadt, Saarbrücken und Karlsruhe zu nennen. Im Jahr 2015 wurde deren Förderung verlängert und aufgestockt: Für den weiteren Betrieb der Zentren wurden für die kommenden vier Jahre rund 40 Millionen Euro zugesagt. Neben der Förderung dieser Zentren hat das Bundesforschungsministerium Anfang 2015 Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt" beschlossen. Privatheit und der vertrauliche Umgang mit persönlichen Informationen im Internet sind von zentraler Bedeutung in diesem Programm.

Während Deutschland die Themen zum Schutz des einzelnen stärker priorisiert, hat die EU diese Themen weniger stark gewichtet. Im Forschungsförderungs-

31 Georg Mascolo, Frederik Obermaier: Gabriel plant Exportstopp von Späh-Software. Süddeutsche, 20.5.2014, *http://www.sueddeutsche.de/digital/internetueberwachung-gabriel-plant-exportstopp-von-spaeh-software-1.1969189*

32 Axel Kannenberg: Gabriel will Export von Spähsoftware beschränken. Heise Online, 19.5.2014, *http://www.heise.de/newsticker/meldung/Gabriel-will-Export-von-Spaehsoftware-beschraenken-2193268.html*

33 Florian Rötzner: Gabriel: Keine Überwachungstechnik für Regime, die Menschenrechte verletzen. Telepolis, 20.5.2014, *http://www.heise.de/tp/druck/mb/artikel/41/41813/1.html*

34 Siehe *http://www.digitale-agenda.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda.pdf?__blob=publicationFile&v=6*

programm »Horizon. 2020« der EU werden die Themen IT-Sicherheit und Privatsphärenschutz im Gegensatz zu früheren Programmen nicht mehr direkt adressiert und nun eher niedrig priorisiert. Bereits 2012, also noch in der Entwurfsphase des Programms, machten der Bitkom und namhafte Leiterinnen und Leiter von Forschungseinrichtungen in einem Positionspapier[35] auf die damit verbundenen Nachteile aufmerksam.

6 Wie kann man sicherstellen, dass relevante Technologien bei Entscheidungen bzgl. Ausfuhrkontrolle berücksichtigt werden?

Um die Kontrolle der Ausfuhr kritischer Güter effektiv und effizient gestalten und durchführen zu können, sind die folgenden Aspekte wichtig:

- Aktuelle und dem Stand der Technik entsprechende Listen von Gütern, welche der Exportkontrolle unterliegen
- Korrekte Zuordnung von Gütern, für welche Exportanträge gestellt werden, zu entscheidenden Einträgen in der Liste mit den Kriterien von exportgenehmigungspflichtigen Gütern
- Informationsaustausch zwischen den Verantwortlichen und Entscheidern bei der praktischen Durchführung von Exportkontrolle zur Vereinheitlichung und Verbesserung der Effizienz in behördlichen Prozessen

Im Folgenden werden diese Aspekte diskutiert.

Die Listen für die Exportkontrolle müssen sich ähnlich schnell entwickeln wie die Technologie selbst. Die Entwicklung von Informations- und Kommunikationstechnologie schreitet nach wie vor rasant voran. Es ist davon auszugehen, dass sich dies in den kommenden Jahren fortsetzen wird. Mit dem fortschreitenden Trend der Diffusion von Informations- und Kommunikationstechnik in alle Bereich des täglichen Lebens vergrößert sich die Angriffsfläche für Überwachung, z.B. durch den Einsatz von Cyberphysical Systems in Gebäuden oder in Fahrzeugen der Zukunft oder durch die Nutzung von Cloud-Diensten. Neben der so immer weiter wachsenden Menge der Anwendungsbereiche, in denen Überwachung stattfinden kann, wächst die Anzahl der Güter, die sich spezifisch für diese Anwendungsbereiche zur Überwachung eignen. Entsprechend

[35] Siehe *http://www.ec-spride.tu-darmstadt.de/fileadmin/user_upload/Group_EC_Spride/files/Gemeinsames_Positionspapier_zur_IT Sicherheitsforschung_im_Programm_Horizon_2020.pdf*

müssen die Listen für die Exportkontrolle kritischer Güter kontinuierlich weiter entwickelt und an das Spektrum vorhandener Technologien, die sich zur Überwachung eignen, angepasst werden. Die Weiterentwicklung der Exportkontrolllisten muss im besten Fall mit der gleichen Geschwindigkeit geschehen, wie sich die Technologie weiter entwickelt. Dies war in der Vergangenheit nicht so. So ist Intrusion Software beispielsweise erst im Jahr 2013 in die Wassenaar-Liste aufgenommen worden, die in den Jahren zuvor im arabischen Raum wie etwa in Bahrain zur Verletzung von Menschenrechten eingesetzt wurden.

Bei der Erstellung der Kontrollkriterien ist erforderlich, dass nicht nur diejenigen Technologien Berücksichtigung finden, die offensichtlich zur Überwachung eingesetzt werden, sondern auch solche, bei denen die Anwendbarkeit zur Überwachung nicht direkt auf der Hand liegt. Anstatt beispielsweise einen entfernten Knoten im Internet so zu manipulieren, dass man in diesem Knoten Inhalte von Kommunikationsbeziehungen mitschneidet, ist es stattdessen auch möglich, die Wegewahl von Datenpaketen im Internet so zu manipulieren, dass die Pakete solche Knoten passieren, die unter der Kontrolle der überwachenden Organisation sind.

Die Personen, welche Entscheidungen über Exportgenehmigungen treffen, brauchen neben den Exportkontrolllisten auch eine Möglichkeit, effektiv und effizient entscheiden zu können, ob bestimmte technische Kriterien aus diesen Listen bei gegebenen Gütern zutreffen oder nicht. Hierfür braucht das Personal entsprechende aktuelle Hintergrundinformationen zum Stand der Technik.

Zur effizienten, konsistenten und objektiven Herbeiführung von Entscheidungen der Exportkontrolle sind die Hintergrundinformationen zu berücksichtigen, die zu den Entscheidungen geführt haben. Hierfür sind Register und Datenbanken wichtig. Neben den oben genannten Gründen tragen diese auch zur Dokumentation und Transparenz behördlicher Prozesse bei und bieten somit auch eine Möglichkeit zur Kontrolle der Exportkontrolle. Auch können sie dabei helfen, Schwächen in den bestehenden Verordnungen und Listen aufzudecken, so dass an diesen Stellen Verbesserungen vorgenommen werden können.

Um sicherstellen zu können, dass Überwachungstechnologien nicht in kritischen Ländern angewendet werden können, ist es erforderlich, dass sich die Regierungen der exportierenden Staaten auf eine fortlaufende Aktualisierung der Listen einigen und neue Kriterien in die Listen aufnehmen. Ohne eine breite Zustimmung der exportierenden Länder lässt sich für die Situation in den Endbestimmungsländern wenig erreichen, da bei Nichterteilung einer Ausfuhrgenehmigung alternative Produkte aus anderen Staaten importiert werden können. Die internationalen Einigungsprozesse zur Aktualisierung von Listen bis hin zu deren Umsetzung dauern heute immer noch sehr lange. Es ist wichtig, dass diese Prozesse künftig beschleunigt ablaufen können.

7 Wie groß ist der Markt für Überwachungstechnologie und Dienstleistungen?

Zur aktuellen Größe des Marktes für Überwachungstechnologie liegen keine gesicherten Zahlen vor. Dies gilt weder für Deutschland, Europa oder den Weltmarkt noch für andere Länder. Die Tatsache, dass hierzu keine gesicherten Daten verfügbar sind, ist nicht überraschend. Dennoch sind einige Zahlen im thematischen Umfeld öffentlich, die belegen, dass der Markt relativ groß ist:

- Durch die Enthüllungen von Snowden ist bekannt geworden, dass im Jahr 2013 die Budgets der amerikanischen Geheimdienste CIA bei 14,7 Milliarden US-$, von NSA bei 10,5 Milliarden US-$ und von NRO bei 10,5 Milliarden US-$ lagen. Die Summe der Budgets für die 16 verschiedenen US-Geheimdienste lag im Jahr 2013 bei 52,6 Milliarden US-$.[36]

- Geheimdienste beziehen in großem Umfang Technologie von Unternehmen. Bei den US-Geheimdiensten besteht die Vermutung, dass sie ca. 70% ihrer Budgets für Technologie oder Dienstleistungen von Dritten aufbringen.[37]

- Der weltweite Markt im Bereich der Videoüberwachung wird für das Jahr 2020 auf 48,32 Milliarden US-$ geschätzt.[38]

- Im Jahr 2015 hat Netzpolitik berichtet, dass der BND plant, 300 Millionen Euro in neue Überwachungstechnologie zu investieren.[39]

- In den Spy Files von WikiLeaks sind Informationen zu rund 130 Unternehmen aus 25 Ländern zusammengetragen, die auf dem Überwachungstechnologiemarkt tätig sind.[40]

36 Friedhelm Greis, Jörg Thoma: Das geheime Budget der US-Geheimdienste. Golem, 30.8.2013, *http://www.golem.de/news/nsa-affaere-das-geheime-budget-der-us-geheimdienste-1308-101301.html*

37 Norman Solomon: Why government surveillance won't protect your data. Fortune, August 26, 2015, *http://fortune.com/2015/08/26/cybersecurity-nsa-att/*

38 Transparency Market Research: Rising Safety and Security Concerns Increase Demand for Video Surveillance and VSaaS Systems: Global Market to Value US$48.32 Billion by 2020. August 28, 2015, *http://www.transparencymarketresearch.com/pressrelease/video-surveillance-vsaas-market.htm*

39 Andre Meister: Strategic Initiative Technology: We Unveil the BND Plans to Upgrade its Surveillance Technology for 300 Million Euros. Netzpolitik, 23. September 2015, *https://netzpolitik.org/2015/strategic-initiative-technology-how-bnd-wants-to-ramp-up-its-tech-capabilities-for-300-million-euros/*

40 WikiLeaks: Spy Files. 2011, *https://wikileaks.org/spyfiles/*

- Der Überwachungssektor in China wird im Jahr 2015 voraussichtlich einen Umsatz von 73,5 Milliarden Euro erzielen. Für die folgenden Jahre wird der Markt in China weiter stark wachsen.[41]

- Die Aufwände für Überwachung sind in Nordamerika und Europa besonders hoch: Pro Kopf werden in den USA und Kanada 11,48 US-$ hierfür ausgegeben. In der EU sind es umgerechnet 12,04 US-$, deutlich mehr als in China, wo pro Kopf nur 3,69 US-$ aufgebracht werden.[42]

Wegen der angestiegenen Überwachung in den vergangenen Jahren wird davon ausgegangen, dass sich der Privacy-Markt zur Abwehr von Überwachung in den kommenden Jahren relativ stark entwickeln wird.[43,44,45]

8 Wie könnte man den Einsatz von Überwachungstechnologie völkerrechtlich regeln?

Wenn die politischen Bedingungen in den Bestimmungsländern einen berechtigten Grund zu der Annahme geben, dass Menschenrechte bedroht sind, dann sollte der Export von Überwachungstechnologie in solche Länder völkerrechtlich bindend verboten werden.

Die Menschen- und Bürgerrechte im digitalen Zeitalter wurden jüngst von EU-Parlamentspräsident Martin Schulz und von Justizminister Heiko Maas hervorgehoben.

EU-Parlamentspräsident Martin Schulz regte vor wenigen Wochen eine Charta der digitalen Grundrechte[46] an. Darin betont er den Grundrechtsschutz: »… Unser Instrument, um einen solchen digitalen Totalitarismus zu verhindern, heißt: Grundrechteschutz. Ich meine die guten alten Menschen- und Bürgerrechte, in allen ihren freiheitlichen Dimensionen, aber auch die sozialen und wirtschaftlichen Ziele, denen sich der Staat verpflichtet hat und die einem effektiven Grundrechteschutz nach modernem Verständnis innewohnen. Unsere

41 Nina Trentmann: Perfide Überwachung ist in China Wirtschaftsfaktor. DIE WELT, 8.12.2015, *http://www.welt.de/149753135*
42 Siehe Fußnote 41.
43 Brian Iverson: Maverick* Research: The Unbearable Cost of Privacy: Gartner, 1 October, 2015
44 Carsten Casper, Earl Perkins, Penny Gillespie: Predicts 2015: Privacy Erodes, Prompts Action From Companies and Regulators. Gartner, 4 December, 2014
45 Carsten Casper: Hype Cycle for Privacy, 2015. Gartner, 24 July, 2015
46 Siehe *http://pdf.zeit.de/2015/48/grundrechte-netz-datenschutz-eugh.pdf*

Grundrechte sind die Werte und Regeln, die unsere Gesellschaft konstituieren und die zugleich einen Hinweis darauf geben, dass es konkurrierende Rechtsgüter gibt, die im Konfliktfall sorgfältig abgewogen werden müssen. Deshalb bin ich davon überzeugt, dass wir eine Charta der Grundrechte für die digitale Zeit formulieren müssen. …«

Justizminister Heiko Maaß griff die Anregung einer Charta für digitale Grundrechte auf und stellte einen Entwurf[47] vor. Darin findet sich »Artikel 12 Die Staaten schaffen ein Völkerrecht des Netzes, um die Freiheit des Internets weltweit zu sichern. Seit Edward Snowden und dem NSA-Skandal wissen wir, dass der digitale Leviathan nicht nur im Silicon Valley lauert. Auch Staaten bleiben eine Gefahr für die Freiheit, wenn sie an den Knotenpunkten des Internets ungezügelt E-Mails mitlesen oder unser Surfverhalten ausspähen. Das Völkerrecht wurde vor 400 Jahren geschaffen, um die Freiheit der Meere zu sichern. Die Weltmeere des digitalen Zeitalters – das ist das Internet, und deshalb brauchen wir eine internationale Verständigung über die Achtung persönlicher Daten, um sie vor dem willkürlichen Zugriff von Geheimdiensten zu schützen.«

Die hier angeregte internationale Verständigung über die Achtung persönlicher Daten sollte die Exportkontrolle von Überwachungstechnologie direkt adressieren. Damit eine einschlägige Initiative Aussicht auf Erfolg hat, muss sie die Gefahr in den Mittelpunkt stellen, sobald Überwachungstechnologie sich in Hand von autoritären und totalitären Regimen befindet. In einem ersten Schritt kann eine solche Initiative die Ächtung hiervon herbeiführen. Eine völkerrechtlich bindende Konvention nach dem Vorbild des Übereinkommens über das Verbot von Antipersonenminen muss das Ziel sein.

9 Welche Besonderheiten existieren für Software im Vergleich zu physischen Gütern?

Software ist beliebig oft kopierbar und kann einfach weitergegeben werden, ihr Einsatz kann verborgen und ihre Verbreitungswege können ebenfalls sehr gut verschleiert werden.

Die Immaterialität von Software und die – technisch einfache – Möglichkeit Vervielfältigungen anzufertigen impliziert, dass die Anzahl von Kopien nicht festgestellt werden kann, nachdem Software einmal an Kunden ausgeliefert wurde. Ein physisches Gut existiert genau einmal und müsste zur Vervielfälti-

47 Siehe *http://pdf.zeit.de/2015/50/internet-charta-grundrechte-datensicherheit.pdf*

gung nachgebaut werden, was in der Regel aufwändig und nicht wirtschaftlich ist. Im physischen Fall sind zudem Original und Kopie meist einfach unterscheidbar.

Der Einsatz von Software kann verborgen werden, ihre Herkunft und ihre Verbreitungswege können verschleiert werden. Beispielsweise blieb die Spionagesoftware „Regin" mindestens sieben Jahre lang[48] unentdeckt.

Bezüglich der Kontrolle der Ausbreitung von exportkontrollierter Überwachungssoftware stellen diese Besonderheiten Herausforderungen dar. Es könnte schwierig und bisweilen unmöglich sein den Weg zu rekonstruieren, den exportkontrollierte Software aus Deutschland nahm, wenn sie in Ländern gefunden wird, in denen Menschenrechte missachtet werden. Es ist möglich, dass deren Einsatz jahrelang unentdeckt bleibt und es kann eine unbekannte Anzahl weiterer laufender Instanzen dieser Software in Staaten geben, in denen ebenfalls Menschenrechte missachtet werden.

Software zeichnet sich gegenüber physischen Gütern dadurch aus, dass die Systeme, auf denen die Software installiert ist, mit Computern des Software-Herstellers im Lebenszyklus der Software in Kontakt stehen können um Daten auszutauschen. Dieser Datenaustausch geschieht beispielsweise für die Übertragung von Updates für die Software oder zur Lizenzkontrolle, so dass überprüft werden kann, ob die Software häufiger verwendet wird als vertraglich vereinbart wurde bzw. ob die Software entgegen der Absprachen in andere Länder weitergegeben wurde. Im Rahmen der Lizenzkontrolle besteht die Möglichkeit, die Software aus der Ferne stillzulegen oder den Umfang der nutzbaren Funktionen einzuschränken. Die Steuerung der Nutzungskontrolle einer Software durch eine wiederkehrende Lizenzkontrolle über das Internet stellt für Anwender mit tiefem technischen Fachwissen keinen unumgänglichen Mechanismus dar, so dass die Möglichkeiten einer harten Nutzungskontrolle eingeschränkt werden können. Auch wenn man mit der Lizenzkontrolle die Nutzungskontrolle nicht gegen alle Macht definitiv durchsetzen kann, bedeutet das nicht, dass man deshalb auf eine Nutzungskontrolle verzichten sollte. Immerhin erfordert das Umgehen der Nutzungskontrolle Personen mit entsprechendem Fachwissen, so dass durch die Nutzungskontrolle die einfache Weitergabe von Software oder ein Verstoß gegen andere Bedingungen deutlich erschwert wird, da hierfür Zeit, Geld und umfangreiche Kompetenzen erforderlich sind.

48 Siehe *http://www.wired.com/2014/11/mysteries-of-the-malware-regin*

10 Welche Besonderheiten gibt es für den Markt von Überwachungsprodukten?

Es gibt viele Hersteller von Überwachungstechnologie und der Markt ist sehr heterogen. Am einen Ende des Spektrums finden sich Hersteller, die sich auf Überwachungstechnologie[49] spezialisiert haben. Am anderen Ende findet sich Überwachungstechnologie als eine Produktfamilie von vielen (beispielsweise Nokia Siemens). Für Spezialprobleme der Überwachung wird am Markt befindliche Spitzentechnik benötigt, die ursprünglich für andere Zwecke entwickelt wurde. Zum Beispiel interessiert sich der BND einem Zeitungsbericht zufolge für die HANA-Technologie[50] von SAP zum Zweck der Live-Auswertung von großen Datenmengen. Die Beibehaltung der bestehenden Marktstrukturen garantiert gegenüber dem gelegentlich geäußerten Alternativvorschlag zur Verlagerung dieses Technologiebereichs in staatliche Bereiche, dass die Qualität der Produkte gerade durch den Wettbewerb entsprechend hoch ist und sogar noch gesteigert werden kann. Das Beispiel SAP HANA zeigt zudem, dass eine für alle Produkte geltende Auflage zur Offenlegung von Quellcodes in Technologien ausschließen würde. HANA wurde eigentlich für andere Anwendungsbereiche und Wirtschaftsbranchen entwickelt. Dass HANA nun auch für Aufgaben im Zusammenhang mit Überwachung eingesetzt werden kann, kann nicht rechtfertigen, dass SAP nun sämtliche Quellen und Dokumentationen zu HANA offenlegen müsste.

Eine weitere Besonderheit des Marktes für Überwachungstechnologie besteht darin, dass der Markt der Überwachungstechnologie praktisch nicht richtig zu fassen ist, da Überwachungstechnologie selbst schwierig einzugrenzen ist. Grundsätzlich kann jede Software mit praktisch beliebigem Anwendungszweck zur Überwachung verwendet werden, wenn sie über entsprechende Hintertüren verfügt. Anwender verwenden Software im Vertrauen darauf, dass diese keine Hintertüren enthalten. Nutzt ein nicht vollständig nach außen abgeschotteter Anwender Software mit einer Hintertür, dann kann jeder, der das entsprechende Wissen über diese Hintertür hat, den Anwender ausspionieren und überwachen. Zum überwiegenden Anteil von Softwareprodukten ist nicht bekannt, ob diese über Hintertüren verfügen.

49 In Vertreter dieser Kategorie ist z.B. die Gamma Group *https://www.gammagroup.com/*.
50 Siehe *http://www.sueddeutsche.de/digital/internet-ueberwachung-bnd-will-gigantische-datenmengen-speichern-1.2059582*

11 Endbetrachtung

Die Entscheidung der Bundesregierung und international besetzter Gremien, die Ausfuhr von Überwachungstechnologie zu kontrollieren und bei kritischen Endbestimmungsländern zu verbieten, war wichtig, und sie zeigt unbestritten in die richtige Richtung, um die Einhaltung von Menschenrechten in anderen Ländern zu stärken. Es ist sehr positiv zu bewerten, dass Deutschland die Beschlüsse internationaler Gremien vorwegnimmt, wie dies in 2015 durch die 4. Änderungsverordnung der Außenwirtschaftsverordnung geschehen ist, und damit bereits die Ausfuhr von Gütern einschränkt, bevor diese Güter offiziell in internationale Listen für Exportbeschränkungen aufgenommen werden. Dieses begrüßenswerte Vorgehen zeigt aber auch ein wichtiges Problem auf: Die Aktualisierung der internationalen Exportkontrolllisten verläuft oftmals noch viel zu langsam. Sie hält nicht Schritt mit der rasanten Entwicklung im Bereich der Informations- und Kommunikationstechnologie und insbesondere nicht im Bereich der Überwachungstechnologie.

Die angewandte Forschung im Bereich der Cybersicherheit kann hierbei mit ihrer Technologieexpertise, ihrem Wissen um Markt und Akteure in diesem Sektor und ihrer Kompetenz in den Anwendungspotenzialen dieser Technologien Politik und Behörden bei der kontinuierlichen Verbesserung der Exportkontrolle von Überwachungstechnologie unterstützen. Das Ziel muss hier darin liegen, die Exportkontrolle von Überwachungstechnologie auf der Ebene der Gestaltung und der Durchführung effektiver und effizienter zu machen. Verzögerungen in der Gestaltung implizieren das Risiko, dass der Exportkontrollrahmen den Stand der Technik nicht adäquat berücksichtigt und bestimmte Überwachungsgüter in kritische Länder exportiert werden, obwohl diese ausfuhrbeschränkt sein sollten. Durch eine engere Zusammenarbeit von Politik und Behörden auf der einen Seite und der Forschung auf der anderen Seite kann die Situation verbessert werden. Diese Zusammenarbeit kann sich sowohl auf Überwachungstechnologie selbst, wie auch auf Prozesse der Exportkontrolle beziehen.

Darüber hinaus kann die anwendungsorientierte Forschung im Bereich Cybersicherheit helfen, Abwehrmechanismen gegen Überwachung zu entwickeln und somit einen Beitrag zur Stärkung der Menschenrechte in anderen Ländern leisten. Dies hilft auch in dem Fall, wenn Überwachungstechnologie aus anderen Staaten in kritische Endbestimmungsländer exportiert wurde und sich Bürger dort gegen Überwachung schützen möchten. Von der Ausfuhr von Abwehrtechnologien könnte als positiver Nebeneffekt auch die deutsche Wirtschaft profitieren.

Damit die anwendungsorientierte Cybersicherheitsforschung die oben angesprochenen Arbeiten und Beiträge leisten kann, ist es wichtig, dass sie entspre-

chende Förderungen und Freiheiten bekommt. Um qualitativ hochwertige Forschung durchführen und praktisch relevante und verwertbare Ergebnisse erzielen zu können, ist es wichtig, dass die Forschung in Deutschland mit anderen Spitzenforschern aus anderen Ländern kooperieren und Ergebnisse und Entwicklungen ohne Auflagen teilen und austauschen können.