REPORTER OHNE GRENZEN
FÜR INFORMATIONSFREIHEIT

Fragen für das Fachgespräch des Ausschusses Digitale Agenda zum Thema „Effektivierung der Kontrolle des Exports von Überwachungs- und Spionagesoftware auf deutscher und europäischer Ebene und öffentliche Auftragsvergabe“ am 16. Dezember 2015

- Antworten von Christian Mihr, Reporter ohne Grenzen e.V. -

1. Seit Jahren wird über die demokratiefördernde Wirkung von Digitalisierung und Internet diskutiert. Weitgehend durchgesetzt hat sich die Ansicht, dass diese Technik wichtig sein kann, Demokratiebewegungen zu vernetzten und journalistische Berichterstattung zu ermöglichen. Wie schätzen Sie vor diesem Hintergrund entsprechende Technologien zur Überwachung und Sperrung von Telefon- und Internetkommunikation ein und welche Gefahren können dadurch ggf. für die Informations- und Meinungsfreiheit oder die Arbeit von Journalisten entstehen? Die anonyme oder pseudonyme Nutzung von Kommunikation ist für Journalisten und ihre Informanten, aber auch für Oppositionelle in autoritären Regimen unverzichtbar. Welche Bedeutung kommt Technologien, die eine durchgehende Ende-zu-Ende-Verschlüsselung von Kommunikation bieten, zu?

Ein Beispiel aus der Praxis vorweg: Als Vizepräsident des Bahrainischen Zentrums für Menschenrechte sammelt Sayed Yousif al-Muhafdha die Berichte der Opfer von Folter und Polizeigewalt in dem arabischen Golfstaat. Auch ausländische Journalisten kamen zu ihm, um mit seiner Hilfe solche Menschen zu treffen. Irgendwann fiel Muhafhdha auf, dass Polizei oder Geheimdienst immer öfter schon vor ihm bei seinen Gesprächspartnern eintrafen. Da ahnte er, dass seine Telefon- und Internetkontakte überwacht wurden. Inzwischen ist Muhafdha mit Hilfe von Reporter ohne Grenzen nach Deutschland geflohen, wo wir weiter eng mit ihm und seiner Organisation zusammenarbeiten. Allerdings muss er damit rechnen, dass der Bahrainische Geheimdienst ihn auch hier im Exil mithilfe deutscher Überwachungstechnik ausspäht. (http://www.capital.de/dasmagazin/finfisher-attacke-auf-deutschland-2308.html)

Während wir hier im Bundestagsausschuss Digitale Agenda zusammensitzen, werden Menschen in Diktaturen gefoltert oder verhört, weil sie mit deutscher Überwachungstechnik ausgeforscht wurden. In den vergangenen Jahren ist die völlige politische Ignoranz bei diesem Thema erfreulicherweise einer etwas kritischeren Bewertung des Exports von Überwachungstechnologien aus Deutschland und der EU gewichen. Nachdem ich bereits 2013 und 2014 in nicht-öffentlichen Anhörungen des Bundestagsunterausschusses für Abrüstung, Rüstungskontrolle und Nichtverbreitung als Sachverständiger reden durfte, freue ich mich, dass der Bundestagsausschuss „Digitale Agenda“ sich heute öffentlich mit diesem Thema beschäftigt.
(https://www.reporter-ohne-grenzen.de/fileadmin/docs/Stellungnahme__Export_dt._UEberwachungstechnologie_17.04.2013.pdf und https://www.reporter-ohne-grenzen.de/uploads/tx_lfnews/media/141112_Anhoerung_Unterausschuss_Ruestungskontrolle.pdf)

Die Überwachung moderner Kommunikationskanäle schränkt das Menschenrecht auf Presse-, Informations- und Kommunikationsfreiheit systematisch ein. Der Menschenrechtsbeauftragte des Europarats spricht angesichts der teils grenzüberschreitenden Kommunikationsüberwachung gar von einer „grundlegenden Bedrohung der Rechtsstaatlichkeit im Internet“.
(https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2727697&SecMode=1&DocId=2258296&Usage=2)

Der Zugang zu Ende-zu-Ende-Verschlüsselungstechnologien ist für Journalisten und Menschenrechtsverteidiger kein Luxus. Er ist überlebensnotwendig, damit professionelle Journalisten und Bürgerjournalisten ihre besonders schutzwürdige Tätigkeit ausüben können. Die Bedeutung sicherer Kommunikationskanäle und von Verschlüsselungstechnologien hat nicht zuletzt David Kaye, UNO-Sonderberichterstatter für die Förderung und Verteidigung des Rechts auf Meinungsfreiheit, in seinem am 22. Mai 2015 an den UNO-Menschenrechtsrat übermittelten Bericht sehr prägnant herausgearbeitet. (http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc).

Neben der politischen Arbeit ist ein wichtiger Aufgabenbereich von Reporter ohne Grenzen die Nothilfe für verfolgte und bedrohte professionelle Journalisten und Bürgerjournalisten. Im Rahmen unserer Nothilfearbeit unterstützen wir weltweit jedes Jahr rund 600 Einzelfälle. Dabei zeigt sich, dass heute eigentlich jeder von uns unterstützte Journalist zumindest in Teilen digital arbeitet und sei es, dass er nur E-Mails schreibt. Mindestens die Hälfte der von uns jedes Jahr weltweit unterstützten rund 600 Journalisten sind in Folge von Überwachung durch Staaten oder private Gewaltakteure sowie aus Mangel an Ende-zu-Ende-Verschlüsselung in bedrohliche Situationen geraten: Das heißt, sie erlitten in Folge von Überwachung gezielte Angriffe und Gewalt, wurden zu Unrecht inhaftiert oder mussten ihre Länder verlassen.
(http://www.faz.net/aktuell/feuilleton/medien/christian-mihr-ueber-die-verfolgung-von-bloggern-13852737.html)

Reporter ohne Grenzen betrachtet deshalb die Überwachung elektronischer Kommunikation in vielen Ländern als eines der größten Probleme für Journalisten, die ihre Quellen verantwortlich schützen wollen. Die Aufklärung über den Einsatz von sicheren Ende-zu-Ende-Verschlüsselungstechnologien ist ein wesentliches Aufgabenfeld unserer Nothilfe. Von ROG weltweit durchgeführte Schulungen in Digitaler Sicherheit zeigen, wie groß die Nachfrage von Journalisten nach Tipps zur digitalen Selbstverteidigung ist. (http://www.bild.de/politik/ausland/menschenrechtskolumne/workshop-fuer-bedrohte-online-dissidenten-43394866.bild.html)

Wir wissen, dass auch terroristische Gruppen wie Boko Haram und der sogenannte Islamische Staat Zugang zu Überwachungstechnologien haben. Das potenziert einerseits die Gefahren und offenbart andererseits umso mehr, dass eine Proliferationskontrolle schwierig ist und der durch die Bundesregierung lange Zeit aktiv geförderte Export von Überwachungstechnologie der Demokratie schadet und menschenrechtlich verantwortungslos ist.

Bezogen auf westliche Demokratien sind verschiedene Studien übereinstimmend zu dem Ergebnis gekommen, dass sich Journalisten angesichts von Überwachung in ihrer Arbeit bedroht fühlen und gezwungen sehen, ihre Arbeitsweise zu ändern oder bestimmte Recherchen nicht weiter zu verfolgen. In Einzelfällen schrecken Informanten sogar davor zurück, Journalisten zu kontaktieren, weil sie fürchten, vom Geheimdienst enttarnt zu werden. Informanten und Whistleblower sind jedoch eine Grundvoraussetzung für unabhängige journalistische Berichterstattung in einer Demokratie.

2. Welche Fortschritte sind in den vergangenen Jahren auf deutscher, europäischer und internationaler Ebene erreicht worden, um der Bedeutung entsprechender Technologien für den Grundrechts- und Menschenrechtsschutz Rechnung zu tragen und welche Rolle hat die Bundesregierung hierbei eingenommen?

Noch vor wenigen Jahren hat die Bundesregierung den Export von Überwachungstechnologie in autoritäre Staaten und Diktaturen mit Steuergeldern unterstützt. Auch mit Mitteln des Deutschen Bundestages finanzierte Konferenzen dienten der Anbahnung von Geschäften in diesem Bereich. Die politische Aufmerksamkeit für die Brisanz des Exportes bestimmter Technologien hat mittlerweile, nicht zuletzt durch die Arbeit verschiedener Menschenrechtsorganisationen wie Reporter ohne Grenzen, auch im Rahmen des CAUSE-Bündnisses, deutlich zugenommen. Nach anfänglichen politischen Widerständen hat sich die Situation auch in Deutschland merklich verändert.

Die zuständigen Stellen im Bundeswirtschaftsministerium und im Auswärtigen Amt waren bis vor drei Jahren weitgehend blind für die in Folge des Exports solcher Überwachungstechnologien begangenen Menschenrechtsverletzungen in Diktaturen und autoritären Regimen. Mittlerweile haben zunächst das Auswärtige Amt und nachholend auch das Bundeswirtschaftsministerium personellen Sachverstand aufgebaut und pflegen einen begrüßenswerten Austausch mit Menschenrechtsorganisationen – selbst wenn einige Ankündigungen von Bundeswirtschaftsminister Gabriel in der Vergangenheit vor allem rhetorischer Natur waren.

Verbesserungsmöglichkeiten bestehen nach wie vor bei der Transparenz. Verlässliche Zahlen zu Dual-Use-Exporten wurden bislang fast nur auf Grund parlamentarischer Anfragen erhoben.

Die UN-Vollversammlung hat Ende 2013 die wegweisende, aber nicht rechtsverbindliche Resolution „Right to Privacy in the Digital Age" verabschiedet, die die Bundesregierung mit initiiert hatte (http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167). Reporter ohne Grenzen erscheint es jedoch wenig glaubwürdig, wenn die Bundesregierung einerseits versucht, andere Regierungen zu mehr Achtung der Informationsfreiheit und zur Förderung von Ende-zu-Ende-Verschlüsselungstechnologien zu bewegen, während deutsche Nachrichtendienste gleichzeitig Bürger massenhaft und gezielt ausspähen – mit Technologien, deren Einsatz wir in Diktaturen und autoritären Regimen kritisieren. Die Bundesregierung muss stattdessen die in der Resolution genannten Forderungen auch im eigenen Land umsetzen und sicherstellen, dass die deutschen Geheimdienste sich bei ihren Überwachungsmaßnahmen an geltende Gesetze halten.
Deshalb hat Reporter ohne Grenzen den Bundesnachrichtendienst verklagt und deshalb engagieren wir uns gegen die anlasslose Vorratsdatenspeicherung. Nicht zuletzt hat auch der Menschenrechtsbeauftragte des Europarats die mangelnde Kongruenz von innen- und außenpolitischem Handeln angemahnt: „Aufgrund der wachsenden Partnerschaften zwischen Strafverfolgungsbehörden und Nachrichten- und Sicherheitsdiensten droht diese Verneinung der Rechtsstaatlichkeit von den letzteren auf Polizeikräfte und Staatsanwaltschaften überzuspringen".
(https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2727697&SecMode=1&DocId=2258296&Usage=2)

3. Wie definieren Sie Überwachungstechnologie, Spionagesoftware, Spähsoftware und Zensursoftware und wie kann sichergestellt werden, dass möglichst alle relevanten Soft- und Hardwareelemente, die zur Verletzung von Menschenrechten und innerer Repression genutzt werden können, in der Definition abgedeckt sind und in der Definition der genehmigungspflichtigen Überwachungs- und Spähtechnologie enthalten sind? Inwieweit bedarf es hierzu beispielsweise eines bundesweiten Registers, in dem Korruptions- und andere Wirtschaftsdelikte eingetragen sind? Sind Sie der Ansicht, dass die Kontrolle von Exporten entsprechender Technologien zur Überwachung und Sperrung von Telefon- und Internetkommunikation heute effektiv geschieht? Wo sehen Sie Mankos in bestehenden Regulierungsregimen auf deutscher, europäischer und internationaler Ebene?

Überwachungstechnologien sind Technologien, die zur Ausspähung bestimmter Ziele eingesetzt werden. Zu unterscheiden sind hier gerichtete und ungerichtete Überwachungstechnologien.
Trojanische Software installiert dabei eine Hintertür auf dem Rechner, Smartphone oder anderen vernetzten Geräten der Nutzer und späht dann bestimmte Daten aus. Dies können Screenshots des Bildschirminhaltes, einzelne Dateien sowie Daten einer im Gerät installierten Kamera, eines Mikrofons oder anderer Sensoren (etwa Gyroskope) sein.

Monitoring Center ermöglichen hingegen die ungerichtete Überwachung von Internetströmen. Hier wird der Internetverkehr nach bestimmten Merkmalen (sogenannten Selektoren, also zum Beispiel Handynummern, IP-Adressen, definierte Stichwörtern, etc.) gefiltert, das Ergebnis entsprechend gespeichert und in der Regel zur weiteren Analyse aufbereitet.

In vielen Diktaturen und autoritären Regimen beobachtet Reporter ohne Grenzen, dass es de facto keine unterschiedlichen Befugnisse für Geheimdienste und Polizeibehörden beim Einsatz dieser Technologien gibt.

Derzeitige Export-Kontrollregime sehen eine Vorabprüfung entsprechend der durch die exportierenden Unternehmen eingereichten Unterlagen vor. Anonym in diesem und im vergangenen Jahr auf zwei Twitter-Konten veröffentlichte Leaks interner Dokumente der Firmen Hacking Team und Finfisher (früher Gamma International) zeigen jedoch, dass Verkäufe in der Regel über eine oder sogar mehrere Tochter- und Vermittlerfirmen abgewickelt werden. Nötig ist daher eine explizite, verpflichtende Endverwenderkontrolle.

Die bisherigen, internen Regelungen der Firmen (unter dem Stichwort „Know Your Customer") sind defintiv nicht ausreichend. Das haben vor allem die von Reporter ohne Grenzen unter anderem gemeinsam mit dem ECCHR, European Center for Constitutional and Human Rights, angestrengten OECD-Beschwerden gegen die deutsche Firma Trovicor und die deutsch-britische Firma Gamma International gezeigt. Beide OECD-Beschwerden haben erhebliche interne Probleme bei der Menschenrechtsverantwortung beider Firmen aufgedeckt. So haben die OECD-Prüfer in Großbritannien festgestellt, dass Gamma keine menschenrechtsbezogene Due-Diligence-Prüfung durchgeführt und intern keine verbindlichen Standards zur Beachtung von Menschenrechten habe. (https://www.reporter-ohne-grenzen.de/deutschland/alle-meldungen/meldung/ruege-fuer-hersteller-von-ueberwachungstechnik/)

Die Effektivität des derzeitigen Kontrollregimes lässt sich darüber hinaus derzeit nur schwer abschätzen. Einerseits ist die Implementierung des Wassenaar-Arrangements noch recht jung – bislang ist noch kein ganzes Jahr vergangen. Andererseits liegen keine umfassenden Zahlen zu Ablehnungen und Annahmen von Export-Anträgen vor.

4. Können Sie abschätzen, wie groß der Markt (Handelsvolumen, Mitarbeiterzahl etc.) deutscher und europäischer Anbieter, die entsprechende Programme und Technologien anbieten, in etwa ist? Sind aus Ihrer Sicht seit 2013 (Revision Wassenaar) Fälle dokumentiert, die belegen, dass entsprechende Programme und Technologien deutscher und europäischer Firmen in den vergangenen Jahren in autoritären und totalitären Staaten zum Einsatz kamen?

Der Marktumfang kann nur geschätzt werden. Einige Experten gehen von einem globalen Marktvolumen von etwa fünf Milliarden US-Dollar aus. Diese Schätzungen sind jedoch schon mehrere Jahre alt und in ihrer Methodik nicht unumstritten. (http://www.egadd.org.uk/2015/12/08/sipri-work-on-dual-use-export-controls-and-cyber-surveillance-technologies/)
Fest steht: Etwa 15 Firmen sind weltweit im besonders heiklen Geschäft mit Trojaner-Software aktiv, darunter die Firmen Finfisher und Trovicor aus München oder die Firma Hacking Team aus Italien, die Reporter ohne Grenzen bereits im Jahr 2013 als Feinde des Internet benannt hat. (https://www.reporter-ohne-grenzen.de/themen/internetfreiheit/alle-meldungen/meldung/rog-bericht-feinde-des-internets-westliche-ueberwachungstechnik-in-den-haenden-von-diktatoren/)

Eine signifikante Anzahl von Mitarbeitern wird in Deutschland nicht beschäftigt. Trovicor gilt in Deutschland als eines der größten Unternehmen in diesem Bereich und beschäftigt als solches rund 170 feste sowie eine unbekannte Zahl freier Mitarbeiter. Andere Firmen wie Finfisher beschäftigen in der Regel weniger als 100 Mitarbeiter. Auch die italienische Firma Hacking Team produziert ihre Software mit einer sehr überschaubaren Zahl an Mitarbeitern, wie wir dank der Leaks wissen.

Signifikante negative Beschäftigungseffekte sind durch eine weitere Exportregulierung nicht zu erwarten – die Nachfrage nach IT-Fachkräften übersteigt das Angebot bei weitem. Reporter ohne Grenzen schätzt, dass es in Deutschland rund 20 Anbieter für internationale Überwachungstechnologien (Hard- und Software) gibt. EU-weit gehen wir derzeit von etwa 200 entsprechenden Unternehmen aus.

Der Export europäischer Software nach dem Jahr 2013 ist zumindest für das Unternehmen Hacking Team durch die öffentlich zugänglichen Leaks eindeutig belegt. Demzufolge lieferte Hacking Team nach 2013 Überwachungstechnologie nach Uganda.

Reporter ohne Grenzen liegen zudem bislang nicht veröffentlichte stichhaltige Hinweise auf den Export von Monitoring-Centern nach 2013 durch das deutsche Unternehmen Atis nach Ägypten sowie in andere Länder mit einer gleichfalls problematischen Menschenrechtssituation vor.

Letztlich sind aber nicht die Exporte nach 2013 entscheidend, um die Wirkung der Exportregulierung durch das Wassenaar-Arrangement zu beurteilen: Erst mit dem Beschluss der neuen EU-Dual-Use-Richtlinie sind die Regeln in Europa verbindlich geworden. Um die Effektivität der Exportkontrolle zu überprüfen, müssten wir also Einblick in die Dual-Use-Statistik von 2015 haben.

5. Der Rechtsrahmen für die Exportkontrolle von Dual-use-Gütern (Güter mit doppeltem Verwendungszweck) wird durch die europäische Verordnung (EG) Nr. 428/2009 (EG-Dual-use-Verordnung) vorgegeben. Auf nationaler Ebene sind zudem in engen Grenzen Beschränkungen des Exports von Dual-use-Gütern insbesondere zum Schutz der Menschenrechte möglich. Wie bewerten Sie den derzeitigen europäischen und nationalen Rechtsrahmen zur Kontrolle des Exports von Überwachungs- und Spionagesoftware und wo sehen Sie Handlungsbedarf? Reicht die Berücksichtigung von Technologien zur Entwicklung von Intrusion Software in der revidierten Fassung (Stand: März 2015) aus? Welche anderen Hard- und Softwaretechnologien könnten oder sollten aufgenommen werden? Dual-use-Güter können auch für legitime zivile Zwecke, zum Beispiel zur Verbesserung der IT-Sicherheit, eingesetzt werden. Wie kann möglichst effektiv verhindert werden, dass entsprechende Export-Kontrollregime negative Auswirkungen auch auf Programme und Technologien haben, die man zu sanktionieren nicht beabsichtigt? Wie können erste Erfahrungen mit dem Abkommen auf diesem Gebiet beschrieben werden?

Reporter ohne Grenzen bewertet die in der Frage beschriebene Implementierung der Regulierung des Wassenaar-Arrangements in der EG-Dual-Use-Verordnung positiv. Für eine abschließende Bewertung ist es allerdings noch zu früh, weil die Implementierung noch sehr am Anfang steht. Nicht in allen Ländern des Wassenaar-Abkommens wurden die Regelungen bisher implementiert – darunter die USA und Russland. In den USA beobachten wir Probleme bei der Implementierung des Wassenaar-Arrangements und Russland ist ebenfalls weiter sehr aktiv beim Export entsprechender Technik – unter anderem nach Ecuador und Mexiko. Reporter ohne Grenzen befürchtet, dass die US-Regierung Druck ausüben wird, das Wassenaar-Abkommen generell zu revidieren. Die deutsche Bundesregierung sollte gemeinsam mit ihren europäischen Partnern Widerstand leisten, wenn nötig.

Überarbeitungsbedarf sehen wir bei der fortwährenden Kontrolle bestimmter Verschlüsselungstechnologien. Auf Grund der mittlerweile in vielen Produkten standardmäßig eingesetzten Verschlüsselungen und der deutlich fordernden IT-Sicherheitsumgebung (Geheimdienste, IT-Kriminalität) sind diese Regelungen schlicht überholt und sollten deshalb ersatzlos gestrichen werden.

Bereits heute sind Forschungsergebnisse, Open-Source-Software und öffentlich für Privatanwender erwerbbare Computersoftware von den Regelungen des Wassenaar-Abkommens ausgenommen. Reporter ohne Grenzen erkennt bislang keine negativen Auswirkungen auf die Verfügbarkeit von entsprechenden Angeboten für Journalisten und Menschenrechtsverteidiger.

Die allermeisten IT-Firmen liefern ohnehin nur an Regierungsakteure: Bei IT-Produkten liegt deshalb der Unterschied zwischen legitimer und illegitimer Nutzung nicht in der Frage, ob die Güter militärisch oder zivil genutzt werden – im Vergleich zu anderen Dual-Use-Produkten.

Die Frage ist vielmehr, ob ein Land über einen geeigneten Rechtsrahmen verfügt, der die Verwendung solcher Güter sinnvoll beschränkt. Weiterhin ist es bei der Beurteilung von Exportanträgen aus Sicht von Reporter ohne Grenzen wichtig, die Trennung von Geheimdiensten, Polizeibehörden und anderen Strafverfolgungsbehörden in den Blick zu nehmen. Zu bedenken ist zudem, dass bestimmte Werkzeuge wie etwa der Finfisher-Trojaner generell nicht geeignet sind, die allgemeine IT-Sicherheit zu verbessern.

6. Seit Ende 2014 sind zudem die zuletzt im Wassenaar-Arrangement beschlossenen Exportkontrollen für Überwachungstechnik mit Aufnahme in die EG-Dual-use-Verordnung EU-weit rechtsverbindlich. Neben der bereits seit langem kontrollierten Verschlüsselungstechnik werden seitdem Ausfuhren von Staatstrojanern sowie Überwachungstechnik für Satellitenfunk, Mobilfunk und Internet kontrolliert. Reichen diese Vorgaben des Wassenaar-Arrangements aus? Die aktuelle Liste des Wassenaar-Arrangements klassifiziert gemäß Nr. 4A003 b Digitalrechner als exportkontrollierte Supercomputer, wenn diese eine Rechenleistung von 8 gewichteten Teraflops haben. (Dies entspricht der Rechenleistung einer hochwertigen Grafikkarte.) Wie werden die Kontrolllisten des Wassenaar-Arrangements insgesamt aktuell gehalten und inwieweit ist eine (fortlaufende) Evaluierung und Erweiterung dieser Kontrolllisten notwendig und möglich?

Die 41 Mitgliedstaaten des Wassenaar-Abkommens beschließen die Kontrolllisten jeweils im Konsens auf der alljährlich im November/Dezember stattfindenden Plenartagung der Vertragsstaaten. Die Anpassung der Dual-Use-Richtlinie auf EU-Ebene im vergangenen Jahr sorgt dafür, dass Änderungen der Listenpositionen auf Basis delegierter Rechtsakte durch die EU-Kommission zeitnah umgesetzt werden können. Eine mehrjährige Verzögerung der Umsetzung von Wassenaar wie in der Vergangenheit ist daher nicht zu befürchten.

Eine Kontrolle von sogenannten Zero-Day-Schwachstellen, wie sie immer wieder diskutiert wird, halten wir nicht für notwendig. Nur in wenigen Fällen werden diese für die direkte Überwachung oder den Einsatz von Malware verwendet. In den allermeisten Fällen kommen dafür andere Techniken wie Phishing, Social Engineering oder das Aufspielen von Malware bei Grenzkontrollen zum Einsatz. Eine Kontrolle von Zero-Days wäre weit weniger praktikabel als die derzeitige Praxis bzw. die dadurch zu erringenden Vorteile wären vermutlich eher gering. Eine Kontrolle von in Software gefundenen Schwachstellen könnte die Arbeit von Sicherheitsforschern tatsächlich gefährden.

7. Die Bundesregierung hat im Sommer dieses Jahres mit der 4. Änderungsverordnung zur Außenwirtschaftsverordnung (AWV) Genehmigungspflichten für die Ausfuhr insbesondere von Monitoringsystemen für Telefonie und entsprechender Vorratsdatenspeicherung eingeführt. Zukünftig sollen darüber hinaus Dienstleistungen (sog. technische Unterstützung) für genehmigungspflichtige Überwachungstechnik kontrolliert werden. Die Bundesregierung will damit nationale Regeln einführen, um den Export von Überwachungstechnologie wirksamer kontrollieren und effektiver unterbinden zu können, als dies auf Basis geltender EU-Regelungen bisher der Fall ist. Wie bewerten Sie diese Änderungen?

IP-Überwachungssysteme, zu denen auch bestimmte Monitoring Center gehören, sind im Rahmen der Regelungen des Wassenaar-Arrangement bereits kontrolliert. Eine zusätzliche Kontrolle von Monitoring-Centern und Lawful-Intercept Anlagen sowie verwandten Dienstleistungen wie Schulungen und direkter Support für Überwachungstechnologien ist dringend geboten: Denn die geleakten Betriebsunterlagen der Firma Finfisher/Gamma haben gezeigt, dass der unternehmenseigene IT-Support nicht nur allgemeine Aufgaben wahrnimmt, sondern Überwachungsmaßnahmen wie die Infektion mit einem Trojaner zum Teil aktiv unterstützt.

Wichtig ist, dass die Bundesregierung Änderungen, wenn immer möglich, im europäischen Kontext unternimmt. Die Unternehmen in diesem Bereich sind sehr flexibel und arbeiten zum Teil mit Reseller-Partnerschaften oder durch Komponentenaustausch zusammen. Eine effektive Kontrolle muss daher europäisch ausgerichtet sein.

Reporter ohne Grenzen misst deshalb der Mitarbeit der Bundesregierung in der sogenannten Surveillance Technology Export Group große Bedeutung zu. Der Bundestag sollte die Diskussionen dort jedoch aktiv begleiten und Informationen einfordern.

8. Welche Art der staatlichen Unterstützung für dieser Kontrolle unterliegenden Firmen durch die Bundesregierung ist Ihnen bekannt (Hermesbürgschaften, Messeauftritte, Bewerbung von Produkten etc.) und wie beurteilen Sie eine etwaige Unterstützung dieser Firmen aus Menschenrechtssicht?

Eigene Recherchen von Reporter ohne Grenzen, die die Vergabe von Hermes-Bürgschaften durch die Bundesregierung für den Verkauf von Überwachungstechnologien nach Russland und Malaysia belegen, haben mittlerweile auch Recherchen des NDR und der Süddeutschen Zeitung bestätigt: Geliefert wurde in den Jahren 2005 und 2006.

Reporter ohne Grenzen hat überdies - bislang noch nicht-veröffentlichte – Hinweise darauf, dass die Bundesregierung Hermes-Bürgschaften für den Export deutscher Überwachungstechnologien vor Ausbruch des Krieges auch nach Syrien vergeben haben könnte. Öffentlich bekannt ist bereits, dass die Firma Trovicor dort Anlagen installiert und gewartet hat.

In der Vergangenheit hat das Bundeswirtschaftsministerium Überwachungstechnik als „Zukunftsmarkt" bezeichnet und diesen Sektor noch 2012 mit dem Programm „Zukunftsmarkt Zivile Sicherheit" ausdrücklich gefördert. Meines Wissens ist dieses Programm mittlerweile nicht mehr Grundlage der Politik der Bundesregierung.

In Kooperation mit dem Nah- und Mittelostverein der deutschen Wirtschaft (NUMOV) und den Ländern des Golfkooperationsrates förderte das Wirtschaftsministerium etwa die „1st German GCC Security Conference" in Düsseldorf, bei der führende deutsche Hersteller von Überwachungs- und Grenzsicherungstechnik ihre Produkte vorstellen konnten. Die Veranstaltung wurde 2012 mit bis zu 40.000 Euro aus dem Haushaltstitel „Erschließung von Auslandsmärkten, Unterposition Markterschließungsmaßnahmen für KMU des produzierenden Gewerbes und Dienstleister" des Wirtschaftsministeriums finanziert.

Diskussionswürdig erscheint es mir, dass das Bundeswirtschaftsministerium im Juni dieses Jahres die Schirmherrschaft für das 18. Deutsch-Arabische Wirtschaftsforum in Berlin übernommen hatte, bei dem laut Programm eines der Themen die „vielversprechenden Kooperationsmöglichkeiten im Bereich Sicherheit und IKT" war. Beim Missbrauch von Überwachungstechnik einschlägig belastete Länder wie Ägypten, Bahrain und Saudi-Arabien, die Regierungsvertreter zu dem Forum entsandt hatten, sind aus Sicht von Reporter ohne Grenzen jedoch keine Partner in dem Themenfeld Sicherheit und IKT.

Erfreulich ist, dass weit gediehene skandalöse Überlegungen der Gesellschaft für Internationale Zusammenarbeit, GIZ, verstärkt Regierungen beim Einsatz von Überwachungstechnik zu beraten, mittlerweile nach meinem Kenntnisstand eingestellt sind.

Jegliche staatliche Unterstützung von Firmen, die Überwachungstechnik in Diktaturen und autoritäre Regime liefern, ist menschenrechtlich verantwortungslos.

9. Inwieweit ist es problematisch, wenn staatliche Stellen ohne Einblick in den Quellcode und Kenntnis der genauen Fähigkeiten der Software auf die Produkte dieser Anbieter zurückgreifen?

Besteht konkrete Gefahr, dass entsprechende, mit öffentlichen Mitteln erstellte Programme, ergänzt um weitere Funktionen, auch an Sicherheitsbehörden autoritärer und totalitärer Staaten weiterverkauft werden?

Eine genaue Prüfung des Quellcodes von entsprechender Technologie beim Einsatz im Inland ist aus Sicht von Reporter ohne Grenzen unerlässlich. Nur so kann gewährleistet werden, dass der Einsatz der Technologien im Einklang mit dem wegweisenden Staatstrojaner-Urteil des Bundesverfassungsgerichts aus dem Jahr 2008 ist.

Uns liegen keine Hinweise auf einen Export der vom BKA entwickelten Trojaner-Software vor. Hier ist ein überwiegendes Geheimhaltungsinteresse der Behörde anzunehmen. Denn je mehr Installationen der Software weltweit existieren, desto größer ist die Gefahr einer ungewollten Entdeckung. Es muss jedoch sichergestellt werden, dass deutsche Behörden auch im Anti-Terror-Kampf, zum Beispiel gegen den sogenannten Islamischen Staat, ausländische Stellen nicht verdeckt und ohne Rechtsgrundlage unterstützen.

10. Sind zur Kontrolle von Überwachungstechnologie, die auch für Kriegsvorbereitungen dienen könnte, auch völkerrechtliche Vorkehrungen notwendig oder geboten? Wie könnten diese konkret aussehen?

Geleakte E-Mails von Hacking Team zeigen, dass das Unternehmen mit dem Export seiner Software in den Sudan bewusst gegen Sanktionen der Vereinten Nationen verstoßen hat. Und vermutlich ist das kein Einzelfall. Es müssen deshalb effektivere Sanktionsmechanismen geschaffen werden. Die Ächtung hoch intrusiver Software mit großem Missbrauchspotenzial in autoritären Staaten ist von großer Bedeutung. Mehrere zivilgesellschaftliche Organisationen, darunter Reporter ohne Grenzen, haben dazu in den 13 Grundsätzen für Menschenrechte in der digitalen Welt bereits 2013 sehr konkrete völkerrechtliche Vorschläge vorlegt. (https://www.reporter-ohne-grenzen.de/pressemitteilungen/meldung/13-grundsaetze-fuer-menschenrechte-in-der-digitalen-welt/)

11. Wie kann auf nationaler und auf europäischer Ebene sichergestellt werden, dass alle relevanten Soft- und Hardwareelemente, die zur Verletzung von Menschenrechten und zur inneren Repression genutzt werden können, in der Definition der genehmigungspflichtigen Überwachungs- und Spähtechnologie enthalten sind? Inwieweit bedarf es hierzu beispielsweise eines bundesweiten Registers, in dem Korruptions- und andere Wirtschaftsdelikte eingetragen sind? Im Gegensatz zu klassischen Gütern fehlt es Software-Produkten in der Regel an einem klassischen physischen Transport- und Vertriebsweg. Wie gestaltet sich die tatsächliche Kontrolle der Ausfuhrbeschränkungen? Wie wird Open-Source-Software zur Überwachung von und zum Eindringen in informationstechnische Systeme vor dem Hintergrund des Wassenaar-Abkommens und nationaler Exportvorschriften betrachtet, sofern sich die Regelungen gegen Hersteller und Exporteure richten? Wie sieht der Informationsaustausch zwischen der Europäischen Kommission und den Mitgliedstaaten sowie zwischen den Aufsichtsbehörden aus und wo bestehen hier möglicherweise Defizite?

Die Item-Listen bedürfen einer genauen und regelmäßigen Überarbeitung, um mit dem technischen Fortschritt mithalten zu können. Derzeit wird auf europäischer Ebene diskutiert, wie ein Rechtsrahmen aussehen könnte, der eine größere Flexibilität und bessere Anpassung an das komplexe Thema Überwachungstechnologie ermöglichen würde, als die derzeitige Dual-Use-Verordnung. Ein Ansatzpunkt

könnte aus Sicht von Reporter ohne Grenzen die Aufnahme von Überwachungstechnik in die EU-Folterverordnung sein.

Der Verkauf von Überwachungstechnik-Produkten erfolgt häufig in einer Kombination aus Software (Trojanern, Auswertungsprogrammen), Dienstleistungen (Beratungen, Schulungen) und auch Hardware (Server, sog. Appliances, Monitoring Center, spezielle Speichervorrichtungen). Daher sind in aller Regel auch physisch kontrollierbare Elemente vorhanden.

Open-Source-Software wird vom Geltungsbereich des Wassenaar-Abkommens derzeit nicht umfasst, sondern ist explizit von den Regelungen ausgenommen.

12. Die Zahl der Hersteller spezifischer Überwachungs- und Spionagesoftware für die Anforderungen von Behörden ist überschaubar. Welche Möglichkeiten sind umsetzbar, die bei der Anbahnung von Aufträgen bereits Entscheidungshilfen geben könnten? Inwieweit sehen Sie es als notwendig an, dass Aufträge zur Programmierung entsprechender Programme nicht privatwirtschaftlich vergeben, sondern von den Sicherheitsbehörden entwickelt und von unabhängigen Stellen (z.B. BfDI) kontrolliert werden? Teilen Sie die Einschätzung, dass die Offenlegung der Quellcodes im Rahmen der Ausschreibungsbedingungen unerlässlich ist, um die Funktionalität der Programme hinsichtlich einer rechtsstaatlichen Anwendung überprüfen zu können?

Bei der Beurteilung möglicher Lieferanten ist unbedingt die Menschenrechtshistorie der Unternehmen zu prüfen. Haben diese Firmen in der Vergangenheit an problematische Staaten geliefert? Ist möglicherweise eine Hintertür eingebaut, die einen unberechtigten Datenzugriff ermöglichen würde? Die Erfahrungen mit dem ersten Bundestrojaner der Firma Digitask zeigen außerdem, dass unbedingt eine tiefgehende Qualitätskontrolle der Software-Lösungen erfolgen muss – die zunächst eingesetzte Software hatte schwere Mängel in puncto IT-Sicherheit.

Für eine Funktions- und Rechtsfolge-Abschätzung ist eine Prüfung des Quellcodes unerlässlich.

Auch wenn die Behörde des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, BfDI, chronisch unterfinanziert ist, verfügt der Bundesbeauftragte aus Sicht von Reporter ohne Grenzen über die höchste Unabhängigkeit und die größte Kompetenz für eine notwendige Prüfung.

Eine Prüfung durch das Bundesamt für Sicherheitstechnik, BSI, ist aus Sicht von Reporter ohne Grenzen auf Grund der Nähe der Behörde zu den deutschen Geheimdiensten hingegen nicht angebracht.

Eine ausschließliche Prüfung durch externe Akteure wie des Chaos Computer Club, CCC, scheidet an dieser Stelle aus naheliegenden Gründen auch aus.

Eine Quellcode-Prüfung durch ein problematisches Unternehmen wie die Computer Sciences Corporation, CSC, scheidet ebenfalls aus.

13. Überwachungssysteme benötigen neben der Software zum Teil Infrastruktur. Wie hat die Exportkontrolle auf Enthüllungen der jüngsten Zeit bezüglich komplexer Überwachungssysteme und den dafür notwendigen Komponenten reagiert?

Eine allgemeine Regulierung von Hardware-Infrastruktur dürfte nur schwer möglich sein. Bekannt gewordene Rechnungen der Unternehmen zeigen, dass hier häufig Standard-Hardware wie Server zum Einsatz kommen. Ein wichtiger Schritt ist die effektive Kontrolle von Dienstleistungen – vor, während und

nach dem Kauf. Auch laufende Dienstleistungsverträge von Überwachungstechnik-Firmen mit autoritären Ländern sollten unbedingt überprüft werden.

14. Welche Auswirkungen auf die Forschung zur Sicherheit informationstechnischer Systeme hat es durch die Verschärfung der Vorschriften des Wassenaar-Abkommens und der nationalen Exportkontrollen gegeben, insbesondere vor dem Hintergrund der Entwicklung von Maßnahmen gegen Überwachung und das Erforschen und Schließen von existierenden Verwundbarkeiten in IT-Systemen? Wie können Exploits der Öffentlichkeit bekannt gemacht werden (full disclosure), wenn der betroffene Hersteller nicht auf vorherige Hinweise (responsible disclosure) über Sicherheitslücken reagiert hat, ohne gegen rechtliche Vorschriften zu verstoßen?

Das Wassenaar-Abkommen hat zahlreiche, zum Teil hysterische und wenig an den Fakten orientierte Diskussionen unter Sicherheitsforschern entfacht. Bislang liegen jedoch keine konkreten Fälle der Behinderung von Sicherheitsforschern vor. Einige Aufregung erzeugte die Absage des Sponsorings des PWN2OWN-Wettbewerbes in Japan im Herbst dieses Jahres durch die Firma Hewlett Packard. Hewlett Packard begründete den Ausstieg mit der lokalen Implementation des Abkommens. Die Konferenz konnte wie geplant stattfinden, über Probleme für Sicherheitsforscher wurden nicht berichtet.

Ansonsten ist anzumerken, dass die Frage von Full- oder Responsible Disclosure die Exportkontrolle kaum berührt. Probleme für Sicherheitsforscher entstehen an dieser Stelle vor allem durch Unternehmen, die unsouverän auf von dritten gefundene Sicherheitslücken in ihren Produkten reagieren. So erwirkte die US-Sicherheitsfirma FireEye eine einstweilige Verfügung gegen die Sicherheitsforscher der Heidelberger Firma ERNW, die schwerwiegende Schwachstellen in FireEye-Produkten gefunden hatten.

Ein besserer Dialog zwischen Sicherheitsforschern und den zuständigen Exportkontrollbehörden könnte helfen, Vorurteile und Ängste abzubauen.