Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
18(24)087

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

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?**

Auch wenn die meisten Debatten über die ‚demokratiefördernde Wirkung von Digitalisierung und Internet’ maßlos überzogen sind, spielen Informations- und Kommunikationstechnologien in allen Gesellschaften eine wichtige Rolle. Je stärker Gesellschaften von Informations- und Kommunikationstechnologien durchdrungen sind, je wirkungsmächtiger werden Maßnahmen zur Abschaltung, Kontrolle und Überwachung von Kommunikation.

Hierbei ist Ende-zu-Ende Verschlüsselung ein unverzichtbarer Bestandteil von menschlicher Kommunikation, die typischerweise in sensiblen Bereichen wie dem Schutz von Quellen oder medizinischen Daten genutzt wird. Eine stärkere Verbreitung von Ende-zu-Ende Verschlüsselung ist daher ausdrücklich zu befürworten, weil sie im besonderen Maße geeignet ist Informations- und Meinungsfreiheit zu schützen und zu stärken.

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?**

Eine ausführliche Übersicht über die aktuelle Debatte zu diesen Themen sowie mögliche Fortschritte finden Sie hier:
https://cihr.eu/wp-content/uploads/2015/11/Export-Controls-of-Surveillance-Technologies_DEF_BW.pdf

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?**

Eine ausführliche Übersicht über die aktuelle Debatte zu diesen Themen finden Sie hier: https://cihr.eu/wp-content/uploads/2015/11/Export-Controls-of-Surveillance-Technologies_DEF_BW.pdf

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?**

Es liegen hierzu meines Wissens wenig verläßliche Zahlen vor. Auf Grundlage einer kleinen Anfrage an die Bundesregierung (BT 18/2067) haben wir versucht eine vorsichtige Schätzung vorzunehmen:
http://www.zeit.de/digital/datenschutz/2014-09/export-finfisher-gamma-gastbeitrag

Gerade hier ist es die Aufgabe der Bundesregierung für Transparenz zu sorgen. Deutlich mehr Transparenz bei Exportkontrollen ist möglich, wie das Beispiel der finnischen Exportkontrollbehörde zeigt.

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?

In den letzten Jahren hat es deutliche Kritik aus der Sicherheitsforschung an der Definition von ‚Intrusion Software' gegeben (Listenpositionen 4.A.5, 4. D. 4 und 4. E. 1.c bei Wassenaar). Dieser Artikel von Sergey Bratus ist hilfreich um eine Übersicht über relevante Kritikpunkte zu bekommen:
http://www.cs.dartmouth.edu/~sergey/drafts/wassenaar-public-comment.pdf

Darüber hinaus wird die Einbindung von Entwicklungswerkzeugen von 'Intrusion Software' immer wieder kritisiert: https://dymaxion.org/essays/wa-items.html

Grundsätzlich herrscht bei der Definition von ‚Intrusion Software' starke Unklarheit und eine sehr divergente internationale Umsetzung. (siehe zum Beispiel: https://www.eff.org/deeplinks/2015/05/we-must-fight-proposed-us-wassenaar-implementation). Daher ist es die Aufgabe der Bundesregierung, der EU, sowie den EU- und Wassenaar- Mitgliedsstaaten hier für mehr Klarheit und Rechtssicherheit zu sorgen.

Daher könnte eine Überarbeitung der bestehenden Definition im Bereich ‚Intrusion Software' sinnvoll sein.

Im Bereich von Massenüberwachung (Listenposition 5. A. 1. j. bei Wassenaar) ist die Definition relativ eng gefaßt. Siehe hierzu auch https://cihr.eu/wp-content/uploads/2014/06/Uncontrolled-Surveillance_March-2014.pdf sowie https://cda.io/r/ConsiderationsonWassenaarArrangementProposalsforSurveillanceTechnologies.pdf

Schließlich findet im Rahmen der Exportkontrolle weiterhin eine Regulierung von Kryptographie statt. In der Antwort zu Frage 1 wurde bereits deutlich welche wichtige Rolle Ende-zu-Ende Verschlüsselung spielt, diese wird aber weiterhin über das Wassenaar-Abkommen kontrolliert. Eine möglichst starke Liberalisierung der Exportkontrollen ist in diesem Bereich zu befürworten. In Europe könnte dies zum Beispiel durch eine von der Industrie geforderte General Export Authorisation (GEA) für Verschlüsselung gewährleistet werden. Siehe hierzu auch:
https://cihr.eu/wp-content/uploads/2015/11/Export-Controls-of-Surveillance-Technologies_DEF_BW.pdf

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. 4A003b 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?**

Diese Änderungen des Wassenaar-Arrangement sind ein erster wichtiger Schritt. Weitere Änderungen der Kontrolllisten werden unabdingbar sein. Die bestehenden Kontrolllisten werden durch die Mitgliedsstaaten aktualisiert.

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?**

Sofern die Definition von Überwachungstechnologien sinnvoll gefaßt ist, ist die Erweiterung auf den Bereich technische Unterstützung eine sinnvolle regulatorische Maßnahme. Bestehende Debatten über Probleme mit diesen Definitionen finden sich ausführlich in der Antwort auf Frage 5.

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?**

-

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?**

Wie beim ‚VW-Skandal' zu manipulierten Abgaswerten deutlich wird, ist es sehr schwer für eine Regulierungsbehörde ein Produkt ohne Kenntnis des dort eingebauten Quellcodes effektiv zu bewerten. Dies muß zumindest auf Nachfrage und unter Beachtung entsprechender Sicherheitsvorkehrungen möglich sein. In besonders sensiblen Fällen ist auch eine Prüfung durch einen unabhängigen Dritten vorstellbar.

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

-

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?**

Hierzu wäre vor allem eine stärkere Verankerung der Menschenrechte in der Aktualisierung der EG-Dual-use-Verordnung sinnvoll. Dies findet teilweise in den Entwürfen der Europäischen Kommission unter dem Schlagwort ‚Human Security' Eingang in die novellierte Dual-use-Verordnung.

Darüber hinaus sollte der Informationsaustausch zwischen der Europäischen Kommission und den Mitgliedsstaaten, sowie die Exportkontrolle an sich deutlich transparenter gestaltet werden.

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?**

Es ist unerläßlich daß der Staat – sofern er solche Technologien einsetzt – in jedem Fall eine rechtsstaatliche Anwendung sicherstellt. Ohne Zugriff auf den Quellcode ist dies nicht möglich, daher ist eine Überprüfung des Quellcodes zwingend erforderlich.

Darüber hinaus sollte die unabhängigen Stellen, die solche Programme kontrollieren, nicht nur Teil der Exekutiven sein. Es ist durchaus denkbar dass unabhängige, nicht-staatliche Experten als Kontrolleure fungieren und diese von Parlament oder Judikative beaufsichtigt werden.

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?**

Hier können Vertreter des BAFA und des BMWI am sinnvollsten Antworten liefern.

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?**

Siehe die Antwort auf Frage 5 oben.