Deutscher Bundestag
Ausschuss Digitale Agenda

Mitteilung

Berlin, den 8. Dezember 2015

Die 53. Sitzung des Ausschusses Digitale Agenda findet statt am
Mittwoch, dem 16. Dezember 2015, 16:00 Uhr
11011 Berlin, Konrad-Adenauer-Str. 1
Sitzungssaal: PLH E.200

Sekretariat
Telefon: +49 30 227-32612
Fax: +49 30 227-36159

Sitzungssaal
Telefon: +49 227-30269
Fax: +49 227-36295

Achtung!
Abweichende Sitzungszeit!

Tagesordnung - Öffentliche Anhörung

Tagesordnungspunkt 1

Öffentliches Fachgespräch zum Thema:
"Effektivierung der Kontrolle des Exports von Überwachungs- und Spionagesoftware auf deutscher und europäischer Ebene und öffentlicher Auftragsvergabe"

a) **Liste der Sachverständigen**

Ausschussdrucksache 18(24)SB23

b) **Fragenkatalog**

Ausschussdrucksache 18(24)SB24

Interessierte Besucherinnen und Besucher werden gebeten, sich unter Angabe ihres Namens und Geburtsdatums bis zum ***15. Dezember 2015, 17.00 Uhr*** beim Ausschusssekretariat anzumelden: ada@bundestag.de
Bitte bringen Sie Ihren gültigen Personalausweis mit.

Jens Koeppen, MdB
Vorsitzender

Liste der Sachverständigen

Öffentliche Anhörung
am Mittwoch, 16. Dezember 2015, 16.00 Uhr im Saal E.200, PLH

Zum Thema:

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

Herr Prof. Dr. Waidner
Fraunhofer-Institut für Sichere Informationstechnologie SIT

Herr Dr. Sandro Gaycken
ESMT European School of Management and Technology

Herr Prof. Dr. Götz Neuneck
Institut für Friedensforschung und Sicherheitspolitik

Herr Dr. Ben Wagner
Centre for Internet & Human Rights
European University Viadrina

Herr Christian Mihr
Reporter ohne Grenzen e.V.

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?

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?

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?

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?

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?

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?

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?

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?

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?

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?

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?

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?