Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
18(24)86 NEU

Anhörung Ausschuss Digitale Agenda, Deutscher Bundestag 16. Dezember 2015

Entwurf 15. Dezember 2015 : Prof. Dr. Götz Neuneck, Dipl.-Inf. Thomas Reinhold, IFSH[1]

1a. 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 Nutzung eines „offenen, friedlichen, sicheren und stabilen" Internets und verwandter Dienste fördert prinzipiell Demokratie und demokratische Entwicklung durch die Möglichkeit der freien Meinungsäußerung und das Recht auf Informations- und Meinungsfreiheit. Die Unterbindung oder Sperrung dieses Dienstes kann die Informations- und Meinungsfreiheit und insb. die Arbeit von Journalisten und Aktivisten massiv beeinträchtigen und zu kriminellen Akten führen. Gerade in arabischen und afrikanischen Ländern werden mobile Kommunikationsmittel und Internetdienste wie soziale Plattformen (Twitter, Whatsapp) noch deutlich stärker für die persönliche Kommunikation verwendet als in Deutschland. Allerdings hat das zeitweilige Ausschalten des Internet während des Arabischen Frühlings eher zu größeren Protesten als zu einer wirkungsvollen Unterdrückung geführt. Autoritäre Regime neigen nur im Notfall zum Abschalten der Kommunikation, eher aber zu einer Verstärkung der Zensur und damit verbunden zu verstärkter Überwachung missliebiger Gruppen, Personen oder Journalisten etc.

1b. Welche Bedeutung kommt Technologien, die eine durchgehende Ende-zu-Ende-Verschlüsselung von Kommunikation bieten, zu?

Ende-zu-Ende-Verschlüsselung (E2EE) kann im Prinzip die sichere Kommunikation zwischen zwei Partnern durch die Nutzung eines Netzes von nicht sicheren Drittparteien (Providern) ermöglichen. So gesehen kommt der flächendeckenden Einführung diese Standards große Bedeutung zu. Schon die permanente Anzeige von E2EE oder Nicht E2EE könnte zu einer Verbesserung des Nutzerverhaltens führen. Allerdings bieten solche Technologien nur einen ausreichenden Schutz, wenn eine starke und verifizierbare Verschlüsselung verwendet wird. In der Vergangenheit gab es in unterschiedlichen Staaten immer wieder Versuche dies zu verhindern und zwar mittels eines Verbots starker Kryptographie oder mit der Forderung nach dem Zugriffsrecht auf kryptographische "Generalschlüssel" für staatliche Bedarfsträger mit denen auch verschlüsselte Verbindungen entschlüsselt werden können.

2.a. 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.

Die Aufnahme von „IP network surveillance" in das Wassenaar-Abkommen, die Einbeziehung von „Intrusion-Software" in die Dual-Use-Güter Verordnung Nr.428/2009 in die Kategorie 4 und die Entschließung des Europäischen Parlaments vom 8.9.2015 sind ein wichtiger Schritt vorwärts. International gibt es allerdings außer der Rüstungsexportkontrolle bisher kein wirkungsvolles Instrument, um zu verhindern, dass Überwachungstechnologie ÜT (Intrusion software, IS) in die Hand autoritärer Staaten gelangt und zu Menschenrechtsverletzungen missbraucht wird. WA-Mitgliedstaaten müssen ihre Entscheidungen nicht öffentlich rechtfertigen. Das Wassenaar Arrangement (WA) von 1996 ist eine international, nicht-

[1] Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg, IFAR[2] Interdisziplinäre Forschungsgruppe für Abrüstung, Rüstungskontrolle und Risikotechnologien, Beim Schlump 83, 20144 Hamburg

bindende Vereinbarung, dem sich 41 Staaten angeschlossen haben, um den Transfer von konventionellen Waffen und doppelverwendungsfähigen Gütern und Technologien zu kontrollieren, um „zur regionalen und internationalen Stabilität beizutragen“. Schutz der Menschenrechte sind bisher kein zentrales Kriterium, denn einem Hersteller von ÜT müsste zumindest nachgewiesen werden, dass seine Lieferung intentional zur Menschenrechtsverletzung beiträgt. Allerdings kann ÜT auch zur Umgehung von Verteidigungs- und Rüstungseinrichtungen in Computernetzwerken genutzt werden, bei der es auch zu einer Ausschleusung („Extraction“) von Daten oder deren Manipulation kommt. Nur dies wäre WA relevant. Ausgenommen ist dabei öffentlich verfügbare Software („open source“). Zu Fragen wäre, ob nicht auch „Advanced Persistent Threat Software“ und damit zusammenhängende Ausrüstung (wie die sogenannten “Zero day exploits” - also unbekannte Sicherheitslücken, die in aller Regel die Grundlage von Tools für den verborgenen Zugriff bilden) einbezogen werden sollte. Die Dual-Use-Güter Verordnung Nr.4.428/2009 gibt die Möglichkeit, Menschenrechtsverletzungen zu berücksichtigen. Bei nachgewiesenen Verletzungen könnten die entsprechenden Länder auf eine ständig zu überprüfende Länderliste gesetzt werden.

2b. Welche Rolle hat die Bundesregierung hierbei eingenommen?
Die Bundesregierung hat die Implementierung im Rahmen des WA durchgeführt und das BAFA mit der konkreten Umsetzung betraut. Zu verstärken wäre die „Verbesserung der Awareness“ der Hersteller, die Analyse und Klassifikation der Fähigkeiten von Infiltrationssoftware und ev. auch die Einführung einer Meldepflicht bzw. die Kennzeichnung von Hardware Komponenten. Technisch interessant ist auch die Verpflichtung bei IS den Einbau von Log-Dateien und Telemetriedaten an eine zu zertifizierende Stelle verpflichtend vorzusehen. Interessant wäre auch zu wissen wie in Deutschland und in Europa der Handel mit Sicherheitslücken geregelt wird. Das Wissen um Sicherheitslücken ist zunächst kaum zu kontrollierendes Wissen („intangible“). Erst der „Exploit“ wird konkret in Software verwendet. Mindestens ein Händler von Exploits (Die ursprünglich französiche Firma „Vupen“) ist 2014 ins Ausland verzogen, um sich den Regularien des Wassenaar-Abkommens zu entziehen.

3a. 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?

Überwachungstechnologie (Hardware/Software) sind alle technischen Maßnahmen, bei der unter Ausnutzung des elektromagnetischen Spektrums Daten und Informationen aus einem Rechner, einem netzfähigen Gerät oder einem Netz extrahiert werden bzw. bei denen auf dem Gerät laufende Prozesse oder das Systemverhalten überwacht wird. Dies kann drahtlos, durch Kontakt oder durch die Einschleusung eines Algorithmus erfolgen und sich auf E-Mail-Verkehr, Audio- oder Videodaten, Rohdaten etc. Beziehen. Auch die reinen internen Daten, die für Kommunikations- und Datendienste benötigt werden wie die Identifikationsnummern von Geräten, Standortdaten, Verbindungen zu Mobilfunkanbietern und deren zeitliche Protokollierung sind bereits im Sinne von Überwachung relevante Informationen.
Spionagesoftware ist ein Programm, das Daten/Informationen eines Computernutzers ohne dessen Wissen oder Zustimmung, an Dritte sendet. Dritte können Behörden, Firmen, Wirtschaftsunternehmen etc. sein. Voraussetzung ist, dass ein Computersystem widerrechtlich infiltriert werden kann und die jeweiligen Schutzmaßnahmen umgangen werden. Eine eindeutige technische Zuordnung von Soft-oder Hardware-Elementen und Menschenrechtsverletzung oder Repression ist nicht möglich, sondern kontextabhängig. Technisch schwierig ist es auch den Unterschied von „intrusion software“ und „intrusion protection software“ zu definieren.

3b. Inwieweit bedarf es hierzu beispielsweise eines bundesweiten Registers, in dem Korruptions- und andere Wirtschaftsdelikte eingetragen sind?

Es ist dem Gutachter unklar, was hier gemeint ist, da nicht ersichtlich ist, worin der Zusammenhang mit ÜT besteht. Generell sinnvoll ist natürlich ein für die Öffentlichkeit einsehbares Register zu haben, in der Firmen stehen, die durch kriminelle Taten und Transfer aufgefallen sind. Wie unter Punkt 2b. genannt, wäre eine Meldepflicht oder eine verbindliche Kennzeichnung sinnvoll, um regionale Häufungen, Verstöße oder Missbrauch verfolgen zu können. Eine weitere Möglichkeit wäre Herstellerfirmen vorab zu zertifizieren, die spezifische ÜT-Software vertreiben. Die Zertifizierung könnte durch einen Firmenverantwortlichen (im Vorstand, Geschäftsführung) erfolgen, der haftbar gemacht würde, wenn ein illegaler Export erfolgt. Solch ein Verfahren ist bei Sicherheitsdienstleistern bereits eingeführt.

3c. Sind Sie der Ansicht, dass die Kontrolle von Exporten entsprechender Technologien zur Überwachung und Sperrung von Telefon- und Internetkommunikation heute effektiv geschieht?

In erster Linie ist entscheidend, welche Kriterien für Effektivität herangezogen werden: Staatliche?, technische?, wirtschaftliche? Menschenrechtsgesichtspunkte? Aussen- und rechtspolitische Kriterien?

Die unmittelbare Wirksamkeit muss zunächst das BAFA beurteilen können bzw. für eine allgemeine Einschätzung wäre eine Studie der Praxis z.B. durch das Büro für Technologiefolgenabschätzung des Deutschen Bundestages (TAB) zum Vergleich realer Handelsströme und vorhandener Menschenrechtsverstöße weiterführend. Da es kein verbindliches internationales Regime gibt und reale Umgehungsmöglichkeiten (Export über Drittstaaten, unvollständige Mitgliedstaaten des WA, unklare Definitionen, politische Kontextabhängigkeit) ist eine effektive, globale Kontrolle der ÜT nicht gegeben. Trotzdem kann ein Staat, in dessen Land ein Hersteller von ÜT wirtschaftlich tätig ist, durch seine Exportregelungen, ein politisches Signal aussenden oder durch die Einigkeit von Wirtschaftsräumen einen erheblichen Effekt haben.

3d. Wo sehen Sie Mankos in bestehenden Regulierungsregimen auf deutscher, europäischer und internationaler Ebene?

Auf deutscher Ebene: klare Definition, Effektivität, Outreach,
Auf europäischer Ebene: Koordinierung und Harmonisierung
Auf internationaler Ebene: kein verbindliches internationales Regime inkl. Verifikation und Rechtsdurchsetzung zur Kontrolle des Handels von intrusion software.

Es gibt zwei mögliche Wege: Klären, 1. ob ein Empfänger vor dem Hintergrund der deutschen oder europäischen Politik legitim ist oder nicht und 2. wie eine effektive Implementierung erfolgen kann. Im ersten Fall wären Kriterien zu entwickeln. Eine Güter/Empfängerländer-Matrix könnte entwickelt werden. So könnte besonders intrusive Software an demokratische Staaten gehen, während Handy-ÜT liberaler gehandhabt wird, aber auch nicht an extrem autoritäre Regime geliefert wird.

4a. Können Sie abschätzen, wie groß der Markt (Handelsvolumen, Mitarbeiterzahl etc.) deutscher und europäischer Anbieter, die entsprechende Programme und Technologien anbieten, in etwa ist?

Uns liegen dafür keinen ausreichenden Daten vor. Die Zahl der Hersteller von Infiltrations Software dürfte aber begrenzt sein. Eine Einschätzung wird auch dadurch erschwert, dass Anbieter ihre Produkte oft eher als Sicherheits-Hilfsmittel und nicht direkt als Spionage-Werkzeuge vermarkten.

4b. 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?

Einzelfälle sind durch die Presse bekannt geworden, so der Export von FinFisher nach Bharain oder der Produkte der italienischen Firma “Hacking Team” zu deren Kunden auch staatliche Institutionen in Marokko, Kasachstan, Aserbaidschan und dem Sudan gehören.

5a. 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?

Der europäische und nationale Rechtsrahmen zur Kontrolle des Exports von Überwachungs- und Spionagesoftware ist recht löchrig. Entscheidend dürfte hier die Handhabung der Praxis, die Koordination und die Überprüfung deren Effektivität durch die Ursprungsländer sein.

5b.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?

Aufgenommen werden könnten wie unter 2 genannt die „advanced presistent threat Software“. Bei sensitiver Technologie gibt es die Möglichkeit der Wahrnehmung der Eigenverantwortung (d.h. Nichtlieferung an menschenrechtlich problematische Staaten, Organisationen, Behörden oder Individuen), die Pflicht zur Endverbleibserklärung mit einem Vetorecht oder die Kennzeichnung von Software/Hardware. Die Gutachter haben keinen Einblick in die tägliche Praxis.

6a. 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?

Eine Einschätzung ist abhängig von den zugrundegelegten Kriterien. Eine hundertprozentige Kontrolle ist sicher nicht möglich. Wie schon ausgeführt ist der Kern des WA die Aufrechterhaltung von „internationaler und regionaler Stabilität“, also eher sicherheitspolitisch als menschenrechtlich legitimiert. Es wäre zu prüfen, inwieweit das WA interpretiert werden kann bzgl. der Kontrolle von ÜT, die zu international verbotenen Handlungen wie z.B. Angriffskriege, schwere Menschenrechtsverletzungen, Völkermord, ethnische Diskriminierung führen.

6b. 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 Grafik-

karte.) Wie werden die Kontrolllisten des Wassenaar-Arrangements insgesamt aktuell gehalten und inwieweit ist eine (fortlaufende) Evaluierung und Erweiterung dieser Kontrolllisten notwendig und möglich?

Die WA-Listen werden jährlich neu diskutiert und aktualisiert. Die Exportkontrolle bei Superrechnern ist nicht erfolgreich gewesen. China ist z.B. nicht Mitglied, verfügt aber über diverse Superrechner. Die kontinuierliche Evaluierung und Erweiterung der Kontrolllisten ist trotzdem notwendig, da die technologischen Fortschritte rasant und oft sprunghaft erfolgen. Rechenleistung, Speicherkapazitäten und Durchsatzleistungen von Netzwerktechnik wächst sehr schnell. Dies gilt auch für die Bandbreite von Internet-Anschlüssen, eine zeitnahe Anpassung der vereinbarten Grenzwerte ist hier geboten.

---

7. Die Bundesregierung hat im Sommer dieses Jahres mit der 4. Änderungsverordnung zur Außenwirtschaftsverordnung (AWV) Genehmigungspflichten für die Ausfuhr insbesondere von Monitoring-Systemen 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?

Dies sind richtige Schritte, um sich nicht nur auf die Technologie an sich zu konzentrieren, sondern auch auf die dazu notwendigen Dienstleistungen.

---

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?

Mit recht benannt werden: Hermesbürgschaften, Messeauftritte, Bewerbung von Produkten etc. Diese bilden nicht nur Indikatoren der jeweiligen Firmenaktivitäten sondern auch Entscheidungspunkte. Dort wo massive Menschenrechtsverletzungen nachgewiesen sind, sollten keine Hermesbürgschaften erfolgen und die Firmen aufgefordert werden keine ÜT zu liefern. Auch sollten zu diesem Zweck verbindliche Länderlisten geführt werden. Exploits und Sicherheitslücken werden oft auch “schwarz” gehandelt. Firmen könnten im Sinne der Transparenz offen legen, mit welchen Vertragspartnern sie arbeiten. Darüber hinaus könnte die Soft- und Hardware durch unabhängige Experten gesichtet und bewertet werden. Begutachtete und genehmigte Software könnte dann ähnlich wie bei Siegeln mit kryptografischen Mitteln “markiert” werden (Thema “Hashes”) um sicherzustellen dass die Software, die verkauft wird auch jene ist, die kontrolliert wurde. Auch bei der staatlichen Förderung von IT made in Deutschland und der propagierten Herausforderungen im Rahmen der sog. “Industrie 4.0” müssen menschenrechtliche Belange trotz legitimer wirtschaftlicher Interessen der deutschen Regierung abgewogen werden.

---

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?

Die Gefahr besteht in der Tat. Es sollten keine Verträge gemacht werden, bei denen kein vollständiger Einblick in den Quellcode gewährt wird und dieser durch Sachverständige be-

gutachtet wurde. Für sensible und sicherheitsrelevante Bereiche sind dringend zertifizierte Audits der Hard- und Software angeraten sowie eventueller späterer Erweiterungen und Sicherheitsaktualisierungen.

---

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

Gerade dies wäre die Ausgabe des WA. Ein Rüstungsexportmonitoring durch die EU und die Mitgliedstaaten könne hier Akkumulationen oder problematischen Handel aufdecken. Die internationale Diplomatie auf der UN-Ebene oder der OSCE sollte verstärkt werden, um ein digitales Wettrüsten zu verhindern. Verbindliche Begriffsdefinitionen, vereinbarte Normen und "best practices" wären ebenso ein wichtiger Schritt vorwärts wie erste umgesetzte Vertrauensbildende Maßnahmen. International ist zu allererst anzustreben, die jeweiligen Exportpolitiken zu vereinheitlichen, um die schärfen Exportpolitiken einzelner Staaten zu umgehen. Möglich wäre dies durch die Ausweitung des Arms Trade Treaty, da dieser bisher nur auf bestimmte Rüstungsgüter und Munition beschränkt ist. Eine andere Möglichkeit wäre eine Einbeziehung in die Menschenrechtskonvention.

11a. 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?

Durch den ausgeprägten Dual-Use-Charakter dieser Technologien kann dies nur durch die Kooperation staatlicher Stellen mit den Herstellerfirmen bzw. durch Eigenverantwortung der Hersteller und Programmierer sichergestellt werden. Eine andere Möglichkeit ist die Erstellung einer Güter/Empfängerländer-Matrix (siehe Punkt 3d)

11b. 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?

Diese Fragen können nur unmittelbar mit der Kontrolle befasste Behörden also z.B. das BAFA beantworten. Schon heute gibt es ja auch genehmigungspflichtige Fertigungsunterlagen, die man per email veschicken kann. Entscheidend sind bei einer Verletzung der Regularien die Strafandrohung und der Reputationsverlust bei Verstößen gegen die Vorschriften. Die Zertifizierung oder Aberkennung derselben könnte hier helfen. Es sind keine Fälle von aktiven Open-Source-Projekten bekannt, die speziell für die Überwachung von Kommunikation entwickelt werden. In aller Regel sind Open-Source-Projekte, gerade aufgrund ihres öffentlichen Charakters und der vollständigen Einsehbarkeit des Quellcodes, von starker moralischer Integrität geprägt. Dennoch sollten hier die gleichen Regeln gelten, geht es doch hier um den potentiellen oder tatsächlichen Missbrauch und nicht um die ursprüngliche Intentionen der Entwickler/Hersteller.

---

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?

Entscheidungshilfen könnten sein: die Erstellung von verbindlichen Länderlisten, die Veröffentlichung von bekannt gewordenen Menschenrechtsverletzungen. Die Einschätzung, dass die Offenlegung der Quellcodes im Rahmen der Ausschreibungsbedingungen unerlässlich ist, wird vollumfänglich geteilt.

---

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?

Diese Frage können nur unmittelbar mit der Kontrolle befasste Behörden also z.B. das BAFA beantworten.

---

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 betroffenen Hersteller nicht auf vorherige Hinweise (responsible disclosure) über Sicherheitslücken reagiert hat, ohne gegen rechtliche Vorschriften zu verstoßen?

Hinweis Exploits: siehe 2b.

Für die Forschung aber auch für Hersteller von IT-Sicherheits-Produkten oder die Anbieter von IT-Diensten ist die Arbeit mit “echten” Angriffsszenarien wie bspw. sogenannten Penetrations-Werkzeugen unumgänglich. Dies bedeutet im Einzelfall auch die Notwendigkeit des Wissens über aktuelle Angriffsmöglichkeiten und Sicherheitslücken. Wie in der Frage angemerkt können Firmen, die Wissen über Sicherheitslücken haben oder erwerben, dieses jedoch nicht veröffentlichen (full disclosure) auch Teil des Problems sein. Eine Verbesserungen der Situation können hier die Meldepflichten auf nationaler und internationaler Ebene von Sicherheitsproblemen sein. Für die Meldung von Sicherheitslücken von Produkten durch Dritte könnten bspw. “blinde Briefkästen” bei unabhängigen nationalen Institutionen eingerichtet werden.

Götz Neuneck, Dec 15, 15, 7:01 PM