Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
18(24)85

DIGITAL SOCIETY INSTITUTE BERLIN

Stellungnahme

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“

von Dr. Sandro Gaycken
Direktor, Digital Society Institute,
ESMT Berlin

Der Befragte nimmt zu den vom Ausschuss gestellten Fragen wie folgt Stellung.

Zu Frage (1.1): Welche Gefahren können durch Überwachungstechnologien in autoritären Ländern entstehen?

Die Überwachung und das gezielte Ausspionieren Oppositioneller und Journalisten durch autoritäre Regime ist in Folge der Digitalisierung zu einem gewichtigen Problem herangereift. Digitale Technologien haben in diesen Ländern inzwischen stark anti-demokratische Wirkungen, indem sie deren Regime zu totaler Kontrolle aller digitalen oder digital berührten Lebensbereiche ermächtigen. Das Internet ist dort zu einer Überwachungs- und Manipulationsmaschine geworden. Dieser vermutlich vielfach irreversible Umbau des Internets in diesen Ländern hat gravierende Bedeutungen für Demokratie, Rechtsstaatlichkeit und internationale Sicherheit, indem das Internet in autoritären Regimen eine vielschichtige und starke Stabilisierung der dortigen Regierungen bewirkt und die meisten Ansätze und Vektoren für regionale oder internationale Einwirkungen zu Demokratisierung frühzeitig identifiziert und beseitigt werden können. Kurz gesagt: Internet stabilisiert autoritäre Herrschaft.

Dieses Verhältnis steht im harten Gegensatz zu naiven und utopistischen Annahmen über die demokratiefördernde Wirkung von Digitalisierung und Internet in autoritären und totalitären Regionen, denen der Autor an dieser Stelle explizit widersprechen möchte. Der arabische Frühling muss rückblickend als Einzelphänomen gewertet werden. Die autoritären Regime waren zu jenem Zeitpunkt nicht bereit für eine Beherrschung digitaler Medien. Da diese Beherrschung aber letztlich eine Frage des Geldes ist, zudem keine Frage großen Geldes, muss inzwischen davon ausgegangen werden, dass diese Regierungen das Internet in ihren Ländern in eine Überwachungsmaschine umgebaut haben oder im Umbau begriffen sind. Regierungen sind aufgrund der Asymmetrie der Mittel und des Zugriffs auf Telekommunikationsstrukturen klar im Vorteil in dem Machtkampf der Beherrschung von IuK-Technologien. Ausnahmen bestehen nur für einige wenige Technologien wie etwa TOR und der TOR-Browser, die von einer aktiven und professionellen Community betrieben und weiterentwickelt werden. Auch bei diesen Technologien bestehen allerdings von Zeit zu Zeit Lücken, zudem werden „unknackbare“ Technologien in autoritären Regimen schlicht verboten und abgestellt. Für eine meist gute Beherrschung der Überwachung spricht auch der Umstand, dass viele dieser Länder Internet inzwischen explizit erlauben und viele Eigenentwicklungen im Feld Social Media freistellen.

Für autoritäre Länder gilt folglich: Das Internet ist von einem Mittel der Freiheit zu einem Mittel der Unterdrückung verkommen. Demokratiefördernde Wirkungen lassen sich allenfalls noch in den bestehenden und gefestigten demokratischen Rechtsstaaten attestieren.

Zu Frage (1.2): Welche Bedeutung kommt der Ende-Zu-Ende-Verschlüsselung in diesem Zusammenhang zu?

Das Potential der Verschlüsselung zum Schutz von Oppositionellen und Journalisten und Quellen wird allgemein falsch bewertet. Es ist nicht davon auszugehen, dass Ende-Zu-Ende-Verschlüsselung einen hinreichenden Schutz entfalten kann. Ein Hauptgrund hierfür ist erneut die Asymmetrie der Mittel zwischen autoritären Regierungen und Oppositionellen und Journalisten. Während autoritäre Regierungen meist auf hochprofessionelle und von Alliierten unterstützte Codebreaker zugreifen können, die auf dem Stand von Forschung und Technik arbeiten, denen Werkzeuge, Nachrichtendienste und große Teams zur Verfügung stehen, müssen Oppositionelle und Journalisten in der Regel als deutlich benachteiligte Laien mit diesen Technologien arbeiten. Mit dieser Asymmetrie entstehen drei unlösbare Probleme, die einer Nutzung widersprechen:

(1) Laien können nicht auf dem Stand der wissenschaftlichen Diskussion operieren und wissen daher nicht zu jedem Zeitpunkt, welche Formen der Verschlüsselung aktuell als sicher zu bewerten sind. Ohne dieses Wissen besteht Gefahr, dass eine unsichere Variante gewählt wird. Die Auswahl einer unsicheren Variante als vermeintlich sichere Variante kann durch nachrichtendienstliche Operationen gestützt werden, wie etwa durch das Platzieren vermeintlicher „Geheimtipps der Community“ in Webforen.
(2) Laien können fortgeschrittene Kryptografieprodukte meist nicht vollkommen fehlerfrei implementieren und betreiben. Kleine Fehler können aber bereits einen vollständigen Verlust der gesicherten Kommunikation bedeuten und ganze Netzwerke von Personen kompromittieren.
(3) Autoritäre Nachrichtendienste kennen viele Seitenkanäle und Zusatzwege, um Verschlüsselung zu umgehen und zu unterwandern. Ein Beispiel ist eine Infektion des Host-Systems, so dass dort alle Nachrichten in Klartext mitgelesen oder mitgehört werden können. Sofern diese Wege nicht alle vollständig bekannt und gesichert sind, ist vom Gebrauch einer Verschlüsselung abzusehen.

Da alle drei Probleme für Laien unlösbar sind, ist die Verwendung von Verschlüsselung durch Laien in autoritären Regimen als hochgefährlich und in keiner Weise empfehlenswert einzuschätzen.

Zusammenfassend zu den Fragen aus (1) soll damit festgehalten werden, dass sich für die Politik und insbesondere für die Außenpolitik eine erste Empfehlung ergibt, nämlich eine Umkehr der Empfehlungsrichtung. Bislang wurden Digitalisierung und Internet in autoritären Regimen empfohlen, mit der Einschränkung, durch Maßnahmen wie Verschlüsselung auf Sicherheit zu achten. Da jedoch diese Maßnahmen inzwischen nicht mehr als zuverlässig und zudem als für gegen professionelle staatliche Organisationen kämpfende Laien zu voraussetzungsreich betrachtet werden müssen, sollte vor der Nutzung digitaler Technologien in autoritären Regionen ausschließlich gewarnt und abgeraten werden.

Zu Frage (2): Welche Fortschritte sind erreicht worden, um der Bedeutung entsprechender Technologien Rechnung zu tragen und welche Rolle hat die Bundesregierung eingenommen?

Die Erweiterung des Wassenaar Arrangements ist ein wichtiger und wertvoller Schritt gewesen. Kritikpunkte aus der IT-Sicherheitscommunity waren unbegründet. Der Kontrolle des Exports der einen Umbau des Internets zu einer Überwachungsmaschinerie ermöglichenden Werkzeuge kommt immense politische und moralische Bedeutung zu. Insbesondere in der aktuellen Phase eines Erstinteresses vieler Regime und der technischen Ausdifferenzierung und Reifung verschiedener Produktvarianten kann noch viel Einfluss auf mögliche Ausgestaltungen genommen werden.

Allerdings muss auch klar gesagt werden, dass Exportkontrollen allein den Umbau des Internets nicht beherrschbar machen, selbst dann nicht, wenn sie in hohem Maße effektiv sind. Vier Ursachen spielen dabei eine Rolle:

(1) Erstens und wie der Autor später noch genauer erläutern wird, sind viele neuere Verfahren der Überwachung und des Ausspionierens bereits unabhängig von dezidierten Werkzeugen und können durch einfache Kombinationen aus regulativen Schritten und gängigen Datenanalyseverfahren erreicht werden.

(2) Zweitens ist die Grenze zur sogenannten „Lawful Interception“, dem legitimen Beobachten Krimineller, zur ausgeweiteten Überwachung politischer Aktivitäten technisch und operativ viel zu fließend, um dauerhaft und flächendeckend eine Proliferation entsprechender Technologien und Techniken zu verhindern. In der Struktur der Technologien lässt sich in den meisten Fällen kein „Democracy-by-Design“ einbauen, mit dem sich eine Modifikation des Zielspektrums auf unliebsame politische Ziele architektonisch verhindern ließe.

(3) Drittens wächst die internationale Toleranz für stärkere Internetüberwachung infolge von Cyberkriminalität, Cyberterror und Cyberwarfare. Viele Staaten sitzen hier dem aus der IT-Sicherheitsindustrie im Rahmen des Trends der „Threat Intelligence“ geförderten Irrglauben auf, dass sich diese Sicherheitsprobleme mit stärkerer Internetüberwachung lösen ließen. Für einen entsprechenden nachhaltigen Zusammenhang gibt es keinerlei belastbare Nachweise. Vielen Regimen dient der Scheinzusammenhang aber als hilfreiche Ausrede, um in scheinbarer Sorge um die Sicherheit in Wirklichkeit totalitäre Kontrolle zu implementieren. In diesem Kontext ist insbesondere auf das internationale Einwirken der sogenannten Shanghai-Gruppe, geführt aus Russland und China, hinzuweisen. Diese Gruppe bemüht sich seit Jahren intensiv um eine höhere Toleranz für eine Variante von Cybersicherheit, die dort als „Informationssicherheit“ geführt wird und die gemäß russischem und chinesischem Sicherheitsdenken Überwachung und Zensur unliebsamer und möglicherweise feindlicher Elemente und gefährdender „Propaganda“ einschließt.

(4) Viertens schließlich ist darauf hinzuweisen, dass harte Exportkontrolle nur unter „like-minded“ Staaten funktionieren, aber nicht außerhalb dieser Staaten und

ihrer Einflusssphären. Bereits jetzt entwickeln aber viele autoritäre Staaten ihre Überwachungssoftware selbst und importieren und exportieren untereinander. Auch wissenschaftlich ist spürbar, dass etwa im asiatischen Raum Forschung und Entwicklung zu „lawful interception" stark angezogen hat und folglich dort stark gefördert wird. Autoritäre Staaten werden also in dieser Frage schon in Kürze unabhängig von den demokratischen Staaten agieren können.

Aufgrund dieser Schwierigkeiten ist bereits unabhängig von einer Effektivierung der Exportkontrollen zu betonen, dass die Verhinderung totalitär stabilisierender Internetumbauten eine herausragende und vielschichtige Aufgabe der Außenpolitik ist und bleiben wird, der nicht nur mithilfe des Werkzeugs der Exportkontrolle beizukommen ist, sondern der deutlich umfangreichere außenpolitische Bemühungen gewidmet werden müssen.

Ein stärkeres Engagement Deutschlands wäre in diesem Kontext außerordentlich hilfreich. Da Deutschland von vielen Ländern als authentischer Akteur für digitale Freiheit und Menschenrechte wahrgenommen wird und gleichzeitig hohe politische Kraft hat, wäre es ein idealer Botschafter für Demokratie und Freiheit im Internet. Bis vor Kurzem haben die USA diese Rolle noch ausgefüllt, die allerdings mit den Enthüllungen Edward Snowdens nicht länger als glaubwürdig agieren können, was ein Vakuum an dieser Stelle hinterlassen hat, von dem vor allem autoritäre Regime profitieren. Die deutsche Außenpolitik wäre also in mehrfacher Hinsicht berufen, hier stärker aktiv zu werden.

Vor diesem Hintergrund ist zu beanstanden, dass das Auswärtige Amt den Posten des „Cyber-Botschafters" wieder eingespart hat. Eine Wiedereinrichtung des Postens und eine deutliche Verstärkung des dazugehörigen Stabes sei an dieser Stelle als besonders dringlich angemahnt, dazu die Aufnahme einer aktiven und führenden Rolle bei der Verteidigung der digitalen Menschenrechte ebenso wie umfangreichere Informationsbeschaffung und Unterrichtung zu diesem Thema in den Bereichen Außen- und Sicherheitspolitik.

Zu den Fragen (3), (5) und (11): Wie kann sichergestellt werden, dass möglichst alle relevanten Soft- und Hardwarelemente, die zur Verletzung von Menschenrechten und innerer Repression genutzt werden können, abgedeckt und in der Definition enthalten sind? Wo sehen Sie Mankos in bestehenden Regulierungsregimen? Wie gestaltet sich die Kontrolle der Ausfuhr? Reicht die Berücksichtigung von Technologien zur Entwicklung von Intrusion Software aus? Welche anderen Hard- und Softwaretechnologien könnten oder sollten aufgenommen werden? Wie kann möglichst effektiv verhindert werden, dass entsprechende Export-Kontrollregime negative Auswirkungen auf Programme und Technologien haben, die man zu sanktionieren nicht beabsichtigt?

Die Definition ist gut getroffen, bedarf aber verschiedener Verbesserungen und Erweiterungen, um lückenlos zu werden. So sind unter anderem einzubringen:

(1) Besitz und Verkauf von Schwachstellen:
Schwachstellen in Software dürfen nicht an autoritäre Regime gelangen, da diese dort direkt zu Überwachungszwecken umgesetzt werden können. Die gesamte Regulierungen zu Softwareschwachstellen ist ohnehin eine unglückliche Baustelle

und bedarf dringend der gesetzlichen Aufmerksamkeit und Revision, eingeschlossen das Patching und Security Management.

(2) Besitz und Verkauf fertiger Exploits:
Fertige Cyberangriffe sind derzeit vom Wassenaar Arrangement ausgenommen, lediglich die Werkzeuge zu ihrer Erstellung sind aufgegriffen. Dies ist unzureichend, da bereits fertige Angriffe ungehindert gehandelt werden können.

(3) Dienstleistungen:
Dienstleistungen sind derzeit ebenfalls ausgenommen, können aber selbst ohne Nutzung der entsprechenden Tools gleiche Wirkungen oder sogar schlimmere Wirkungen entfalten (etwa der Support von Überwachungstechnik wie durch Intech, ein Training einer Überwachungseinheit in einem autoritären Land, Hilfe bei Entwicklung oder die gezielte Entwicklung eines Angriffs auf Oppositionelle). Dienstleistungen müssen folglich ebenfalls erfasst und reguliert werden.

(4) Forschung und Entwicklung zu Lawful Interception, Schwachstellen und Exploits:
Ein besonders offener Punkt ist zudem die offene Forschung zu entsprechenden Technologien oder den zugrundeliegenden Schwachstellen. Diese ist nicht reguliert und sorgt oft für einen unabsichtlichen Knowhow-Flow aus den hochentwickelten industrialisierten Ländern in weniger entwickelte autoritäre Regime, die folgend unbeeindruckt von Exportkontrollen eigene Entwicklungen angehen können.

Darüberhinaus muss dringend beachtet werden, dass die Praxis der Überwachung in den letzten Jahren fortgeschritten ist und bereits in weiten Teilen nicht mehr von den Wassenaar Formulierungen zu Network Intrusion und Network Surveillance Produkten abgedeckt wird. Die Wassenaar-Definition ist in dieser Hinsicht leider schon wieder in großen Teilen veraltet.

Für eine echte Effektivierung der bestehenden Exportkontrollen müssen dringend die taktische Entwicklung und neue Trends zur Erreichung maximaler Überwachung anerkannt und regulativ umgesetzt werden.

Zunächst einige Hinweise zur taktischen Entwicklung. Die Überwachung unliebsamer Oppositioneller und Journalisten lässt sich bereits seit längerer Zeit klar nach verschiedenen taktischen Phasen und Partikularinteressen trennen, die unterschiedliche Ansätze und Technologievarianten zulassen. Als Gebrauchskontexte mit unterschiedlichen Fragestellungen lassen sich erkennen:

1. *GK1. Identifikation und Implementierung oder Nutzung von Datenquellen*: Woher kommen die Daten? Wo gibt es Daten? Wie kommt der Überwacher an diese Daten heran? Wie kann der Überwacher mehr Daten generieren?

2. *GK2. Erkennung von Erstindikatoren*: Wie kann der Überwacher möglichst viele (und am besten alle) Daten erhalten? Wie kann er aus einer Vielzahl heterogener Daten kritische und interessante Informationen gewinnen?

3. *GK3. Analyse und Kontextualisierung von Daten*: Was bedeuten verschiedene Arten von Daten? Was will der Überwacher alles wissen? Wie hängen unterschiedliche

Daten zusammen? Welche Daten lassen sich zu welchen Informationstypen clustern?

4. *GK4. Abbilden von sozialen Netzwerken*: Welche Personen gehören zusammen? Wie lassen sich Hierarchien und organisatorische und Machtstrukturen abbilden? Wer ist in welcher Weise für ein Netzwerk funktional? Wie können diese Funktionen beeinträchtigt werden? Wo können menschliche Quellen eingeschleust oder angeworben werden?

5. *GK5. Profiling von Personen oder Kontexten aus Daten*: Was genau macht eine Person oder einen spezifischen Inhalt, ein Thema, einen Kontext genau aus? Was und wer gehört alles dazu? Wo sind die Stärken und Schwächen? Was sind typische Muster?

6. *GK6. Infiltration von sozialen Netzwerken*: An welchen Stellen kann der Überwacher technisch oder operativ ideal in Netzwerke eindringen? Welche Form des Eindringens wird am ehesten akzeptiert? Was sind die Bedingungen für Akzeptabilität? Wie kann er sich in den Netzwerken weiter bewegen? Welche Taktiken stehen zur Verfügung und wie können weitere Infiltrationen unterstützend wirken?

7. *GK7. Gezielte Überwachung ausgesuchter Zielpersonen*: Wie kann der Überwacher ausgesuchte Zielpersonen möglichst lückenlos beobachten? Wie findet er sie unter Pseudonymen, in Anonymisierung und in codierten Kommunikationen? Welche Geräte stehen für eine lückenlose Überwachung zur Verfügung? Wie kann das Vertrauen der Zielpersonen in diese Geräte verstärkt werden?

8. *GK8. Manipulation von Personen und Kontexten*: Wie kann der Überwacher Personen und Kontexte manipulieren? Zu welchen Handlungen möchte er sie bringen? Welche Inhalte oder Strukturen stehen für taktische Manipulationen zur Verfügung? Wie können kausale Wirkungen der Veränderungen von Inhalten und Strukturen vorhergesagt werden? Wie können Manipulationen authentisch sein? Welche Wirkungen werden die folgenden Handlungen im Netzwerk haben? Wie gut müssen bestimmte Handlungen taktisch synchronisiert werden können?

9. *GK9: Datenbasierte Vorhersage möglicher Entwicklungen*: Wie können die Entwicklungen von Personen und Kontexten vorhergesagt werden? Was wird mit dem Netzwerk in den nächsten Monaten geschehen? Was ist wahrscheinlich, was ist weniger wahrscheinlich? Wie können wahrscheinliche und ungünstige Entwicklungen frühzeitig vermieden werden?

Es ist klar erkennbar, dass dieses inzwischen existierende Spektrum der Optionen je andere Technologien, Dienstleistungen und Verfahren erforderlich macht oder anempfiehlt. Viele dieser Technologien, Dienstleistungen und Verfahren werden nicht oder nicht eindeutig aus dem Wassenaar-Arrangement abgedeckt werden.

In dieser Hinsicht sind auch verschiedene neue technische und regulative Trends bemerkenswert, auf die nun eingegangen werden soll. Drei Trends sind besonders bemerkenswert: (1) die Vervielfältigung der Quellen, (2) eine starke Verbesserung der Datenanalysen sowie (3) die stärkere Verbindung regulativer und technischer Ansätze

und der damit verbundene Wandel der Bedeutung vieler IT-Basistechnologien zu Dual Use-Technologien mit hohen Überwachungsfunktionen.

(1) Die Vervielfältigung der Quellen kommt durch das Entstehen neuer und die erhöhte Verbreitung bestehender digitaler Technologien in unterschiedlichen Lebensbereichen zustande. In den ärmeren autoritären Regimen spielen etwa Smartphones bereits eine essentielle kommunikative und wirtschaftliche Rolle und bewirken im Gegenzug eine Ausstattung der Bevölkerungen mit abhörbaren, ausforschbaren und lokalisierbaren Geräten, die meist von den Regimen auch entsprechend umfunktioniert werden. In reicheren autoritären Regimen dagegen entstehen seit Jahren eigene Ökosysteme digitaler Dienstleistungen und Produkte, die oft bereits ab Werk oder durch staatlich verabreichte oder verordnete Angriffe (staatlich breit verordnete Updates mit Trojanern sind bereits bekannt geworden) umfangreich mit Überwachungsmöglichkeiten ausgestattet werden. In diesem Kontext sind vor allem die zahlreichen digitalen Dienstleistungen auf Basis privater oder beruflicher Daten im Feld der Social Media bedenkenswert. Sie stellen eine Vielzahl leicht zugänglicher und verwertbarer Daten über große Teile der Bevölkerungen zur Verfügung, die ein autoritärer Staat leicht abgreifen und nutzen kann. Auch Gaming oder andere private Kontexte werden immer stärker in den Fokus von Überwachungstechnik gezogen. In Zukunft wird zudem die „Smartification" der Welt viele weitere Datenquellen aufbauen, die in autoritären Regimen nicht datenschutzsensibel gebaut und genutzt werden und so in vielen Fällen große Mengen personalisierter oder personalisierbarer Daten generieren werden.

(2) Der zweite große Trend innerhalb der Nutzung von Überwachungstechnologien ist ein Shift von einer Aufmerksamkeit auf Datenquellen hin zu größerer Aufmerksamkeit auf Datenanalysen. Dieser neue Trend basiert auf dem Fakt, dass eigentlich bereits genug bis zu viele Daten zur Verfügung stehen und dass daher die Datenerhebung weniger bedeutsam wird als die Datenanalyse, mittels derer aus den großen Mengen Daten kritische und korrekte Informationen erhoben werden können. In diesem Feld der Datenanalyse sind eine ganze Reihe neuer „Überwachungstechnologien" entstanden wie Technologien der semantischen Erkennung von Inhalten und Personen, Technologien der automatisierten Kontextualisierung und Erstellung von Profilen und Technologien der massenhaften Speicherung solcher Profile. Firmen wie Palantir oder Attensity sind bekannte Vertreter dieser Technologien. Sie ermöglichen inzwischen eine absolut lückenlose Überwachung aller digitalen Aktivitäten (Telefon eingeschlossen) von Journalisten und Oppositionellen, ihren Quellen, Freunden, Kollegen und Familien in einer sehr hohen Auflösung mit einer Vielzahl von automatisch nutzbaren Analysen und Verfahren zusammengeführten Daten. Besonders für das Feld der Überwachung adaptierte Fortschritte aus dem Feld der Big Data erschließen in Anwendung auf Überwachungsdaten eine Reihe deutlich über das bisherige Maß hinausführender Möglichkeiten wie die Identifikation und Beobachtung von Meinungsströmen, von dazugehörigen Interessengruppen, das Erkennen von Codeworten, das Erkennen von digitalen Bildinhalten wie Gesichtern, ein frühzeitiges Erkennen möglicher politischer Aktivitäten, die frühzeitige Identifikation möglicher „werdender" Oppositioneller und sogar über Datenanalystechniken der sogenannten „Predictive Analytics" eine Vorhersage möglicher Aktivitäten von Zielpersonen und Gruppen über einen Zeitraum von einigen Monaten. Zudem bringt Big Data Probleme für die Pseudonymisierung und Anonymisierung, die beide mit Big Data in weiten Teilen reversibel werden und nicht länger garantiert werden können. Ein reines Löschen von Namen oder eine Verwendung von Pseudonymen werden in keiner Weise mehr ausreichend sein, um unerkannt zu

bleiben. Zudem ist durch die Vielzahl der Möglichkeiten der Auswertung von Daten ein weiterer Untertrend entstanden: eine Erweiterung der Anwendung von Personen auf Kontexte. Viele Nutzer von Überwachungstechnologien wollen nicht mehr länger nur Menschen erkennen, sondern auch stärker abstrakte Gegenstände wie sich entwickelnde Geschichten, politische Strömungen und Haltungen, neue Ideen und Netzwerke.

(3) Ein weiterer Trend schließlich entsteht in der Fusion technischer und regulativer Ansätze. Regulative Ansätze zu Überwachung erreichen eine Beschaffung oder Analyse von Daten über gesetzliche Regelungen an anderen Orten, zumeist in der nationalen Wirtschaft. Sie sind ein probates Mittel, wenn die zu erhebenden Daten oder auch deren Analysen ohnehin bereits an anderen Stellen vorgenommen werden oder leicht vorgenommen werden können. In diesen Fällen sparen sich die staatlichen Stellen erheblichen Arbeitsaufwand und können zudem auf die im Schnitt bessere Fachexpertise in der Wirtschaft zugreifen, so dass diese Ansätze inzwischen für viele Gebrauchskontexte favorisiert, in jedem Fall aber immer mitevaluiert werden. Im Fokus für entsprechende „Kooperationen" sind vor allem Telekommunikations- und IT-Unternehmen (Produkte wie Dienstleister), bei denen direkt oder mittelbar über deren Technologien relevante Daten erhoben und analysiert werden können. So werden IT-Basistechnologien und IT-Dienstleistungen direkt in Überwachungstechnologien umfunktioniert. Weitere und besondere Überwachungssoftware ist meist nicht länger nötig. Betroffene Unternehmen stehen den gesetzlichen Anforderungen bis auf wenige Ausnahmen besonders regierungsnaher Unternehmen kritisch und ablehnend gegenüber, da bei Bekanntwerden der Kooperationen deutliche Marktverluste zu erwarten sind, gesteigert dann, wenn diese Firmen international agieren. Dies hat wiederum den Effekt, dass die bereits aus taktischen Gründen überaus große Bedeutung hoher und höchster Geheimhaltung dieser Kooperationen nochmals unterstrichen und von den Unternehmen auch im Eigeninteresse strengstens eingehalten wird, so dass Einsichten in Art und Umfang entsprechender Zusammenarbeiten nur mit auslandsnachrichtendienstlichen Mitteln zu erlangen sind.

Aus Plausibilitätsüberlegungen heraus ist es prima facie geboten anzunehmen, dass in autoritären Staaten weltweit umfassende regulative Ansätze zur Erhebung von Überwachungsdaten über Kooperationen existieren oder in Entstehung begriffen sind. Umfang und Effektivität dieser Kooperationen werden sehr unterschiedlich sein und von den Fähigkeiten und Interessen der verschiedenen involvierten Akteure abhängen. Die letzten Jahre haben jedoch gezeigt, dass autoritäre Staaten bereits ab einem nur geringen Durchdringungsgrad von IT und Internet umfangreiche Überwachungsinteressen und Kontrollängste ausbilden, zu denen meist direkt der Kontakt zu wirtschaftlichen Akteuren gesucht wird, die in autoritären Regionen leider auch stärker in einer Kooperationspflicht sind als in anderen Staaten und denen weniger rechtliche Mittel zum Einspruch zur Verfügung stehen. Die Leaks zur Kundenliste der italienischen Überwachungsfirma „Hacking Team" sind in dieser Hinsicht indikativ. Zu den Kunden gehörten die Regime der Länder Mexico, Kolumbien, Azerbaijan, Kazakhstan, Uzbekistan, Oman, Sudan, Malaysia, Äthiopien und Saudi Arabien.

Alle drei Trends liegen in weiten Teilen außerhalb der Definitionen von Network Intrusion Software und Network Surveillance Software des Wassenaar Arrangements und haben in sich bereits ein hohes Potential für katastrophale Wirkungen. Die eingangs getroffene Beobachtung, dass Internet autoritäre Herrschaft stabilisiert, lässt sich

angesichts der schnellen und harten Intensivierung der Kontrollmöglichkeiten steigern in die Beobachtung: Je mehr Internet, desto autoritärer.

Für die Exportkontrolle suggerieren taktische Entwicklung und Trends folglich eine breitere Perspektive. Insbesondere das abseits der Wassenaar Formulierungen liegende Zusammenspiel regulativer Ansätze mit Basis-IT-Technologien und Dienstleistungen stellt eine Reihe neuer Herausforderungen und Möglichkeiten auf. Es ergeben sich neue Anforderungen (1) an eine Kontrolle möglicher Datenquellen, (2) an Kontrollen von Kooperationen zu Datenverkehr, und (3) es könnten Umdeutungen bestehender datenorientierter Technologien erforderlich werden.

(1) Werden etwa Datenerhebungen durch vollständigen Zugang zu Telekommunikationsunternehmen und durch staatlich verordnete Zugänge („Hintertüren“) und Datensammlungen an IT- und IT-Sicherheitsprodukten sowie an IT-Dienstleistungen aus dem Feld der Social Media ermöglicht und – etwa aus Kostengründen – auch direkt im privaten Sektor gesammelt, so liegen die technischen Erfordernisse des autoritären Staates deutlich stärker bei „Big Data“-Technologien der Datenauswertung und damit aus Sicht der Exportkontrolle weniger stark bei den für staatliche Institutionen oft schwerer beherrschbaren Intrusion Software-Varianten.

(2) Kooperationen im Datenverkehr könnten betroffen sein, wenn etwa Daten über ins Ausland geflüchtete Oppositionelle oder im Ausland sitzende investigative Journalisten durch externe Datenspeicherungen in Clouds, durch grenzübergreifende IT-Dienstleistungen, durch Datenrouting-Verfahren oder internationale Abkommen in oder durch diese Länder geführt werden. In diesen Fällen kann oft nicht sichergestellt werden, dass sensible Daten zur Kontrolle politisch unliebsamer Personen und Prozesse nicht gespeichert und abgeführt werden. In dieser Hinsicht ist auch das EUGh-Urteil zu „Safe Harbor“ bedeutsam, das klar herausstellt, dass Datenhaltung (in extenso auch Datenrouting und grenzübergreifende Datendienstleistung) in Ländern, in denen Überwachungsinteressen bekannt sind und in denen der nationalen Sicherheit ein höherer Rechtsrang zukommt als Datenschutzgesetzen, prinzipiell nicht als vertrauenswürdig gelten kann – ganz egal, welche Versprechen von staatlicher oder wirtschaftlicher Seite dazu gemacht werden. Exportkontrolle sollten also in dieser Erweiterung auch Varianten der Datenleitung, grenzübergreifender Datendienstleistung und Datenhaltung umfassen, sofern autoritäre Staaten dadurch Zugang auf die Daten politisch Verfolgter erhalten.

(3) Umdeutungen könnten verschiedene Dual Use-Technologien erfahren, die durch eine wirtschaftliche oder industrielle Nutzung in einem autoritären Land zu Quellen oder Analysewerkzeugen totalitärer Überwachung werden. Dies ist mit „Big Data“-Analysetechnologien bereits passiert, wird aber im Zuge der „Smartification“ noch mit vielen weiteren Technologien geschehen. Aktuell ist etwa bereits deutlich absehbar, dass verschiedene der im Kontext der Smart Cities entwickelten Technologien eine starke Dual Use-Komponente erhalten werden, da die dabei entstehenden und genutzten Daten über regulative Ansätze direkt als Überwachungsdaten zweitgenutzt werden können. Für eine Kontrolle des Exports von Überwachungstechnik ist dies indirekt relevant, indem die in Zukunft auf diesen Wegen erhobenen Datenmengen sowie die Qualität der Analyse dieser Datenmengen durch Anwendung normaler kommerzieller Big Data-Technologien so umfassend und präzise sein werden, dass davon auszugehen ist, dass sie derzeit marktgängigen Überwachungs- und Spionageprodukten deutlich überlegen sein werden.

Anders formuliert: Exporte dieser Dual Use-IT-Basistechnologien in autoritäre Länder werden dort eine derart hohe Befähigung zu hocheffizienter Überwachung über Regulierung ermöglichen, dass alle Exportkontrollen spezifischer Überwachungs- und Spionagesoftware irrelevant sein werden. Im übergeordneten Sinne eines Erhalts investigativen Journalismus und einer Ermöglichung von Demokratiebewegungen in diesen Ländern ist also deutlich breiter vom Export datenintensiver Technologien mit möglichem Dual Use-Charakter abzusehen, wobei hier allerdings die wirtschaftlichen Implikationen immens sind.

Damit ist einsichtig, dass auch Kontrollen zu Exporten von Datenanalyseverfahren, die im Kontext des „Big Data"-Paradigmas entwickelt werden, wünschenswert wären, da diese oft ohne große Anpassungen von einer Nutzung auf Geschäftsdaten zu einer Nutzung auf Personen- und politische Kontextdaten umgewidmet werden können. Indikativ für diesen fließenden Übergang ist etwa die US-Firma „Palantir" aus dem Silicon Valley, die für die US-amerikanische CIA Big Data-Analysetechnologien zu Überwachungszwecken entwickelt hat und diese inzwischen mit großem Erfolg auch im „zivilen" Bereich in der Industrie wie etwa bei europäischen Versicherern untergebracht hat, um dort Analysen von Geschäftsdaten zu ermöglichen. Umgekehrt wird dies folglich auch möglich, respektive können autoritäre Regime bei Firmen wie „Palantir" schlicht eine Software zur Analyse von Geschäftsdaten kaufen, die folgend in ihren Originalzweck zurückgesetzt wird.

Zur Frage von bestehenden Mankos lässt sich – wie oft in solchen Fällen – die Implementierung der Regulierung erwähnen. Damit beauftragte staatliche Stellen müssen eine hohe Expertise in der Beurteilung der Technologien, der damit zusammenhängenden Grundlagen und Forschungen sowie der politischen Kontexte des Einsatzes vorweisen, um nicht zu falschen Schlüssen zu gelangen und um entsprechende Gruppen und Firmen auch unabhängig von deren offiziellen Erklärungen erkennen zu können. Nur durch eine strenge Aufsicht dieser Firmen kann auch eine illegitime Ausfuhr verhindert werden.

Es muss folglich eine ausreichend starke und IT-sicherheitsfundierte Einheit aufgebaut werden, die allerdings aus Gründen, die unter Antwort auf die Frage (8) gegeben werden, nicht im Bundesamt für Sicherheit in der Informationstechnik angesiedelt werden sollten. Eine effektive Einheit ist zudem eine wichtige Maßnahme, um negative Folgen für nicht zu sanktionierende Technologien und Programme zu gewährleisten. Legitime Aktivitäten in diesem Bereich wie Sicherheitsforschung, Aufdeckung von Schwachstellen oder Penetration Testing sind wichtig und relevant für die allgemeine Sicherheit und müssen aufgrund der Marktdynamiken ohne Zeitverluste operieren können. Monatelange Genehmigungsprozesse können dort nicht toleriert werden, so dass also eine effektive Einrichtung einer entsprechenden Einheit auch dabei helfen wird, Konfliktpotentiale frühzeitig abzubauen.

Es ergeben sich damit eine Reihe von Optionen zur Effektivierung der Regulierungen:

1. Die Exportkontrolle klassischer Überwachungssoftware im Sinne ist wichtig, muss aber dringend erweitert werden auf die eingangs erwähnten Elemente Schwachstellen, Exploits, Dienstleistungen sowie auf Forschung und Entwicklung, auf datengenerierende Technologien und Dienstleistungen sowie auf „Big Data" Datenanalyseverfahren, da diese in der Überwachung letztlich wesentlich

bedeutender sind als Softwarevarianten, die explizit als „Überwachungssoftware“ geführt werden.

2. Es wäre zu untersuchen, ob in stark datengenerierenden Technologien im Export nicht entfernbare oder zu umgehende Anonymisierungstechniken implementiert werden können oder ob andere Ansätze zu „Democracy-by-Design“ identifiziert werden können. Dies ist allerdings sehr unwahrscheinlich. Bei grenzüberschreitenden digitalen Dienstleistungen dagegen können entsprechende Technologien eher implementiert und ihre Befolgung gesetzlich besser garantiert werden.

3. Generell sollte in autoritären Regimen von der Nutzung des Internets zu politischen Zwecken abgeraten werden.

4. Außen- und Sicherheitspolitik müssen die starken Implikationen der stabilisierenden Wirkung von Internet auf autoritäre Herrschaft besser verstehen und politisch einbeziehen und adressieren. Ein Ausbau der Außenpolitik auf diesen Fokus ist dringend erforderlich.

5. Neben der Exportkontrolle muss sich die digitale Außenpolitik dringend und intensiv mit der Aufdeckung und der Anklage digitaler Überwachung und Kontrolle befassen. Es sollte expliziter Arbeitspunkt deutscher Außenpolitik werden, sich für „Freiheit und Demokratie trotz Internet“ einzusetzen.

6. Nachrichtendienstliche Aufklärung des BND sollte Technologien und Kooperationen zu Überwachung in autoritären Ländern aufklären, um das Ausmaß der Kontrollen erkennbar zu machen und um Chancen und Risiken für Journalisten und Oppositionelle besser bewertbar zu machen.

7. Der BND sollte darüberhinaus Überwachungstechnologien und zugehörigen Verfahren infiltrieren, persistente Zugänge legen und im Sinne eines „quis custodiet ipsos custodes“ beobachten und manipulieren, was autoritäre Überwacher beobachten und manipulieren. So können demokratiefördernde Aktivitäten geschützt und unterstützt werden, während parallel das Vertrauen der Überwacher in ihre eigenen Werkzeuge unterminiert wird. Dies muss jedoch dringend in sorgfältiger taktischer und strategischer Planung und mit hoher offensiver Expertise aus staatlichen Stellen betrieben werden und darf nicht in vermeintlicher Selbstjustiz von Aktivistengruppen übernommen werden.

Ergänzende Anmerkungen zu den Fragen (3), (5) und (11): Manipulation von Kontexten und Inhalten als neuer demokratiegefährdender Trend

Neben den erwähnten Technologien und Interessen bestehen für Demokratisierungsbewegungen im Internet inzwischen auch weitere Gefahren, auf die zum Ende der allgemeinen Bemerkungen hingewiesen werden soll. So lässt sich durch verschiedene nachrichtendienstnahe Quellen und durch die Leaks von Edward Snowden klar erkennen, dass viele Staaten – autoritäre und demokratische – das Feld der

Information Operations als interessant erkannt haben und inzwischen umfangreich erarbeiten. Neben dem Design klassischer Propaganda und von Täuschungsmanövern wie False Flag und False Rescue Operationen wird dabei vor allem die Rolle des Internets in der Bildung von politischem Wissen und Meinen adressiert. Die gezielte ebenso wie die massenhafte Manipulation von politischen Meinungen und Inhalten im Web wird von vielen staatlichen Nachrichtendiensten als herausragend effizientes und kosteneffizientes Mittel der politischen Einflussnahme modelliert. Die Leaks von Edward Snowden zu den Information Operation Tools des britischen GCHQs haben dabei einen erschreckenden Implementierungsgrad erkennen lassen. Landesweite Veränderungen von Suchergebnissen, breite und granulare Zensur, Zugriff auf viele verschiedene Social Media Plattformen, automatisierte Manipulation von Online-Umfragen, automatisiertes Fluten unliebsamer Twitter-Feeds, das Streuen falscher, aber vermeintlich authentischer Informationen und die massenhafte heterogene Verbreitung gefälschter Meinungen über digitale „Teilhabe“ am öffentlichen Diskurs durch sorgfältig aufgebaute falsche politische Identitäten in pseudonym operierenden Foren sind harte Realität. Vieles davon findet auch bereits viel Anwendung von „oben“ durch staatliche Stellen wie von „unten“ durch Aktivisten – im Mittleren Osten lassen sich entsprechende Phänomene inzwischen genauso zahlreich beobachten wie in Südamerika.

Insbesondere in weniger demokratischen Ländern, in denen das Vertrauen in die anonymen und pseudonymen Inhalte des Internets größer ist als in die meist staatlich gelenkte Printpresse, können durch diese Maßnahmen langfristige große strategische Wirkungen erzielt werden.

Gegenwärtig ist es äußerst schwierig, diesen Einflüssen zu begegnen. Vieles davon ist ausnehmend schwer zu erkennen und noch schwere zu bekämpfen. Eine „Kontrolle“ möglicher feindlicher Informationen führt sehr schnell und unmittelbar zur Zensur unliebsamer Inhalte wie etwa in Russland, wo unliebsame politische Inhalte pauschal als feindliche Information Operations behandelt und zensiert werden. Für demokratische Staaten ist dies folglich nur in extremen Fällen eine Option.

Aktuell lassen sich daher nur einige wenige und teils kontroverse weiterführende Empfehlungen für diesen besonderen Kontext aussprechen:

(1) Die Manipulation politischen Wissens und Meinens im Internet muss als undemokratisch gebrandmarkt und als politisches Thema stärker in den Fokus gerückt werden.

(2) Es sollte (innen- und außenpolitisch) wesentlich stärker über entsprechende Aktivitäten aufgeklärt werden. Identifizierte involvierte PR-Firmen und Info Ops sollten publik gemacht werden.
(3) Information Operations anbietende Dienstleister und Produkte sollten unter Export- und Rüstungskontrollen gestellt und eng beobachtet werden.

(4) Klassischer investigativer Journalismus muss als Korrektiv dringend deutlich gestärkt werden, notfalls mit unabhängigen staatlichen Hilfen.

(5) Vor dem Gebrauch des Internets zur Bildung politischen Wissens und Meinens muss explizit gewarnt werden. Auch hier muss eine Umkehr der

Empfehlungsrichtung stattfinden, die den politischen Illusionen der Netzutopisten hart widersprechen muss.

(6) Die demokratischen Staaten sollten erwägen, autoritäre Manipulationen von Wissen und Meinen nachrichtendienstlich aufzuklären und mit eigenen taktischen Gegenmanipulationen durch echte politische Informationen zu beantworten, um diesen wichtigen Wirkungsvektor nicht ausschließlich autoritären Regimen zu überlassen.

Zu Frage (4): Wie groß ist der Markt der unter Wassenaar operierenden Firmen?

Das Marktvolumen weltweit beträgt nach Schätzungen etwa 5 Mrd. USD jährlich. Autoritäre und totalitäre Regime gelten als große Abnehmer. Davon abgesehen ist dieser Markt schwer zu beobachten und zu beziffern. Der Markt zu dezidierter Lawful Interception Software ist eher klein in Deutschland und Europa, da die Technologien als rechtlich und im Export unsicher und ohne große Abnehmer bewertet werden. Lawful Interception Technologien und Dienstleistungen werden hier oft von kleinen mittelständischen Firmen wie trovicor, Amesys, Digitask, Datafusion, satec, Creativity Software oder Utimaco angeboten, deren Mitarbeiterzahlen meist unter bis deutlich unter 300 liegen. Direkt mit kontroversen Exporten und Dienstleistungen sind zudem die Firmen Gamma Group (FinFisher), Intech und Hacking Team bekannt geworden, alle drei ebenfalls mit kleinen Mitarbeiterzahlen. Davon abgesehen liegen derzeit viele Anbieter im asiatischen Raum (Beispiele sind Lintas, Skytech, SSI) oder im osteuropäischen Raum (Beispiel Safesoft), beides Regionen, in denen staatliche Überwachung deutlich etablierter ist und in denen infolge ein höherer Markt zu erwarten ist mit anderen ökonomischen Skalierungen. Besonders im asiatischen Raum lassen sich auch viele wissenschaftliche und Entwicklungstätigkeiten zu Überwachungssoftware beobachten. Übergreifend dazu gibt es Überwachungssoftware und Dienstleitungen bei großen internationalen Anbietern wie Cisco oder SAP (über deren Tochter NS2).

Allerdings umfassen die Formulierungen von Wassenaar darüberhinaus auch Penetration Testing Firmen und Security Berater, von denen es deutlich mehr gibt, die allerdings fast ausnahmslos explizit keine Überwachungsprodukte oder Dienstleistungen für autoritäre und totalitäre Regime anbieten.

Zu Frage (6) und (7): Reichen die Vorgaben des Wassenaar-Arrangements aus? Wie bewerten Sie die 4. Änderungsverordnung zur Außenwirtschaftsverordnung?

Zu den Fragen wurde bereits unter Antwort auf die Fragen (3) und (5) umfangreich Stellung genommen. Die Vorgaben sollten wie indiziert erweitert werden. Ein Einschluss von Dienstleistungen ist wünschenswert.

Zu Frage (8): Welche Art der staatlichen Unterstützung für die Kontrolle unterliegenden Firmen durch die Bundesregierung ist Ihnen bekannte und wie beurteilen Sie eine etwaige Unterstützung aus Menschenrechtssicht?

Staatliche Institutionen halten sich bislang zurück, was die offene Unterstützung entsprechender Firmen betrifft, auch aufgrund des „Hacking"-Aspekts dieser Firmen und des damit verbundenen Misstrauens. Davon ausgenommen sind größere Firmen aus dem Sicherheitsbereich, die allgemein Unterstützung aus der Bundesregierung erhalten und die unter diesem Banner entsprechende Software theoretisch anbieten könnten. Es sind dem Autor hier allerdings nicht alle möglichen Zusammenhänge bekannt, da diese kaum publik werden.

Erst im Graubereich der stärker auf Dual Use gehenden Produkte werden deutsche Förderungen sichtbar. Hier ist erneut die Firma „Palantir" zu nennen, die, wie oben erwähnt wurde, für die und von der CIA via In-Q-Tel gegründet wurde und die ihre Überwachungsanalysewerkzeuge auch in menschenrechtsfeindliche Regime wie die Arabischen Emirate exportiert. Sie ist weltweit als eine der stärksten und kontroversesten Überwachungsfirmen berüchtigt und ist in Deutschland durch den Lobbyverband „Cyber-Sicherheitsrat Deutschland e.V." vertreten. Diese Vertretung erhält aktuell politische Brisanz, da der Vorsitzender des Cyber-Sicherheitsrates, Arne Schönbohm, zum neuen Präsidenten des Bundesamtes für Sicherheit in der Informationstechnik gewählt wurde. Damit ist leider ausgerechnet eine der zentralen Figuren der deutschen Cyberpolitik eng mit einem der größten kontroversen Überwachungsexporteure verbunden. Eine Einbindung des Bundesamtes für Sicherheit in der Informationstechnik in die Exportkontrollen ist damit politisch schwierig.

Zu Fragen (9) und (12): Inwieweit ist es problematisch, wenn staatliche Stellen ohne Einblick in den Quellcode und Kenntnis der Software auf diese Produkte zugreifen? Besteht konkrete Gefahr, dass mit öffentlichen Mitteln erstellte Programme um Funktionen ergänzt und an autoritäre und totalitäre Staaten weiterverkauft werden? Teilen Sie die Einschätzung, dass die Offenlegung unerlässlich ist, um die Funktionalität hinsichtlich einer rechtsstaatlichen Anwendung überprüfen zu können?

Dies ist in der Tat ein problematischer Sachverhalt. Staatliche Stellen müssten Quellcode und Funktionalität prüfen können, um mögliche direkte Anlagen oder die indirekte Eignung zu Überwachungs- und Spionagezwecken prüfen und bewerten zu können. Prima facie ist allerdings ohnehin davon auszugehen, dass die meisten dieser Softwarevarianten sich durch einfache Skalierung legitimer Funktionen bereits zu Überwachungszwecken umfunktionieren lassen. Insbesondere für die Lawful Interception Software Varianten oder für soziale Netzwerkanalysen sind Standardfunktionen für die kriminalistische Arbeit über einfache Skalierungen und das legitime Hinzufügen weiterer Indikatoren zu Überwachungszwecken umgestaltbar. Zudem sind die Voraussetzungen für eine Kontrolle des Quellcodes schwierig. Die Hersteller müssen kooperieren, und die staatlichen Stellen müssen zeitlich und in der Kompetenz in der Lage sein, effizient zu prüfen. Beides ist gegenwärtig nicht gegeben. Ein Einblick in Quellcode ist schließlich auch wünschenswert, um absichtlich eingebrachte Fehler oder Hintertüren zu finden. Eine Infiltration dieser Softwarevarianten ist für viele

Nachrichtendienste ebenso wie für Kriminelle interessant, so dass bei einigen Varianten mit entsprechenden Zusatzfunktionen zu rechnen ist.

Zu Frage (10): Sind zur Kontrolle von Überwachungstechnologien, die auch für Kriegsvorbereitungen dienen könnten, auch völkerrechtliche Vorkehrungen notwendig oder geboten?

Unbedingt. Die Überwachungsprodukte der Firma „Palantir" können erneut als Beispiel dienen, da die Software auch vom Pentagon zur Identifikation von Zielen für gezielte Tötungen durch Luftschläge genutzt wird. Ähnliche Fälle sind aus Russland bekannt. Den Formulierungen des Wassenaar-Arrangements kommen folglich neben einer Kontrolle von Überwachung auch Rüstungskontrollfunktionen zu. Zudem erlauben es die Formulierungen, dass nicht nur Überwachungskontexte, sondern auch die Konstruktion von „Cyberwaffen" allgemein damit eingeschlossen werden kann, indem insbesondere exportierbare Network Intrusion Software, in Teilen aber auch exportierbare Network Surveillance Software wichtige Bestandteile für die allgemeine Entwicklung von Cyberangriffen für staatlichen Cyberwarfare und Auslands-Cyberspionage sind. Hier sind Exportkontrollen im oben skizzierten Umfang ebenfalls dringend notwendig, da von der Verbreitung dieser Technologien eine hohe Gefährdung der internationalen Sicherheit ausgeht. Insbesondere versuchen gegenwärtig viele kleinere Staaten sowie irreguläre Akteure, an entsprechende Werkzeuge zu kommen, um sich zu umfangreichen digitalen Spionage- und Sabotageaktivitäten zu befähigen, und viele der besseren Produkte sind gegenwärtig noch vorrangig aus dem industrialisierten Westen zu beziehen. Davon abgesehen gelten allerdings die gleichen allgemeinen Einschränkungen, die bereits oben getroffen wurden sowie die gleichen Probleme in der Effektivierung der bestehenden Arrangements. Eine Stärkung des Wassenaar-Arrangements aus völkerrechtlicher Sicht ist also erforderlich und wünschenswert. Die dafür zur Verfügung stehenden Kontexte und Optionen liegen außerhalb der Kenntnisse des Autors.

Zu Frage (14.1): Welche Auswirkungen auf die Forschung zur Sicherheit informationstechnischer System hat es durch die Verschärfung der Vorschriften des Wassenaar Abkommens gegeben?

Bisher sind keine nennenswerten Auswirkungen zu erkennen. Die Cybersicherheitscommunity war zwar aufgeregt, ist aber de facto durch die Ausnahmeregelungen nicht intensiv von der Regulierung betroffen, wenn keine Exporte in entsprechende Länder geplant sind. Auch geschäftlich ist keine Einschränkung zu erwarten, sofern die Prozesse effizient gestaltet werden, wie oben geschildert. Es sollte aber stets ein vertrauensvoller Austausch über Schwachstellen und deren mögliche Ausbeutung ermöglicht werden.

Zu Frage (14.2): Wie können Exploits der Öffentlichkeit bekannt gemacht werden, wenn der betroffene Hersteller nicht reagiert?

Der gesamte Disclosure- und Patching-Prozess bedarf wie oben bereits skizziert dringend der Reform. Selbst große deutsche Softwarehersteller reagieren immer noch realitätsfern auf ihnen mitgeteilte Sicherheitslücken, da die Kosten für das Patching hoch sind und da

Reputationsschäden befürchtet werden. Sicherheitsforscher kommen damit schnell in die unangenehme Lage, zwar substantiell zur Sicherheit beitragen zu können, dies aber nicht effektiv tun zu können, da ihnen mit harten rechtlichen Schritten gedroht wird. Gegenwärtig liegt wieder ein aktueller Fall in dieser Form vor, bei dem eine Offenlegung ungemein wichtig wäre, wobei das betroffene deutsche Softwareunternehmen aber bereits auf die verantwortungsvolle Offenlegung gegenüber dem BSI mit Klagen und Drohungen reagiert hat. Der Autor dieser Stellungnahme hat bereits mehrfach zur Verbesserung des Disclosure- und Patching-Prozesses publiziert und hätte eine Reihe von Empfehlungen, um hier gesetzlich nachzubessern. Insbesondere sollten Softwarehersteller zur eigenen Suche nach Schwachstellen, zum Aufsetzen angemessener Entlohnungen von Schwachstellen (sogenannte „Bug Bounty“ Programme), sowie zur sofortigen Information aller Betroffenen und Behebung aller Schwachstellen verpflichtet werden. Ein abgestufter Meldeprozesse über verschiedene kompetitiv aufgestellte staatliche Stellen könnte dazu entwickelt werden, mit engen Firsten und steigenden Strafen für Softwarefirmen, die entsprechende Sicherheitslücken nicht bearbeiten oder nur mit Lobbying, Marketing und Rechtsabteilungen bearbeiten.

Dr. Sandro Gaycken
Direktor, Digital Society Institute Berlin
ESMT Berlin

Berlin, d. 14.12.2015