Schriftliche Stellungnahme von Reporter ohne Grenzen e.V. anlässlich der Sitzung des Unterausschusses "Abrüstung, Rüstungskontrolle und Nichtverbreitung" am 17. April 2013

Export deutscher Überwachungstechnologie – Möglichkeiten einer verbesserten Kontrolle

Zusammenfassung:

Deutsche Überwachungssoftware und -infrastruktur werden in die ganze Welt exportiert, darunter auch in Staaten mit einem zweifelhaften Ruf in Bezug auf Pressefreiheit und andere Menschenrechte. IT-basierte Überwachungstechnologie kann Festplatten von Computern durchsuchen, verschlüsselte E-Mails mitlesen sowie Kamera und Mikrofon eines Computers oder eines Handys aus der Ferne aktivieren.

Solche Technologien stellen eine Gefährdung der Pressefreiheit dar, und mindern letztendlich die Qualität der verfügbaren Nachrichten. Journalisten können, wenn sie unter solcher Überwachung stehen, nicht mehr frei recherchieren, da sie sich und ihre Quellen in Gefahr bringen würden. Die beschriebene Technologie wird nicht nur zur direkten Ausspähung genutzt. Dokumentiert sind auch Fälle, in denen Menschenrechtsaktivisten während der Gefangenschaft unter Folter mit Transkripten ihrer Korrespondenz (Email, SMS) konfrontiert wurden.[1]

Deutsche Firmen spielen eine wichtige Rolle im globalen Markt für Sicherheitstechnologie, der Schätzungen zufolge ca. 200 Unternehmen umfasst. Ein Großteil der Firmen stammt aus der EU, den USA oder Israel.

Eine zielgenaue Regulierung der Exporte ist dringend angebracht und kann ohne negative Auswirkungen auf freie Meinungsäußerung umgesetzt werden. Auch die Verfügbarkeit von Software, etwa zur Umgehung von Zensur, für Endanwender und Firmen wird nicht beeinträchtigt.

Problem:

IT-basierte Überwachungstechnologien werden heute von Strafverfolgungsbehörden weltweit verwendet. Mit einigen dieser Produkte ist es möglich, Festplatten von Computern zu durchsuchen, verschlüsselte E-Mails mitzulesen sowie Kamera und Mikrofon eines Computers oder eines Handys aus der Ferne zu aktivieren.[2]

Naturgemäß setzen auch autoritär regierte Staaten solche digitalen Waffen ein, um Journalisten und Bürger zu überwachen. Dabei wird die Grenze zur legitimen Strafverfolgung unserer Kenntnis nach regelmäßig überschritten, die Technologie also zur Unterdrückung freier Berichterstattung oder zum Ausspähen der politischen Opposition genutzt. Funktionierende rechtsstaatliche Kontrollen können nur in einer Minderheit der belieferten Länder vorausgesetzt werden.

Auch in Deutschland fordern Sicherheitsbehörden immer wieder erweiterte Befugnisse für Zugriffe auf Computer, Mobiltelefone und Email-Postfächer. Das Bundesverfassungsgericht hat

[1] http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html
[2] http://www.zeit.de/2013/08/Bahrain-Software-Trojaner

sich in seinem Urteil zur Online-Durchsuchung [3] ausführlich mit dieser Problematik auseinandergesetzt und kam zu dem Ergebnis, dass der Einsatz solcher Technologie schon in einem demokratischen Rechtsstaat wie Deutschland hochproblematisch, und nur unter sehr engen technischen und rechtlichen Vorkehrungen zulässig ist.[4]

Das Engagement deutscher Firmen in menschenrechtlich fragwürdigen Staaten wurde in den vergangenen Jahren von Menschenrechtsaktivisten vermehrt kritisiert. Hervorzuheben sind aus unserer Sicht die Gamma International GmbH, die ehemalige Siemens-Tochter Trovicor sowie Elaman und Utimaco.[5]

In den letzten Jahren wurde der Export dieser umstrittenen Technologie mehrfach mit Hermes Exportkreditgarantien abgesichert. Die Bundesregierung hat es bislang versäumt, Transparenz über die Vergabe von Bürgschaften herzustellen.

Um eine Prüfung der Menschenrechtspraktiken von Lieferanten von Überwachungstechnik zu veranlassen, hat Reporter ohne Grenzen gemeinsam mit Partnerorganisationen wie dem European Centre for Constitutional and Human Rights OECD-Beschwerden gegen Trovicor und Gamma International eingereicht. Die Zulassung der Beschwerde wird derzeit von der Nationalen Kontaktstelle im Bundesministerium für Wirtschaft und Technologie geprüft. Diese Prüfung sollte demnächst abgeschlossen sein, eine parlamentarische Begleitung der Anfragen hat sich in der Vergangenheit als sehr hilfreich erwiesen.

Wie umfangreich das Engagement westlicher Firmen in autoritären Regimen ist, zeigte sich vor allem nach dem sogenannten Arabischen Frühling. Ein Angebot der deutschen Firma Elaman für Finfisher-Trojaner wurde bei der Erstürmung der Geheimdienstzentrale in Ägypten gefunden, in Libyen war nachweislich Technologie der französischen Firma Amesys im Einsatz.[6] Journalisten und Aktivisten aus Bahrain wurden mit Produkten der Firmen Trovicor und Gamma International überwacht, in Marroko wurden die Redaktionsräume des Online-Portals Mamfakinch vermutlich mit Software der italienischen Firma Hacking Team abgehört. Diese Liste ließe sich fast beliebig fortsetzen, allein die Firma Trovicor gibt an, in mehr als 100 Ländern weltweit aktiv zu sein.

Der Markt für Überwachungstechnologien wird häufig übertrieben groß dargestellt. Trovicor, eine der Branchengrößen, beschäftigt in Deutschland ca. 170 Mitarbeiter, Gamma International am Standort München nur rund 30. Insgesamt ist davon auszugehen, dass in Deutschland deutlich weniger als 1000 Menschen für Hersteller von Überwachungstechnologie arbeiten.

Derzeit bestehen allgemeine Export-Sanktionen gegen Syrien und den Iran, davon sind auch Überwachungstechnologien betroffen. Diese Sanktionen sind aus Sicht von Reporter ohne Grenzen hilfreich und notwendig, aber nicht ausreichend. Wir haben die Bundesregierung bereits

[3] http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html
[4] Zuletzt bestätigt in einem Urteil des OLG Köln, Aktenzeichen "16 Wx 16/12•
[5] Eine Liste mit deutschen Unternehmen und einer groben Einordnung ihrer Tätigkeit finden Sie im Anhang.
[6] http://www.spiegel.de/netzwelt/netzpolitik/ueberwachung-in-libyen-reporter-finden-hinweise-auf-westliche-spaehtechnik-a-783303.html

im Sommer 2012 in einem Positionspapier[7] aufgefordert, den deutschen Exportkontrollrahmen an digitale Waffen anzupassen. Im Rahmen des Internet Governance Forums in Baku haben wir unsere Forderungen explizit auch an die EU-Kommission adressiert.

Lösungsmöglichkeiten:

Das Exportkontrollregime der Bundesrepublik Deutschland bietet verschiedene Möglichkeiten an, um den Export zu kontrollieren. Eine Einschränkung des Exports ist nach europäischem Recht möglich, wenn zu erwarten ist, dass Menschenrechte durch die gelieferte Technologie verletzt würden.[8] Auch wenn die beschriebene Technologie nicht direkt militärischen Zwecken dient, ist ihre Wirkung in vielen Fällen vergleichbar.

Nach deutschem Recht wäre eine Aufnahme von Überwachungsinfrastruktur in die Anlage AL zur Außenwirtschaftsverordnung ein denkbares Kontrollinstrument. Darüber hinaus sollte die Bundesregierung unverzüglich klarstellen, ob und in welchem Ausmaß in der Vergangenheit Hermes-Exportbürgschaften für die Lieferung von Überwachungstechnologie vergeben wurden.

Die EU-Dual-Use-Verordnung dient auch als Grundlage für die nationalen Verordnungen. Hier liegen Vorschläge für eine konkrete Ausgestaltung bzw. Erweiterung vor, etwa im Bericht über eine *„Digitale Freiheitsstrategie in der Außenpolitik der Europäischen Union“* der vom Europarlament überparteilich angenommen wurde.[9]

In Großbritannien interpretiert die Regierung mittlerweile die EU Bestimmungen über den Export von Verschlüsselungstechnologie dahingehend, dass Produkte wie der Finfisher-Trojaner und die benötigte Infrastruktur einer Exportkontrolle unterliegen. Diese Lösung kann jedoch höchstens ein erster Schritt sein, da Technologie häufig modular aufgebaut ist und die Verschlüsselung durch externe Lösungen nach erfolgtem Export nachgerüstet werden könnte.[10]

Die umfassendste, aus Sicht von Reporter ohne Grenzen beste, Lösung wäre eine Integration von Überwachungstechnologie in das Wassenaar-Abkommen für Exportkontrolle. Verschiedenen Quellen zufolge liegen bereits verhandelte und abgestimmte Texte vor, die einen Einschluss von Überwachungstechnologie ermöglichen würden. Diese Texte könnte die Bundesregierung kurzfristig implementieren, um so Druck auf die internationalen Partner auszuüben.

---

[7] http://www.reporter-ohne-grenzen.de/fileadmin/rte/docs/Positionspapier.pdf

[8] VERORDNUNG (EG) Nr. 428 /2009 DES RATES vom 5. Mai 2009 über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung und der Durchfuhr von Gütern mit doppeltem Verwendungszweck, Artikel 8 (1)

[9] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2012-0374+0+DOC+PDF+V0//DE&language=DE, http://www.reporter-ohne-grenzen.de/presse/pressemitteilungen/meldung-im-detail/artikel/eu-muss-handel-mit-digitalen-waffen-strenger-kontrollieren/

[10] Produkte, die Verschlüsselungstechnologie enthalten und einer Exportbeschränkung unterliegen, sind unter Kategorie 5, Teil 2 der EU Dual-Use Liste aufgeführt