Stellungnahme zur 7. Anhörung des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres

LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens on electronic mass surveillance of EU citizens

14.10.13, Straßburg

Constanze Kurz

Vielen Dank für die Einladung zur Anhörung. Ich möchte die Gelegenheit nutzen, zu den bekanntgewordenen Praktiken der Geheimdienste Stellung zu nehmen, und beziehe mich insbesondere auf den britischen GCHQ.

Wir haben in den vergangenen Monaten eines gelernt: Die technischen Möglichkeiten, die digitalen Transaktionen und den Netzverkehr ganzer Kontinente abzuhören, sind heute nicht nur vorhanden, sie werden auch genutzt – und nicht nur in Diktaturen, sondern mitten in Europa. So kann das vom britischen Geheimdienst GCHQ entwickelte TEMPORA-Programm an den überwachten Glasfaserleitungen den gesamten Netzverkehr für mehrere Tage speichern, um nach der Analyse das Herausfiltern von Informationen durchzuführen.

Ein möglicher Rechtsweg gegen den GCHQ wird mit der Beschwerde beim Europäischen Gerichtshof für Menschenrechte nun beschritten.[1] Ob die Überwachungsmaßnahmen des GCHQ wie

---

[1] App. No. 58170/13 http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/bbw_org_ep_ck_v_uk_/bbw_org_ep_ck_v_uk_en.pdf

gesetzlich festgeschrieben (Regulation of Investigatory Powers Act, RIPA) im Einzelnen nach britischem Recht verhältnismäßig und notwendig oder auch nur zielführend sind, ist ohnehin fragwürdig. Ob aber diese Geheimdienstpraktiken mit Blick auf die Europäische Menschenrechtskonvention einfach unverändert weiterlaufen dürfen, nachdem sie nun öffentlich bekannt sind, wird eine vom Gerichtshof zu bewertende Frage sein: Bricht das nationale britische Gesetz, das das Kommunikationsgeheimnis nicht nur eines Großteils aller Europäer untergräbt, internationales Recht? Denn der britische Geheimdienst muss für das Belauschen ausländischer Kommunikation und damit auch europäischer Bürger, Unternehmen und Behörden keinerlei Zielpersonen benennen oder sonst Sachgründe vorbringen.

Wenn Mitglieder der britischen oder der US-amerikanischen Regierung nun ankündigen, wenigstens darüber nachdenken zu wollen, die inländische parlamentarische Kontrolle der Geheimdienste zu verbessern, dann beziehen sich diese Ankündigungen lediglich darauf, den rechtlichen Schutz für Inländer zu verbessern. Für Schutz vor der massenhaften Überwachung durch den GCHQ bedeutet das konkret: Der Rest der Europäer wäre weiterhin außen vor, für ihre Kommunikation gilt keine Restriktion beim Belauschen oder beim ebenfalls bekanntgewordenen Hacking durch den Geheimdienst.

RIPA (Section 8) gibt dem britischen GCHQ das Recht, Kommunikation abzuhören, sofern sie Großbritannien verlässt oder auf die britische Insel kommt – nicht etwa von und nach Europa. In RIPA ist dafür der Begriff „External data“ definiert, die ohne nennenswerte Beschränkungen und auch ohne nachträgliche Benachrichtigung der Betroffenen oder der Öffentlichkeit belauscht werden darf. Sofern die britische Regierung also in Zukunft den Schutz vor der massenhaften Überwachung verbessern sollte, so ist

lediglich der Schutz der britischen Datengeber gemeint. Die „Externen“, das sind wir Resteuropäer, deren Rechte Großbritannien nach Artikel 8 der Menschenrechtskonvention aber mit der Unterzeichnung der Konvention 1951 ebenfalls zu schützen versprochen hat.

Nach den veröffentlichten Snowden-Unterlagen wird der europäische Internetverkehr durch den GCHQ fast vollständig erfasst und analysiert. Insbesondere belauscht der Geheimdienst Überseekabel sowie mindestens zwei Dutzend weitere Glasfaserleitungen, darunter auch innereuropäische. Die Betreiber-Firmenkonsortien dieser Leitungen dementieren das Abhören ebensowenig wie der Geheimdienst. Es sind zwar neben britischen auch ausländische Unternehmen betroffen, etwa Verizon, Interoute oder die Deutsche Telekom, sie verweisen aber auf Verschwiegenheitsverpflichtungen nach britischen Recht und haben, anders als einige US-amerikanische Unternehmen, keine rechtlichen Schritte gegen des Anzapfen ihrer Leitungen angekündigt.

Es geht jedoch nicht nur um Fragen der Eingriffe in die Privatsphäre von Menschen durch die massenhafte Überwachung an Telekommunikationsleitungen. Letztlich führen zusätzlich auch die nun bekanntgewordenen offensiven Angriffe auf kritische Infrastrukturen von Nachbarländern zu einer Unsicherheit auf mehreren Ebenen. Insbesondere der Fall des geheimdienstlichen Hackings von Belgacom[2] ist als Angriff auf die nationale Souveränität eines EU-Landes zu verstehen. Die Computer des belgischen Unternehmens, das teilweise in Staatsbesitz ist, wurden heimlich mit professioneller Schadsoftware infiltriert, um sämtliche Passwörter

[2] http://www.standaard.be/cnt/dmf20130920_00752574

und kryptographische Schlüssel abzugreifen.[3] Als Kunden von Belgacom sind dadurch übrigens auch die Europäische Kommission und das EU-Parlament direkt betroffen. Weitere Kunden von Belgacom sind etwa Swift oder die NATO.

Auch das EDGEHILL-Programm[4] des GCHQ, das das systematische Untergraben oder Umgehen von Verschlüsselungsmaßnahmen zum Ziel hat, muss neben der Überwachungsproblematik auch als „Anti-Sicherheitsprogramm“ verstanden werden, das wesentliche Sicherheitsmaßnahmen und das Vertrauen in die alltägliche Kommunikation über die Netze nachhaltig kompromittiert. Durch eingebaute Hintertüren, aber auch in die Unternehmen eingeschleuste V-Männer wurden gängige Verschlüsselungsverfahren strukturell geschwächt. EDGEHILL zielt insbesondere auf Service-Provider wie Hotmail, Google, Yahoo und Facebook sowie auf Betreiber sogenannter Virtual Private Networks, die von Privatpersonen und Unternehmen genutzt werden, um eine sichere Verbindung zu ihren Systemen herzustellen.

Wir müssen uns nicht nur fragen, ob wir mit Blick auf die Europäische Menschenrechtskonvention dauerhaft dulden wollen, von Geheimdiensten durchleuchtet zu werden. Wir müssen uns auch fragen, wie sicher unsere digitalen Übertragungen vor dem Hintergrund dieser und weiterer Berichterstattungen über geheimdienstliche Angriffsmethoden in einem offenbar rechtsfreien Raum noch sind. Dabei ist nicht nur an Naheliegendes wie Industriespionage zu denken, sondern auch beispielsweise an Online-Wahlen, wie sie in Estland und der Schweiz durchgeführt werden, aber auch in Pilotversuchen in Österreich. Denn die gesetzlichen

---

[3] http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html

[4] http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

Regelungen des britischen Intelligence Services Act (ISA) und Regulation of Investigatory Powers Act (RIPA) zielen neben der Überwachung der Telekommunikation aus Gründen der „nationalen Sicherheit“ auch explizit darauf, außenpolitische und ökonomische Interessen von Großbritannien zu sichern.

Ich bin der Auffassung, dass wir uns mit dem nun vorhandenen detaillierten Wissen um die kaum durch Kontrollen behinderte Überwachung durch die Geheimdienste nicht abfinden dürfen. Selbstverständlich ist das einer der Gründe, warum meine Mitstreiter und ich unsere Beschwerde beim Europäischen Gerichtshof für Menschenrechte vorgelegt haben. Dennoch müssen wir auch politische Antworten finden, die darauf hinauslaufen, dass zumindest die europäischen Regierungen dem Fernmeldegeheimnis und dem Recht auf eine digitale Privatsphäre einen deutlich höheren Stellenwert einräumen sowie untereinander digitale Nicht-Angriffspakte schließen und die Integrität ihrer technischen Infrastrukturen gegenseitig nicht kompromittieren.