15. Aug. 2013

von kolliarakis

in Cyber Security, Sicherheitskultur, Zivilgesellschaft

Kommentare (3)

Die Überwachung, die Übertreibung und die Überforderung

von Georgios Kolliarakis

Eigentlich hätte es nicht passender kommen können: Edward Snowdens Geschenk zum jährlichen multimedialen Sommerloch – und zwar international! Die Enthüllungen über das *Portal for Real-time Information Sharing Management* PRISM, das Datenspeicherungs- und Überwachungsprogramm der amerikanischen *National Security Agency*, haben (fast) alle überrascht und wurden sofort von allen Seiten dementiert. Die öffentliche Krisenkommunikation verlief dann nach Textbuch: Anhand der Salami-Taktik wurde in den vergangenen acht Wochen immer deutlicher, dass eigentlich alle beteiligten Akteure und Behörden – europaweit, auch in Deutschland – über solche flächendeckenden Überwachungs- und Datensammlungsprozesse seit Jahren Bescheid wussten, sie genehmigt und sogar aktiv gefördert haben.

„Wozu die Aufregung?“ fragte sich der ehemalige Bundesinnenminister Schily. Dies könnte doch eher ein Zeichen dafür sein, dass die Nachrichtenbehörden als unabdingbare Hilfe für die Sicherheitspolitik seit Jahrhunderten und insbesondere nach 9/11 endlich mal technologisch effektiver werden. Dies sei bitter nötig angesichts diffuser terroristischer und krimineller Bedrohungen, gegen die Staaten im Interesse ihrer Bürger aktuell zu kämpfen haben. Außerdem überwachen Programme wie PRISM & co genau dort, wo sie relevanten Informationen zur Konzeption, Planung und Koordination von illegalen Handlungen auf die Spur kommen könnten: im Email-Verkehr und im Datenaustausch der Bürger in sozialen Medien. Da müsste man zwar ein wenig indiskret werden bei der Handhabung der Privatsphäre der Bürger, aber dies ist immer der Preis des Kompromisses, um Anschläge rechtzeitig verhindern zu können. Der amtierende Bundesinnenminister Friedrich hat Klartext gesprochen: Es ist das „Supergrundrecht Sicherheit“, das handlungsweisend bei den Aufgaben der staatlichen Schutzpflicht ist. Bundesjustizministerin Leutheusser-Schnarrenberger dagegen sah die Sache ein wenig anders: Solche Aktionen gefährden die Bürger, statt sie zu schützen. Und das Auswärtige Amt ernannte umgehend einen sog. „Cyber-Außenbeauftragten“, der in Zukunft irgendwie für solche Angelegenheiten im guten bürokratischen Stil zuständig sein soll.

Online-Aktivisten haben sich bereits früh in die Debatte eingemischt: Mit

Expertengehabe und viel Alarmismus haben sie einen libertären Diskurs vorangetrieben und spekulativ auf die Gefahren des panoptischen Staates hingewiesen. Das Deutungsschema ist bekannt und simpel: Bürger = Opfer / Staat = Täter. Engagierte Bestseller-Autorinnen wie Juli Zeh haben in Robin-Hood-Manier öffentliche Briefe an die Kanzlerin formuliert und Unterschriften für die rechtsstaatliche Bewahrung der Freiheit gesammelt. Die dabei für gewöhnlich bediente begriffslogische Leerformel (anders: Floskel) „Freiheit vs. Sicherheit" eignet sich traditionell genauso gut für politische Entscheidungsträger und Journalisten zur Stimmungsmache und emotionalen Mobilisierung.

Was möchten allerdings die Bürger selbst? In den USA zumindest hat sich nach fast 10 Jahren die öffentliche Meinung umgekehrt: Laut der letzten Pew-Center Umfrage meinen seit Juli 2013 47% der US-Bürger (im Gegensatz zu 35%), dass die Antiterrormaßnahmen der Regierung zu weit gegangen seien. Seit 2004 gaben konstant zwischen 50% und 60% der US-Bürger an, dass die Regierung nicht genug täte, um sie vor Terrorismus zu schützen. In Europa steigt laut der vergleichenden Eurobarometer-Umfragen seit 2003 die Akzeptanz der EU-Bürger für invasive staatliche Internetkontrollen: In 2008, z.B. meinten 75% der EU-Bürger und sogar 80% der Deutschen, dass das Internet-Monitoring angesichts des internationalen Terrorismus ermöglicht werden sollte [1]. Die Deutschen halten es vielmehr für selbstverständlich (70%), dass sie ihre Daten im Internet offenbaren müssen [2]. Merkwürdigerweise bewerten die Deutschen die Bedrohung durch Cyber-Kriminalität signifikant stärker als der EU-Durchschnitt [3], obwohl sie sich kaum von Cyber-Kriminalität und Datenklau betroffen fühlen (61%-90%) [4]. Dieser angebliche Widerspruch spiegelt auf erstaunlicher Weise das Sicherheitsparadox in wohlhabenden Gesellschaften: Das Versprechen von „mehr Sicherheit" führt zu einer Senkung der Toleranz gegenüber Bedrohungen und paradoxerweise zu einer Verstärkung der Unsicherheitswahrnehmung. Dies könnte eventuell auch den immer expliziter werdenden Wunsch nach Überwachung und Kontrolle erklären.

BELIEBT KOMMENTARE NEU

Hell yeah, it's Political Science! Wissenschaftliche Podcasts

Das Internet darf ein cyberfreier Raum sein

Deutschlands Irak-Politik – Verantwortung nach außen, Intransparenz nach innen.

Wir haben Geburtstag!

It's not Cyberwar, stupid!

KATEGORIEN

Außenpolitik (59)

Bürgerkriege (16)

Cyber Security (42)

Demokratisierung (9)

Drohnen (15)

Humanitäre Interventionen (15)

Innere Sicherheit (24)

Interviews (10)

Katastrophen (4)

Konferenz (20)

Militär (28)

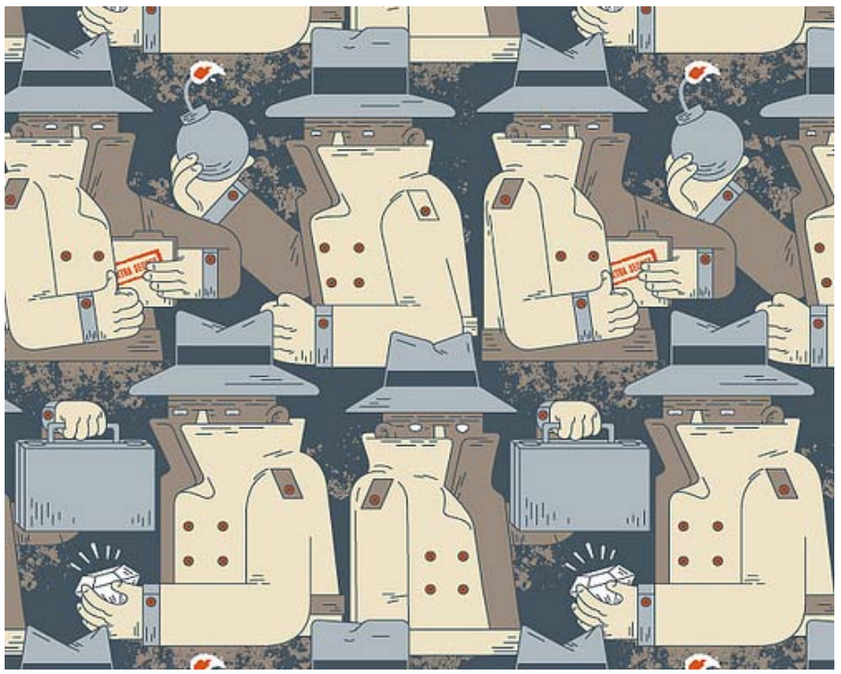
Pandemien (2)

Podcast (7)

Popkultur (21)

Sanktionen (8)

Security Culture (14)



Die aktuelle lebendige Debatte über die Überwachungsaffäre lässt jedoch leider – nicht zuletzt durch die Wahlkampf-Politisierung – noch eine Reihe von Dimensionen vermissen:

Die Rolle der deutschen und der EU-Sicherheitsforschung als eine Kernkomponente proaktiver Sicherheitspolitik ist gänzlich abwesend. Die Forschung für zivile Sicherheit seit 2007 sowohl auf EU-Ebene (FP7 2007-2013; 1.400 Millionen EUR) als auch auf deutscher Ebene (Sicherheitsforschungsprogramm der Bundesregierung 2007-heute; >400 Millionen EUR) generiert einen Pool von „innovativen Lösungsansätzen", die sich überwiegend auf die Bereiche „Überwachung", „Detektion" und „Mustererkennung" konzentrieren. Da sind high-tech-industriepolitische sowie exportpolitische neben sicherheitspolitischen Überlegungen im Spiel. Undiplomatischer gesagt wären die Europäer und die Deutschen gern so weit wie die Amerikaner mit ihren Technologien, damit sie einerseits autonom wären und andererseits selbst an andere Interessenten verkaufen könnten.

Die Perspektive einer **strategischen Analyse** ist fast abwesend von der aktuellen Debatte: Da muss zunächst nach dem Ergebnis des Einsatzes von Überwachung gefragt werden: Hat es was gebracht? Oder eher nichts? Oder hat es sogar kontraproduktive Effekte gegeben? In dieser Hinsicht wurde in kaum einem Bericht der praktisch enorm wichtige Unterschied zwischen Möglichkeit und Wahrscheinlichkeit formuliert: Dass die technischen Möglichkeiten zum umfassenden Datensammeln steigen heißt nicht notwendigerweise, dass auch die Wahrscheinlichkeit zum erfolgreichen Einsatz gegen Terrorismus oder zum Missbrauch von privaten Daten gleichmäßig steigt. Für Strategieexperten genauso wie für Entwicklungspsychologen ist Potenzial (*capacity*) nicht gleich Fähigkeit (*capability*). Da müssen noch viele (nicht immer steuerbare) Rahmenbedingungen mitspielen. Viele Kommentatoren scheinen das sog. „Law of Diminishing Returns" zu ignorieren: Mehr Einsatz von

Sicherheits-Kommunikation (14)
Sicherheitskultur (205)
Sozialwissenschaft Online (57)
Stellenangebote (42)
Strategie (10)
Terrorismus (14)
Theorie (2)
Umwelt (1)
Versicherheitlichung (22)
Visualisierung (5)
Whistleblowing (8)
WikiLeaks (17)
WMD (10)
Zivilgesellschaft (48)

BLOGROLL

Arbeitskreis soziale Bewegungen
Augen geradaus
Dan Drezner
Dart-Throwing Chimp
David Campbell
de.hypotheses.org
Demokratieforschung Göttingen

Überwachung bringt irgendwann nicht mehr Sicherheit; aber auch zunehmender Verzicht auf staatliche Überwachung sorgt nicht für mehr Schutz der Privatsphäre.

Die Reaktionen seitens der politischen Entscheidungsträger jeglicher Parteicouleur folgen etablierten Mustern [5]. Erstens, **Aktionismus**: Forderungen nach mehr Kontrollgremien, Sonderbeauftragten, Gesetzen u.Ä., als ob es nicht bereits genug Möglichkeiten gäbe, solche Entscheidungsprozesse und -umsetzungen zu beeinflussen und zu kontrollieren. Zweitens, **Symbolpolitik**: „Wir sind kein Überwachungsstaat, wir sind ein Rechtsstaat", wobei die Staaten souveranitätstechnisch so etwas in der Praxis nicht (mehr) garantieren können. Garantieansprüche oder -versicherungen in Bezug auf den rechtsstaatlichen Schutz der Daten von Bürgern sind momentan irreführend, zumal sich die Sache international noch in einer rechtlichen Grauzone und erst in Anfangsverhandlungen zwischen Staaten und transnationalen Firmen befindet; Drittens, **High-Tech-Pfaddependenz**, die zusammen mit dem weit verbreiteten Glauben einhergeht, dass Technologien geeignete Lösungen für komplexe gesamtgesellschaftliche Problemlagen bereitstellen können. Und dies, ohne Bumerang-Effekte zu verursachen (z.B. noch mehr Vulnerabilität ins System einführen) und ohne das gesellschaftliche Vertrauen zu unterminieren (z.B. durch politische Unglaubwürdigkeit der Sicherheitsprogramme). Solche Muster zeugen oft von der Überforderung des Staates, sein Hobbes'sches Versprechen an die Bürger einzulösen, und gehören neben dem dominanten „Die-Wirtschaft-über-alles"-Paradigma zum Mainstream der aktuellen Sicherheitskultur in Deutschland.

Die öffentlichen Empörungswellen (was Medienwissenschaftler „moral panics" nennen), kein seltenes Phänomen in der deutschen Politik, sind opportunistischer als man denkt und kein guter Kompass zur nachhaltigen Policy-Planung. Nach der Aufdeckung z.B. eines Datenschutz-Missbrauchsfalls wie aktuell bei der PRISM-Affäre ist es zu erwarten, dass Oppositionspolitiker, Journalisten, Experten und Aktivisten für „Freiheit" plädieren und die zu starke, unrechtmäßige Einmischung des Staates („zu viel getan") rügen. Umgekehrt plädieren die gleichen Oppositionspolitiker, Journalisten, Experten und Aktivisten nach ereigneten oder knapp abgewendeten Anschlägen für „Sicherheit" und bemängeln die ineffektive Schutzleistung des Staates („zu wenig getan") trotz massivem Einsatz von Steuergeldern. Die Pflicht zu mehr Transparenz in der Kommunikation von sicherheitsrelevanten Entscheidungen sowie eine klarere Haftungsverteilung bei Unregelmäßigkeiten könnten einer solchen Übertreibung in beide Richtungen widerstehen und zu mehr gesellschaftlichem Vertrauen beitragen (s. auch die Online-Debatte über öffentliche Krisenkommunikation).

Selten werden „Sicherheit" und „Freiheit" zu konkreten politischen Zielen operationalisiert (Was genau bedeutet Sicherheit in der Praxis? Schutz? Vorsorge? Prävention? Kompensation? Resilienz? Abwehr?) und genauso selten in legislativen und anderen Policy-Maßnahmen explizit instrumentalisiert. Meistens werden „Sicherheit" und „Freiheit" ohne weitere

Duck Of Minerva
Future and Politics
Hylaean Flow
Internet und Politik
IR Blog
Just Security Blog
justsecurity.org
Killer Apps
Kings Of War
netzpolitik.org
percepticon
shabka.org
Terrorismus in Deutschland
theorieblog.de
Verfassungsblog
Vom Bohren harter Bretter
whistleblower-net.de

ARCHIV

Wähle den Monat

Präzisierung einfach als Nullsummenspiel betrachtet. Dies lenkt von der Spannung zwischen „*Sicherheit als Zweck*“ und „**Sicherheit als Mittel zum Zweck**“ als Handlungsparadigmen auf der Arena einer demokratischen sicherheitspolitischen Planung ab. Es kann gut sein, dass im heutigen alternden, konservativer werdenden Europa der Trend eher in die erstere Richtung geht. Bundesinnenminister Friedrich trifft mit seiner Diagnose vom „Supergrundrecht Sicherheit“ möglicherweise einen empfindlichen Nerv breiter gesellschaftlicher Gruppen. In den „post-panoptischen“ Gesellschaften des 21. Jahrhunderts (Zygmunt Bauman), wo der Datenverkehr einen freiwilligen oder aufgezwungenen oder exhibitionistischen oder auch unabsichtlichen Charakter haben kann, müssen allerdings Bürger realistischerweise feststellen, dass es kein „free meal“ gibt, solange sie den Nutzen der IC-Technologien genießen möchten. Nichtsdestotrotz sind sie nicht nur Opfer dieser Situation: Sie haben doch selber einen Anteil an Entscheidungsmacht – und an Verantwortung, um ein Stück weit mitzubestimmen, wohin diese Reise geht.

Bild: CC-BY-NC by Emory Allen

1. Eurobarometer „Data Protection“ 225, 2008
2. Eurobarometer „Data Protection and Electronic Identity“ 359, 2011
3. Eurobarometer 75.4 „Internal Security“, 2011
4. Eurobarometer 77.2 „Cyber-Security“, 2012
5. Siehe dazu auch *Kolliarakis, G.* 2011: Die neue Ambivalenz in der Sicherheitspolitik: Sicherheitskultur als tiefer Kontext. In: Sicherheit + Frieden 2/2011, Spezialheft Sicherheitskultur, 72-78

Tags: Datenschutz, Leaking, Leaks, nsa, prism, snowden, supergrundrecht, Überwachung

« Stellenanzeigen August 1/2

Ein staatliches Wissensmonopol – wer ist dagegen? »

3 Kommentare zu “Die Überwachung, die Übertreibung und die Überforderung”

Pohlschröder | 19. Aug. 2013 um 21:08 | **#1**

Danke für den wirklich sehr interessanten Blogbeitrag. Top! Lg, Mina

ANTWORTEN

S. Meyer | 27. Aug. 2013 um 10:26 | **#2**

Während die Begründung zur Terrorabwehr anscheinend so gut wie alles möglich macht, bleibt der Blick auf das wesentliche – zum Beispiel die stetig steigende Kriminalität im Bereich Medium Internet auf der Strecke.
Was nützt das abhören wenn der Anschlag von Boston doch nicht verhindert wurde und zeitgleich die Polizei nicht in der Lage ist trotz IP Nummern oder Lieferadressen zig tausende Straftaten aufzuklären.
Ob der Bürger, wie im Schlusssatz genannt, wirklich Anteil an der Entscheidung hat bleibt für mich fraglich. Wenn das eine Programm eingestellt wird um die Öffentlichkeit zu beruhigen wird doch zeitgleich das nächste wieder aktiviert.

ANTWORTEN

bekannt | 31. Aug. 2013 um 14:02 | **#3**

1. dass menschen verhungern, ist das nicht wichtiger?
2. wieviele arbeits-, verkehr- etc unfälle haben heute stattgefunden?
3. wieviele menschen sind heute “umsonst” gestorben, an heilbaren krankheiten gestorben, da sie keine dollars für die behandlung gehabt haben?
3. 1,2,3 bedeuten keine “sicherheit”?
5. was herr dr. Kolliarakis hier schreibt, ist es nur absolut und ganz “normal” – allerbeste auftragsforschung
6. weiter so! und bloß nicht in richtung GRiechland gucken! da hungern menschen aus! wuu, (zukünftige) proffessoren wollen so was überhaupt nicht wissen
7. keine akademische sprache, weil das hier alles mögliche ist, nur foschung nicht

ANTWORTEN

Einen Kommentar hinterlassen

Name

Email

Webseite

Kommentar

Geben Sie den Text ein.

reCAPTCHA

Bestätigen

Datenschutz - Nutzungsbedingungen

Kommentar senden

☑ Benachrichtige mich über nachfolgende Kommentare per E-Mail.