

5. Jul. 2013

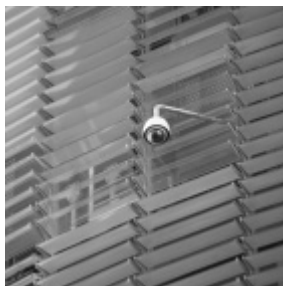
von pano

in Cyber Security,
Innere Sicherheit,
Sicherheitskultur,
Whistleblowing

Kommentare (3)

Überwachen und speichern

von Philipp Offermann



Alle reden vom Vertrauensbruch, vom angemessenen Verhalten unter Freunden. Um es mit Innenminister Friedrich zu sagen: **“Diese Mischung aus Anti-Amerikanismus und Naivität geht mir gewaltig auf den Senkel.”** Denn abzuhören, Informationsbeschaffung ohne Wissen der ausgeforschten Personen, das ist nun mal das wesentliche Mittel, welches Geheimdienste

einsetzen: Es ist ihr Wesenszweck. Staaten oder sonstige Akteure haben immer per Spionage zumindest auch ihre Sicherheit verteidigt. Einiges an gerade zu vernehmender Empörung geht deshalb am Kern vorbei. PRISM und Tempora sind eine Katastrophe, aber aus weit wichtigeren Gründen, die im “Hättet Ihr uns das nicht früher sagen können”-Schmollwinkel leicht untergehen: weniger die mangelnde Transparenz ist das Problem, als vielmehr die anlasslose Datensammelwut, die kulturell tief in in dieser Hinsicht weitestgehend unregulierten Sicherheitsapparaten verwurzelt zu sein scheint.

Informationsbeschaffung ist der Kern geheimdienstlicher Arbeit. Das muss man nicht mögen, aber diesen Umstand zu verleugnen ist realitätsfremd. Dabei bewegen sich die Dienste oft genug in einer gesetzlichen Grauzone, im amerikanisch-völkerrechtlichen Neusprech auch als *Extra-Legale Zone* bezeichnet. Deutsche und französische Geheimdienste werden sicher nicht jeder Zielperson eines Lauschangriffs einen Ankündigungs-Brief schicken. Wäre ich ein Geheimdienst, ich würde es jedenfalls wirklich nicht machen. Und sogar die deutschen Dienste scheinen immerhin hier ihre Hausaufgaben gemacht zu haben und sind offenbar ebenfalls in einem zentralen Internet-Knoten eingeklinkt, wie uns etwa netzpolitik.org verrät.

Doch “Wir sind nicht mehr im Kalten Krieg”, Angela Merkels erste Reaktion auf den Lauschangriff der US-Amerikaner auf die EU-Vertretungen, demonstriert einmal mehr, das es für deutsche Administrationen offenbar noch einiges an #Neuland zu betreten und zu erforschen gilt. Denn auch Kalter Krieg, also ein etabliertes Freund-/Feind-Schema mit klarer Bedrohungslage, ist die völlig falsche Metapher: Die Gesellschaft befindet sich heute in einem Dauerzustand von Verunsicherung und Bedrohungsgefühl. Wer heute noch als Freund gilt, kann morgen schon die Bombe zünden.

SOCIAL MEDIA



SUCHE

TWITTER FEED

Ben Kamis: The concept of #cyberpeace is linguistic trolling. Cyberpeace: post-war is war, only more so <http://t.co/fkaHhcgekK> #cyberwar
ungefähr 3 Stunden her von &s

Wer wissen will was #cyberpeace ist, sollte wissen was dieser sog. #cyberkrieg ist: Matthias Schulze dazu bei uns <http://t.co/LyvFdE29dN>
8. Dezember 2014, 11:08 von &s

Neue #Jobs für Politikwissenschaftler_innen!
<http://t.co/f3vSzfJpMG>
5. Dezember 2014, 9:03 von &s

TAGS

Diese Fragen von heute und morgen sind aber zentral, und hier wird die Unterscheidung zwischen anlassbezogenem **live monitoring** und der anlasslosen Speicherung von Daten (Tempora) oder auch 'nur' Metadaten (PRISM) wichtig, die mir in der aufgeladenen Debatte (jedenfalls außerhalb der Netzpolitik-Filterbubble) oft zu kurz kommt. Wenn man akzeptiert, dass ein Staat die Aufgabe hat, seine Angehörigen vor asymmetrischen Bedrohungen zu schützen, dann gehören verdeckte Ermittlungen und vielleicht auch Abhören zum Repertoire, derer sich eine mit dieser Aufgabe betraute staatliche Stelle bedienen kann. Ein solcher Eingriff in die menschliche Privatsphäre unterliegt deshalb in Ländern, welche gerne mal in Übersee die 'Einhaltung demokratischer Mindeststandards' anmahnen und auch überwachen, einer Kontrolle durch unabhängige Stellen (Gerichte, Parlamentsausschüsse etc.) – so schwierig diese Kontrolle in der Praxis auch zu gewährleisten und zu bewerkstelligen ist. Deshalb erfolgen solche Maßnahmen anlassbezogen, zur Verhinderung der berühmten schweren Straftaten, die zur Rechtfertigung solcher Programme (manchmal zurecht, manchmal vorgeschoben) erhalten müssen. Auch terroristische Aktivitäten, die Planung von Anschlägen etc., fallen in diese Kategorie.

Aber warum genau braucht es nun die anlass- und wahllose **Speicherung** aller Verkehrsdaten, derer man habhaft werden kann? Natürlich ist es von Nutzen, die Vergangenheit einer aktuell verdächtigen Person auf Knopfdruck aus dem Datenberg abrufen zu können. Das erleichtert die ansonsten beschwerliche Informationsbeschaffung merklich: nicht immer ist es einfach, ein offenes Geständnis eines Täters zu bekommen. In der Post- 9-11 Welt war es deshalb offensichtlich möglich, mehr oder weniger heimlich zu foltern, sollte der Täter nicht geständig sein. Aus der Eigenlogik der Informationsbeschaffung ist das natürlich zielführend, solange es sich nicht um falsche Geständnisse handelt.



Nur ist die Eigenlogik der Sicherheitsapparate eben nicht die allein bestimmende Logik. Das leuchtet beim Folterverbot unmittelbar ein, und das sollte meiner Meinung nach auch für die anlasslose Speicherung privater

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)

Internet-Inhalte gelten. Zumal diese ähnlich wie die Videoüberwachung öffentlicher Plätze die Taten selber eher nicht verhindert, sondern eben bei der nachträglichen Aufklärung hilft. Auch darum gibt es eine Vielzahl sehr guter Gründe, warum etwa in Deutschland um die Speicherung der sogenannten **Vorratsdaten** gerungen wird. Nun scheint sogar die CDU/CSU bereit zu sein, eine entsprechende Abwägung vorzunehmen. Im Bundestags-Wahlprogramm 2013 ist zu lesen:

“ *Der Staat muss persönliche Kommunikationsdaten der Menschen schützen. Zugleich dürfen wir jedoch Schutzlücken bei Strafverfolgung und Gefahrenabwehr nicht hinnehmen.*
[Quelle]

Im Falle der britischen und US-amerikanischen Überwachungsprogramme sucht man nach einer solchen Abwägung vergeblich. Die Eigenlogik der Sicherheitsapparate hat eine Maschine hervorgebracht, die eben durch die massenhafte Speicherung von Daten eine völlig entgrenzte Rasterfahndung in der Vergangenheit möglich macht. Wie Andrew Denison bei Anne Will diese Woche schon sagte: “Die NSA ist da, um die Gesetze anderer Länder zu brechen, zu verletzen, ohne die Gesetze der Amerikaner zu brechen.” Ähnliches gilt für die meisten anderen Geheimdienste und daran wird sich in absehbarer Zukunft kaum etwas ändern. Außerdem steht der überzeugende Beweis, dass andere Dienste nicht ähnliche Programme aufgelegt haben, noch aus. Ersten Vermutungen nach hat Frankreich zum Beispiel ein **ähnliches Programm**. Deshalb ist es nötig, nicht beleidigt nach Amerika zu zeigen (wieso scheinen die Briten dabei eigentlich besser wegzukommen?), sondern der Überhitzung der Sicherheitsbehörden entgegenzuwirken.

Die fortwährende Verharmlosung datenschutzrechtlicher Probleme scheint jedenfalls vom Tisch – in Deutschland wie auch in der internationalen Diplomatie. Mögliche konkrete Verbesserungsvorschläge beinhalten zum Beispiel das konsequente Fördern von End-to-End Verschlüsselung, die Umsetzung von besseren Datenschutzstandards (mit tatsächlichen Sanktionen bei Verletzung), eine transparentere Kontrolle von geheimdienstlichen Aktivitäten und möglicherweise auch das Aushandeln internationaler Datenschutzabkommen. Insbesondere sollte auch darauf geachtet werden, dass ausländische Dienste nicht einfach Daten mit anderen Geheimdiensten verdachtslos tauschen und so über Ecken Auslandsgeheimdienste doch die eigenen Bürger überwachen. Darauf sollte sich die Politik konzentrieren, anstatt sich über die Drei-Klassen-Diplomatie zu ärgern.



Teaserbild <http://pixabay.com/>; Bild “Auffällig unauffällig”: CC BY SA [jpbader](#)



Tags: **Cyber Spionage**, **cybersecurity**, **cybersicherheit**, **diplomatie**, **prism**, **snowden**, **spionage**, **Überwachung**

| |
|--------------------------------|
| Sicherheits-Kommunikation (14) |
| Sicherheitskultur (205) |
| Sozialwissenschaft Online (57) |
| Stellenangebote (42) |
| Strategie (10) |
| Terrorismus (14) |
| Theorie (2) |
| Umwelt (1) |
| Versicherheitslichung (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
- Duck Of Minerva
- Future and Politics
- Hylaeon Flow
- Internet und Politik
- IR Blog
- Just Security Blog
- justsecurity.org
- Killer Apps
- Kings Of War

« **Stellenanzeigen Juni 2/2** **Houston, wir haben nach wie vor Probleme!** »



percepticon



shabka.org



Terrorismus in Deutschland



theorieblog.de



Verfassungsblog



Vom Bohren harter Bretter



whistleblower-net.de

ARCHIV

Wähle den Monat

3 Kommentare zu “Überwachen und speichern”

dr. n.w. | 10. Jul. 2013 um 19:13 |

#1

gibt es zu, liebe Leute,
ihr seid einfach kalt erwischt worden... IB-Leute sehen “es” nie sehen kommen... sei es
“die Wende”, sei es weiß ich was. sie haben es nicht sehen können, und jetzt kommen sie
mit irgendeiner alt-bekannteren Staatstheorie. was ist daran IB-spezifisch??? und ich
meine es, wofür braucht man, IB studiert zu haben, um solche “kommentare”
abzugeben?

ANTWORTEN



pano | 10. Jul. 2013 um 22:20 |

#2

Naja, um von Dr. N.W getrollt zu werden – dafür hat es immerhin gereicht. Was
genau der Gehalt dieses Kommentars sein soll, bleibt leider etwas im Nebel, oder
nicht?

ANTWORTEN

Trackbacks/Pingbacks

1. **Sicherheit über alles? | sicherheitspolitik-blog.de** - 26. Jul. 2013

[...] diesem Blog bereits breit diskutiert, sei es nun aus völkerrechtlicher oder aus ethischer Sicht. Überwachung ist vor allem in Deutschland zunehmendem Gegenwind ausgesetzt, und die Vorratsdatenspeicherung [...]

Einen Kommentar hinterlassen

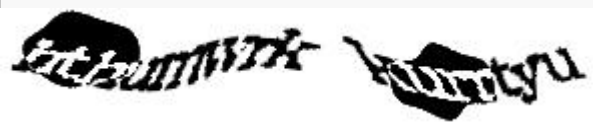
Name

Email

Webseite

Kommentar

Geben Sie den Text ein.



[Datenschutz - Nutzungsbedingungen](#)

Benachrichtige mich über nachfolgende Kommentare per E-Mail.



Impressum | 

Dieses Werk bzw. Inhalt steht unter einer Creative Commons Namensnennung-NichtKommerziell-KeineBearbeitung 3.0 Unported Lizenz.

Über diese Lizenz hinausgehende Erlaubnisse können Sie unter redaktion@sicherheitspolitik-blog.de erhalten