bitte vormerken – bitte vormerken – bitte vormerken – bitte vormerken – bitte vormerken

FIfF-Jahrestagung 2014

Der Fall des Geheimen – Blick unter den eigenen Teppich

7. bis 9. November 2014 in Berlin (Mitte)

Themenumriss: Wir wollen die Rolle Deutschlands und insbesondere der deutschen Geheimdienste im Kontext der neueren Erkenntnisse (Snowden, Foschepoth) bearbeiten. Wie kommt es, dass Deutschland oft als *Datenschutzmekka* und *Demokratievorzeigestaat* bezeichnet wird, obwohl sich gerade hier einer der Dreh- und Angelpunkte von Folterflügen, Drohnenmordkoordination, Kriegslogistik und Infrastruktur für flächendeckende Überwachung innerhalb Europas zu befinden scheint. Inwiefern ist die Rolle Deutschlands keine widerwillig helfende, ja fast opferhafte, sondern ganz im Gegenteil eine rege, aktive, tragende Säule des sich immer weiter offenbarenden antidemokratischen Zustandes der Welt? Dabei mutete es fast schon als eine Plattitüde an, wenn gesagt wird, dass dieser Zustand auf das Werk einer Techniker-Gemeinde zurückführbar ist – aber wie sind diese Systeme gebaut und nach welchen normativen Weltauffassungen wurden sie konzipiert?

Dazu wollen wir das Thema in drei Dimensionen beleuchten: 1) mit historischem Blick auf die deutschen Geheimdienste und ihre technisch-organisatorische Entwicklung, 2) mit aktuellen Analysen der gegenwärtigen Lage der Geheimdienste, ihres technischen Apparats und ihrer rechtlichen Einhegung; gerade die Verflechtungen zwischen den Geheimdiensten, Telkos und der Techniker-Gemeinde bedürfen einer besonderen Aufmerksamkeit; 3) mit Erfahrungsberichten direkt Betroffener oder gar Erzählungen von Whistleblowern (wenn wir welche kriegen).

Kurzum: Von allem den fehlenden technischen Aspekten (Kompetenz des FIfF) soll in der Debatte um die deutschen Geheimdienste Rechnung getragen werden, aber für ein Verständnis der Lage ist natürlich mehr nötig, daher wollen wir auch Vortragende aus anderen Bereichen einladen und uns explizit von Verschwörungstheorien abgrenzen.

bitte vormerken – bitte vormerken – bitte vormerken – bitte vormerken – bitte vormerken

Sara Stadler

Log 1/2014

Ereignisse, Störungen und Probleme der digitalen Gesellschaft

Immer wieder gibt es Ereignisse, Verlautbarungen und Entscheidungen, die im Zusammenhang mit dem fortschreitenden Abbau der Bürgerrechten stehen. Wir dokumentieren hier einige davon. Die Aufzählung ist sicherlich nicht vollständig; mit einigen besonders bedeutsamen Ereignissen wollen wir aber auf die weiterhin besorgniserregende Entwicklung hinweisen.

Oktober 2013

31. Oktober 2013: Im Rahmen der Koalitionsverhandlungen sprechen Union und SPD über die Bedingungen für eine Wiedereinführung der Vorratsdatenspeicherung (Quelle: Heise).

31. Oktober 2013: Die Bundesregierung legt eine Unterrichtung zum großen Lauschangriff vor. 2012 wurden neun Wohnungen akustisch überwacht, die Maßnahmen wurden auf Bundesebene wegen Bildung einer kriminellen bzw. terroristischen Vereinigung und auf Landesebene in Bremen, Niedersachsen und Nordrhein-Westfalen meist im Zuge von Ermittlungen wegen Mord und Totschlag eingesetzt. Betroffen war von der Abhöraktion, die ausschließlich in Privatwohnungen vorgenommen wurde, auch eine große Zahl von Personen, „die sich nicht identifizieren ließen" und daher auch im Nachhinein nicht über die Maßnahme informiert wurden. In drei Fällen brachte die Maßnahme keinerlei Ergebnisse. Gegenüber 2011 haben die Zahlen abgenommen (Quelle: Heise).

November 2013

1. November 2013: Neue Quellen aus dem Fundus Edward Snowdens legen nahe, dass die weltweite Überwachung des Internetverkehrs noch umfangreicher ist, als bisher angenommen. Laut der *Washington Post* greifen diesen Dokumenten zufolge NSA und GCHQ im Rahmen des Programms ‚Muscular' auf die Server von Google und Yahoo auch durch die Hintertür zu, indem sie sich Zugriff auf die Datenleitungen zwischen den Rechenzentren verschafft haben. Auf diesen Wegen können KundInnendaten unverschlüsselt abgegriffen werden. Von einer solchen Abhörmaßnahme wären etwa sämtliche Google-Cloud-Dienste sowie die ohne Google-Dienste kaum zu betreibenden Android-Smartphones betroffen (Quelle: The Washington Post, Heise).

2. November 2013: Mit großer Wahrscheinlichkeit gibt es auch in Wien eine Abhörstation der NSA. Dies folgert zumindest der Whistleblower Thomas Drake aus dem *Spiegel* vorliegenden Snowden-Dokumenten (Quelle: Der Spiegel, Heise).

2. November 2013: Wie der *Guardian* berichtet, hat der GCHQ bei der Entwicklung von Technik zur Internetüberwachung eng mit dem Bundesnachrichtendienst (BND) zusammengearbeitet. Auch die Geheimdienste Frankreichs, Spaniens und Schwedens seien an der Entwicklungskooperation beteiligt gewesen (Quelle: The Guardian, Heise).

3. November 2013: Wie Frank Bsirske, Vorsitzender der Dienstleistungsgesellschaft ver.di, in einem Interview mit *heise online* berichtet, skizzieren InnenpolitikerInnen aus CDU und CSU in einem Forderungspapier Pläne zu einer umfassenden Internetüberwachung im Stil der NSA. In den Koalitionsverhandlungen mit der SPD möchten die konservativen PolitikerInnen gerne eine Ausleitung des Datenverkehrs an den Netzknoten, wie etwa dem zentralen Austauschpunkt DE-CIX in Frankfurt, beschließen. Die ausgeleiteten Daten sollen von Geheimdiensten und Polizeien ausgewertet werden können. CDU und CSU dementieren derart umfangreiche Pläne am Folgetag (Quelle: Heise).

5. November 2013: Die *Washington Post* kann den Vorwurf erhärten, dass die NSA Daten an den Leitungen zwischen den Rechenzentren von Google abgreift. In weiteren Folien aus dem Fundus Edward Snowdens seien Datenstrukturen enthalten, die unverschlüsselt das interne Netz von Google niemals verließen. Auch seien Datenformate aufgelistet, die bei Google nur intern Verwendung fänden (Quelle: The Washington Post, Heise).

5. November 2013: Der Geheimdienstexperte Duncan Campell legt in einem Artikel im britischen *Independent* nahe, dass auch von der britischen Botschaft aus die Kommunikation in Berlin abgehört wird. Dies folgert er aus einer auf deren Dach angebrachten Struktur, die an die Anlagen der ehemaligen US-Abhörstation auf dem Teufelsberg in Berlin erinnere (Quelle: The Independent, Heise).

6. November 2013: Nachdem die SPD den von Innenminister Friedrich geforderten Zugriff auf Mautdaten zunächst abgelehnt hatte, weicht sie einem Bericht von *heise online* zufolge in neuen Koalitionsverhandlungen von dieser Haltung ab. In zukünftigen Koalitionsverhandlungen soll definiert werden, unter welchen Bedingungen die strikte Zweckbindung der Daten zu LKW-Maut aufzuheben und ihr Einsatz zu Fahndungszwecken gerechtfertigt werden soll (Quelle: Heise).

7. November 2013: Angeregt durch eine entsprechende Aussage Jacob Applebaums spekulieren verschiedene Kryptografie-Experten darüber, ob es der NSA möglich ist, die RC4-Verschlüsselung, mit der mehr als die Hälfte der verschlüsselt im Web übertragenen Daten gesichert werden, in Echtzeit zu knacken. Das Ergebnis: durchaus möglich! (Quelle: Heise)

12. November 2013: Auf der Herbsttagung des Bundeskriminalamtes (BKA) zeichnet sich ab, in welchem Ausmaß Internetüberwachung zukünftig zu erwarten ist. So hat BKA-Chef Jörg Ziercke dort den Aufbau einer kriminaltechnischen Servicestelle ‚Cyberlab' vorgestellt, in deren Rahmen sich über 100 Cyber-SpezialistInnen der „Kryptoanalyse und Dekryptierung von Verschlüsselung" widmen sollen. Zudem ist der Aufbau eines Bereichs Cyberspionage in der Abteilung *Polizeilicher Staatsschutz* geplant. Quellen-TKÜ und Onlinedurchsuchung sollen zukünftig mit einer selbst entwickelten Software betrieben werden, durch die das Einhalten des rechtlichen Rahmens – erinnert sei hier an dessen Überschreitung durch den von DigiTask für das bayrische LKA entwickelten Staatstrojaner – gewährleistet werden solle. Als Voraussetzung für die erfolgreiche Arbeit der neu geschaffenen Stellen sieht er die schnelle Einführung einer umfassenden Telekommunikationsüberwachung mit einer ausreichend langen Speicherung der IP-Adressen bei den Providern an. Klaus-Dietrich Fritsche, Staatssekretär im Bundesinnenministerium, möchte sich dabei nicht allein auf IP-Adressen beschränken, sondern plädiert für eine „technikoffene Lösung". Zudem möchte er die internationale geheimdienstliche Zusammenarbeit, etwa im Rahmen des EC3-Centers, bei Europol forcieren (Quelle: Heise).

13. November 2013: Der Internetkonzern Google schaltet in den USA eine offene Warteliste zum Test der Datenbrille Google Glass frei. Nicht thematisiert werden die schweren Eingriffe in die Privatsphäre, die durch die Brille möglich gemacht werden. So kann die Brille alle Personen im Blickfeld aufnehmen, ohne dass diese es bemerken und leitet die Daten automatisch an einen Server weiter. Dass Apps zur Gesichts- und Spracherkennung der gefilmten Personen entwickelt würden hat Google zwar zunächst ausgeschlossen aber eben nur „at this time" (Quelle: Heise).

14. November 2013: In einer Bund-Länder-Arbeitsgruppe hat die Bundesagentur für Arbeit den Vorschlag unterbreitet, die Internet-Daten von Hartz-IV-EmpfängerInnen zu überwachen, um möglicherweise nicht gemeldete Nebeneinkünfte aus dem Online-Handel aufzudecken. Auch ein erweiterter Datenabgleich mit anderen Stellen, wie Versicherungsunternehmen, wurde angeregt. Diese Vorschläge zur verdachtsunabhängigen Überwachung stießen allerdings bislang nur auf eingeschränkt positive Resonanz (Quelle: Der Spiegel, Heise).

14. November 2013: Berichten der *Süddeutschen Zeitung* und des *NDR* zufolge haben die USA von Deutschland aus unter anderem Drohneneinsätze organisiert. Auch seien deutsche Behörden aktiv an der Umsetzung des „Krieges gegen den Terror" beteiligt (Quelle: NDR, Süddeutsche Zeitung).

15. November 2013: Wie die *New York Times* und das *Wall Street Journa*l berichten, sammelt die CIA Daten zu grenzüberschreitenden Bargeld-Transfers. Nach Vorgaben des Intelligence Surveilliance Courts müssten dabei lediglich die Identitätsangaben von US-BürgerInnen anonymisiert werden (Quelle: New York Times, Wall Street Journal, Heise).

Sara Stadler

Sara Stadler studiert Informatik an der Hochschule Bremen und arbeitet in der FIfF-Geschäftsstelle.

19. November 2013: Aus Medienberichten geht hervor, dass auch der norwegische Geheimdienst in großem Stil Daten sammelt und diese auch an die NSA weitergibt. Ziel der Datensammlung sei die Unterstützung norwegischer Militäroperationen sowie des „Krieges gegen den Terror" (Quelle: Heise, Wall Street Journal).

Dezember 2013

2. Dezember 2013: Wie niederländische Medien berichten, verschafft sich auch der dortige In- und Auslandsgeheimdienst AIVD Zugriff auf NutzerInnendaten aus Internetforen (Quelle: Heise).

3. Dezember 2013: Apple erhält ein Patent für Gerätesteuerung durch Gesichtserkennung. Benannter Zweck des Geräts ist die Autorisierung der NutzerInnen. Dass sich eine solche Technologie vielfältig einsetzen lässt, steht außer Frage (Quelle: Heise).

5. Dezember 2013: Neue Snowden-Dokumente geben Aufschluss über das Ausmaß der Erfassung von Handy-Standortdaten durch die NSA. Bereits 2012 seien den der *Washington Post* vorliegenden Dokumenten zufolge weltweit täglich knapp 5 Milliarden Standortdaten gesammelt worden. Die Daten flössen in eine riesige Datenbank, wo sie mit dem Analysewerkzeug Co-Traveler ausgewertet würden. Ziel sei es, Kontakte von Zielpersonen über Bewegungsprofile zu erkennen (Quelle: The Washington Post, Heise).

9. Dezember 2013: Die französische Sicherheitsbehörde ANSSI hat durch einen Man-in-the-Middle-Angriff SSL-verschlüsselte Verbindungen ausspioniert. Das entdeckte der Konzern Google, da die Behörde dazu gefälschte Google-Zertifikate nutzte. Entsprechende Zertifikate wurden im Anschluss auch bei Mozilla und Microsoft erkannt und aus den Zertifikatslisten entfernt (Quelle: Heise).

9. Dezember 2013: Der *Guardian* veröffentlicht gemeinsam mit der *New York Times* und *ProPublica* neue Dokumente aus dem Snowden-Fundus. Daraus geht hervor, dass auch Multiplayer-Spielwelten und Xbox-Live-Netzwerke von NSA und GCHQ angezapft werden. Zudem seien auch Agenten der Geheimdienste in den virtuellen Welten unterwegs (Quelle: The Guardian, Heise).

9. Dezember 2013: Wie die *Süddeutsche Zeitung* berichtet hat die Bundesregierung Millionenaufträge an private Sicherheitsdienstleister vergeben, die für die NSA Abhörprogramme entwickelt haben, darunter der ehemalige Arbeitgeber Edward Snowdens, Booz Allen Hamilton (BAH). Ebenfalls auf der Gehaltsliste stünden Unternehmen, die bei CIA-Verschleppungen halfen, wie die CSC oder über Tochterunternehmen an Misshandlungen in Abu Ghuraib beteiligt waren, hier namentlich L-3 Communications. Gegenstand der Aufträge sei etwa die „Analyse von kritischen Infrastrukturbereichen in Deutschland" gewesen (Quelle: Süddeutsche Zeitung).

9. Dezember 2013: Eine Abmahnwelle wegen Streaming-Konsums beim Pornovideoportal *Redtube* sorgt für öffentliches Aufsehen. Vieles spricht dafür, dass die den abgemahnten Personen vorgeworfenen Urheberrechtsverletzung von den RechteinhaberInnen mittels der Umleitung des Traffics über einen Proxy selbst generiert wurde. Dabei wurden offensichtlich auch die IP-Adressen geloggt. Die AbmahnerInnen selbst äußern sich sich nicht über das genutzte Verfahren zur IP-Ermittlung. Die Herausgabe der Namen zu den IP-Adressen durch die Provider hatte das Landgericht Köln bewilligt. Dies führte zu zahlreichen Beschwerden, denen das Landgericht schließlich stattgeben musste (Quelle: Heise).

10. Dezember 2013: Die Hessische Polizei testet den Einsatz sogenannter Body-Cams. Die am Körper der Beamten angebrachten Kameras sollen diese nach eigenem Ermessen nutzen können, um Übergriffe zu verhindern. Dass dadurch auch Übergriffe durch PolizistInnen dokumentiert werden, wie ein Sprecher des hessischen Innenministeriums behauptet, ist erfahrungsgemäß eher unwahrscheinlich (Quelle: Heise).

11. Dezember 2013: Die Kassenärztliche Vereinigung weist darauf hin, dass entgegen ursprünglich anders lautender Behauptungen die alten Versicherungskarten bis zum aufgedruckten Verfallsdatum ihre Gültigkeit behalten. An der Einführung der Elektronischen Gesundheitskarte ändert das prinzipiell jedoch nichts (Quelle: Heise).

11. Dezember 2013: Aus neueren Snowden-Dokumenten geht dem kanadischen TV-Sender *CBC* zufolge hervor, das der kanadische Geheimdienst CSEC in 20 Staaten Abhörstationen für die NSA betrieben habe (Quelle: CBC, Heise).

12. Dezember 2013: In einem Rechtsgutachten stellt der Generalanwalt am Europäischen Gerichtshof Pedro Cruz Villalón fest, dass die umstrittenen Richtlinien zur Vorratsdatenspeicherung in der aktuellen Form nicht mit den Europäischen Grundrechten vereinbar sind. Grundsätzlich erachtet der Gutachter die Vorratsdatenspeicherung jedoch für legitim (Quelle: Der Spiegel, Heise).

12. Dezember 2013: In Frankreich stimmt nach der Nationalversammlung auch der Senat einer erweiterten Klausel zur Internetüberwachung zu. Danach dürfen nicht mehr nur französische Geheimdienste, sondern auch zahlreiche Behörden Verbindungs- und Standortdaten bei Providern sowie Inhaltsdaten bei Dienstanbietern zukünftig in Echtzeit abgreifen. Statt einer richterlichen Genehmigung ist zukünftig nur noch ein Gesuch bei einem nationalen Konsortium erforderlich (Quelle: Heise).

14. Dezember 2013: Wie die *Washington Post* unter Berufung auf Snowden-Dokumente berichtet, kann die NSA massenhaft Handy-Gespräche unter Ausnutzung der unsicheren Verschlüsselung des Mobikfunk-Standards GSM abhören. Auch neuere Verschlüsselungs-Mechanismen seien für die NSA möglicherweise knackbar (Quelle: The Washington Post, Heise).

14. Dezember 2013: Der Apple-Zulieferer Foxconn verstößt in seinen chinesischen Werken weiterhin gegen geltende Arbeitszeitregeln. Die geht aus dem Abschlussbericht der Fair Labor Association (FLA) hervor (Quelle: FLA).

14. Dezember 2013: Google übernimmt das unter anderem für seine Militärroboter bekannte Unternehmen Boston Dynamics, zu dessen Auftraggebern auch das Pentagon gehört. Zu-

vor hatte der Konzern bereits sieben andere auf Robotik spezialisierte Unternehmen übernommen (Quelle: Der Spiegel).

21. Dezember 2013: Aus neu veröffentlichten Snowden-Unterlagen geht hervor, dass sich der Sicherheitssoftware-Anbieter RAS Security mit zehn Millionen Dollar von der NSA für eine Hintertür in der Krypto-Bibliothek BeSafe bezahlen lies. Konkret wurde hier der von der NSA entwickelte trojanische Zufallsgenerator Dual_EC_DRBG eingebaut. Im Effekt wurde dadurch – auch von nichts ahnenden EntwicklerInnen – Sicherheitssoftware erstellt, deren Krypto-Schlüssel einfach zu knacken sind (Quelle Heise).

29. Dezember 2013: NSA und GCHQ greifen in massivem Umfang Daten an der transkontinentalen Netzinfrastruktur ab. Wie *Spiegel Online* berichtet, hat die NSA auch Zugriff auf ein Unterseekabel zwischen Europa und Asien (Quelle: Der Spiegel, Heise).

Januar 2014

2. Januar 2014: Mit Unterstützung des Wehrbeauftragten des Bundestages fordert die Bundeswehr die schnelle Anschaffung bewaffneter Kampfdrohnen (Quelle: Der Spiegel, Heise).

3. Januar 2014: Es häufen sich Berichte über Backdoors bei diversen Routermodellen namenhafter Hersteller wie Cisco, Linksys und Netgear, mittels derer die Router über das Internet ausspioniert und manipuliert werden können (Quelle: Heise).

8. Januar 2014: Wie aus der Antwort des Bundesinnenministeriums auf eine Anfrage der Linksfraktion im Bundestag hervorgeht, will die Bundesregierung die polizeiliche Zusammenarbeit und den Datentransfer auf EU-Ebene ausbauen. Konkret geht es unter anderem um den Bereich Cyber-Sicherheit sowie den Ausbau des europäischen Grenzsystems. Derartige Äußerungen lassen vermuten, dass nachfolgende Regelungen das für den Zeitraum von 2010-2014 gültige *Stockholm-Programm*, das bereits eine Echtzeitüberwachung digitaler Kommunikation vorsieht, noch übertreffen werden (Quelle: Heise).

9. Januar 2014: Wie aus einer Antwort des Innenministeriums auf eine Anfrage der Linksfraktion hervorgeht, plant die Bundesregierung die Einrichtung einer Datenbank über „reisende Gewalttäter". „Gewaltbereite Störer" sollen im Vorfeld von Veranstaltungen aus den Bereichen Freizeit, Politik oder Umwelt besonders beobachtet werden (Quelle: Heise).

10. Januar 2014: Wie aus den nun veröffentlichten Jahresbericht des parlamentarischen Kontrollgremiums des Bundestages für die Geheimdienste (PKGr) hervorgeht, haben das Bundesamt für Verfassungsschutz (BfV) und der Bundesnachrichtendienst (BND) im Jahr 2012 ihre Anti-Terror-Befugnisse noch eifriger ausgeschöpft als 2011. Insgesamt 176 Personen, die im Nachhinein nur teilweise informiert wurden, waren von der geheimdienstlichen Ausspähung mittels Auskunftverlangen bei Telekommunikations- und Luftfahrtfirmen sowie Kreditinstituten oder von IMSI-Catcher-Einsätzen betroffen. In das Post- und Fernmeldegeheimnis haben Geheimdienste im gleichen Jahr 157 mal eingegriffen (Quelle: Heise).

14. Januar 2014: In den USA hat ein Bundesberufungsgericht die Auflagen der Federal Communications Commission (FCC) zur Netzneutralität für rechtswidrig erklärt (Quelle: Heise).

14. Januar 2014: Google kauft das Unternehmen Nest Labs, das vernetzte Haushaltstechnik wie Thermostate und Rauchmelder entwickelt. Damit fließen zukünftig auch private Daten aus Haushalten zu Google (Quelle: Heise).

15. Januar 2014: Als Reaktion auf eine Kampagne des *Every Day Sexism Project* nehmen Apple und Google Spiele aus ihren Stores, in denen die SpielerInnen Schönheits-Operationen an vermeintlich übergewichtigen Mädchen durchführen sollen (Quelle: Heise).

15. Januar 2014: Die *New York Times* berichtet unter Berufung auf einen anonymen Geheimdienst-Informanten, dass die NSA aktuell fast 100.000 Computer und Netzwerke weltweit mit Spähsoftware infiziert habe (Quelle: The New York Times, Heise).

16. Januar 2014: Wie der *Guardian* berichtet, greift die NSA täglich bis zu 200 Millionen SMS ab (Quelle: The Guardian, Heise).

21. Januar 2014: Wie der *Guardian* berichtet, sollen in Großbritannien zukünftig PatientInnendaten zentral gesammelt und gegen Entgelt an Universitäten, Versicherungskonzerne oder Pharmafirmen weitergegeben werden. Zwar sollen die Daten pseudonymisiert werden, mit ein bisschen Aufwand lassen sich daraus aber theoretisch die psychischen Erkrankungen oder Trinkgewohnheiten konkreter Personen ermitteln (Quelle: The Guardian, Heise).

22. Januar 2014: In einer Anhörung des NSA-Untersuchungsausschusses spricht der russische Journalist und Geheimdienst-Experte Andrej Soldatow über das Abhörprogramm SOROM, mit dem der russische FSB die gleichen Ziele verfolge wie die NSA mit dem Programm PRISM, auch wenn ihm dafür nicht die gleichen Möglichkeiten zur Verfügung stünden (Quelle: Heise).

24. Januar 2014: *Heise Online* gibt einen Bericht des Fachblattes *Defense News* wieder, demzufolge die US-Army ihre Streitkräfte zukünftig verstärkt auf autonome Roboter umstellen möchte. Zunächst sollen diese einem Sprecher der Armee zufolge jedoch nur für Hilfsarbeiten wie Transporte eingesetzt werden (Quelle: Heise).

24. Januar 2014: Thomas de Maizière, der deutsche Innenminister, möchte weiter am Ausbau der Festung Europa mithilfe eines elektronischen Grenzsystems nach US-amerikanischem Vorbild arbeiten. Dies geht aus den Äußerungen des CDU-Politikers anlässlich des Treffens der europäischen Justiz- und Innenminister in Athen hervor (Quelle. Heise).

27. Januar 2014: Über ein von der britischen Bürgerrechtsorganisation *Statewatch* veröffentlichtes Arbeitsprogramm des EU-Polizeinetzwerks ENLETS (European Network of Law Enforcement Technology Services) werden dessen Pläne bekannt, in in der EU zugelassenen Fahrzeugen eine Technologie einzubauen, die deren Anhalten per Funk ermöglicht. Zudem will ENLETS die polizeilichen Kompetenzen in der „Funkaufklärung" in Telekommunikationsnetzen erweitern und damit die Grenze zur geheimdienstlicher Tätigkeit weiter verwischen (Quelle: Heise).

27. Januar 2014: Google kauft mit DeepMind eine Firma, die sich führend mit künstlicher Intelligenz beschäftigt. Deren Technologien können unter anderem zur Auswertung großer Datenbestände genutzt werden (Quelle: Heise).

28. Januar 2014: Aus neu veröffentlichten Snowden-Dokumenten geht hervor, dass der GCHQ die massenhaft an den Glasfaserkabeln abgegriffenen Daten von Facebook, Google, Youtube und Co. unter anderem dazu nutzen möchte, Proteste vorherzusagen und gesellschaftliche Entwicklungen berechenbar zu machen (Quelle: Heise).

28. Januar 2014: Der *Guardian*, die *New York Times* und *ProPublica* berichten von neuen Snowden-Dokumenten, denen zufolge NSA und GCHQ auch über Smartphone-Apps ins Internet übertragene Daten abgreifen. Auch aus den Daten von Spielen wie *Angry Birds*, lassen sich den Medien zufolge Einzelheiten über die Geräte und ihre NutzerInnen gewinnen (Quelle: The Guardian, The New York Times, Heise).

Stephan Geelhaar

Ausbau der Internet-Polizei

Nachschlag zur Bestandsdatenauskunft

Während sich die FIfF-Kommunikation noch im Druck befand, stand die Zeit nicht still. An dieser Stelle daher ein kurzes Update zur Neuregelung der Bestandsdatenauskunft, die in der letzten Ausgabe, Seite 27, ausführlich betrachtet wurde.

Inzwischen hat das Bundesland Sachsen mit einer Novellierung seines Polizei- und Verfassungsschutzgesetzes im Eiltempo nachgezogen. Ein entsprechender Gesetzesentwurf wurde erst am 27. September 2013 bekannt gegeben und schon am 17. Dezember mit den Stimmen der Regierungskoalition im Sächsischen Landtag verabschiedet.

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Die verabschiedeten Inhalte glei… desländer und auch die Vorbehalt… Datenabfrage weisen nur gradue… die im vorigen Heft betrachtet wu… die Rollen im Landtag. Während zur Regierungskoalition neben der CDU auch die FDP gehört, gönnten sich die Sozialdemokraten – als Teil der Opposition – den Luxus, mal gegen Gesetzesverschärfungen zu argumentieren.

In Sachsen wurde erneut das Argument ausgespielt, man brauche den Zugriff auf Passwörter und andere *Zugangscodes,* um Suizid-gefährdete Personen oder Amokläufer zu lokalisieren. Bereits im Vorfeld stellten die Grünen eine *Kleine Anfrage* an die Staatsregierung, um zu erfahren, ob denn Informationen darüber vorliegen, wie viele Suizide und Amokläufe per Telefon oder Internet angekündigt wurden. Die Antwort war denkbar knapp. Es gebe keine entsprechenden Statistiken und dies sei auch nicht „automatisiert recherchierbar". In der Landtagsdebatte selbst wurde dann deutlich, dass keine Evaluation vorliegt, die einen sinnvollen Einsatz der Auskunftsersuchen in solchen Fällen nahelegt.

Dennoch sind es solche extremen Beispiele, welche die Debatte bestimmen, während sich der weitaus wahrscheinlichere Anwendungsfall erst auf dem zweiten Blick offenbart. So nennt der Abgeordnete Christian Hartmann (CDU) auf Nachfrage folgendes Szenario:

> *Sie stellen zum Beispiel fest, dass es eine Veranstaltungsankündigung für ein Konzert im Naturschutzgebiet gibt. Nun können Sie darüber lachen, doch Naturschutz sollte Ihnen wichtig sein. Im Übrigen haben wir in der Dresdner Heide so etwas gehabt. Es gab Informationen, die zu einer Party im Naturschutzgebiet aufriefen, und es wurde angegeben, dass man zu einem bestimmten Zeitpunkt eine Handynummer anrufen soll. Hier haben … me, an der Sie entsprechend*

…men der eigentliche Grund für …heitspolitiker an den neuen Regeln zur Datenabfrage sind, gerät bei der emotional geführten Diskussion um Beispiele von Selbstmorddrohungen oft in den Hintergrund.

Dabei hat das Bundesland bereits einen eigenen Skandal um die massenhafte Abfrage von Handydaten hinter sich. Im Februar 2011 wurden während der Proteste gegen einen Neonazi-Aufmarsch in der Dresdner Innenstadt innerhalb von zwei Tagen insgesamt 1.034.000 Verbindungsdaten von Handybenutzern abgefragt. Darunter alle 20.000 Gegendemonstranten und viele Anwohnerinnen und Anwohner. Erst im vergangenen Jahr hatte ein Gericht die Rechtswidrigkeit der Maßnahme festgestellt.

Angesichts der nun verabschiedeten Gesetze steht zu befürchten, dass wir auch in Zukunft nicht von ähnlich bösen Überraschungen verschont bleiben werden. Die neu gewählte Bundesregierung (hier wiederum ohne FDP und mit SPD) hat bereits eine Gesetzesinitiative zur Vorratsdatenspeicherung angekündigt, zum *Großen Bruder* der Bestandsdatenauskunft.

Anmerkung

1 *Zitiert nach dem Protokoll der 88. Sitzung des Sächsischen Landtags (Plenarprotokoll 5/88), S. 67.*

Stephan Geelhaar studiert Informatik an der Universität Rostock und ist Neumitglied des FIfF.