Stefan Hügel

Log 1-2/2015

Ereignisse, Störungen und Probleme der digitalen Gesellschaft

Immer wieder gibt es Ereignisse, Verlautbarungen und Entscheidungen, die im Zusammenhang mit dem fortschreitenden Abbau der Bürgerrechte 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.

November 2014

18. November 2014: Das Bundessozialgericht in Kassel hat entschieden, dass das Foto auf der elektronischen Gesundheitskarte nicht gegen die informationelle Selbstbestimmung verstößt und damit rechtmäßig ist (Quelle: Bundessozialgericht, Heise).

18. November 2014: Die britische Regierung will den Zugang zu Polizeidatenbanken auf dem europäischen Festland vereinfachen und zugleich eigene einschlägige Systeme Strafverfolgern aus anderen EU-Staaten öffnen. Ziel ist der weitgehende Anschluss an den Prümer Vertrag von 2007, demzufolge Sicherheitsbehörden der beteiligten Länder etwa DNA-, Fingerabdruck- und Fahrzeugregisterdaten elektronisch einfacher austauschen können (Quelle: Heise).

19. November 2014: Der Senat hat die Reform der Spionagepraktiken der NSA mehrheitlich abgelehnt. Es fehlten zwei der benötigten 60 Stimmen, um den sogenannten „Freedom Act" zur Debatte und anschließenden Abstimmung zu bringen. Das Gesetz sollte der Sammlung von Telefondaten im Rahmen des „Patriot Act" engere Grenzen setzen; unter anderem war vorgesehen, dass die NSA keinen direkten Zugriff mehr auf Verbindungs- und Standortdaten aus der Telekommunikation bei Providern haben soll. Vor allem Republikaner blockierten das Vorhaben. Sie argumentierten, die USA könnten bei einer Verabschiedung nicht mehr ausreichend vor Terroranschlägen beschützt werden (Quelle: Heise).

20. November 2014: Die Bundesregierung hat ihre Auskunft über Pläne des BND, Zero-Day-Exploits zu kaufen und einzusetzen, unter die höchste Geheimhaltungsstufe gestellt. Nach Auskunft der Bundesregierung setzen weder das Bundeskriminalamt noch die Bundespolizei, der Verfassungsschutz, der Militärische Abschirmdienst oder das Zollkriminalamt Zero-Day-Exploits ein. Dies sei auch nicht geplant. Anders sieht dies beim Bundesnachrichtendienst aus. Pläne dazu seien aber VS-Geheim. Die Bundesregierung ist der Meinung, dass die Veröffentlichung dieser Informationen die Sicherheit der Bundesrepublik Deutschland gefährden und dem Staate schweren Schaden zufügen kann (Quelle: Andrej Hunko MdB, Heise).

21. November 2014: Aus Dokumenten von Edward Snowden geht hervor, dass der britische Geheimdienst GCHQ möglicherweise über Vodafone bzw. dessen Tochterfirma Cable & Wireless deutsche Kunden abhört. Dies würde gegen deutsches Recht verstoßen. Das BSI hält das für möglich. Vodafone dagegen betonte, dass das Unternehmen „Geheimdiensten und staatlichen Behörden in keiner Form den Zugang zu Kundendaten" gestatte, es sei denn, es sei „von Gesetzes wegen dazu verpflichtet und erhalte entsprechende Aufforderungen" (Quelle: WDR, NDR, Süddeutsche Zeitung, Heise).

21. November 2014: Das Versicherungsunternehmen Generali will Versicherte für gesunde Lebensführung belohnen. Dazu werde ein Modell entwickelt, bei dem die Versicherten regelmäßig mit ihrer Versicherung kommunizieren sollen. Für eine gesunde Lebensführung sollen sie z. B. mit Rabatten und Gutscheinen belohnt werden. Laut Süddeutscher Zeitung setze die Versicherung auf Telemonitoring; Kunden müssen regelmäßig Daten zu ihrem Lebensstil, z. B. Vorsorgeterminen, sportlichen Aktivitäten etc. übermitteln (Quelle: Süddeutsche Zeitung, Heise).

24. November 2014: In Saudi-Arabien wird laut der Menschenrechtsorganisation *Human Rights Watch* das Vorgehen gegen Netzaktivisten verschärft. Dabei würden vor allem Bürger verfolgt, die über Twitter kritische Nachrichten veröffentlichten. Grundlage dafür sei ein Gesetz gegen Cyberkriminalität, das verbiete, Inhalte zu produzieren, die „die öffentliche Ordnung schädigen" (Quelle: Human Rights Watch, Heise).

24. November 2014: Mit der Spionage-Software *Regin* wurden jahrelang Unternehmen und Behörden, vor allem in Russland und Saudi-Arabien, ausgespäht. Laut der Sicherheitsfirma Symantec sei die Software dabei so komplex, dass als Auftraggeber nur Staaten in Frage kämen. Betroffen seien vor allem Betreiber von Telekommunikationsnetzen, Fluggesellschaften, Forschungseinrichtungen und das Hotelgewerbe. Weiteren Berichten zufolge wurde *Regin* auch für den Angriff auf das belgische Telekommunikationsunternehmen Belgacom eingesetzt, der nach von Edward Snowden veröffentlichten Dokumenten vom britischen Geheimdienst GCHQ ausging, der eng mit der NSA zusammenarbeitet (Quelle: The Intercept, Heise).

25. November 2014: Durch einen Angriff auf das Firmennetz von Sony Pictures wurde dessen Betrieb zum Erliegen gebracht. Unbekannte, die sich selbst als *Guardians of Peace* (GOP) bezeichnen, haben Medienberichten in den USA zufolge die gesamte IT-Infrastruktur bei Sony Pictures übernommen. Die Gruppe droht damit, interne Daten der Firma zu veröffentlichen, wenn bestimmte Forderungen nicht erfüllt werden. In einer ZIP-Datei, die die Angreifer ins Netz gestellt haben, sollen sich unter anderem Finanzberichte, private Krypto-Schlüssel, interne Präsentationen und Kopien von Pässen von Mitarbeitern befinden (Quelle: Heise).

25. November 2014: Ein britischer Gesetzentwurf soll Internet-Provider verpflichten, dafür zu sorgen, dass Internetnutzer eindeutig per IP-Adresse identifiziert werden können. Damit sollten

die im Sommer dieses Jahres in Großbritannien beschlossenen Notstandsgesetze ergänzt werden. Die Befugnisse zur Datenspeicherung sollten eng begrenzt werden und nicht dazu dienen, Zugriffe auf Server mit illegalen Inhalten nachzuvollziehen (Quelle: The Guardian, Heise).

27. November 2014: Aus Sicht des bayerischen Innenministeriums hat sich das Verfahren *Precobs* (Pre Crime Observation System), mit dem Einbrüche vorhergesagt werden sollen, bewährt. Die Machbarkeitsstudie der Software aus dem Institut für musterbasierte Prognosetechnik in München und Nürnberg seit September 2014 soll nun auf ganz Bayern ausgedehnt werden. *Precobs* ist eine Statistiksoftware auf Basis der Theorie der *near repeats*. Einbrecher, Straßenräuber und Autoknacker gehen nach bestimmten, erfolgreich „getesteten" Mustern vor; diese werden von *Precobs* gespeichert. Gemeinsam mit statistischen Korrelationen ähnlicher Gebiete werden „Treffer" erzielt, indem bestimmte Planquadrate errechnet werden, die dann stärker von der Polizei bestreift werden (Quelle: Bayerisches Innenministerium, Heise).

27. November 2014: Im NSA-Untersuchungsausschuss hat ein früherer Sachgebietsleiter des BND eingeräumt, dass der Geheimdienst seine Überwachungsbefugnisse nutze, um „Routine"-Kommunikation zu erfassen und weiterzuleiten. Es habe Bedenken gegeben, ob die „Ableitung von Routineverkehren" aus einer gesetzlich zulässigen, aber zugleich beschränkten Maßnahme rechtmäßig sei. Dies sei in einem Rechtsgutachten für das zu dieser Zeit von Frank-Walter Steinmeier geführte Bundeskanzleramt bejaht worden; dieses habe daraufhin zugestimmt (Quelle: Heise).

Dezember 2014

5. Dezember 2014: Nach Ansicht des zuständigen britischen Gerichts verstoßen die Überwachungsprogramme des Geheimdiensts GCHQ nicht gegen die Europäische Menschenrechtskonvention. Die Menschenrechtsgruppen Amnesty International, Privacy International und Liberty hatten argumentiert, die Massenüberwachungsprogramme des GCHQ verstießen gegen das Recht auf Achtung des Privat- und Familienlebens und gegen das Recht auf freie Meinungsäußerung. Die Organisationen haben Beschwerde beim Europäischen Gerichtshof für Menschenrechte angekündigt (Quelle: Heise).

6. Dezember 2014: Die Internet-Seiten des Chaos Computer Clubs (CCC) waren zeitweise in Großbritannien für einen Teil der Internetnutzer nicht zugreifbar. Dies wurde offenbar durch die Jugendschutzsysteme der britischen Internet-Provider verhindert. Der CCC teilte mit, dass seine Seiten anscheinend auf der schwarzen Liste des britischen Pornographie-Filters gelandet seien. Der Filter war für den Jugendschutz eingeführt, dann aber auf terroristische und extremistische Inhalte ausgeweitet worden. Für den CCC ist dies eine Bestätigung, dass solche Filter für Zensur missbraucht werden können bzw. durch „Overblocking" Inhalte unabsichtlich gesperrt werden. Viele britische Kunden haben den Filter nicht aktiviert, so ist unklar, wie viele Nutzer tatsächlich die Seiten des CCC nicht erreichen konnten (Quelle: CCC, Heise).

7. Dezember 2014: Das Bundesjustizministerium verweigert die Herausgabe eines Schreibens der US-Regierung vom 5. September 2014, in dem es möglicherweise um die Auslieferung von Edward Snowden geht. Der NSA-Untersuchungsausschuss hatte das Schreiben angefordert, zur Klärung, ob Snowden bei einer Einreise nach Deutschland ausgeliefert werden könnte. Das Bundesjustizministerium hält das Schreiben nach langer Prüfung für nicht erforderlich, um die Sachverhalte zu klären, für die der Untersuchungsausschuss eingesetzt wurde. Aus Sicht des Abgeordneten der Linken, André Hahn, sei diese Ablehnung „*eine erneute und nicht hinnehmbare Brüskierung des gesamten Untersuchungsausschusses durch die Bundesregierung*" (Quelle: Heise).

8. Dezember 2014: Angesichts der Veröffentlichung des Berichtes über die CIA-Folterpraktiken in den USA hat der frühere Präsident George W. Bush den Geheimdienst verteidigt. Er lobte die CIA-Mitarbeiter gegenüber CNN: „*Das sind Patrioten und was auch immer in dem Bericht steht, wenn er ihre Beiträge zu diesem Land herabwürdigt, liegt er unglaublich falsch.*" Die USA könnten sich glücklich schätzen, diese Frauen und Männer zu haben, so Bush weiter (Quelle: CNN, Heise).

8. Dezember 2014: Der Menschenrechtskommissar des Europarats, Nils Muižnieks, kommt in einem neuen Bericht über Rechtsstaatlichkeit zu dem Ergebnis, dass geheime, massive und unterschiedslose Überwachung rechtliche Grenzen überschreite. Muižnieks erkennt darin zwar die Notwendigkeit des Kampfs gegen Cybercrime und Terrorismus an. Die Überwachung könne aber die Demokratie zerstören, anstatt sie zu schützen (Quelle: The Guardian, Heise).

9. Dezember 2014: Die US-Regierung hat erneut für weitere 90 Tage angeordnet, dass Telefonanbieter die Verbindungsdaten aller Telefongespräche an die NSA weiterleiten müssen. Dies sei erforderlich, solange die von US-Präsident Obama geplante Reform noch nicht verabschiedet sei. Die Reform sieht vor, dass die Daten bei den Providern verbleiben und nur noch auf Anfrage herausgegeben werden sollen. Gleichzeitig wurde in einer Erhebung des Softwareherstellers Open-Xchange ermittelt, dass in den USA 15 %, in Großbritannien 20 % und in Deutschland 37 % der Nutzer wegen des NSA-Skandals mindestens einen Online-Dienst verlassen hätten. Meistens sei Facebook davon betroffen gewesen, in geringerem Umfang auch Google (Quelle: US-Justizministerium, Heise).

9. Dezember 2014: In der Zusammenfassung des Berichts über die „Erweiterten Verhörmethoden" erhebt der Geheimdienstausschuss des US-Senats schwere Vorwürfe gegen die CIA. Offenbar hat der Geheimdienst Regierung und Kongress über brutale Folter und deren Effektivität getäuscht. Die Methoden seien brutaler und gleichzeitig weniger effektiv gewesen, als von der CIA behauptet (Quelle: US-Senat, Heise).

11. Dezember 2014: Der Europäische Gerichtshof hat entschieden, dass auch bei privater Videoüberwachung des öffentlichen Raums die europäische Richtlinie für den Datenschutz zu beachten ist. Die betroffenen Personen müssen auch bei den Aufnahmen einer Videoüberwachungskamera der Verarbeitung ihrer Daten zugestimmt haben. Ausgenommen seien nur Videoaufnahmen, die „*zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten*" vorgenommen werden (Quelle: EuGH, Heise).

11. Dezember 2014: Gegen den Software-Hersteller Gamma werden offenbar keine Ermittlungen aufgenommen. Gegen Gamma war vom European Center for Constitutional and Human Rights Strafanzeige gestellt worden. Mit der Gamma-Software FinFisher/FinSpy waren in Bahrain Oppositionelle und eine Regierungskommission ausgespäht worden. Da aber der Hersteller in seinen Vertragsbedingungen ausdrücklich den rechtswidrigen Einsatz der Software untersage, sei die Klage gegenstandslos (Quelle: Heise).

12. Dezember 2014: Offenbar unbemerkt von vielen Kongressmitgliedern hat der US-Kongress mit der Autorisierung des Budgets der Geheimdienste einen Absatz mitbeschlossen, der das Ausspähen von US-Bürgern erlaubt. Der Paragraph 309 des *Intelligence Authorization Act* legitimiert das eigentlich „unbeabsichtigte" Aufzeichnen von Inhalts- oder Metadaten eigener Bürger beim Erfassen von Kommunikationsströmen, die primär auf „Auslandsstrecken" ausgerichtet sein sollen (Quelle: Heise).

13. Dezember 2014: Journalisten von *The Intercept* kommen zu dem Schluss, dass der Angriff auf den belgischen Internet-Provider Belgacom offenbar aggressiver und umfassender war, als bisher dargestellt. Aus Sicht von Edward Snowden handelt es sich um das erste dokumentierte Beispiel eines Cyberangriffs eines EU-Staates auf einen anderen. Zu den Kunden von Belgacom zählen auch die Europäische Kommission, das Europäische Parlament und der Europäische Rat. Genutzt wurde dabei offenbar die Cyberwaffe *Regin* (Quelle: The Intercept, Heise).

14. Dezember 2014: Nach einem Bericht des Spiegel haben BND und CIA gemeinsam Provider in Deutschland angezapft. Der BND habe im Jahr 2005 das deutsche Tochterunternehmen eines US-Netzbetreibers aufgefordert, *„Zugang zu Kommunikationsverbindungen des Unternehmens in Düsseldorf"* zu gewähren. Das Unternehmen und der BND hätten sich dann auf eine Zusammenarbeit unter Einbindung der CIA unter dem Codenamen *Globe* geeinigt. Die Daten seien in die BND-Außenstelle Rheinhausen geleitet worden (Quelle: Der Spiegel, Heise).

16. Dezember 2014: Einer Umfrage zufolge hält ca. die Hälfte der US-Bürger Folter wie Waterboarding, die die CIA angewandt hat, zumindest teilweise für gerechtfertigt. 36 % lehnten Folter ab, 57 % sind der Ansicht, Folter könne verlässliche Informationen liefern und so Terroranschläge verhindern. Dies steht im Gegensatz zum Ergebnis des CIA-Folterreports, der zu dem Ergebnis kommt, Folter sei nicht effektiv gewesen (Quelle: CBS, Heise).

19. Dezember 2014: Mit der Operation *Eikonal* wurde laut der Deutschen Telekom grundrechtssensibles Material erfasst. Laut einer Aussage im NSA-Untersuchungsausschuss warnte die Telekom den BND, dass durch die Operation bis zu 90 % Kommunikation von geschützten Grundrechtsträgern abgegriffen werden könnte. Damit bestand eine erhebliche Gefahr, dass Datenverkehr deutscher Bürger, der unter das G10-Gesetz fiel, nicht korrekt ausgefiltert und an die NSA weitergeleitet wurde (Quelle: Heise).

22. Dezember 2014: Die Überwachung und Manipulation von Rechnern, mit denen ein Ausschuss im US-Senat die Folterpraxis des Geheimdiensts untersuchen sollte, bleibt für die CIA wohl ohne Konsequenzen. Fünf Mitarbeiter der CIA, die die Maßnahmen durchgeführt hatten, haben das Vorgehen als rechtmäßig verteidigt und sich dabei auf Anordnungen des CIA-Chefs John Brennan berufen. Im Frühjahr war bekannt geworden, dass die CIA Senatoren und Mitarbeiter, die die Foltermethoden untersucht hatten, ausspioniert hatten. Betroffen waren vor allem Computer, mit denen die Dokumente der CIA analysiert wurden. Dabei seien nach Aussage der Ausschussvorsitzenden Dianne Feinstein auch Daten gelöscht worden (Quelle: Heise).

29. Dezember 2014: Einem Medienbericht zufolge wurde auf einem Rechner im Bundeskanzleramt die Spionagesoftware *Regin* entdeckt. Eine Referatsleiterin hatte nach Berichten der Bild-Zeitung eine Datei auf ihrem privaten Laptop bearbeitet; als sie diese Datei mit einem USB-Stick auf ihren Dienstrechner übertragen wollte, schlug der Virenscanner Alarm. Untersuchungen der Rechner im Bundeskanzleramt ergaben keine weiteren Funde; das IT-System des Kanzleramts sei nicht infiziert worden (Quelle: Bild, Heise).

Januar 2015

2. Januar 2015: Gegen das massenhafte Scannen von Kfz-Kennzeichen und deren Abgleich mit Fahndungsdateien wurde Verfassungsbeschwerde eingelegt. Kläger ist der IT-Experte Benjamin Erhart, der von dem Freiburger Anwalt Udo Kauß vertreten wird, der bereits bei ähnlichen Beschwerden in Hessen und Schleswig-Holstein erfolgreich war. In dem Entwurf der Beschwerdeschrift heißt es, ohne Korrektur der bisherigen Rechtsprechung drohten *„weitreichende negative Folgen für den Grundrechtsschutz"*. Weiter heißt es, dass bei konsequenter Durchführung *„der Staat ohne gesetzliche Grundlage und ohne jegliche Einschränkung Informationen über menschliches Verhalten erfassen und auswerten kann"* (Quelle: Heise).

12. Januar 2015: Zum Gedenken an die Opfer der terroristischen Anschläge in Paris sind Millionen Menschen auf die Straße gegangen. Gleichzeitig werden die Anschläge von Sicherheitspolitikern für die Ankündigung neuer Maßnahmen genutzt. Bundesinnenminister Thomas de Maizière forderte, mehr Informationen auszutauschen. Das gelte insbesondere für die Geheimdienste. Das Europaparlament soll die Blockade des europäischen Fluggastdaten-Abkommens beenden. *„Wer jetzt ein europäisches Fluggastdaten-Abkommen ablehnt, weiß nicht, was die Stunde geschlagen hat."* Justizminister Heiko Maas (SPD) kündigt ein Gesetzespaket mit Maßnahmen für einen effektiveren Anti-Terrorkampf an. Eine Wiedereinführung der Vorratsdatenspeicherung lehnt Maas zu diesem Zeitpunkt jedoch weiter ab (Quelle: Heise).

12. Januar 2015: Bilder, die in den Clouds US-amerikanischer Anbieter hochgeladen werden, werden offenbar automatisch gescannt und dabei auch auf Darstellungen des Missbrauchs von Kindern durchsucht. Meldungen über mutmaßlich illegales Material werden demnach auch an deutsche Strafverfolgungsbehörden gemeldet. Der Rechtsanwalt Udo Vetter berichtet in seinem Blog, dass bei einem seiner Mandanten ein einzelnes fragwürdiges Bild unter mehreren tausend zu einer Meldung an das Bundeskriminalamt geführt habe (Quelle: lawblog.de, Heise).

13. Januar 2015: Großbritanniens Premierminister Cameron findet, dass jede Kommunikation für Geheimdienste einsehbar sein müsse. Für den Fall seiner Wiederwahl kündigte er neue Befugnisse für die Sicherheitsbehörden seines Landes an. Einerseits soll die 12-monatige Vorratsdatenspeicherung festgeschrieben werden, die bislang nur bis 2016 gilt. Auch Kommunikationsdienste, bei denen der Inhalt der Dialoge durch Verschlüsselung vor dem Zugriff von Sicherheitsbehörden geschützt ist, dürften nach Ansicht von Cameron nicht möglich sein (Quelle: Heise).

14. Januar 2015: Nach Statistiken zur Telekommunikationsüberwachung fragen Ermittler verstärkt Verbindungs- und Standortdaten ab. Nach 9901 Anordnungen 2012, Verbindungs- und Standortdaten auszuforschen, kam dies 2013 bereits in 12.572 Fällen vor. Dies geht aus einer jetzt veröffentlichten Übersicht des Bundesjustizamts hervor (Quelle: Heise).

14. Januar 2015: Auch Bundeskanzlerin Angela Merkel reiht sich in die Phalanx der Politiker ein, die sich die terroristischen Anschläge von Paris zu Nutze machen, gebetsmühlenartig die Einführung einer Vorratsdatenspeicherung zu fordern. Justizminister Maas lehnt die Vorratsdatenspeicherung nach wie vor ab – das wird sich später noch ändern (Quelle: Heise).

15. Januar 2015: Es ist nun sicher, dass die Ausspähung der Computer des US-Senatsausschusses zur Untersuchung der Folterpraxis der CIA keine Konsequenzen haben wird. Die Abgeordneten und der Geheimdienst hätten sich nicht auf Grundregeln für die Zusammenarbeit verständigt (Quelle: Heise).

16. Januar 2015: Nach Ansicht des ehemaligen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Peter Schaar, war die vertragliche Grundlage für das BND- und NSA-Projekt *Eikonal* zur Datenausspähung vermutlich rechtswidrig. Er sei auch nicht darüber unterrichtet worden, dass von einem Frankfurter Netzknoten zwischen 2004 und 2008 Daten abgegriffen und teilweise an die NSA weitergeleitet worden waren. Sei die Ausspähung lediglich auf Basis einer vertraglichen Vereinbarung, ohne Anordnung nach dem G10-Gesetz erfolgt, könne sie nicht rechtskonform sein (Quelle: Heise).

18. Januar 2015: Einem Bericht des Spiegel zufolge entwickelt der US-Geheimdienst NSA Waffen zur Führung von Cyberkriegen. In solchen Auseinandersetzungen soll wichtige Infrastruktur wie Strom- und Wasserversorgung gezielt ausgeschaltet werden. Beispiele für solche Cyberwaffen sind *Stuxnet* und *Regin*. Es sollen auch fremde Angriffe erkannt und Erkenntnisse fremder Geheimdienste genutzt werden. Wichtig sei es dabei, eigene Aktionen glaubhaft abstreiten zu können (Quelle: Der Spiegel, Heise).

21. Januar 2015: Zum Kampf gegen den Terror fordert jetzt auch Bundesinnenminister Thomas de Maizière, dass Sicherheitsbehörden in der Lage sein müssen, *„verschlüsselte Kommunikation zu entschlüsseln oder zu umgehen"*. Dies hätten die Anschläge von Paris deutlich gemacht (Quelle: AFP, Heise).

27. Januar 2015: Aus einem geheimen Verhandlungspapier zum „Freihandelsabkommen" TTIP geht offenbar hervor, dass sich die USA und die EU künftig über Gesetzentwürfe und weitere Vorhaben abstimmen sollten. Gesetze, Verordnungen, Standards oder spezifische Regeln, beispielsweise zum Verbraucher- und Datenschutz, sollen demzufolge in Europa nicht mehr ohne Mitsprache der USA verabschiedet werden (Quelle: Heise).

29. Januar 2015: Bundesinnenminister Thomas de Maizière fordert den Austausch von Fluggastdaten auch zwischen europäischen Staaten. Dies sei die logische Konsequenz aus dem entsprechenden Abkommen zwischen der EU und den USA (Quelle: Heise).

30. Januar 2015: Im NSA-Untersuchungsausschuss räumt der technische Leiter der Operation *Eikonal* ein, dass die Netzüberwachung der Geheimdienste nicht mit der Rechtslage vereinbar sei. Dies sei im Geheimdienst selbst thematisiert worden (Quelle: Heise).

30. Januar 2015: Einem Medienbericht zufolge greift der Bundesnachrichtendienst noch mehr Daten ab, als bisher angenommen. Demnach werden täglich 220 Millionen Verbindungsdaten erfasst und an die NSA und andere Dienste weitergeleitet. Dabei würden nicht mehr einzelne Verdächtige gezielt überwacht, sondern die Daten würden massenhaft gesammelt. Dies erfolge in fünf Dienststellen des BND. Gleichzeitig werde gezielt die parlamentarische Kontrolle behindert, indem den Kontrollgremien die Arbeit so schwer wie möglich gemacht werde (Quelle: Die Zeit, Heise).

Februar 2015

1. Februar 2015: Die von Bundesjustizminister Heiko Maas initiierte Verschärfung des Sexualstrafrechts tritt in Kraft. Anlass dafür war die Affäre um den ehemaligen Bundestagsabgeordneten und Vorsitzenden des NSU-Untersuchungsausschusses Sebastian Edathy. Edathy hatte Bilder von Kindern aus dem Internet heruntergeladen, deren Besitz möglicherweise nicht strafbar war, aber nach Ansicht der Strafverfolgungbehörden auf den Besitz strafbaren Materials hingewiesen hat. Der Besitz dieser Art von Bildern soll nun auch unter Strafe gestellt werden. Kritiker befürchten, dass nun auch unbedarfte Hobbyfotografen sich durch Bilder, beispielsweise von spielenden Kindern am Strand, strafbar machen könnten (Quelle: Heise).

2. Februar 2015: Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Andrea Voßhoff, ist von ihrer früheren Position, die Vorratsdatenspeicherung zu befürworten, abgerückt. *„Ich sehe nicht, dass eine Vorratsdatenspeicherung mit den strengen Auflagen des EuGH noch den Effekt erzielt, den die Sicherheitsbehörden mit diesem Instrument erreichen wollen"*, sagte sie in einem Spiegel-Interview. Angesichts des massiven Eingriffs in die Persönlichkeitsrechte könne sie die Maßnahme nicht mehr befürworten. Als Bundestagsabgeordnete hatte sich Voßhoff noch für die Vorratsdatenspeicherung ausgesprochen (Quelle: Der Spiegel, Heise).

3. Februar 2015: Jeremy Hammond, Mitglied von *Anonymous* und bekannt geworden als Stratfor-Hacker, steht auf einer Terror-Watchlist der US-amerikanischen Behörden. Dies wurde versehentlich bekannt. Beamte sollten das *Terrorist Screening Center* bei einem Kontakt informieren, aber dabei keinen Verdacht erregen. Warum Hammond, der gerade eine zehnjährige Haft-

strafe verbüßt, als Terrorist angesehen wird, ist unklar (Quelle: Daily Dots, Heise).

4. Februar 2015: Die US-Überwachung ausländischer Politiker wurde nach einem Bericht der National Intelligence Agency, der Dachorganisation der US-Geheimdienste, eingeschränkt. Verbindungsdaten von Ausländern sollen nun nach fünf Jahren gelöscht werden, vorausgesetzt, es gibt keine Sicherheitsbedenken. Wenn politische Führungspersönlichkeiten ausgespäht werden, sollten auch die diplomatischen Konsequenzen berücksichtigt werden. Diese Persönlichkeiten sollten nur ausspioniert werden, wenn dringende Sicherheitsbedenken vorlägen. Empörung hatte zuvor unter anderem die Ausspähung des Mobiltelefons von Bundeskanzlerin Angela Merkel ausgelöst (Quelle: National Intelligence Agency, Heise).

5. Februar 2015: Die zweitgrößte US-amerikanische Krankenkasse Anthem ist Opfer eines Hackerangriffs geworden. Dabei wurden die Kundendaten von Millionen Mitgliedern erbeutet, so der Präsident von Anthem, Joseph R. Swedish. Offenbar haben sich die Täter Datensätze mit Namen, Geburtsdaten, Kranken- und Sozialversicherungsnummern, Postanschriften, E-Mail-Adressen, Anstellungsverhältnissen und Gehaltsauskünften verschafft, jedoch keine Kreditkarteninformationen oder Krankenakten (Quelle: Heise).

5. Februar 2015: Der NSA-Untersuchungsausschuss wirft dem Bundesnachrichtendienst vor, ihm eine Falle gestellt zu haben, um ihn zu diskreditieren. Durch eine gezielte Indiskretion sollte dem Ausschuss Geheimnisverrat angelastet werden. In einer halböffentlichen Sitzung hätten BND-Chef Gerhard Schindler und Geheimdienstkoordinator Klaus-Dieter Fritsche detailliert über eine Operation berichtet, und gleichzeitig darauf bestanden, dass die Information nicht an die Öffentlichkeit gelangen dürfe. Es ging dabei um die Drohung des britischen GCHQ, die Kooperation mit dem BND zu beenden (Quelle: Süddeutsche Zeitung, Heise).

6. Februar 2015: Das zuständige Gericht in Großbritannien hat entschieden, dass die Überwachung britischer Bürger durch den Geheimdienst GCHQ im Rahmen der Programme Prism und Upstream gegen die Europäische Menschenrechtskonvention verstößt und damit illegal ist. Durch die Verarbeitung der Daten britischer Bürger und Bürger in Großbritannien, die von der NSA abgegriffen worden sind, sei gegen deren Recht auf Achtung des Privat- und Familienlebens verstoßen worden. Inzwischen halte sich der GCHQ aber an die Gesetze (Quelle: The Guardian, Heise).

9. Februar 2015: Der Berliner Datenschutzbeauftragte Alexander Dix zeigt sich besorgt über private Überwachungskameras, die immer billiger zu kaufen sind und immer größere Verbreitung in Geschäften, Imbissen, Kneipen, Tankstellen und Privatgrundstücken finden. Es gebe dadurch kaum noch unbeobachtete Stellen; das Recht, sich im öffentlichen Raum unbeobachtet zu bewegen, werde immer mehr eingeschränkt. Als Grund dafür sieht Dix die Technikgläubigkeit der Menschen, durch Kameras Sicherheit zu produzieren (Quelle: Heise).

9. Februar 2015: Nach den Anschlägen von Paris ist in Frankreich ein Gesetz in Kraft getreten, das den Terrorismus bekämpfen soll und dafür Provider zur Sperrung von Internet-Seiten auf Verlangen der Regierung verpflichtet. Die Seiten müssen innerhalb von 24 Stunden nach einem entsprechenden Hinweis der zuständigen Behörde gesperrt werden. Die Bürgerrechtsorganisation *La Quadrature du Net* kritisiert die Regelung als Einschränkung der Redefreiheit als wichtigster Errungenschaft der Demokratie (Quelle: The Register, Heise).

9. Februar 2015: Die im „Freihandelsabkommen" TTIP vorgesehene Schiedsgerichtsbarkeit für Investoren (ISDS) wird im EU-Parlament kritisiert. Sie sei angesichts der weit entwickelten Rechtssysteme in den USA und der EU unnötig; ein Schlichtungsverfahren und der normale Rechtsweg reichten aus (Quelle: Heise).

11. Februar 2015: Ein Studie des Bundeskriminalamts (BKA) kommt zu dem Ergebnis, Hacktivisten entstammten der Mittelschicht, seien überwiegend männlich und zwischen 16 und 30 Jahren alt. Sie gingen wie Cyberkriminelle vor, seien dabei aber nicht profitorientiert, sondern verfolgten politische oder moralische Zielsetzungen. Dabei zählt das BKA auch Kim Dotcom, Gründer des Filehosting-Dienstes Megaupload, zu den Hacktivisten. Das BKA fürchtet vor allem die nachrichtendienstliche Lenkung hacktivistischer Projekte (Quelle: Bundeskriminalamt, Heise).

13. Februar 2015: Informationen über Delikte, die die Verkehrssicherheit gefährden, sollen künftig in der gesamten EU weitergegeben werden können. Dafür hat das Europäische Parlament einen Richtlinienentwurf mit 640 Ja-Stimmen beschlossen. Der Entwurf beruft sich auf die Verbesserung der Verkehrssicherheit. Einen ersten Anlauf für den Datenaustausch gab es bereits 2011; die damalige Rechtsgrundlage, die polizeiliche Zusammenarbeit in der EU, befand der Europäische Gerichtshof (EuGH) für nicht ausreichend und den damaligen Richtlinienentwurf deswegen für nichtig (Quelle: Heise).

16. Februar 2015: Tödliche Anschläge in Kopenhagen macht sich die CSU erneut zunutze, die Einführung der Vorratsdatenspeicherung zu fordern. Die SPD solle ihren Widerstand gegen dieses Instrument aufgeben (Spoiler: Sie wird es bald tun). CDU-Innenpolitiker Wolfgang Bosbach erklärte, es gelte, das Thema Vorratsdatenspeicherung auf der Tagesordnung zu halten (Quelle: Die Welt, Nordwest-Zeitung, Heise).

17. Februar 2015: Einer Auskunft der Bundesregierung zufolge beobachtet der Generalbundesanwalt den Einsatz der Überwachungssoftware *FinFisher* gegen die Opposition in Bahrain. Es werde immer noch geprüft, ob es sich dabei um eine geheimdienstliche Tätigkeit handle. Das *European Center for Constitutional Human Rights* (ECCHR) hatte im Oktober 2014 Strafanzeige gestellt (Quelle: Kleine Anfrage der Fraktion *Die Linke*, Heise).

20. Februar 2015: Nach einem Gesetzentwurf von Bundesinnenminister Thomas de Maizière sollen die Überwachungsbefugnisse des Bundesnachrichtendienstes (BND) weiter ausgeweitet werden. Die strategische Fernmeldeaufklärung soll künftig auch zur Abwehr von „Cyber-Gefahren" Daten ausspähen dürfen. Zusätzlich zu den bisherigen Befugnissen soll nun auch im Fall eines *„internationalen kriminellen, terroristischen oder staat-*

lichen Angriffs mittels Schadprogrammen oder vergleichbaren schädlich wirkenden informationstechnischen Mitteln auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland" der Abgriff der Daten erfolgen dürfen – bei „Gefahr im Verzug" durch das Innenministerium bei Zustimmung des Vorsitzenden des sonst zuständigen Parlamentarischen Kontrollgremiums (PKG). Das Gesetz, das sich auf das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme („Computer-Grundrecht") beruft, bedeutet eine erhebliche Ausweitung der Überwachungsbefugnisse. Der Entwurf wird am 25. März 2015 ohne wesentliche Änderungen vom Bundeskabinett beschlossen (Quelle: Heise).

25. Februar 2015: *Oscar Health*, ein Startup-Unternehmen im Krankenversicherungsmarkt, will die Fitnessdaten seiner Kunden aufzeichnen und einen Bonus an Versicherte zahlen, die ein Trainingsprogramm erfolgreich absolvieren. Die Daten dafür liefern Apps für iPhones und Android-Smartphones. Beim Erreichen bestimmter Fitness-Ziele erhalten Versicherte Smartwatches und Prämien; absolvieren sie das Trainingsprogramm erfolgreich, gibt es einen Dollar pro Tag – maximal 20 Dollar pro Monat (Quelle: New York Times, Heise).

25. Februar 2015: Der Berichtsentwurf für eine geplante EU-Richtlinie sieht vor, Flugpassagierdaten auch auf innereuropäischen Strecken zu sammeln und auszuwerten. Die Daten sollen dabei für fünf Jahre gespeichert, aber nach 30 Tagen anonymisiert werden. Bei Verdacht auf schwere oder terroristische Straftaten sollen Rückschlüsse auf Personen möglich sein (Quelle: netzpolitik.org, Heise).

März 2015

2. März 2015: Die Überwachungsbefugnisse der NSA wurden erneut auf Antrag der US-Regierung durch den *Foreign Intelligence Surveillance Court* (FISC) verlängert. Die Befugnisse gelten nun bis zum 1. Juni 2015; danach laufen einige Bestimmungen des *Patriot Act* aus, unter anderem Abschnitt 215, auf dem die Überwachungsbefugnisse der NSA basieren. Es wird jedoch damit gerechnet, dass der US-Kongress bis dahin eine modifizierte Form der entsprechenden Bestimmungen beschließt (Quelle: Heise).

2. März 2015: Eine Studie des Bayerischen Landesamts für Datenschutzaufsicht in Ansbach hat ergeben, dass in Smart-TVs Datenschutzbestimmungen nicht ausreichend umgesetzt werden. Alle Vorgänge lösen bei einzelnen der 13 überprüften TV-Geräte Datenflüsse zum Hersteller aus. Die TV-Geräte müssen aber in der Grundeinstellung anonym nutzbar bleiben (Quelle: Heise).

4. März 2015: Es gibt Hinweise, dass der gesicherte Blackberry des Vorsitzenden des NSA-Untersuchungsausschusses Patrick Sensburg ausspioniert worden ist. Nach einer Funktionsstörung wurde das Gerät in einem verplombten Behälter zum Bundesamt für Sicherheit in der Informationstechnik (BSI) gesendet; offenbar wurde dieser auf dem Weg geöffnet. Das BSI soll nun prüfen, ob das Mobiltelefon ausgelesen worden ist (Quelle: Die Welt, Heise).

9. März 2015: Im Rahmen einer umfassenden Umstrukturierung soll der US-amerikanische Geheimdienst *Central Intelligence Agency* (CIA) stärker auf Cybersecurity ausgerichtet werden. Dazu soll ein Direktorat für digitale Innovationen eingerichtet werden. Es soll sich um Datenbeschaffung, digitale Spionage, Cybersecurity und Schutz der eigenen Infrastruktur kümmern. Die Bereiche der CIA sollen stärker miteinander verzahnt werden (Quelle: Washington Post, Heise).

10. März 2015: Rund 20.000 Menschen aus Medien, Politik und Diplomatie wurden offenbar in Mazedonien jahrelang gezielt ausspioniert. Die Opposition hat angebliche Mitschnitte von Telefonaten der Regierung veröffentlicht. Demnach bestehe ein Netzwerk aus Medien, Justiz, Polizei, Regierung und Geheimdiensten, das die Gesellschaft kontrolliere. Initiator der Ausspähung ist der Opposition zufolge Premierminister Nikola Gruevski. Die Regierung spricht von einem Putschversuch (Quelle: Der Standard, Economist, Heise).

10. März 2015: Einem Bericht von *The Intercept* zufolge arbeiten NSA und CIA gemeinsam daran, Sicherheitsvorkehrungen von Microsoft und Apple zu umgehen und Daten von deren Nutzern auszuspähen. Offenbar werden jährlich in einer geheimen Veranstaltung Sicherheitslücken diskutiert und Entwicklungswerkzeuge manipuliert (Quelle: The Intercept, Heise).

11. März 2015: Die Regelung zur Vorratsdatenspeicherung in den Niederlanden muss vorerst außer Kraft gesetzt werden. Nachdem der Europäische Gerichtshof (EuGH) die entsprechende EU-Richtlinie für rechtswidrig erklärt hatte, hat dies nun ein Gericht in Den Haag entschieden. Die Vorratsdatenspeicherung verletze das Recht auf Achtung des Privatlebens. Gegen die in den Niederlanden gültige Speicherfrist von einem Jahr hatten Telekommunikationsanbieter, Juristen und Journalisten geklagt (Quelle: netzpolitik.org, Heise).

12. März 2015: In Bulgarien hat das Verfassungsgericht die Regelung zur Vorratsdatenspeicherung außer Kraft gesetzt. Ombudsmann Konstantin Pentschew hatte in seiner Klage argumentiert, die Freiheit und das Geheimnis der Korrespondenz, die in der bulgarischen Verfassung garantiert sind, würden durch die Speicherung verletzt (Quelle: Heise).

14. März 2015: Die Regierungen der EU-Mitgliedstaaten weichen offenbar die Regelungen der geplanten EU-Datenschutz-Grundverordnung deutlich auf. Standards von Grundprinzipien des Datenschutzes, der Zweckbindung und der Datensparsamkeit, sollen dabei reduziert und „legitime Interessen" von Firmen und Ämtern an Personendaten über die Interessen der Betroffenen gestellt werden. Der Berichterstatter für die Datenschutzreform im Europäischen Parlament, Jan Philipp Albrecht hatte bereits zuvor erklärt, damit sei eine *„Rote Linie überschritten"*. Das Parlament könne einer solchen Position nicht zustimmen; dies würde das Ende der Datenschutzreform bedeuten. Unverständlich sei auch, dass sich offenbar die deutsche Bundesregierung für einen niedrigeren Standard als in der heute gültigen Richtlinie von 1995 einsetze (Quelle: statewatch.org, netzpolitik.org, Heise).

15. März 2015: Wirtschaftsminister Sigmar Gabriel (SPD) setzt sich für die Wiedereinführung der 2010 vom Bundesverfassungsgericht zurückgewiesenen Vorratsdatenspeicherung ein.

„Wir brauchen das … wir erleben doch gerade, dass die Welt ziemlich gefährlich geworden ist", erklärte er. Es müsse im verfassungsrechtlich vertretbaren Umfang reagiert werden können. Gabriel hatte die Datenspeicherung im Gegensatz zu Justizminister Heiko Maas bereits zuvor befürwortet (Quelle: Deutschlandfunk, netzpolitik.org, Heise).

17. März 2015: Die Spielzeugpuppe *Hello Barbie* spricht beim Spielen mit den Kindern und zeichnet dabei deren Gespräche auf. Dadurch können die Gespräche mit Spracherkennungssoftware ausgewertet und passende Antworten generiert werden. Die Puppe stelle Fragen, deren Beantwortung sensible Informationen über das Kind und seine Familie liefere, die für Marketing genutzt werden können, so die *Campaign for a Commercial-free Childhood* (CCFC). Offenbar werden die Daten auch weiterverarbeitet, um die Spracherkennungssoftware weiterzuentwickeln, und darüberhinaus an Dritte weitergegeben. Nach Aussagen des Herstellers der Spracherkennungssoftware *ToyTalk* sei für das Mitschneiden der Gespräche das Einverständnis der Eltern erforderlich; die Daten würden nicht für Marketingzwecke eingesetzt (Quelle: CCFC, Washington Post, Heise).

17. März 2015: Die französische Regierung plant eine Reform des Geheimdiensts, bei der dessen Befugnisse erweitert werden sollen. Ohne richterliche Kontrolle dürften dann Wohnungen, Büros und Autos der Zielobjekte überwacht werden; dies sei aber heute bereits Praxis. Weitere Befugnisse seien der Einsatz von IMSI-Catchern, erweiterte Möglichkeiten des Abhörens von Skype und die Verfolgung von Kommunikation über Facebook und Twitter. *Human Rights Watch* kritisiert den Entwurf, insbesondere die Kompetenz für den Premierminister, Überwachungsmaßnahmen zu autorisieren und die Pflicht für Provider, *„heimlich unspezifizierte, vom Staat vorgegebene Mittel zum Analysieren verdächtigen Verhaltens"* einzusetzen (Quelle: Le Monde, Figaro, Telepolis, netzpolitik.org, Heise).

26. März 2015: In einem Schnellverfahren hat das bulgarische Parlament die zuvor vom Verfassungsgericht gestoppte Vorratsdatenspeicherung wieder eingeführt. Dabei gelten nun kürzere Speicherfristen von einem halben anstatt einem Jahr. Die Arbeit der Sicherheitsdienste dürfte nicht erschwert werden, so die konservative Regierungspartei (Quelle: Heise).

26. März 2015: Einem Vertreter der EU-Kommission zufolge schützt des *Safe-Harbour*-Abkommen nicht ausreichend vor Datenmissbrauch. Wer fürchtet, dass seine Daten vor der NSA nicht sicher seien, *„sollte sich überlegen, ob er seinen Facebook-Account nicht besser löscht"*, erklärte er. *„So wie* Safe Harbour *derzeit in den USA rechtlich verankert ist, gibt es keine Garantie dafür, dass fundamentale EU-Datenschutzrechte beachtet werden"* (Quelle: Irish Times, Heise).

27. März 2015: Das australische Parlament hat eine sehr weitgehende Regelung zur Vorratsdatenspeicherung verabschiedet. Provider müssen Verbindungs- und Standortdaten einschließlich Geräteadressen zwei Jahre lang aufbewahren. Für den Zugriff benötigen Polizei und Geheimdienste in der Regel keine richterliche Genehmigung; diese ist nur erforderlich, wenn auf Daten von Journalisten zugegriffen werden soll. Betroffene müssen nicht über den Datenzugriff benachrichtigt werden (Quelle: Heise).

31. März 2015: Nach Vorstellung von Verteidigungsministerin Ursula von der Leyen soll Deutschland gemeinsam mit Italien und Frankreich eine Kampfdrohne entwickeln. Die Verteidigungsexpertin der Linken, Christine Buchholz, erklärte dazu, Deutschland dürfe sich *„nicht am völker- und menschenrechtswidrigen internationalen Drohnenkrieg beteiligen"* (Quelle: Der Spiegel, Heise).

April 2015

8. April 2015: Die US-Drogenpolizei hat offenbar jahrelang Verbindungsdaten auf Vorrat gespeichert und ausgewertet. Dies ist nun Gegenstand eines Gerichtsverfahrens, das *Human Rights Watch* und die *Electronic Frontier Foundation* (EFF) angestrengt haben. In der Klage wird gefordert, die Auswertung der Daten zu unterbinden und rechtswidrig gesammelte Informationen zu löschen (Quelle: EFF, netzpolitik.org, Heise).

9. April 2015: Der französische Fernsehsender *TV5Monde* ist offenbar das Ziel islamistischer Hacker geworden. Dabei fielen alle Kanäle des Senders zeitweise aus; auf den Seiten im Web und bei Facebook waren islamistische Drohungen zu lesen. Nach Aussage der IT-Chefin, Hélène Zemmour, hatten die Angreifer gleichzeitig die internen IT-Systeme und die Sendeanlagen unbrauchbar gemacht und Web-Seite, Facebook- und Twitter-Konto unter ihre Kontrolle gebracht (Quelle: FranceTVInfo, Heise).

10. April 2015: Die Menschenrechtsorganisation *Amnesty International* reicht gemeinsam mit den Organisationen *Liberty* und *Privacy International* beim Europäischen Gerichtshof für Menschenrechte Klage gegen Großbritannien wegen der Überwachungspraxis des Geheimdienstes GCHQ ein. Basis sind Dokumente, die Edward Snowden zugänglich gemacht hatte. Obwohl ein Teil der Praktiken des GCHQ in Großbritannien für illegal erklärt worden waren, kann die Überwachung von Telefon- und E-Mail-Verkehr fortgesetzt werden (Quelle: Amnesty International, netzpolitik.org, Heise).

10. April 2015: Die Anzahl der Abfragen von Bankkonten durch deutsche Behörden ist laut einer Statistik des Bundesfinanzministeriums von 142.000 im Jahr 2013 auf 230.000 im Jahr 2014 gestiegen, das entspricht einem Wachstum von mehr als 60 %. Die Bundesdatenschutzbeauftragte Andrea Voßhoff stellt dazu fest, dass die Abfragen nicht mehr nur das Austrocknen der Finanzströme von Terroristen zum Ziel hätten, wofür das Instrument ursprünglich vorgesehen gewesen sei. Inzwischen würden ohne Anlass alle Kontoinhaber in Deutschland erfasst (Quelle: Heise).

17. April 2015: Die bisherigen strengen Vorgaben für die Weitergabe von Daten aus der LKW-Maut sollen aufgeweicht werden. Die Große Koalition will die Daten auch für *„Zwecke der Verkehrslenkung und Verkehrsforschung vollständig anonymisiert und in enger Abstimmung mit den Datenschutzbeauftragten"* Dritten zugänglich machen. Die strenge Bindung an Abrechnungszwecke war bei Einführung der Maut Voraussetzung gewesen; bereits in der Vergangenheit gab es aber wiederholt Begehrlichkeiten, die Daten auch anderweitig zu nutzen (Quelle: Handelsblatt, Heise).

19. April 2015: Der Luftwaffenstützpunkt Ramstein spielt offenbar eine zentrale Rolle im Drohnenkrieg „gegen den Terror" der USA. Geheimen Dokumenten zufolge werden praktisch alle Drohnenangriffe der US-Air-Force über Ramstein abgewickelt. Ein US-Amerikaner, der mit dem Programm vertraut sei, habe die Dokumente weitergegeben: *„Von Ramstein wird das Signal übermittelt, das den Drohnen befiehlt, was sie tun sollen. Ohne Ramstein könnte keine der Drohnen gesteuert werden – jedenfalls nicht in der bisher geübten Weise."* Bereits vor einem Jahr gab es Hinweise auf diese zentrale Rolle; der ehemalige Drohnenpilot Brandon Bryant hatte damals erklärt, der Drohnenkrieg des US-Militärs sei ohne Deutschland nicht möglich (Quelle: Der Spiegel, The Intercept, NDR, WDR, Süddeutsche Zeitung, netzpolitik.org, Heise).

20. April 2015: Die Vorratsdatenspeicherung soll noch vor der Sommerpause im Schnellverfahren vom Deutschen Bundestag verabschiedet werden. Bundesjustizminister Heiko Maas, der sich zuvor immer gegen die Vorratsdatenspeicherung ausgesprochen hatte, hat nach vollzogener Kehrtwende „Leitlinien" vorgelegt, die er nun zügig zu einem Gesetzentwurf weiterentwickeln und im Bundeskabinett beschließen lassen will. Die Leitlinien sehen eine Speicherfrist von 10 Wochen vor. Unter anderem sollen offenbar Standortdaten von jedem Kommunikationsvorgang archiviert werden; dies wäre wohl auch der Fall, wenn ein Mobiltelefon automatisch prüft, ob bei sozialen Netzwerken oder Chat-Diensten Nachrichten eingegangen sind. Die liberalen Politiker Wolfgang Kubicki und Ex-Bundesinnenminister Gerhart Baum haben im Fall der Verabschiedung erneut Klage vor dem Bundesverfassungsgericht angekündigt. Aus Sicht der Bundesdatenschutzbeauftragten Andrea Voßhoff ist zweifelhaft, ob die vorgelegten Leitlinien mit der Europäischen Grundrechtecharta vereinbar sind (Quelle: Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, taz, Neues Deutschland, netzpolitik.org, Heise).

22. April 2015: Der Betreiber des Internetknotens DE-CIX in Frankfurt am Main hat Klage beim Bundesverwaltungsgericht gegen die Ausleitung von Daten durch den BND angekündigt. Bei einer Niederlage würde man auch vor das Bundesverfassungsgericht gehen. Aufsichtsrat Klaus Landefeld erklärte, dass das Unternehmen die Maßnahmen für unzulässig halte. Ein Gutachten zur Unterstützung der Klage wurde unter anderem vom ehemaligen Bundesverfassungsrichter Hans-Jürgen Papier erstellt (Quelle: netzpolitik.org, Heise).

23. April 2015: Das Projekt *Eikonal*, mit dem der BND einen Frankfurter Netzknoten ausspioniert und Daten an die NSA weitergeleitet hat, war stärker gegen europäische und deutsche Interessen gerichtet, als bisher bekannt. Bis zu 40.000 Selektoren – etwa IP-Adressen, Mobiltelefonnummern oder Suchkriterien – waren gegen diese Interessen gerichtet. Scheinbar wurden auch Politiker gezielt und unrechtmäßig ausgespäht. Dieter Urmann, früherer Leiter der Abteilung Technische Aufklärung, erklärte, dass die Ausspähung der NSA beispielsweise auch auf die Begriffe „EADS", „Eurocopter" und „französische Behörden" abgezielt hätte (Quelle: Der Spiegel, netzpolitik.org, Heise).

25. April 2015: Holger Münch, Präsident des Bundeskriminalamts (BKA) kündigt an, dass eine von seiner Behörde entwickelte Software zur Ausspähung der Computer und Smartphones Tatverdächtiger im Herbst 2015 einsatzbereit sein soll. Die Software, in der Öffentlichkeit als Staatstrojaner oder Bundestrojaner bezeichnet, kann beispielsweise Internet-Telefonie, Messenger-Dienste und E-Mail-Verkehr protokollieren (Quelle: Der Spiegel, Heise).

26. April 2015: Medienberichten zufolge ist dem Bundeskanzleramt bereits seit 2008 bekannt, dass die NSA versucht hat, dem BND illegale Ausspähziele unterzuschieben (Quelle: netzpolitik.org, n-tv, Heise).

28. April 2015: Das Europäische Parlament hat mit großer Mehrheit einen Verordnungsentwurf beschlossen, nach dem ab Ende März 2018 bei neu eingeführten Automobil-Modellreihen der Einbau des Notrufsystems eCall vorgeschrieben ist. Der Notruf soll bei einem Unfall manuell oder automatisch, wenn der Airbag ausgelöst wurde, die Notrufnummer 112 anwählen und Fahrzeugklasse, Treibstoffart, Zeit und Ort des Unfalls übermitteln. Die Daten dürfen nicht ohne Genehmigung an Dritte weitergegeben werden und müssen vom Fahrer dauerhaft gelöscht werden können (Quelle: Heise).

29. April 2015: Im Zusammenhang mit dem BND-Skandal hat die Bundesregierung offenbar falsche Angaben gegenüber Parlamentariern gemacht. In der Antwort auf eine Kleine Anfrage der Linksfraktion wurde angegeben, es lägen keine Erkenntnisse zu Wirtschaftsspionage durch die NSA oder andere US-Dienste in anderen Staaten vor. Mittlerweile scheint aber klar, dass der BND das Bundeskanzleramt bereits seit Jahren auf Versuche der NSA hingewiesen hat, Wirtschaftsspionage in Europa und Deutschland zu betreiben (Quelle: Deutscher Bundestag, Heise).

30. April 2015: Das Verfassungsgericht der Slowakei hat entschieden, dass die Bestimmungen des dortigen Gesetzes zur Vorratsdatenspeicherung gegen die Verfassung der Slowakischen Republik, die Europäische Menschenrechtskonvention und die Charta der Grundrechte der Europäischen Union verstoßen. Geklagt hatte das *European Information Society Institute* (EISI) (Quelle: netzpolitik.org)

30. April 2015: Das Flugzeugunternehmen *Airbus* kündigt an, Strafanzeige gegen Unbekannt wegen Industriespionage zu erstatten. Offenbar wurde der Konzern und das Vorgängerunternehmen EADS jahrelang von englischsprachigen Geheimdiensten, den *Five Eyes*, ausgespäht. Tom Enders, der Chef von *Airbus*, soll sich über das Schweigen der Bundesregierung verärgert gezeigt haben; er forderte sie auf, endlich Stellung zu den Vorwürfen zu beziehen (Quelle: Der Spiegel).

Stefan Hügel

Stefan Hügel ist Vorsitzender des FIfF, arbeitet als IT-Berater und lebt in Frankfurt am Main