# Grumpy Cat against NSA


Via Anke Domscheit-Berg

---

# Truecrypt

Fefe schreibt etwas Vernünftiges über Truecrypt.

---

# Verschlüsselte E-Mails auslesen?

Tagesschau: „Die neuen Erkenntnisse zu den Anstrengungen von NSA und GCHQ bedeuten nicht zwangsläufig, dass die

Geheimdienste alle verschlüsselten Mails auslesen. Sie haben nach Ansicht von Experten dadurch in Verdachtsfällen die Möglichkeit jede E-Mail zu knacken – sollten die Angaben Snowdens der Wahrheit entsprechen.“ (Danke, Ruben: „Was berichten die Medien als Nächstes? Das Gerät NSA kann jetzt alles, auch Kaffee kochen?“)

Was ist denn das für ein Unsinn? Und welche „Experten“ wurden da gefragt?

Gestern zitierte ich Edward Snowden. u.a. laut Wired:
*Properly implemented strong crypto systems are one of the few things that you can rely on," he said, though cautioning that the N.S.A. often bypasses the encryption altogether by targeting the computers at one end or the other and grabbing text before it is encrypted or after it is decrypted.*

Heise übersetzt das so: „Verschlüsselung funktioniert. Sauber implementierte, starke Verschlüsselung ist eines der wenigen Dinge, auf die man sich noch verlassen kann.“ Die Betonung liegt auf „sauber implementiert“.

Wie ich immer in meinem Seminaren sage: Man kann sich das Niveau der Berichterstattung deutscher Medien über Sicherheitsthemen nicht unterirdisch genaug vorstellen.

---

# Deutsche Medien im Kriegsrausch

Telepolis: „Deutsche Medien im Kriegsrausch (…) entdecken deutsche Medien den moralischen Imperativ von Massenvernichtungswaffen – ein Beispiel für die kuriosen Begründungen für einen sinnlosen Rachefeldzug.“

Interessant ist auch, was die Graswurzelrevolution vor drei Jahren über den Kriegshetzer Bernd Ulrich schrieb, der in der ZEIT die Front der Bellizisten anführt: „Von 1984 bis 1988 war Bernd Ulrich, heute stellvertretender Chefredakteur der Zeit und Leiter ihres „Politik-Ressorts“, Journalist bei der Graswurzelrevolution.“

---

# WAF


Via Kiezneurotiker

---

# Grossangriff auf Verschlüsselung

*Well, when the president does it, that means it is not*

*illegal. (Richard Nixon)*

Heise: „Laut Guardian verlangten Vertreter der Geheimdienste von der britischen Zeitung und ihren Partnern New York Times und ProPublica, die Enthüllungs-Artikel über die Angriffe von NSA und GCHQ auf Verschlüsslung im Internet zu unterlassen. Begründung: Zielpersonen im Ausland könnten durch die Veröffentlichung veranlasst werden, zu neuen Formen der Verschlüsselung oder der Kommunikation im Allgemeinen zu wechseln, die schwerer zu sammeln und zu entschlüsseln wären. Guardian, New York Times und ProPublica lehnten das Ansinnen zwar ab. Sie entschieden sich aber, bestimmte detaillierte Informationen aus den Artikeln zu entfernen."

Was für Weicheier! Ich bin mal gespannt, ob deutsche Medien, die eventuell mit dem *Guardian* in der causa Snowden kooperiert haben, sich ähnlich feige verhalten. Aber vermutlich werden sie auf Grund ihrer obrigkeitshörigen Attitude (Interviews werden autorisiert, E-Mail-Verschlüsselung ist weitgehend unbekannt) erst gar nicht berücksichtigt.

Man muss bei dem Begriff „Verschlüsselung" auch genauer hinschauen. Ist SSL gemeint? [Wikipedia über SSL] Oder geht es um public-key-Verfahren, also zum Beispiel um OpenPGP? Letzteres hat Snowden selbst benutzt und empfohlen, man kann also eine Hintertür ausschließen (nicht aber im Betriebssystem, mit dem man das nutzt).

Der Guardian schreibt:
*A 10-year NSA program against encryption technologies made a breakthrough in 2010 which made „vast amounts" of data collected through internet cable taps newly „exploitable".*
Leider werden wir im Unklaren darüber gelassen, was genau damit gemeint ist. Die New York Times ist ähnlich vage:
*Beginning in 2000, as encryption tools were gradually blanketing the Web, the N.S.A. invested billions of dollars in a clandestine campaign to preserve its ability to eavesdrop. Having lost a public battle in the 1990s to insert its own*

*„back door“ in all encryption, it set out to accomplish the same goal by stealth.*

Immerhin. Wenn man den Artikel in der *New York Times* aufmerksam liest, erkennt man auch viel Wünschen und Wollen wie das Agitprop hiesiger interessierter „Kreise“: „The N.S.A. hacked into target computers to snare messages before they were encrypted.“ Da haben wir fast wortwörtlich, was auch hier zum Thema „Online-Durchsuchung“ herausposaunt wurde. Ich würde schon gern mehr und Genaueres wissen, wie sie das angestellt haben wollen. Die Wired hat darüber vor sieben Jahren geschrieben: „FBI Spyware: How Does the CIPAV Work?“ Man sollte auch noch einen zehn Jahre alten Artikel über den so genannten „Clipper Chip“ erwähnen.

*Some of the agency’s most intensive efforts have focused on the encryption in universal use in the United States, including Secure Sockets Layer, or SSL; virtual private networks, or VPNs; and the protection used on fourth-generation, or 4G, smartphones.*

Damit kommen wir der Sache schon näher.

*For at least three years, one document says, GCHQ, almost certainly in collaboration with the N.S.A., has been looking for ways into protected traffic of popular Internet companies: Google, Yahoo, Facebook and Microsoft’s Hotmail*.

Ich denke, dass die Metadaten, die Google et al erheben, viel mehr aussagen als wenn man die angeblichen „Sicherheits“-Features dieser Firmen knackt. Wer seine E-Mails verschlüsselt, kann auch weiter über Google-Mail vertrauliche kommunzieren, aber nur was die Inhalte angeht. Wer mit wem kommuniziert, wird and die Geheimdienste weitergereicht.

Bevor alle in Panik ausbrechen, bringt die *New York Times* noch ein Original-Zitat Snowdens:
*„Properly implemented strong crypto systems are one of the few things that you can rely on,“ he said, though cautioning that*

*the N.S.A. often bypasses the encryption altogether by targeting the computers at one end or the other and grabbing text before it is encrypted or after it is decrypted.*
Heise übersetzt das so: „Verschlüsselung funktioniert. Sauber implementierte, starke Verschlüsselung ist eines der wenigen Dinge, auf die man sich noch verlassen kann.“ Die Betonung liegt auf „sauber implementiert“.

Quod erat demonstrandum. Sichere Verschlüsselung auf einem unsicheren System bedeutet, das Schloss vor die Tür zu nageln.
*At Microsoft, as The Guardian has reported, the N.S.A. worked with company officials to get pre-encryption access to Microsoft’s most popular services, including Outlook e-mail, Skype Internet phone calls and chats, and SkyDrive, the company’s cloud storage service.*

Man sieht aber auch, dass es neben der Totalüberwachung der Bevölkerung um Industriespionage geht:
*By this year, the Sigint Enabling Project had found ways inside some of the encryption chips that scramble information for businesses and governments…*

Bruce Schneier gibt folgenden Rat:
*– Be suspicious of commercial encryption software, especially from large vendors.*
*– Try to use public-domain encryption that has to be compatible with other implementations.*

---

# Was macht der Pofalla eigentlich hauptberuflich?


---

# Bayerische Richter und deren stupender Starrsinn

Gustl Mollaths Anwalt Michael Kleine-Cosack (laut Spiegel online) über die erfolgreiche Verfassungsbeschwerde und die bayerischen Richter:
*Die Richter in Bayern hätten Mollath mit „unverantwortlicher Leichtfertigkeit“ in der Psychiatrie untergebracht und trotz neuer Erkenntnisse mit „stupendem Starrsinn an ihren Fehlentscheidungen festgehalten“.*

---

# An die Nicht-WählerInnen

Für alle wohlwollenden Leserinnen und geneigten Leser, die sich über mein Wahlverhalten und das theoretisch-

philosophisch-historische Drumherum aufgeregt haben: Hier ist eine Alternative zum Nicht-Wählen, die ich reinen Gewissens auch empfehlen kann. (Die Quellenangaben oben rechts sind auch sehr gut.)

---

# Quiz für Berlin-KennerInnen

Welche Brücke ist das? Und welches Gebäude ist da im Hintergrund mit einer Kuppel?

---

# Surveillance Industry

# Documents

Wikileaks: „Today, Wednesday 4 September 2013 at 1600 UTC, WikiLeaks released ‚Spy Files #3' – 249 documents from 92 global intelligence contractors. These documents reveal how, as the intelligence world has privatised, US, EU and developing world intelligence agencies have rushed into spending millions on next-generation mass surveillance technology to target communities, groups and whole populations."

---

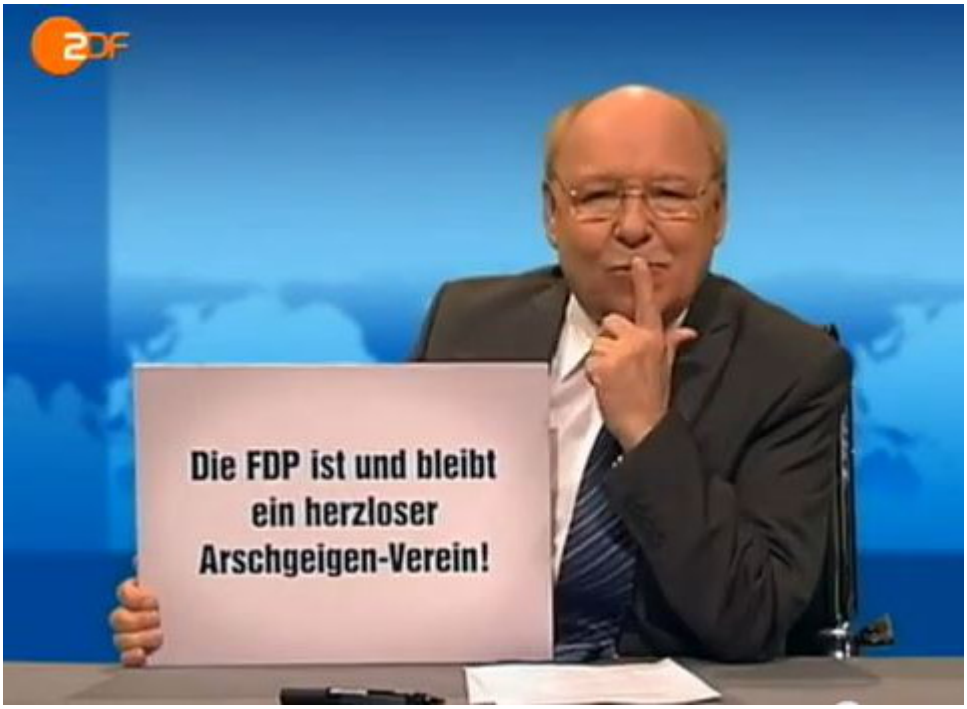
# Warum nicht 18 Penisse?


Ein Artikel von mir in Telepolis: „Mehr als die Hälfte der australischen Bevölkerung hat eine Vulva. „Honi Soit", die Studentenzeitung der Universität von Sidney, hielt das für normal und zeigenswert. Auf der Titelseite einer ihrer August-Ausgaben platzierte sie 18 Vulvae von Studentinnen. Es

geschah, was zu erwarten war (…)

---

# Es ist entschieden




Ich habe heute schon gewählt. Beide Parteien, mit denen ich sympathisierte, bekamen eine Stimme. Die wohlwollenden Leserinnen und geneigten Leser können jetzt raten. Ich hoffe, ihr wisst, dass die Zweitstimme (auf der rechten Seite des Wahlzettels) entscheidet und die Erststimme nur etwas bedeutet, wenn es um Überhangmandate geht?

Hier noch ein paar Argumente zur Wahl an sich.

*Wahlen ändern nichts. Wenn das anders wäre, wären sie verboten.*
Man kann die parlamentarische Demokratie als Sedativum verstehen, im Kapitalismus den Wählern das Gefühl zu geben, sie hätten etwas zu sagen. Die Regierung hat aber weniger zu bestimmen als gemeinhin angenommen wird. Die Regierung ist

auch nicht die herrschende Klasse, sondern nur deren Erfüllungsgehilfe. Angela Merkel hat ja im so genannten „TV-Duell“ zugeben, dass sie nur das macht, was die Europäische Zentralbank rät. Ausserdem ist die herrschende Klasse kein monolitischer Block, der identische Interessen hat.

In Nicaragua ist die nach der Revolution abgewählte FSLN durch Wahlen wieder an die Macht gekommen. Auch in Chile ist Salvador Allende 1970 in freien und geheimen Wahlen Präsident geworden, in Südafrika Nelson Mandela. Die deutschen Revolutionäre haben 1848/49 im Kampf für Wahlen mit der Waffe in der Hand gekämpft.

Wahlergebnisse können den Willen der Mehrheit dokumentieren, wie auch immer der zustandekommen. Wahlergebnisse können auch dukumentieren, dass die Wähler zuviel vom Opium des Volkes genossen haben. „Pressefreiheit ist die Freiheit von 200 reichen Leuten, ihre Meinung zu verbreiten… Da die Herstellung von Zeitungen und Zeitschriften immer größeres Kapital erfordert, wird der Kreis der Personen, die Presseorgane herausgeben, immer kleiner.“ (Paul Sethe)

Wer nicht wählt, sollte auch sonst konsequent das Maul halten und sich in seine Biedermeier-Datsche zurückziehen und Mücken beobachten oder neue Grassorten züchten.

*Es gibt keine Partei, die es wert wäre, gewählt zu werden.*
Das stimme ich natürlich zu. Es gibt aber nur zwei Wege, wie das Volk versuchen kann, seine Ideen punktuell in Gesetze zu formen: Über das System der politischen Parteien oder über Volksabstimmungen.

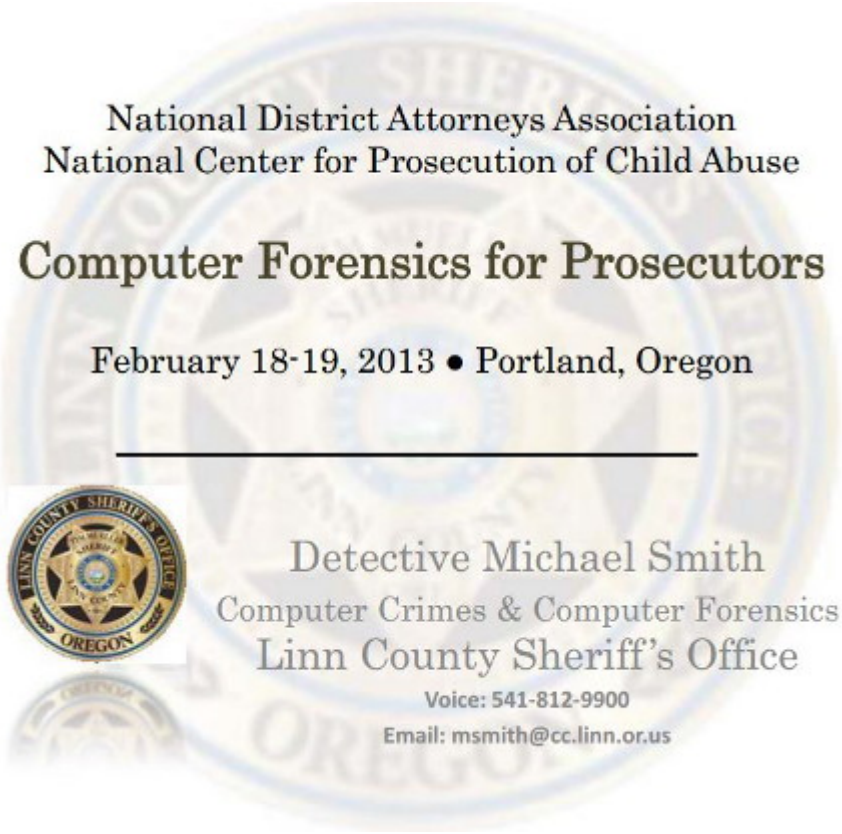
Ich stehe Volksabstimmungen sehr kritisch gegenüber, da sie erstens meistens das „gesunde“ Volksempfinden widerspiegeln, also das Grauen, insbesondere in Deutschland (das gilt auch für das piratische Liquid Democracy). Volksabstimmungen können noch mehr von den Medien manipuliert werden als Wahlen.

Zweitens bilden sich politische Ideen innerhalb von Parteien

immer auf der Basis des kleinsten gemeinsamen Vielfachen, weil nicht die Klügsten und Besten das Sagen haben, sondern die größten Opportunisten, die deshalb nach vorn geschubst werden, weil sie nur wenigen weh tun und immer zur richtigen Zeit am richtigen Ort herumstehenn, um von vielen gesehen zu werden. Das gilt für die CDU genauso wie für die Piraten oder die Linke. Man hat also bei der Art und Weise, wie man den Willen des Volkes feststellt, die Wahl zwischen Pest und Cholera. Es gibt aber keine Alternative.

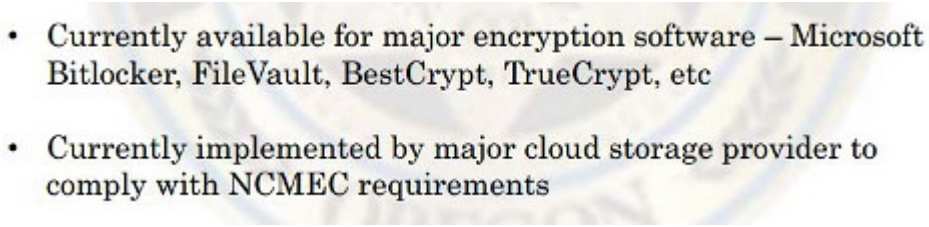
---

# Computer Forensics for Prosecutors




Cryptome: Computer Forensics for Prosecutors 2013 und Computer Forensics for Prosecutors 2012 (via Fefe).

Ich finde es spannend, wenn die behaupten, sie könnten Truecrypt knacken. Es sei eine Hintertür vorhanden (S. 15). Wenn der oder die Betreffende keinen Fehler macht, gibt es kein realistisches Angriffsszenario gegen Truecrypt. Natürlich wird aber alles ausgehebelt, wenn das Opfer sich einen Keylogger unterjubeln lässt. Die Schwachstelle ist nicht Truecrypt, sondern das Passwort: „Seit Juli 2009 kursiert ein Bootkit für alle Windows-Versionen der x86-Architektur, welches die Eingabe des Kennworts für die TrueCrypt-Pre-Boot-Authentifizierung ausspähen kann.“ Das Rootkit muss aber erst auf den Rechner gelangen, und das geht nicht, wenn das Opfer nicht total bescheuert ist.


- Currently available for major encryption software – Microsoft Bitlocker, FileVault, BestCrypt, TrueCrypt, etc
- Currently implemented by major cloud storage provider to comply with NCMEC requirements

Ansonsten sind die Folien relativ „harmlos“ – nach der Devise: Schaut mal her, was wir schon alles können“ – und zum Teil Aufschneiderei wie schon die steilen Thesen der üblichen Verdächtigen, sie könnten einfach mal so „onlinedurchsuchen“.

---

# Gendarmenmarkt, Deutscher Dom

---

# Was guckst du?

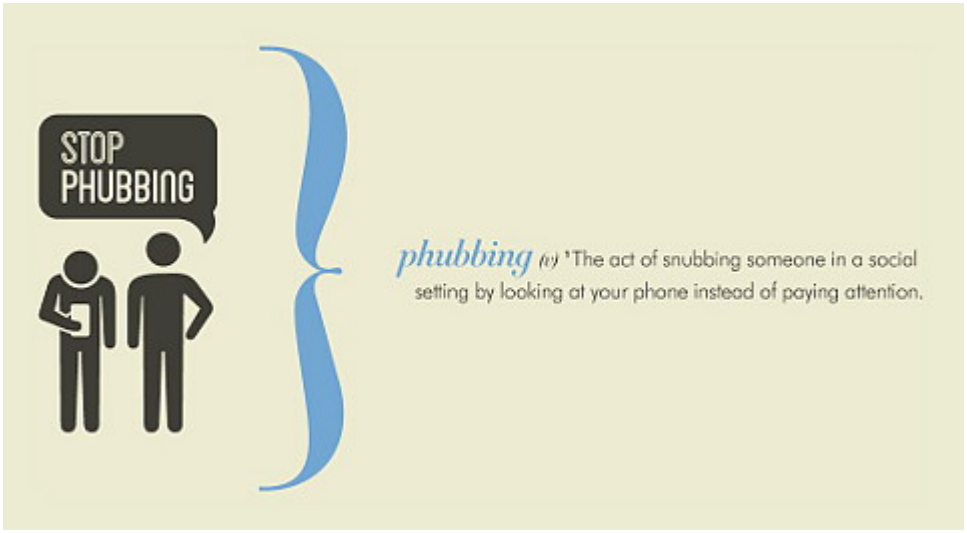
# Lonely Rider à la Turka

Mit freundlicher Erlaubnis vom „à la Turka Imbiss“ am S-Bahnhof Sonnenallee.

# So sieht ein richtiges Duell aus

---

# Das nervt




Alex Haigh in Technology Review über seine Kampagne Stop Phubbing: „Menschen greifen selbst mitten in einer Unterhaltung zu ihrem Handy. Sie glauben, sie könnten zwei Dinge gleichzeitig tun. Das aber glaube ich nicht. Man spricht also mit Menschen, die eigentlich etwa anderes tun. Das nervt.“

# Selnar

German „BTB“ Gor.