25. Aug. 2016

von gast
in Cyber Security
Kommentare (1)

Kryptopolitik: Wenn Sicherheitspolitik uns unsicher macht

von Matthias Schulze

Der deutsche und französische Innenminister haben eine Initiative gestartet um gegen Verschlüsselung vorzugehen. Ihr Argument, was von mehr oder weniger allen Geheimdiensten/Strafverfolgungsbehörden unisono vorgetragen wird lautet, dass verschlüsselte Kommunikation die Arbeit der Behörden behindere. Bereits im Jahr 1993 wurde die gleiche Debatte geführt, endete aber mit dem Konsens, dass die Vorteile von Verschlüsselung die Nachteile deutlich überwiegen. Dieser Konsens, getragen von Industrie, Datenschützern und Politik (sowohl Liberale als auch Konservative) schien sicher, war er doch die vernünftigste Antwort auf ein komplexes Problem. Heute stellen die von Rechtspopulisten getriebenen Innenminister wieder einmal die Verschlüsselung in Frage. Warum das eine schlechte Idee ist, soll dieser Beitrag klären.NSA Chef Inman argumentierte bereits 1980: "There is a very real and critical danger that unrestrained public discussion of crypto-logic matters will seriously damage the ability of this government to conduct signals intelligence and the ability of this government to carry out its mission of protecting national security information from hostile exploitation" (1980). Kern dieses "going dark" Arguments ist also, dass digitale Überwachung schwerer würde, wenn alle verschlüsseln. Terroristen und andere bad guys könnten also nicht mehr gefangen werden. Die Debatte ist also gar nicht so neu und überraschend wie immer behauptet wird.

Im Jahr 1993 wurde sie zum zweiten Mal geführt. Hier argumentierten FBI und NSA, dass der Staat zugriff auf verschlüsselte Kommunikation haben müsse. Sie lobbyierten deswegen für eine Hardwareverschlüsselung, der Clipper Chip, mit eingebauter Hintertür für staatliche Behörden. Der Clipper-Vorstoß endete mit einer Ohrfeige für die US Regierung. Industrie, Datenschützer und Demokraten aber auch Republikaner starteten eine enorm erfolgreiche Gegenkampagne. Die Mehrheit der Bevölkerung war laut einer Umfrage dagegen. Kurz darauf wurde eine Schwachstelle im Clipper System festgestellt, welche die Logik der Regierung ad absurdum führte. Man gelangte zur Einsicht, dass staatliche Hintertüren wie Clipper unsicherer im Vergleich zu Systemen ohne Hintertür sind. In den Worten von NSA Chef Hayden "We didn't get the Clipper Chip, we didn't get the back door. And we than began the greatest 15 years in the history of electronic surveillance. It didn't matter. We figured out ways…". Forscher sind sich einig, dass die Lehre der Clipper Debatte war, dass der umfassende Einsatz von Verschlüsselung, in so vielen Systemen wie möglich, einen größeren Nutzen hat verglichen mit dem Kosten nicht mehr abhörbarer Kommunikation. Hayden dazu: "America is simply more secure with unbreakable end-to-end encryption."

Der Vorschlag

Der dt. und franz. Innenminister fordern: "Es müssen Lösungen gefunden werden, die effektive Ermittlungen mit Blick auf verschlüsselte Daten im Zusammenhang mit terroristischen Aktionen ermöglichen und zugleich der Notwendigkeit des Schutzes digitaler Privatsphäre der Bürgerinnen und Bürger durch Gewährleistung der Erhältlichkeit starker Kryptographie-Systeme sowie dem Grundsatz der Erforderlichkeit und

Verhältnismäßigkeit, den Grundrechten und dem Rechtsstaat Rechnung tragen." Und weiter " Zum Beispiel sollten für alle Kommunikationsdiensteanbieter unabhängig davon, ob es sich um internet-basierte Dienste oder Telekommunikationsdienste handelt, im jeweiligen Land, in dem die Kommunikationsdienstleistung angeboten wird, dieselben Verpflichtungen zur Zusammenarbeit mit Sicherheitsbehörden gelten (unabhängig davon, wo sich der rechtliche Sitz des Diensteanbieters befindet". Die EU solle effektive Maßnahmen prüfen.

Die Probleme

Was ist nun davon zu halten? Es gibt hier eine Reihe technischer, politischer und rechtlicher Probleme, die in den Forderungen nicht angedacht werden. Diese haben aber enorme Implikationen für unsere Sicherheit. Zunächst einmal fällt auf, dass die Forderungen sehr wage sind. Es soll staatlichen Zugriff (oftmals exceptional access genannt) auf verschlüsselte Kommunikation wie iMessage oder WhatsApp geben, gleichzeitig aber die Privatsphäre geschützt werden. Dies ist löblich, aber es bleibt unklar, wie dies genau umgesetzt werden soll. Beide Ziele, also sichere Kommunikation ohne Zugriff durch Dritte, und gleichzeitig legalen Zugriff für den Staat zu ermöglichen ist schwierig umsetzbar und mit enormen Sicherheitsrisiken verbunden. Einige Forscher kommen daher zu dem Schluss, dass es dieses Problem hochkomplex und im schlimmsten Fall ohne größere Kollateralschäden und Risiken nicht lösbar ist. Schauen wir uns die Umsetzungsmöglichkeiten einmal an.

Schlüsselkopien

Bei Clipper setzte man 1993 auf "key escrow". Staatliche Behörden sollten einen zusätzlichen Schlüssel erhalten, der auf Regierungsservern gespeichert werden sollte. Mit einem Richterbescheid hätte der Schlüssel freigegeben, und die Kommunikation entschlüsselt werden können. Alternativ schlug man vor, dass die Hersteller von Telekommunikationstechnologie die Schlüsselkopien speichern könnten. Der Kongress errechnete damals, dass eine solche Schlüsselinfrastruktur mehrere Millionen Dollar Betriebsskosten hätte, da enorme Sicherheitsvorkehrungen hätten getroffen werden müssen, damit die Schlüssel nicht durch Dritte gestohlen, oder von Regierungsmitarbeiter missbraucht würden. Solche Kosten würden kleine Start-ups wie Telegram oder Signal in den wirtschaftlichen Ruin zwingen.

Die zentrale Gefahr bei diesem Modell ist, dass diese Schlüsselserver ein lukratives Ziel für Hacker werden. Ein oder mehrere Server, auf dem die Schlüssel zu Whatsapp, iMessage, Telegram PGP von 81 Millionen Deutschen, oder allen EU Bürgern liegen, wäre DAS Ziel überhaupt für Kriminelle, aber auch die Geheimdienste von anderen Staaten. Russland hätte z.B. ein Interesse daran die Whatsappschlüssel deutscher Politiker zu erlangen. Dass die Gefahr des Diebstahls real ist, zeigt sowohl der Hack des Office of Personal Management, bei dem sensible Daten über US Regierungspersonal gestohlen wurden (inklusive Anschrift, Fingerabdrücke und Sicherheitsfreigabe), als auch der jüngste NSA Shadow Broker Vorfall. Wenn der kompetenteste Nachrichtendienst der Welt seine Server nicht schützen kann, wer erwartet dies dann vom Innenministerium? Wo das Innenministerium durch das BSI vielleicht (!) noch die nötige Kompetenz hat, fehlt diese mitunter aber bei kleineren Telekommunikationsanbietern auf dem freien Markt. Nahezu alle Unternehmen, Facebook, Apple, Microsoft oder Google hatten in der Vergangenheit mit Hackereinbrüchen zu tun. Schlüsselkopien sind also ein enormes Sicherheitsrisiko mit Missbrauchspotenzial.

Es gibt noch ein weiteres Problem mit Schlüsselkopien. Diese gehen gegen aktuelle Industrietrends und "best-practices". Forward secrecy ist ein Verfahren, bei dem der Schlüssel nach Gebrauch gleich gelöscht, also gar nicht gespeichert wird. Andere Dienste verzichten ganz auf das Speichern einer Schlüsselkopie. Bei iPhones zum Beispiel ist der Dechiffrierungsschlüssel nur auf dem jeweiligen Gerät in einem sicheren Prozessor gespeichert und an die Hardware des Geräts gekoppelt. D.h. Apple hat gar keinen Schlüssel den es herausgeben kann, wenn Strafverfolgungsbehörden dies Verlangen. Deswegen lobbyiert das FBI gegenwärtig heftig gegen Apples Verfahren und plädiert dafür, eine Schwachstelle in iOS einzubauen, was uns zum nächsten Modell bringt.

Staatliche Hintertüren

Im Apple vs FBI Fall forderte das FBI, dass Apple sein iOS Betriebssystem umbaut um staatlichen Überwachungsanforderungen gerecht zu werden. Das US Gesetz CALEAverbietet allerdings staatliche Einflussnahme darauf, wie private Firmen ihre Produkte zu bauen haben. D.h. eine Firma zu zwingen, eine Schwachstelle in ein System zu bauen wäre ein verfassungsrechtlich bedenklicher Akt. Der dt. Innenminister scheint aber sowas im Sinn zu haben wenn er argumentiert, dass für Messenginganbieter die gleichen rechtlichen Kriterien gelten sollen wie für Internetserviceprovider. Das Abhören von Kommunikation bei Serviceprovidern wie Telefonanbietern ist in Deutschland machbar. Aber auch dieses Modell ist risikoreich und wäre ein Präzedenzfall: kein anderes Land, nicht mal Russland oder China gehen bisher so weit.

Software ist komplex. Je mehr Zugänge in ein System gebaut werden, desto komplexer, aber auch desto unsicherer wird es. Ein NSA Mitarbeiter dazu: “When it comes to security, complexity is not your friend. Indeed it has been said that complexity is the enemy of security.” Eine Technologie, die sichere Kommunikation zwischen zwei Parteien, und zusätzlich noch einen dritten Zugang für Strafverfolger (mit hoffentlich guten Intentionen) bietet ist technisch komplex, wenn nicht gar unmöglich. Einige top Kryptowissenschaftler verfassten dazu 2015 eine Analyse. Ihr Ergebnis: “law enforcement demands for exceptional access would likely entail very substantial security risks, engineering costs, and collateral damage.” Die zentrale Einsicht dabei ist, dass Hintertüren nicht nur für Strafverfolger funktionieren, sondern auch für die bad-guys: Kriminelle, staatliche Hacker und fremde Geheimdienste. Ein Kryptomantra lautet daher: es gibt keine Sicherheitslücke, die nur die Guten kennen. Eine per Gesetz mandatierte Schwachstelle in ein ansonsten sicheres System zu bauen würde also die Sicherheit nicht erhöhen, sondern reduzieren. Dies wäre genau so wie wenn man in einen sicheren Banktresor eine geheime Hintertür einbaut, die aber nur die Mitarbeiter kennen. Im schlimmsten Verfall verplappert sich ein Mitarbeiter oder wendet sich aus Groll gegen die Bank, und verkauft das Wissen an die russische Mafia. Putin gefällt das. Cybercrime und Hacking sind allgegenwärtige Probleme mit Milliardenschäden. Gute Verschlüsselung verhindert viele dieser Schäden und macht unsere digitale Infrastruktur sicherer. Der ehemalige NSA Chef Hayden dazu: “we are probably better served by not punching any holes into a strong encryption system, even a well-guarded hole.”

Gag orders

Eine weitere Idee wäre, staatlichen Zugang zu mandatieren, das ganze aber im Geheimen zu machen und Firmen mittels “gag orders” zu zwingen, diese Arrangements nicht öffentlich machen zu dürfen. In den USA scheint dies mit den National Security Letters und dem PRISM Programm bereits gängige Praxis zu sein. Wer eine “gag order” erhält, darf nicht juristisch dagegen vorgehen. Dieses zentrale Prinzip des Rechtstaats wurde mit dem Patriot Act und den Anti-Terrorgesetzen – die genau wegen solchen invasiven Maßnahmen befristet sind, aber immer fleißig verlängert werden – abgeschafft. Neben dem weiterhin bestehenden Sicherheitsrisiko stellt sich aber hierbei die Frage, ob eine solche Praxis, wie sie in autoritären Staaten Gang und Gäbe ist, in demokratischen Rechtsstaaten angemessen ist.

Eine offene Frage ist auch, wie man mit kleineren Emailanbietern umgeht. Prinzipiell hat jeder die Möglichkeit einen eigenen Email, IRC oder Messengerserver zu erstellen und diesen mit PGP oder anderer Verschlüsselungssoftware auszustatten. Entsprechende Tutorials findet man auf Youtube und länger als einen Nachmittag dauert das auch nicht. D.h. man bräuchte gar keine Firmen um verschlüsselt zu kommunizieren. Was der Gesetzgeber da machen will, ist unklar.

Nachrichtendienste, Bundestrojaner und Zero-Days

Das FBI knackte dereinst das iPhone des San Berndino Angreifers mit Hilfe einer dritten Partei. Ob dies die NSA war, ist unklar. James Comey, Chef des FBI dementiert dies, aber andere Beobachter wie z.B. der ehemalige Cyber-Security Zar Richard Clarke bezweifeln, dass die NSA nicht in der Lage dazu wäre. D.h. Geheimdienste könnten eine größere Rolle spielen, indem sie z.B. eine Trojanersoftware auf einem Gerät aufspielen, welches die Kommunikation abschöpft, bevor diese verschlüsselt wird. Die meiste Kryptografie wird nicht “gebrochen” oder “entschlüsselt”, sondern durch andere Schwachstellen im System umgangen. Wenn diese Schwachstellen dem

Hersteller nicht bekannt sind, kann er diese auch nicht schließen. Diese sogenannten Zero Day Exploits sind daher ein lukratives Mittel, sowohl im staatlichen Konflikt im Internet ala Stuxnet, als aber auch beim staatlichen Hacking wie ZITIS. In Deutschland würde sich aber die Frage nach dem Trennungsgebot stellen, wenn nun auf einmal der BND die Telefone deutscher Staatsbürger (die meisten Terroristen haben die Nationalitäten ihrer jeweiligen Länder) hacken würde.

Darüber hinaus stellt sich auch hier das Sicherheitsrisiko: es gibt keine Garantie, dass Sicherheitslücken nur von den "Guten" benutzt werden. Jede existierende Sicherheitslücke macht ein System unsicherer. Eine Sicherheitslücke in Android betrifft nämlich nicht nur ein Gerät, sondern potenziell die gesamte Nutzerschaft (über 1 Milliarde Menschen). Daher ist es im Nahmen der Cybersicherheit eine "best-practice", dass die Hersteller diese Lücken melden, damit sie für alle Geräte geschlossen werden können. Das deutsche BSI empfiehlt genau dies und die deutsche Cybersicherheitsstrategie sieht dies auch vor. Diese Sicherheitslücken für Strafverfolgung zu horten, d.h. nicht öffentlich zu machen, ist somit eine Praxis, die der allgemeinen Cybersicherheit aller unzuträglich ist. Auch dieses Wissen ist für Hacker interessant und macht die Behörde, die Sicherheitslücken speichert zum potenziellen Ziel. Dies wird insbesondere am NSA Shadow Broker fall deutlich, wie die Zeit dokumentiert. Mit Sicherheitslücken wird Namen der Sicherheit die Unsicherheit erhöht.

Die Implikationen von staatlichem Zugriff auf Verschlüsselung

Wie gezeigt wurde, ist staatlicher "exceptional access", auch wenn er gut gemeint und gut gemacht ist, ein enormes Sicherheitsrisiko für deutsche und europäische Bürger, im Zweifel aber auch für die gesamte IT-Infrastruktur. Diese Initiative ist darüber hinaus mit unklaren Kosten verbunden und es ist alles andere als sicher, dass sie positive Effekte hat. Wer wirklich kriminell kommunizieren will, findet Wege, auch wenn Staaten die Verschlüsselung kontrollieren.

Nicht nur ist ein "exceptional access" System technisch komplex und somit potenziell unsicherer als vergleichbare Systeme ohne Hintertür, es wäre auch auf dem Markt weitaus unattraktiver. Niemand würde so ein System nutzen wollen. Im US Senat stellte man 1994 fest, dass niemand, der auch nur annähernd bei Verstand wäre, ein System nutzen würde von dem er weiß, dass Strafverfolgungsbehörden Zugriff darauf haben. Das trifft insbesondere bei illegale Tätigkeiten zu. Staatliche Regulierung von Verschlüsselung würde Nutzer in die Arme ausländischer Firmen treiben und hätte somit auch negative wirtschaftliche Effekte. Kryptoexperte Bruce Schneier hat einmal nachgezählt. Es gibt weltweit ca. 865 verschiedene Hard und Software Verschlüsselungssysteme aus 55 Ländern. Viele davon, wie z.B. PGP oder OTR sind Open Source, d.h. frei verfügbar und modifizierbar. Wenn nun also die EU im Kampf gegen Terroristen beschließen würde, Apple, Google, Whatsapp und Facebook zu zwingen, staatlichen Zugang zu gewährleisten würden die "bad guys" einfach eine andere Technologie nutzen, während rechtschaffene EU Bürger mit einem unsichereren System leben müssten. D.h. EU Bürger wären dem Risiko von Cyberangriffen und Online Kriminalität ausgesetzt, während Terroristen sicherere Systeme nutzen würden. Die Ironie ist bezeichnend: eine Sicherheitsmaßnahme reduziert die Sicherheit der eigenen Bevölkerung und bestärkt jene der Terroristen, und das im Namen des Kampfes gegen den Terrorismus.

Selbst wenn man Messenger reguliert, gibt es noch tausend andere Möglichkeiten. Al Qaeda kommunizierte z.B. lange Zeit über Gmail Accounts, bei denen Emails im Postausgang gespeichert, aber nicht abgeschickt wurden. So wurden einfach die Login-Daten verteilt und der Account regelmäßig gewechselt. Wegwerf Email Accounts und Wegwerf Handies mit wechselnden Simkarten, wie z.B. in der US Serie "the Wire" zu sehen, sind auch eine Möglichkeit. Aber auch andere Wege sind denkbar, wie z.B. geheime Foren, ad-hoc IRC Chats oder der Einsatz einer chiffrierten Sprache, die mit Codes operiert. Chinesen umgehen z.B. die staatliche Zensurinfrastruktur durch den geschickten Einsatz von Codewörtern und Emojis. Doppelverschlüsselung, also eine Verschlüsselung des Textes innerhalb des verschlüsselten WhatsApp systems wäre auch denkbar. Dieses Problem wurde auch schon während der Clipper Debatte 1993 identifiziert. Aber auch traditionelle Briefe und Boten sind ein Abwehrkonzept, welches von Kriminellen genutzt wird, je mehr der Staat in den digitalen Bereich vordringt. Es ist

also eine Illusion zu glauben, dass man mit der Regulierung von Verschlüsselung terroristische Kommunikation unterbinden kann. Erschweren vielleicht, unterbinden kaum. Selbst wenn man dies aber täte, wäre dies mit immensen Kosten verbunden zu denen der Nutzen in keinerlei sinnvollem Verhältnis steht.

Dazu kommt noch eine weitere Komponente, die auch schon 1993, aber auch im Apple/FBI Case ein nicht zu vernachlässigendes Problem darstellte. Wenn westliche Demokratien damit beginnen, Verschlüsselungssysteme rechtlich zu unterwandern, würde dies eine Signalwirkung an autoritäre Systeme haben, gleiches zu tun. Es würde im schlimmsten Fall einen Prozess der internationalen Normsetzung in Gang bringen. Das Problem dabei ist, dass Verschlüsselungstechnologie, wie das US State Department argumentiert, lebenswichtig für Dissidenten, die Opposition, Journalisten aber auch Ärzte in autoritären Gesellschaften ist. Wenn westliche Staaten, im Namen der Terrorbekämpfung Verschlüsselung aufweichen, würde dies einen Präzedenzfall schaffen und Russland und Co würden unter dem gleichen Vorwand gegen ihre Opposition vorgehen. Putin gefällt auch das.

Eine andere internationale Komponente stellt sich im Übrigen auch bei key-escrow Verfahren. Wie geht man damit um, wenn China anklopft und von Deutschland den Schlüssel eines chinesischen Dissidenten, wie z.B. Ai Wei Wei haben will, der aber einen deutschen Kryptodienst benutzt hat?

Die bessere Lösung

Internetexpertin Susan Landau argumentierte im Apple-FBI Fall vor dem US Senat, dass staatliche Sicherheitsbehörden umdenken müssen. Sicherheitsbehörden sind, nach ihrer Ansicht, im veralteten Paradigma der *nationalen* Sicherheit gefangen, welches von physischen Bedrohungen – Staatenkrieg, Terrorismus– ausgeht. Sie argumentieren also aus einer bestimmten, partikularen Positionen heraus, dass Verschlüsselung im Kampf gegen den Terror umgangen werden müsse. Nun ist Terrorismus aber ein vergleichsweise kleines Problem, auch wenn die gegenwärtige Medienpanik anderes vermuten lässt. Die ökomischen Kosten des Terrors sind gering und es sterben immer noch mehr Menschen in Europa durch Milchkühe. Dagegen ist die Bedrohung durch Cyberkriminalität, staatliches Hacking und Überwachung aber real und enorm kostspielig – je nach Schätzung mit Milliardenkosten. Durch das Internet sind wir global verbunden, d.h. Cybersicherheit geht uns alle an. Sie muss global gedacht werden, im Sinne der “common security”, wie sie in den späten 1970ern entworfen wurde. Wenn ich eine Sicherheitslücke in Deutschland geheim halte und horte, leiden alle darunter. Dem stehen aber staatliche Nachrichtendienste und Strafverfolgungsbehörden mit ihrem nationalen, und durch den Terrorismus verengten, Fokus im Wege. Das Problem daran ist, dass Innenminister aber vorwiegend auf diese Partikularinteressen hören.

Sicherheitsparadigmen und die falsche Dichotomie

Die Debatte um das Aufweichen der Verschlüsselung ist also ein Clash verschiedener Sicherheitsparadigmen: einer modernen Cybersecurity, welche globale Probleme im Blick hat und einer Partikularsicht auf nationale Sicherheit. Deswegen ist die Dichotomie Sicherheit vs. Freiheit, wie der Innenminister es in seinen Forderungen schreibt, irreführend. Verschlüsselung ist eine Sicherheitstechnologie, aber auch eine Freiheitstechnologie. Mehr Verschlüsselung erhöht unsere Sicherheit, aber auch unsere Freiheit. Vielmehr geht es um Sicherheit vs. Sicherheit, konkret der Schutz aller Menschen in einer digital vernetzten Infrastruktur vor dem allgegenwärtigen Problem vom Kriminalität und Hacking, vs. dem Schutz vor Terrorangriffen, die nur sehr selten stattfinden und vergleichsweise marginal erscheinen. Der ehemalige NSA Chef Hayden argumentiert ähnlich: “the overall health of the American computer industry was far more important to the security mission of NSA.” Mit anderen Worten ist die Fähigkeit, ist verschlüsselte Kommunikation zu knacken vergleichsweise unwichtiger als das größere Gut, die “Gesundheit” der amerikanischen IT Landschaft durch gute Verschlüsselung.

Digitale Überwachung in der Sackgasse

Hayden noch eine weitere interessante Bemerkung. Das Diktum der Notwendigkeit der Überwachung von Kommunikationsinhalten führe in eine Sackgasse. Verschlüsselung wird kommen, aber es mache die Arbeit der

Nachrichtendienste nicht schwerer, wenn diese sich clever anstellen: “Content will be more out of our reach no matter what we do in this case. This is just an inevitable advance of technology”. Ja, durch Verschlüsselungstechnologie mag *ein* Kommunikationskanal versiegen und Kommunikationsinhalte werden schwerer zu erreichen sein. Das heiße aber nicht, dass nachrichtendienstliche Tätigkeit und Strafverfolgung unmöglich würde, denn:

> “My point is, there is a lot of digital exhaust out there. And Mike McConnell, one of my predecessors at NSA actually lived through that movie. It was called Clipper Chip and Mike wanted to bake-in the backdoor into the silicon. The Clinton Administration would have none of it. And Mike didn’t tell us the tale, thus began the **greatest 15 years in the history of electronic surveillance**, because everyone going to **digital devices created this ocean of data,** much of it meta, as opposed to content. And with metadata you could do an awful lot. So to specifically answer your question. Under any circumstances we get less content**, but it doesn’t mean we’re gonna get less intelligence”**

Amerikanische IT-Experten aus Harward machen ein ähnliches Argument. Strafverfolgungsbehörden haben heute, im Gegensatz zu 1993, viel mehr Möglichkeiten: DNA sampling, biometrische Gesichtserkennung, vernetzte Datenbanken, geo-profiling, target-chaining etc.. Zudem liegen so viele Daten wie noch nie offen, z.B. bei Facebook. Das Internet der Dinge wird diesen Trend noch weiter bestärken. Das “going dark” Problem sei bewusst irreführend, weil es so viele alternative Lichtquellen gibt. Diese müssten nur intelligent genutzt werden. Strafverfolgungsbehörden in den letzten Jahren seien zu verwöhnt geworden, weil digitale Überwachung immer einfacher wurde. Dies ist aber kein Naturgesetz und keine Notwendigkeit. So war es in der Vergangenheit auch möglich, nicht abhörbar zu kommunizieren, etwa durch einfaches Flüstern oder das verbrennen von Briefen. Wenn aber digitale Überwachung schwieriger wird, ist es vielleicht an der Zeit, über einen Strategiewechsel nachzudenken. Die Doktrin seit 2001 war immer mehr digitale Überwachung, mehr Daten und mehr Datenaustausch, also Signals Intelligence. Was dabei vergessen wurde ist die gute, investigative Polizeiarbeit oder auch “human intelligence”. Wenn also digitale Überwachung nicht mehr funktioniert, sollte einfach die Operationsstrategie geändert werden. Ein gutes Beispiel hierzu ist Großbritannien:

> Faced with the problems posed by encryption, European counter-terrorism officials have sometimes gone to unusual lengths to get round it.
>
> In a recent terror raid in the UK, undercover police posed as human resources officials at the target’s employer so they could ask to see his work phone. A trove of information was retrieved, including communications with Isis operatives in Syria. (Quelle: Financial Times)

Zum Schluss möchte ich noch einmal NSA Chef Hayden zitieren. With exceptional access, sagt er, “even done well, you have actually opened up greater possibilities for degrading what would otherwise be almost unbreakable end-to-end encryption […] I just don’t know if its a wise thing for the government to demand this.”

Matthias Schulze M.A. ist Doktorand und wissenschaftlicher Mitarbeiter am Lehrstuhl für Internationale Beziehungen der Friedrich-Schiller Universität in Jena. Seine Doktorarbeit trägt den Titel „From Cyber-Utopia to Cyber-War. Advocacy Coalitions and Normative Change in Cyberspace“.
Dieser Beitrag ist ein Crosspost von seinem Blog: https://percepticon.wordpress.com

Tags: Deutschland, EU, Hintertüren, Krypto, Verschlüsselung, WhatsApp

« Stellenanzeigen Juli/August 2016
Turmoil in the Middle East: Regional Dimensions Beyond Religion »

Ein Kommentar zu “Kryptopolitik: Wenn Sicherheitspolitik uns unsicher macht”

1. Thorsten | 27. Aug. 2016 um 10:27 | **#1**

Sehr gut, wie viel hier in dem Blog umrissen wird. Vorallem, dass die ganzen Hintergründe hinzugezogen und dabei kein Blatt vor den Mund genommen wird.
Ich selbst denke auch, dass jeder lieber privat über seine eigene Sicherheit bestimmen sollte. Ich habe auch auf http://ueberwachungskamera24.net nachgeguckt und somit bin ich bestens selber versorgt, auch ohne Staat.
Liebe Grüße

Antworten

Einen Kommentar hinterlassen

Name

Email

Webseite

Kommentar

Kommentar senden

Benachrichtige mich über nachfolgende Kommentare per E-Mail.

Social Media

Suche

Suche... Suche

Twitter Feed

- Today, Hakim Khatib of @MPCJournal looks at turmoil in the Middle East: Regional Dimensions Beyond Religion https://t.co/00taHOI2vK
  about 5 hours ago from Twitterrific
- Kryptopolitik: Wenn Sicherheitspolitik uns unsicher macht.Matthias Schulze/@percepticonblog zu Hintertüren in Krypto https://t.co/4Ux6HaYfOr
  25. August 2016, 10:58 from TweetDeck
- Es gibt mal wieder neue #Stellenangebote für #Politikwissenschaft #IB #Sicherheitspolitik! https://t.co/r0CBBtJMu1
  17. August 2016, 10:30 from Twitter for Android

Tags

BELIEBT KOMMENTARE NEU

Preparing for (intellectual) civil war – the New Right in Austria and Germany

"War in peace. The return of civil war in Mozambique?"

But – where do these people come from? The (Re)Emergence of Radical Nationalism in Finland

Linkhinweis: Berlinangst. Ein Podcast zum Umgang Berlins mit der Terrorbedrohung

Patterns of far right and anti-Muslim mobilisation in the United Kingdom

Kategorien

- Außenpolitik (71)
- Bürgerkriege (27)
- Cyber Security (53)
- Demokratisierung (14)
- Digitalisierung (1)
- Drohnen (15)
- Entwicklung (1)
- Europa (2)
- Flüchtlinge (18)
- Humanitäre Interventionen (15)
- Innere Sicherheit (34)
- Interviews (10)
- Katastrophen (4)
- Konferenz (32)
- Militär (31)
- Pandemien (3)
- Podcast (8)
- Popkultur (23)
- Raketenabwehr (1)
- Rechtsradikalismus (27)
- Sanktionen (8)
- Security Culture (27)
- Sicherheits-Kommunikation (16)
- Sicherheitskultur (243)
- Sozialwissenschaft Online (72)
- Stellenangebote (58)
- Strategie (12)
- Terrorismus (67)
- Theorie (5)
- Umwelt (2)
- Versicherheitlichung (23)
- Visualisierung (6)
- Whistleblowing (8)
- WikiLeaks (17)
- WMD (10)
- Zivilgesellschaft (67)

Blogroll

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

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

Archiv

Archiv Wähle den Monat