Cryptoparty 25.6.22 Vortrags-Transskript

Als FOLIE 1:
MENSCHENRECHTE UND KRYPTOGRAPHIE
CRYPTOPARTY am 25.6.2022
im Rahmen der Menschenrechtswoche Tübingen

Thema der diesjährigen Menschenrechtswoche Tübingen ist:
Ressourcen fallen nicht vom Himmel - Wovon hängen Menschenrechte ab?

Als Tübinger Cryptoparty wollen wir dazu einen Beitrag leisten. Seit Juli 2014 trefen wir uns bis zu 10x im Jahr, um uns über Privatspärenschutz im digitalen Raum auszutauschen. In Referaten erarbeiten wir Hintergrundwissen zu digitalen Strukturen und Abläufen, in Workshops zeigen wir konkrete Schutzmaßnahmen, Gesellschaftspolitische Themen wie Stalking und Wahlmanipulation haben wir bearbeitet. Und bei dem Thema Privatsphärenschutz sind wir nicht allein:

Beim Tübinger Tag der Digitalen Freiheit vor 3 Wochen z.B. gab es schon einen lebendigen und gut besuchten Workshop zum Thema wie die Geschäftspraktiken von Facebook, also einem kommerziell ausgerichtetem Unternehmen, Menschenrechte verletzen. Amnesty international engagiert sich bemerkenswert gegen staatliche und kommerzielle Menschenrechtsverletzungen auch im digitalen Raum z.B. bei Drangsalierung von Menschenrechtsaktivisten überall auf der Welt und z.B. auch gegen den zunehmenden Einsatz automatisierter Gesichtserkennung bei uns.
https://amnesty-digital.de/unsere-themen/

Als FOLIE 2:
Die Möglichkeit vertraulich zu kommunizieren mit Menschen, denen man etwas <u>anvertrauen</u> will, ist ein unverzichtbarer Bestandteil der Menschenrechte und gleichzeitig Voraussetzung für die Wahrnehmung von Menschenrechten.

Bei Wikipedia werden Menschenrechte so definiert:
Sie werden als „moralisch begründete, individuelle Freiheits- und Autonomierechte bezeichnet, die jedem Menschen allein aufgrund seines Menschseins gleichermaßen zustehen.[1]
Sie sind universell (gelten überall für alle Menschen), unveräußerlich (können nicht abgetreten werden) und unteilbar (können nur in ihrer Gesamtheit verwirklicht werden).[2]
Sie umfassen dabei bürgerliche, politische, wirtschaftliche, soziale und kulturelle Rechtsansprüche.
Die Menschenrechte werden häufig von Naturrechten und der unantastbaren Menschenwürde abgeleitet.

Das Recht auf Privatsphäre, d.h. das Privatleben und die private Kommunikation wird geschützt durch Art.12 der Allgemeinen Erklärung der Menschenrechte, durch Artikel 8 der Europäischen Menschenrechtskonvention und im UN-Zivilpakt im Art.17.
> Dieses Recht steht uns einfach zu! Wir können es einfordern und brauchen nicht darum zu betteln.

Bedroht werden mittels digitaler Technologien insbesondere die Menschenrechte:
Art. 1 (Freiheit, Gleichheit, Brüderlichkeit)
Art. 12 (Freiheitssphäre des Einzelnen)
Art. 19 (Meinungs- und Informationsfreiheit)
Art. 21 (Allgemeines und gleiches Wahlrecht)

Daß **Kryptographie**, die Kunst der Verschlüsselung eine Bedeutung für mein eigenes Leben hat, habe ich eigentlich erst begriffen, nachdem Edward Snowden uns im Sommer 2013 mit dem Ausmaß und den Methoden anlassloser Massenüberwachung staatlicher Geheimdienste konfrontiert hat:

FOLIE 3 PRISM Collection Details:
https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/images/prism-slide-4.jpg

Überwacht werden Telefonate (jetzt digital), E-Mails, Chats, SMS, Standorte von Mobiltelefonen (Bewegungsprofile), Das komplette Internet

FOLIE 4: Upstream + PRISM

https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

Die Informationen gehen an die NSA direkt von den Servern der großen Internet-Konzerne und durch direkte Überwachung der Info-Ströme in den weltweiten Glasfaserkabeln.

FOLIE 5: Provider für PRISM

https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

FOLIE 6: Glasfasernetze global

https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

ALS FOLIE 7:

“Even if you aren’t doing anything wrong, you are being watched and recorded.” Edward Snowden

https://www.democracynow.org/2013/6/10/youre_being_watched_edward_snowden_emerges

FOLIE 8: New Collection Posture:

Den allumfassenden Anspruch der NSA bzw. der verbündeten Geheimdienste der „Five Eyes“ zu staatlicher Überwachung zeigt die von Snowden gelieferte Folie: „New Collection Posture: Sniff it all, Know it all, Collect it all, Process it all, Exploit it all, Partner it all“
https://external-preview.redd.it/MSgx5reLE1Y_BvxJXM3KFOtnVCATHKeW-JMhCtbinJc.jpg?auto=webp&s=a9a20383ecf602882e32d3f4b92510f3d7b7390b

Ich selbst habe etliche Monate gebraucht, um erste praktische Konsequenzen zu ziehen: Umzug von Googles E-Mail-Dienst zu einem Provider mit dem Geschäftsmodell Privatsphärenschutz und Installation einer E-Mail-Verschlüsselung. Irgendwann merkt man aber, daß Änderung im eigenen Kommunikationsverhalten auch die Kommunikationspartner einbeziehen muß. Außerdem gibt es da noch viel interessantes zu lernen:

Die Lösung: Cryptoparty

Folie 9: Lets start The Cryptoparty

https://github.com/cryptoparty/artwork/blob/master/cryptoparty_global_artwork/CC_BY_3.0_another_party_by_xp0s3.jpg

Cryptoparties gibt es weltweit. https://www.cryptoparty.in/
In Tübingen regelmäßig seit Juli 2014: https://cryptoparty-tuebingen.de/

Privatsphäre ist kein isoliertes Gut, ein Luxus früherer Tage, auf das man heutztage ggf. verzichten kann.
Denn die Überwachung von Kommunikation beeinträchtigt auch:
- Das Recht auf Meinungs-und Informationsfreiheit
- Das Recht auf friedliche Versammlung (Demonstrationsrecht)
- Das Recht auf Freiheit von Diskriminierung

Wir haben übrigens keinen Grund zu glauben, daß staatliche Begehrlichkeiten und Praktiken bzgl. Überwachung in Rußland oder China wesentlich anders sind.

Geschichtlich gesehen hat sich mit dem Einzug der Computertechnik in unser aller Alltag, d.h. der Codierung von Sprache d.h. Buchstaben und Ziffern in Nullen und Einsen eine absolut neue Situation ergeben.
Diese Nullen und Einsen sind, wenn sie abgefangen und aufgezeichnet werden, maschinell (KI) relativ leicht massenhaft durchsuchbar und auswertbar.

Wirksame Verschlüsselung hilft dagegen!

Als Folie 10: Beispiel eines verschlüsselten E-Mail-Texts (PGP-Message)

```
-----BEGIN PGP MESSAGE-----

hQIMA1LEgXrO0ZzQAQ/+JkLjY3/X/UrBK8Jsxzgzs7qP7T2OjExRs5Oq7Q8lHRx+
9FJY0Ui4WCqN9+h160aeIUHFcZ1Jiinpmp46wd2peYa8cR5iHRS5LQkHzOQbBxJC
qjakIotdR5eVv/rcJ9ZyorEQRpB9jdX648khh8XHAvfNbQAOq1QiONqr+mrJFlT6
HzgZ7251Fhc+s+wPJwotDKbgCbYUC83hl8KylGnf+HY/NiX4fhPrf5PmBYus7Mat
tPmbgJhCVJ8Hje1IUz9oLN2lQWueYO1ifaFVSBMtrODG4gLTGgxxH7UPOj9oR1Sy
GorZi6SMGzd7vnI1ZKFROFkyLZaRfIR/cLNz/0kcQekrJtLW8Q4OYxWkA5cCqYM2
5ZmCXJfGjCXXEAFjan5TveZEd43UXj7JKM+mt8w6qXmgVRHvNY9cz8MNCmdZwgqy
gToAFl8c98BmFu5RQ4QoG0WWT0RYw3uzs/ZNYMJ0pU7o7t2G5Wxp3cCtfyZ4n0Zr
mQB1ZyHYLrv+ab+1wyZzt02LZbW8hurxzJUe7swfarC15VoDAC2UNiRvqDxE+aAH
hdAdSnV87pxoqlvmKoQcCagY3LVQuxLfjHEGX8o8/+EnXkbx0eJqGDFr16o6njfh
ZwmevKVKphXPw78v5d3aBrFmVo8Md1aRyb+tcFnfW5a/I6p2dD47YBjfHrUq+RDS
tQGqx8p6TQslffSUUIHUzCQcKHj5D07BVrCNUmPfaC8ug2djYZIS8hw/XTdpThk7
dpCbB7YFRKUXAlMwrpSPHd+2rq58YGLN2AhGsoJhcxsKaA31/fiSqdJGUMrGQV4r
/fdJd3TVqUEdGV5n7HAeQfl+qF8Av1lbO0sK31McYTAZBruPZTjT+77XPzsI37Qs
kPs0YviJTgA568A9x9AhFyw1hs5u4rqxC2EPQPj6M7Lzh2964tc=
=LY9/
-----END PGP MESSAGE-----
```

Im Klartext: **Kommt alle zur nächsten Cryptoparty!**

Wenn seit dem Altertum Botschaften verdeckt oder verschlüsselt übermittelt wurden, betraf das militärische oder politische Zusammenhänge, heute dagegen ist unser aller Alltags-Kommunikation von der Neugier Dritter betroffen.

Beispiele, Skytale, Caesar-Verschiebung, Geheimschrift von Maria Stuart, Enigma, Smartphone (Folien s.a. Wikipedia)

FOLIE 11: Skytale

FOLIE 12: Caesar-Verschiebung
Verschlüsselung ist möglich durch „Transposition“ oder „Substitution“ von Buchstaben

FOLIE 13: Maria Stuart, Geheimschrift

FOLIE 14: Enigma

FOLIE 15: Smartphone

Verschlüsselungsmethoden d.h. Krytographie zielen darauf, eine sprachliche Botschaft (bzw. sonstige Texte/Daten) für Dritte unzugänglich zu halten. Nur Berechtigte, Sender und Empfänger sollen den Inhalt kennen. Für uns als Privatleute hat das mit der Computertechnik einen ganz neuen Stellenwert bekommen.
Überwachungstechnik ist nicht wie offene Repression direkt sinnlich erfahrbar, trotzdem findet sie täglich statt.
„Die Spionagesoftware „Pegasus“ der israelischen Firma NSO Group wird immer wieder mit Menschenrechtsverletzungen in Verbindung gebracht. Das Unternehmen gibt zwar an, die Software nur für Verbrechensbekämpfung an Regierungen zu verkaufen, wie sie letzten Endes eingesetzt wird, prüft die Firma selbst aber nicht. Von Spionage mit solcher Software betroffen sind häufig Journalist:innen und Aktivist:innen, die sich gegen Unterdrückung und Ungerechtigkeit in ihren Ländern einsetzen. Autoritäre Regime können sie mit Hilfe der Spionagesoftware über Ländergrenzen hinweg überwachen und unter Druck setzen.“

Quelle: https://netzpolitik.org/2021/nso-whatsapp-hack-betroffene-von-handy-spionage-berichten/

Digitale Technik wird von den Herrschenden nicht nur zur Überwachung privater Kommunikation genutzt:

Wir haben davon gehört, daß China eine digitale Rundum-Überwachung seiner Bürger realisiert hat. Beispielhaft und brutal durchgesetzt hat die chinesische Führung damit ihre NULL-COVID-STRATEGIE. Soziales Verhalten wird in China auch sonst damit umfassend erfasst, bewertet und ggf. abgestraft.

2014 erhielten die Besitzer georteter Mobiltelefone in KIEW von der damaligen Regierung die einschüchternde SMS: „Sehr geehrter Kunde, Sie wurden als Teilnehmer an einem Massenaufruhr erfasst“ (Bruce Schneier: Data und Goliath S.8)
In Michigan / USA wurden 2010 die Besitzer von Mobiltelefonen in der Nähe eines erwarteten Streiks registriert - ohne gesetzliche Grundlage oder richterlichen Beschluss. (Bruce Schneier: Data und Goliath S.8)

Korrumpierung freier Wahlen durch gezielte Beeinflussung von noch unentschiedenen Wählern mit „Microtargeting“- Meldungen. Sie sind uns zuerst aus Amerika bekannt geworden (Cambridge Analytica, Trump) Auch beim Brexit wurde u.a. damit manipuliert
https://www.bpb.de/themen/medien-journalismus/digitale-desinformation/290522/microtargeting-und-manipulation-von-cambridge-analytica-zur-europawahl/

Existierende, geplante oder mögliche Schutzmaßnahmen für die Internet-Nutzer werden von staatlichen Institutionen auch mal untergraben:
iCloud Verschlüsselungspläne wurden auf Druck des FBI gestoppt.. (Meldung vom Januar 2020)
https://mobilsicher.de/aktuelles/apple-kippt-verschluesselungsplaene-fuer-icloud

Wir haben es nicht nur mit Autokraten und Diktaturen zu tun: Immer wieder kommen auch gewählte Vertreter aus demokratisch verfaßten Staaten auf die Idee, neue Methoden zur massenhaften anlasslosen Überwachung von uns allen einzuführen. Und bei solch flächendeckender Überwachung gilt die Unschuldsvermutung und Verhältnismäßigkeit der Maßnahmen erst mal nicht:

Die wiederkehrenden staatlichen Versuche eine Vorratsdatenspeicherung einzuführen bzw. durchzusetzen böten Stoff für eine eigene Veranstaltung
Quellen: https://netzpolitik.org/?s=Vorratsdatenspeicherung

Cryptowars
Nicht gemeint ist damit „Cyberwar“ i.S. von militärischen Aktivitäten und kriegerischen Auseinandersetzungen im virtuellen Raum, sondern staatliche Bestrebungen, private Verschlüsselung zu unterbinden.
In den 90erJahren sollten Anbieter von Kommunikationsdiensten verpflichtet werden, US-Regierungsbehörden auf Anfrage Zugriff auf die Kommunikation der Nutzer zu verschaffen. Heftige Proteste der Zivilgesellschaft folgten, auch hat
Phil Zimmermann darauf hin die asymmetrische Kryptographie (mit öff. u.priv. Schlüssel) als Software **PGP** der Allgemeinheit international zugänglich gemacht. Er wurde über 3 Jahre bis 1996 wie ein Waffenschieber von US-Zollbehörden verfolgt.
Quellen: Simon Singh: Codes - Die Kunst der Verschlüsselung ISBN 9783446201699
Geschichte der Cryptographie: Antike bis Gegenwart
und Steven Levy: Crypto: How the Code Rebels beat the Government, saving Privacy in the digital Age. ISBN 0140244328

FOLIE 16: Clipper-Chip

Clipper-Chip (Hardware-gestützte Verschlüsselung mit Hintertür) für amerikanische Telefone zur Zeit Clintons, wurde letztlich nach Protesten der US-Zivilgesellschaft eingestellt.

Quellen:
https://www.betriebswirtschaft-lernen.net/erklaerung/clipper-chip/
https://www.cryptomuseum.com/crypto/usa/clipper.htm mit Abbildungen

Über das Interesse der US-Geheimdienste an Schwächungen der kryptografischen Technik bzgl. Zufallsgeneratoren und Schlüsselgröße berichtet
Steven Levy: Crypto: How the Code Rebels beat the Government, saving Privacy in the digital Age. ISBN 0140244328

Immer wieder wird Verschlüsselung von unseren Politikern auch heute noch attackiert:
Innenminister de Maizière forderte 2015: Polizei und Geheimdienste sollen verschlüsselte Nachrichten mitlesen können. - Es gab gleichlautende Forderungen aus Großbritannien und den USA. Unklar blieb wie die Forderungen umgesetzt werden sollen.
(Quelle: Süddeutsche.de am 21. Januar 2015)
Auch: https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/de/pdf
und die Übersicht: https://tresorit.com/blog/de/40-jahre-crypto-wars/

FOLIE 17: de Maizière …

Hochaktuell ist derzeit die sog. **Chatkontrolle**, eine von der EU-Kommissarin Ylva Johansson (Norwegerin, also aus einem wohl demokratisch orientierten Staat) initiierte Gesetzesvorlage
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0209&from=EN
mit der Auswirkung, daß Botschaften, Bilder und Videos bei allen Messengern mit Ende-zu-Ende-Verschlüsselung wie WhatsApp, Threema und Signal auf den Endgeräten schon vor dem Verschlüsselungsvorgang durchsucht und ggf. ausgeleitet werden = **Client-Side-Scanning** - **CSS**.
Alternativ zu CSS müßte zur Realisierung der Chatkontrolle die Ende-zu-Ende-Verschlüsselung durch Hintertüren unwirksam gemacht werden.
https://netzpolitik.org/2022/eu-plaene-einfach-erklaert-warum-die-chatkontrolle-grundrechte-bedroht/
Bisher noch sträuben sich Grüne und FDP-Minister dagegen.
Auch von mehreren Kinderschutzorganisationen wird die Chatkontrolle als untauglich zur Bekämpfung von sexueller Gewalt an Kindern und unverhältnismäßig, als massiver Eingriff in rechtsstaatliche Grundsätze abgelehnt: Entschieden ist die Sache aber jetzt im Juni 2022 noch nicht.
Quellen:
https://netzpolitik.org/2022/massenueberwachung-das-sagen-kinderschutz-organisationen-zur-chatkontrolle/
https://digitalcourage.de/blog/2022/chatkontrolle-brief-kommission-juni

Dass es in Europa, konkret in Großbritannien, ziemlich wenig staatliche Skrupel bzgl. Überwachung der Bürger gibt, zeigt beispielhaft der noch folgende Vortrag von Georgia.

Es wäre leichtgläubig, sich auf programmatische Ausrichtungen bestimmter Parteien zugunsten Privatsphärenschutz zu verlassen, solange sie in der Opposition sind:
Die in Baden-Württemberg regierenden Grünen gerieten ab 2017 wegen eines geplanten Polizeigesetzes in die Kritik.
https://www.stuttgarter-zeitung.de/inhalt.kritik-am-einsatz-von-staatstrojanern-verfassungsbeschwerde-gegen-polizeigesetz.3a10a0f2-5c64-4025-bbab-3633821d0ff0.html
Auch die modifizierte Fassung vom 06.10.2020 erlaubt in § 54 weiterhin eine Überwachung der Telekommunikation per Staatstrojaner.
https://www.landesrecht-bw.de/jportal/portal/t/rlm/page/bsbawueprod.psml?pid=Dokumentanzeige&showdoccase=1&js_peid=Trefferliste&fromdoctodoc=yes&doc.id=jlr-PolGBW2021pP54&doc.part=S&doc.price=0.0#focuspoint

Das Problem dabei: Sogar wenn Staatstrojaner nur mit Richtervorbehalt und gezielt eingesetzt werden, erfordert das ein Offenhalten von Sicherheitslücken, um Geräte aus der Distanz infiltrieren zu können. Bislang unbekannte Sicherheitslücken (Zero-day-exploits) werden dabei nicht an die

Programm-Hersteller gemeldet, können aber von Kriminellen und ausländischen Geheimdiensten ggf. auch entdeckt, gestohlen, gekauft und ausgenutzt werden. Gravierendes Beispiel: „Wanna-Cry“: 230.000 Computer in 150 Ländern waren von Kriminellen infiziert worden, um Lösegeldzahlungen. zu erpressen. Fünf Jahre hatte die NSA die Windows-Sicherheits-Lücke selbst genutzt ohne Microsoft zu informieren!
https://de.wikipedia.org/wiki/WannaCry

Zur Begründung von Überwachungs-Maßnahmen wird auf Schwerstkriminalität verwiesen, wahlweise die Bekämpfung von Kinder-Pornografie oder Terrorismus herangezogen. Je nach aktueller Konjunktur in den Medien. In der Folge besteht nach Einführung von Chatkontrolle, Staatstrojaner oder Vorratsdatenspeicherung die Tendenz bzw. das Risiko, daß die Überwachung auf andere Ermittlungs-Bereiche ausgedehnt wird, einfach weil das Werkzeug dazu verfügbar ist.

Immerhin: In seiner Entscheidung bestätigte das Bundesverfassungsgericht die Auffassung der klagenden Gesellschaft für Freiheitsrechte (GFF), „dass staatliche Stellen Grundrechte verletzen, wenn sie Sicherheitslücken in IT-Systemen geheim halten, ohne ihre Risiken zu bewerten.“
https://freiheitsrechte.org/ueber-die-gff/presse/pressemitteilungen-der-gesellschaft-fur-freiheitsrechte/pm-grundsatzentscheidung-it-sicherheit

Unsere „letzte Rettung“ nach diversen oft ignorierten Protesten der Zivilgesellschaft („Freiheit statt Angst-Demos“) : Wenn die höchsten Gerichte die bereits z.T. in Kraft getretenen Gesetze doch noch in wesentlichen Teilen als unvereinbar mit Menschenrechten oder Verfassung für ungültig erklären. So geschehen bei mehreren Anläufen, die Vorratsdatenspeicherung durchzusetzen. Unabhängigkeit der Justiz im Sinn einer Gewaltenteilung bekommt da eine ganz besondere Bedeutung.
https://netzpolitik.org/2020/haeufig-gestellte-fragen-was-die-neuen-gerichtsurteile-zur-vorratsdatenspeicherung-bedeuten/
https://netzpolitik.org/2019/verfassungsgericht-in-oesterreich-kippt-staatstrojaner/

Man kann unser Thema international nicht isoliert betrachten:
Noch können wir hier in Deutschland uns so wie heute treffen um über Verschlüsselung zu reden. Nach Gestapo und Stasi gibt es in Deutschland eine allgemein höhere Sensibilität in Fragen Staatlicher Überwachung und Verletzung der Privatsphäre als anderswo.
Entscheidungen und Praxis hierzulande werden allerdings im Ausland registriert und ggf. nachgemacht. So wie auch unsere Geheimdienste nach den NSA-Enthüllungen zunehmende Mittel und Kompetenzen erhielten.

Die deutsch-britische Firma GAMMA hat jahrelang Spionagesoftware FINFISHER an repressive Staaten verkauft, die damit Mobiltelefone verwanzt haben um Oppositionspolitiker, Menschenrechtsaktivisten, Rechtsanwälte, Gewerkschafter und Journalisten zu verfolgen.
Auch das BKA hat diese Software offenbar zu „Prüfzwecken“ eingekauft.
Quellen:
https://netzpolitik.org/2014/gamma-finfisher-ueberwachungstechnologie-made-in-germany-gegen-arabischen-fruehling-in-bahrain-eingesetzt/
https://netzpolitik.org/2013/geheimes-dokument-bundeskriminalamt-kauft-international-bekannten-staatstrojaner-finfisherfinspy-von-gamma/

Etwa zeitgleich mit dem Gefängnisaufenthalt des deutschen Journalisten Denis Yüksel hat Erdogans Türkei vom 5. Juli 2017 bis 25.Oktober 2017 den deutschen Menschenrechtsaktivisten Peter Steudtner
https://de.wikipedia.org/wiki/Peter_Steudtner
wegen Schulung Türkischer Menschenrechtsaktivisten in gewaltlosem Widerstand und IT-Sicherheit unter dem Vorwand „Mitgliedschaft in einer Terrororganisation“ eingesperrt. Erst im Juli 2020 lange nach Intervention der deutschen Regierung kam es zum Freispruch für Steudtner. Über Gegenleistungen Deutschlands wurde Stillschweigen bewahrt.

Nach den Enthüllungen von Edward Snowden über Methoden der NSA war in Deutschland der mediale Aufschrei und die angebliche Betroffenheit politischer Entscheidungsträger zwar groß. „Ausspähen unter Freunden das geht gar nicht“ (A.Merkel 10/2013)

https://www.welt.de/newsticker/news1/article162121864/Merkel-bekraeftigt-Ausspaehen-unter-Freunden-geht-gar-nicht.html
Die im NSA-Untersuchungs-Ausschuß teilweise aufgedeckten Verwicklungen und Praktiken der deutschen Geheimdienste führten aber nicht zur Einhegung und besserer Kontrolle, sondern zur Ausweitung von Kompetenzen und Mitteln: ZITIS eine neugeschaffene Bundes-Behörde, die das Brechen von Verschlüsselungsmaßnahmen erforschen und ermöglichen soll.
https://netzpolitik.org/?s=zitis
https://www.zitis.bund.de/DE/Home/home_node.html

Auch gab es die nachträgliche Legitimierung der Geheimdienst-Praktiken. Motto: „Das was die NSA kann, wollen wir auch."
https://netzpolitik.org/2015/nsa-untersuchungsausschuss-der-bnd-baut-sich-einen-rechtsfreien-raum/
https://netzpolitik.org/2018/ein-jahr-nach-dem-nsa-untersuchungsausschuss-bloss-keine-geheimdienstkontrolle/

>>>> DAS BEISPIEL GROßBRITANNIEN …

——— Pause ———

Als FOLIE 18: KONSEQUENZEN
Was können wir unter den geschilderten Verhältnissen selbst im Alltag tun?
Generell: **Digitalen Fußabdruck reduzieren!**
Schrittweise vorgehen: Abwägen von Aufwand und Nutzen, idealerweise mit Partnern gemeinsam vorgehen
(Beispiele sind ohne Anspruch auf Vollständigkeit)

Als FOLIE 19: Angriffsflächen verkleinern
- Angriffsflächen verkleinern: Unnötige Programme meiden bzw. deinstallieren
- System aktuell halten: Sicherheits-Updates, Betriebssysteme aktuell halten, Programm-Updates
- Solide Info-Quellen zu Daten-/Privatsphärenschutz nutzen: mobilsicher.de, Kuketz-blog.de
- Smartphone auch mal ausschalten, daheim lassen, WLAN-Empfang bei Reisen ausschalten (Standortverfolgung)
- Bezahlvorgänge möglichst analog: Bar, Rechnung, Überweisung
- Suchmaschine Google ersetzen durch Startpage oder MetaGer
- Umstieg auf E-Mail-Provider mit konsequent umgesetzten Geschäftsmodell Privatsphäre wie MAILBOX.ORG, POSTEO.DE:
- >> Dauerhafter Schutz für 1€/Monat, Testsieger bei Stiftung Warentest

Als FOLIE 20:
- Alternativer App-Store F-Droid statt Google-Play-Store (Tracking- und Google-freie Programme)
- Tracking-und Werbe-Blocker nutzen: Blokada, Noscript oder uMatrix, uBlock Origin …
- Messenger mit „Privacy by Design" nutzen: SIGNAL, THREEMA
- noch besser aber z.T. aufwendiger dezentral organisierte Messenger bzw soziale Medien: MASTODON, Adium, Jabber
- Wo immer möglich (!) Ablösung von bisher genutzten proprietären Programmen, Nutzung quelloffener Anwendungen: LibreOffice statt
  Microsoft Office, mit Add-Ons angepasster Firefox-Browser stattGoogleChrome, GIMP statt Photoshop etc.. Aber: Lock-In-Effekt
- TOR-Netzwerk nutzen und stärken: TOR-Browser, TAILS, SNOWFLAKE-Add-On
  Das ermöglicht die Umgehung von Zensur, läßt uns unbeobachtet surfen und kommunizieren
- Ggf. Betriebssystem Linux statt Windows oder MacOS. (Linux User Groups)
- Ggf. Lineage-OS oder /e/ statt Google-Android auf Smartphones als Betriebssystem
- E-Mail-Verschlüsselung mit ebenfalls engagierten Partnern. (Leider nicht massentauglich, Metadaten sind nicht vermeidbar)
- Die einfachen Dinge zuerst angehen! (z.B. Ende-zu-Ende verschlüsselnder Messenger Signal o. Threema vor E-MailVerschlüsselung)

Als FOLIE 21: Politische Konsequenzen

Welche **politischen Konsequenzen** können wir ziehen?
Die Sachverhalte und digitale Techniken sind kompliziert und komplex. (Mülltrennung kann man viel leichter erklären und dafür werben.)
Bescheidenheit in den Zielvorgaben! Es hilft, sich nur als kleines Teil eines Netzwerks zu begreifen.

- Eigenes Wissen erwerben als Voraussetzung um
- Die Thematik qualifiziert in der Dikussion zu halten.
- Valide Informationen einholen: netzpolitik.org …
- Wissensquellen teilen
- Keine Berührungsängste in der Diskussion (nicht auf gleichgesinnte sich jammernd beschränken)
- Unterstützung bereits existierender NGOs: Amnesty, Digitalcourage, NOYB: Juristische u. Öffentlichkeits-Kampagnen, Infos, Spenden
- Der DSGVO zur Durchsetzung verhelfen.
- Austausch auf Cryptoparties, Kompetenzen schrittweise erweitern und weitergeben
- Beispiel geben in eigener Nutzung digitaler Technik!

Als FOLIE 22:
„Privacy is a right like any other. You have to exercise it or risk losing it.“
Phil Zimmermann, der Erfinder von Pretty Good Privacy, PGP (zur E-Mail-Verschlüsselung)
Quelle: https://www.cybersociology.com/files/7_bigbrotheronline.html

Als FOLIE 23:
Cryptoparty Tübingen
Website: cryptoparty-tuebingen.de
Kontakt: lamm5714@posteo.de
———————————————————

Empfehlungen zum Eigenstudium auf unserer Website:
https://cryptoparty-tuebingen.de/corona.php
Aktueller Film aus der Mediathek des ZDF: „Digitale Rebellen - Kampf gegen die Mächtigen“ Film von Anna Loll
https://www.zdf.de/dokumentation/digital-empire/digitale-rebellen-china-russland-zensur-assange-100.html