Intern. Strategien zur Stabilisierung der Machtverhältnisse

Die totale Überwachung ist erreicht

von Laurenz Nurk, Dortmund

Nach dem Ende der bipolaren Welt im Jahr 1989 und dem Abhandenkommen von Gegnern und Grenzen wurden unter der Regie der USA auch alle Einschränkungen im Verkehr von Gütern und Kapital aufgehoben. Dies zu einem Zeitpunkt, an dem sich fast die Hälfte der Staaten der Welt erstmalig dem ausländischen Kapital öffnete, das dann auf ein riesiges Angebot an billigen und qualifizierten Arbeitskräften, einem enormen Vorkommen an Naturschätzen und einem noch nicht da gewesenen großen Absatzmarkt traf. Das kam vor allem dem Kapital der USA, als neue unipolare Macht zugute.

Gleichzeitig bekam die Verbreitung des **Neoliberalismus** einen Schub, bei dem das Kapital von Einschränkungen befreit und der Arbeitsschutz, die öffentliche Daseinsvorsorge und der Sozialstaat nachhaltig abgebaut wurden. Vor dem Hintergrund des globalen Kapitalismus mit seinen sozialen Desintegrationsprozessen wurden parallel dazu internationale Strategien entwickelt, um zu gewährleisten, dass die Machtverhältnisse auch stabil bleiben. Dazu wurde vor allem die Polizei militarisiert, das Militär im Inneren einsetzbar gemacht und es gibt mittlerweile kaum ein gesellschaftliches Problem mehr, auf das seitens der Politik nicht mit der Verschärfung des Strafrechts reagiert wird.

Gleichzeitig wurde ein Überwachungssystem errichtet, in dem die Bevölkerung total überwacht, von jeder Person massenhaft Informationen gesammelt, sie erpressbar gemacht und ein immenses Meinungs- und Unterhaltungsangebot mit dem Internet aufgebaut wurde, damit die Massen beschwichtigt und ablenkt werden.

Das digitale Zeitalter hat Überwachung so billig und einfach gemacht, wie noch nie, auch deshalb, weil ein Großteil der Daten freiwillig von den E-Phons geliefert werden.

Umfassend bekannt wurde die Möglichkeit der vollständigen Kontrolle aller Menschen weltweit durch die Enthüllungen von Edward Snowden. Das sogenannte PRISM [3]-Programm der National Security Agency (NSA) verschafft dem Geheimdienst einen direkten Zugriff auf die Daten von Google, Facebook, Microsoft, Yahoo, Paltalk, Youtube, Skype, AOL und Apple. Diese Möglichkeit kostet lediglich 20 Millionen Dollar pro Jahr, bei einem Jahresbudget der NSA von weit über 10 Milliarden Dollar.

► Massenhaft Informationen über die Bevölkerung sammeln

Obwohl das World Wide Web im Jahr 1989 im Forschungslabor der Europäischen Organisation für Kernforschung (CERN [4]) in Genf erfunden wurde, ist es schnell zu einem rein US-amerikanischen Unternehmen geworden. Mehr als 90 Prozent des weltweiten Internetverkehrs wird über Technologien abgewickelt, die sich im Besitz von der US-Regierung selbst oder von US-Firmen befinden, von ihnen entwickelt wurden die heute mehr denn je am Ein- und Ausschalter des Systems sitzen und dies jeder Zeit bedienen können.

Auch die Software ist überwiegend in US-amerikanischen Händen, genauso wie Hardware und anderes Zubehör, wie Chips, Router, Modems und Plattformen. Der Mailverkehr, die sozialen Netzwerke und Speichersysteme in der Cloud sind in der Regierungshand oder werden von Privatfirmen wie Amazon [5], das der Regierung Cloud-Dienste und das halbe Internet bereitstellt, betrieben.

Selbst wenn diese Unternehmen im Ausland produzieren, unterliegen sie dem US-amerikanischen Recht. Damit ist die US-Regierung in der Lage, alle Menschen zu beobachten, die einen Computer oder ein Telefon bedienen.

⇒ „Kooperation der Dienste“ mit Telekommunikations- und Softwareunternehmen

Im Januar 2007 wurde durch die Berichte der Washington Post die Zusammenarbeit zwischen Microsoft und der NSA bekannt. Microsoft begründete diese Kooperation damit, dass dies die Sicherheit ihres Betriebssystems erhöht habe und das Unternehmen aufgrund seiner herausragenden Marktstellung die Kompatibilität ihrer Produkte mit den Bedürfnissen der (amerikanischen) Regierung sicherstellen wollte. Andere IT-Unternehmen folgten schnell dem Beispiel von Microsoft.

Auch das deutsche "Bundesamt für Sicherheit in der Informationstechnik" BSI [6]) hielt die Kooperation der Firmen mit Geheimdiensten für „eher vorbildlich als verwerflich“ und betonte die „Win-Win-Situation“ für den Endnutzer sowie für die Unternehmen. Berichte über die Zugriffsmöglichkeiten der NSA auf die Betriebssysteme der IT-Unternehmen wurden rasch als Verschwörungstheorien abgetan.

Seit Anfang 2012 ist die NSA Mitentwickler des Betriebssystem „SELinux“ und hat auch das „SEAndroid“ Betriebssystem für Google entworfen. Ein Jahr später wurde bekannt, dass die NSA im Rahmen des Programms „Planing tool for Resource Integration, Synchronization und Management“ (PRISM) in großem Umfang weltweit das Internet ausspähen soll, indem es systematisch die Daten großer Konzerne wie Google, Microsoft, Yahoo, Paltalk, Youtube, Skype, AOL und Apple und deren Nutzer auswertet.

⇒ **Kabel und Cloud**

Große Teile der Daten im Internet laufen über Glasfaserkabel, viele internationale und interkontinentale Verbindungen laufen über Seekabel. Um diese Datenströme zu leiten liegen auf den Meeresböden seit fast 50 Jahren entsprechende Kabel die das weltweite Netz verbinden.

Geheimdienste wie die NSA nutzen viele verschiedene Technologien, um Kommunikationsverkehre abzuhören und zu speichern. Neben dem Hacken von Systemen können sie auch durch die Kooperation mit Betreibern an die gewünschten Daten kommen. Der Telekommunikationskonzern AT&T hat der NSA in San Francisco exklusiv einen eigenen Raum gegeben, in den es die Daten lieferte.

Ein Anzapfen der Kabel selbst ist ebenfalls gängige Praxis und wird mit verschiedenen Techniken ausgeführt: Am einfachsten ist die Attacke auf die Lichtsignale [7], in dem die Glasfaserstrecke aufgetrennt und ein zusätzliches Gerät zwischen Sender und Empfänger eingebaut wird. Mit der Splitter-Coupler-Methode biegen Angreifer die Glasfasern, um mittels spezieller „Biegekoppler“ dann heimlich auf den Informationsfluss zugreifen zu können. Nicht nachweisbar sind Einbrüche, die den direkten Kontakt mit der Datenleitung völlig vermeiden (non-touching methods). Solche Angriffsmethoden beruhen darauf, dass aus jedem Kabel minimale Lichtmengen strahlen, die mit hochempfindlichen Fotodetektoren aufgefangen und verstärkt werden.

In Deutschland gibt es Übergabepunkte auch bei Telekomanbietern, sie heißen hierSINA [8]-Boxen. Der Vorgang läuft so ab: Die Behörde schickt einen Gerichtsbeschluss mit der Datenanforderung, das Unternehmen prüft ihn und gibt anschließend die Daten frei. Die werden dann über die Schnittstelle automatisch an den Dienst übertragen.

Viel effektiver und umfassender als das Anzapfen der Kabel ist das Cloud Computering, bei dem sich weltweit Menschen anmelden, freiwillig ihre Videos, Musikfavoriten, Fotos und private Kommunikation in der „Wolke“ abladen und sich den Anbietern dieses Services bedingungslos unterwerfen.

Gelockt werden die Datenlieferanten damit, dass sie mit jedem PC, Smartphones, Laptops und Tabletts ohne irgendwelche teuren Zusatzgeräte, ihre Daten dort in den riesigen Speicherzentren ablegen und verwalten lassen können. "Verwalten" heißt hier, das dem einzelnen Nutzer seine eigenen Daten nicht mehr gehören und wenn er sie nicht auf seinen eigenen Geräten abgespeichert hat, sind sie weg. Er hat alles abgetreten und die Unternehmen können nach Belieben damit machen, was sie wollen. Mit ihren bis zu 6000 Seiten umfassenden Verträgen haben sich die Firmen diese Rechte gesichert. Gesichert haben sie auch ihr Recht, Daten willkürlich zu löschen, den Nutzen den Zugriff auf seine gespeicherten Daten zu verweigern und eine Kopie in der Firmenablage abzuspeichern oder ohne das Wissen und Einverständnis an die Behörden aushändigen zu können.

⇒ **Metadaten**

Ende des letzten Jahrtausends bereiteten die gigantischen Datenmengen, die beim Abhören anfielen noch große Probleme. Aber die steigende Rechenleistung von Supercomputern und Mega-Rechenzentren ermöglichen es, dass heute ein einzelner Analyst in den Diensten Informationen aus riesigen Mengen von Rohdaten extrahieren kann. Aber nicht nur die Quantität der Daten musste in den Griff bekommen werden, auch die Qualität der Unmengen an Daten warfen Probleme auf.

Heute haben die Informationen Priorität, die ungeschrieben sind, unausgesprochen werden, aber viel über die Verhaltensmuster des einzelnen Menschen aussagen. Hier wurde der Begriff der Metadaten kreiert, gemeint sind Aktivitätsdaten, die Auskunft geben über alles, was mit den elektronischen Geräten gemacht wird und was die Geräten selbständig tun. Bei einem Telefonanruf umfassen solche Metadaten Datum, Uhrzeit und Dauer des Anrufs, die Nummer, des Anrufers, die Nummer des Angerufenen und seinen Aufenthaltsort. Bei einer E-Mail können die Metadaten Auskunft geben, auf welchen Computertyp geschrieben wurde, wem der Computer gehört, wo, wann und von wem die Mail gesendet wurde, wer sie erhalten hat und auch wer eventuell außer dem Sender und Empfänger wo und wann ebenfalls Zugang zur E-Mail hatte.

Die Metadaten geben auch über sehr private Dinge Auskunft. Dem Überwacher verraten sie, wo die Person übernachtet hat, wann sie aufgestanden ist und verraten, wo sie sich aufgehalten hat und wie viel Zeit sie dort verbracht hat und damit auch mit wem sie Kontakt hatte und wer mit ihr.

Metadaten liefern genau die Informationen, die als Ausgangspunkt für die Überwachung benötigt werden. Dabei helfen vor allem die Metadaten die automatisch entstehen und die der einzelne Mensch nicht beeinflussen kann. Die Maschine sammelt, speichert und analysiert eigenständig, ganz autonom und Diskretion ist dabei ein Fremdwort. Sie kontaktiert den nächsten Mobilfunkmast und sendet Signale aus, die niemals lügen.

Für die Geheimdienste können die Aktivitätsaufzeichnungen nicht nur durch die Analyse flächendeckender Daten ein Bild vom großen Ganzen bieten, auch im kleinen Bereich können sie punktgenaue Zusammenfassungen über das Leben einer Person erstellen und sie meinen sogar, Vorhersagen über ihr zukünftiges Verhalten ableiten zu können.

⇒ **Die Internetüberwachungsprogramme PRISM und Upstream Collection**

Mit der Einführung des Überwachungsprogramms PRISM konnte die NSA Daten in einer unglaublichen Anzahl sammeln. Sie generiert sie aus E-Mails, Fotos, Video- und Audiochats, Webbrowsing-INHALTE, Anfragen an Suchmaschinen und alle Daten, die in den Clouds gespeichert waren. Dazu kommen noch die routinemäßig gelieferten Daten von Google, PalTalk, YouTube, Microsoft, Yahoo, Facebook, Skype, AOL und Apple.

PRISM ist nicht allein eine Software oder ein Datenzentrum, es besteht aus mehreren Komponenten. Die wichtigste ist dabei eine Ausleitungsschnittstelle, über die Daten von den Firmen an die Dienste übergeben werden. Dabei funktioniert sie wie ein elektronischer Briefträger.

Das Programm Upstream Collection ermöglicht die permanente Datensammlung unmittelbar aus der Internetinfrastruktur des privaten Sektors, hervorgeholt aus den Switches und Routern, die den Internetverkehr aus den am Meeresboden verlegten Kabeln oder über die Satelliten abwickeln. Das Programm ist mit seinen Werkzeugen in Lage, ganz nah an der überwachten Person und seiner Privatsphäre zu operieren. Jedes Mal wenn die Person eine Website besucht, einen Webbrowser öffnet, die URL eingibt, geht die Anfrage auf Serversuche. Bevor die Anfrage den entsprechenden Server erreicht, muss sie aber die mächtigste Waffe der NSA die sogenannte TURBULENCE durchlaufen. Bei dem Durchlauf muss die Anfrage einige „schwarze Server“ überwinden, die übereinander gestapelt kaum größer als ein Quadratmeter sind und in allen verbündeten Staaten in besonderen Räumen der Telekommunikationsunternehmen aufstellt sind, ebenso auf US- Militärstützpunkten und in US-Botschaften rund um den Globus.

Die TURBULENCE enthält 2 wichtige Werkzeuge:

• TURMOIL betreibt das „passive Datensammlung“ indem es Kopien der durchlaufenden Daten sammelt und bei seiner Wächterfunktion untersucht sie die Metadaten, ob sie etwas enthalt, was „prüfungswert“ erscheint bis hin zu bestimmten Schlüsselwörtern. Werden die Daten als verdächtig eingestuft, gibt TURMOIL den Internetverkehr weiter an die

• TURBINE, dieses Werkzeug gibt die Anfrage auf die Server der NSA weiter. Dort wird mit Hilfe von Algorithmen entschieden, welche Schadprogramme der NSA gegen die Person eingesetzt werden. Die Entscheidung wird durch den Typ der Website die angefragt begründet oder durch die Software des Computers und die Art der Internetverbindung. Das ausgewählte Schadprogramm wird dann wieder an die TURBINE gesendet. Diese führt das Schadprogramm zurück in den Kanal des Internetverkehrs und liefert sie dem Anfragenden frei Haus zusammen mit der gewünschten Website. Der gesamte Vorgang dauert weniger als 680 Millisekunden, ohne dass der Nutzer etwas mitbekommen hat. Ab diesem Zeitraum gehört das gesamte digitale Leben des Nutzers dem Geheimdienst.

Beide Programme können durch die obligatorische Datensammlung auf den Servern der Provider (PRISM) und durch die unmittelbare Datensammlung aus der Internetinfrastruktur (Upstream Collection) über den gesamten Globus Informationen überwachen, egal ob sie gespeichert oder übermittelt wurden.

⇒ **Uneingeschränkte Unternehmensmacht gekoppelt mit unkontrollierbaren staatl. Diensten**

Das Internet ist eine grundlegende Infrastruktur für die Ausübung zahlreicher Menschenrechte. Konzerne wie Facebook und Google sind Torhüter dieser digitalen Welt. Sie haben eine historisch einmalige Macht über den „digitalen öffentlichen Platz“ und bestimmen auch, unter welchen Bedingungen und mit welchen Einschränkungen Meinungs- und Informationsfreiheit online ausgeübt werden können und welchen Preis man dafür zahlen muss.

Die Dominanz von Onlinediensten, wie sie IT-Riesen wie Google und Facebook anbieten, geben diesen Unternehmen eine nie dagewesene Macht über die persönlichsten Daten von Millionen Menschen: 2,8 Milliarden Personen pro Monat nutzen einen Facebook-Dienst, mehr als 90 Prozent aller Internetsuchen finden auf Google statt und mehr als 2,5 Milliarden Handys nutzen das Google-Betriebssystem Android.

Konzerne wie Facebook und Google sammeln Daten in einem unfassbaren, nie dagewesenen Ausmaß – unbeschränkt, dauerhaft. Dies umfasst nicht allein freiwillig zur Verfügung gestellte Informationen, sondern die digitale Erfassung und Überwachung aller Aktivitäten, weit über die Nutzung einzelner Social-Media-Plattformen hinaus. Auch ist es nicht auf die Daten derer beschränkt, die sich bewusst dafür entschieden haben, diese Dienste zu nutzen.

Während internationales Recht und Verfassungen elementare Menschenrechte garantieren, staatliche Behörden reglementieren und diese einer rechtsstaatlichen Gewaltenkontrolle unterwerfen, haben diese Konzerne ein privates Überwachungsregime geschaffen, welches sich der unabhängigen öffentlichen Kontrolle weitgehend entzieht. Parallel zum Ausbau des weltweiten Überwachungssystems, in dem die Bevölkerung total ausgehorcht, von jeder Person massenhaft Informationen gesammelt werden, sie erpressbar macht, wurde parallel dazu ein immenses Meinungs- und Unterhaltungsangebot mit dem Internet aufgebaut, mit dem man die Massen beschwichtigen und ablenken will. Dazu kommt, dass die USA und auch die europäischen Staaten über ein Heer von Einflussjournalisten in Kooperation mit der monopolisierten Medienmacht verfügt, die globale Kommunikation weitgehend steuert.

Mehr noch, in der Zusammenarbeit der staatlichen Behörden und Geheimdienste, IT-Unternehmen und Medienkonzernen ist ein Überwachungssystem entstanden, das sich selbst George Orwell in seinem utopischen Roman

„1984 [9]“ nicht ausmalen konnte.

Laurenz Nurk, Dortmund

Quellen:

netzpolitik.org; "1984" von George Orwell; Amnesty-Bericht: "**Surveillance Giants [10]**“;

"Permanent Record: Meine Geschichte" von Edward Snowden, S. Fischer, FFM, ISBN: 978-3-10-397482-9 (Hardcover), voraussichtl. ab Okt. 2020 auch als Taschenbuch, ISBN: 978-3-596-70069-1;

"Gegenrevolution. Der Kampf der Regierungen gegen die eigenen Bürger", S. Fischer, FFM 2019, ISBN: 978-3-10-397436-2 von Bernard E. Harcourt [11];

► **Quelle:** Erstveröffentlicht am 5. Mai 2020 auf gewerkschaftsforum-do.de >>**Artikel** [12]. Die Texte (nicht aber Grafiken und Bilder) auf gewerkschaftsforum-do.de unterliegen der Creative Commons-Lizenz (CC BY-NC-ND 3.0 DE [13]), soweit nicht anders vermerkt.

ACHTUNG: Die Bilder, Grafiken, Illustrationen und Karikaturen sind **nicht** Bestandteil der Originalveröffentlichung und wurden von KN-ADMIN Helmut Schnug eingefügt. Für sie gelten ggf. folgende Kriterien oder Lizenzen, s.u.. Grünfärbung von Zitaten im Artikel und einige zusätzliche Verlinkungen wurden ebenfalls von H.S. als Anreicherung gesetzt.

► Bild- und Grafikquellen:

1. Pentagonaler Abfluss der Freiheit - **Grafik:** Bernd Wachtmeister. **Quelle:** Pixelio.de [14] >> Grafik [15]. Nur redaktionelle Nutzung!

2. OHNE Amazon. Grafik: freie Verwendung. Herzlichen Dank an AG Küste - c/o Elisa Rodé >**weiter [16]**.

3. Abhörgerät Biegekoppler an einem Glasfaserkabel (Coupler-Methode). **Urheber:** © 1971markus. Diese Datei ist lizenziert unter der Creative-Commons-Lizenz „Namensnennung – Weitergabe unter gleichen Bedingungen 4.0 international“ (CC BY-SA 4.0 [17]). Diese Datei steht unter einer Lizenz, die mit den Lizenzbedingungen von Facebook inkompatibel ist. Es ist daher nicht gestattet, diese Datei auf Facebook hochzuladen. Dies beinhaltet auch die meisten anderen sozialen Netzwerke wie Instagram und WhatsApp.

4. Beim Einsatz der Biometrie zur automatisierten Erkennung [18] von Personen kommt es darauf an, individuelle biometrische Verhaltens- oder Körpercharakteristika zu finden, die sich u. a. durch folgende Eigenschaften auszeichnen:

• Einmaligkeit: Der Messwert des Charakteristikums ist für möglichst alle Personen unterschiedlich

• Konstanz: Der Messwert hängt nicht vom Alter der Person oder dem Messzeitpunkt ab

• Messbarkeit: Es sollte eine gut definierbare Messgröße existieren, für die es geeignete Sensoren [19] gibt

• Universalität: Das Charakteristikum kommt bei möglichst vielen Personen vor.

Illustration: geralt / Gerd Altmann, Freiburg. **Quelle**: Pixabay [20]. Alle Pixabay-Inhalte dürfen kostenlos für kommerzielle und nicht-kommerzielle Anwendungen, genutzt werden - gedruckt und digital. Eine Genehmigung muß weder vom Bildautor noch von Pixabay eingeholt werden. Auch eine Quellenangabe ist nicht erforderlich. Pixabay-Inhalte dürfen verändert werden. Pixabay Lizenz [21]. >> **Illustration** [22].

5. Eine **Serverfarm** ist eine Gruppe von gleichartigen, vernetzten Server [23]-Hosts [24], die zu einem logischen System verbunden sind (auch: *Data-Center*). Sie optimiert die internen Prozesse durch Verteilung der Auslastung zwischen den einzelnen Servern und beschleunigt die Computerprozesse durch Ausnutzung der Rechenleistung mehrerer Server. **Foto:** ColossusCloud / Colossus Cloud, Las Vegas/USA. **Quelle**: Pixabay [20]. Alle Pixabay-Inhalte dürfen kostenlos für kommerzielle und nicht-kommerzielle Anwendungen, genutzt werden - gedruckt und digital. Eine Genehmigung muß weder vom Bildautor noch von Pixabay eingeholt werden. Auch eine Quellenangabe ist nicht erforderlich. Pixabay-Inhalte dürfen verändert werden. Pixabay Lizenz [21]. >> Foto [25].

6. FUCK facebook AND LIVE LIFE! Freie Nutzung.

Quell-URL: https://kritisches-netzwerk.de/forum/intern-strategien-zur-stabilisierung-der-machtverhaeltnisse

Links
[1] https://kritisches-netzwerk.de/user/login?destination=comment/reply/8671%23comment-form
[2] https://kritisches-netzwerk.de/forum/intern-strategien-zur-stabilisierung-der-machtverhaeltnisse
[3] https://de.wikipedia.org/wiki/PRISM
[4] https://de.wikipedia.org/wiki/CERN
[5] https://kritisches-netzwerk.de/forum/kn-kauftipp-schnauze-alexa-ich-kaufe-nicht-bei-amazon
[6] https://de.wikipedia.org/wiki/Bundesamt_f%C3%BCr_Sicherheit_in_der_Informationstechnik

[7] https://www.datacenter-insider.de/glasfaserkabel-abhoeren-fuer-hacker-ein-leichtes-spiel-a-279367/
[8] https://de.wikipedia.org/wiki/Sichere_Inter-Netzwerk_Architektur
[9] https://de.wikipedia.org/wiki/1984_(Roman)
[10] https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF
[11] https://de.wikipedia.org/wiki/Bernard_E._Harcourt
[12] https://gewerkschaftsforum.de/internationale-strategien-zur-stabilisierung-der-machtverhaeltnisse-die-totale-ueberwachung-ist-erreicht/#more-7506
[13] https://creativecommons.org/licenses/by-nc-nd/3.0/de/
[14] https://www.pixelio.de/
[15] https://www.pixelio.de/media/675667
[16] https://ohneamazon.wordpress.com/
[17] https://creativecommons.org/licenses/by-sa/4.0/deed.de
[18] https://de.wikipedia.org/wiki/Automatische_Identifikation_und_Datenerfassung
[19] https://de.wikipedia.org/wiki/Sensor
[20] https://pixabay.com/
[21] https://pixabay.com/de/service/license/
[22] https://pixabay.com/de/illustrations/gesichtserkennung-scan-scannen-4762379/
[23] https://de.wikipedia.org/wiki/Server
[24] https://de.wikipedia.org/wiki/Host_(Informationstechnik)
[25] https://pixabay.com/de/photos/server-wolke-entwicklung-gesch%C3%A4ft-1235959/
[26] https://kritisches-netzwerk.de/tags/abhoren
[27] https://kritisches-netzwerk.de/tags/algorithmen
[28] https://kritisches-netzwerk.de/tags/biegekoppler
[29] https://kritisches-netzwerk.de/tags/bsi
[30] https://kritisches-netzwerk.de/tags/bundesamt-fur-sicherheit-der-informationstechnik
[31] https://kritisches-netzwerk.de/tags/cern
[32] https://kritisches-netzwerk.de/tags/cloud-computering
[33] https://kritisches-netzwerk.de/tags/conseil-europeen-pour-la-recherche-nucleaire
[34] https://kritisches-netzwerk.de/tags/coupler-methode
[35] https://kritisches-netzwerk.de/tags/datenkraken
[36] https://kritisches-netzwerk.de/tags/datensammlung
[37] https://kritisches-netzwerk.de/tags/datenzugriff
[38] https://kritisches-netzwerk.de/tags/einflussjournalisten
[39] https://kritisches-netzwerk.de/tags/geheimdienst
[40] https://kritisches-netzwerk.de/tags/informationsfluss
[41] https://kritisches-netzwerk.de/tags/lauschangriff
[42] https://kritisches-netzwerk.de/tags/marktmacht
[43] https://kritisches-netzwerk.de/tags/massenuberwachung
[44] https://kritisches-netzwerk.de/tags/medienmacht
[45] https://kritisches-netzwerk.de/tags/medienmonopol
[46] https://kritisches-netzwerk.de/tags/metadaten
[47] https://kritisches-netzwerk.de/tags/national-security-agency
[48] https://kritisches-netzwerk.de/tags/neoliberalismus
[49] https://kritisches-netzwerk.de/tags/nsa
[50] https://kritisches-netzwerk.de/tags/planing-tool-resource-integration-synchronization-and-management
[51] https://kritisches-netzwerk.de/tags/prism
[52] https://kritisches-netzwerk.de/tags/schadprogramme
[53] https://kritisches-netzwerk.de/tags/seandroid
[54] https://kritisches-netzwerk.de/tags/seekabel
[55] https://kritisches-netzwerk.de/tags/selinux
[56] https://kritisches-netzwerk.de/tags/sozialabbau
[57] https://kritisches-netzwerk.de/tags/sozialstaatsabbau
[58] https://kritisches-netzwerk.de/tags/splitter-coupler-methode
[59] https://kritisches-netzwerk.de/tags/turmoil
[60] https://kritisches-netzwerk.de/tags/uberwachung
[61] https://kritisches-netzwerk.de/tags/uberwachungsprogramm
[62] https://kritisches-netzwerk.de/tags/uberwachungsregime
[63] https://kritisches-netzwerk.de/tags/uberwachungssystem
[64] https://kritisches-netzwerk.de/tags/unipolare-macht
[65] https://kritisches-netzwerk.de/tags/unternehmensmacht
[66] https://kritisches-netzwerk.de/tags/upstream-collection