Freitag, 24. Juli 2026, 16:00 Uhr
~12 Minuten Lesezeit

Die Überwachungsparanoia

Der beschlossene Angriff auf Datenschutz und Privatsphäre schürt die Angst vor einem aufziehenden Überwachungsstaat — dabei ist dieser längst Realität. Teil 2 von 2.

von Simone Hörrlein
Bild: Collage mit Foto von Shutterstock.com (B.Dpunkt)

Die Aufregung ist groß: Die jüngst von der Europäischen Union (EU) im dritten Anlauf

verabschiedete Chat-Kontrolle erhitzt die Gemüter ebenso wie der am 22. April 2026 verabschiedete Gesetzesentwurf, der Internetanbieter verpflichtet, IP-Adressen und die zugehörigen Port-Nummern für drei Monate vorsorglich zu speichern. Dabei ist die Überwachung und langfristige Speicherung privater Kommunikation im Internet schon seit vielen Jahren traurige Realität. Was gerade in der EU und in Deutschland ganz offiziell geschieht, ist nichts anderes als die schrittweise Legalisierung der Massenüberwachung, welche der „Sicherheitsapparat" schon seit Jahrzehnten illegal betreibt. Die totale Überwachung kommt nicht mit der Chat-Kontrolle und anderen aktuell aufflackernden Überwachungsmaßnahmen, und sie dient auch nicht primär dem Schutz von Kindern, Jugendlichen und anderen vulnerablen Gruppen. Ginge es um Pädophile und andere Perverse, dann würde man ganz andere Techniken einsetzen und auch die Epstein-Clique rigoros ausräuchern. Die Tatsache, dass das nicht getan wird, zeigt ganz deutlich, dass es um etwas anderes geht — nämlich darum, die totale Überwachung unter dem Vorwand von Schutz und Sicherheit Schritt für Schritt mehrheitsfähig zu machen. Es geht um den Übergang von einer „freundlichen Diktatur", auch Demokratie genannt, in eine weit weniger freundliche Technokratie, in der die totale Kontrolle des Einzelnen durch künstliche Intelligenz zur „Neuen Normalität" werden soll. Wer das nicht versteht, lebt in einer Traumwelt.

Werkzeuge für den Datenklau und die Rolle der Netzbetreiber

Zum Abfangen und zur Analyse der im Netz kursierenden Rohdaten nutzen Geheimdienste spezialisierte Hardware- und Softwaretools. Der Abgriff erfolgt an strategischen Punkten, wozu Unterseekabel, Internet-Knotenpunkte oder Provider-Zugänge zählen. Es erfolgt zwar keine passive Aufzeichnung des gesamten globalen Internets, aber eine extrem weitmaschige Sammlung von Datenströmen, die durch Filter wie TEMPORA (https://dcssproject.net/tempora/index.html) (UK) sowie PRISM (https://stateofsurveillance.org/articles/surveillance/prism-mass-collection/), BLARNEY, FAIRWVIEW oder STORMBREW (USA) laufen. Während PRISM „downstream collection" betreibt, also die Daten nicht vom Kabel, sondern direkt von den Servern der Tech-Konzerne abgreift, zapfen die anderen US-Programme die Daten „upstream (https://en.wikipedia.org/wiki/Upstream_collection)" an, also direkt an der Infrastruktur wie Glasfaserkabel, Router und Switches. Sobald eine Datenquelle als relevant eingestuft wird, und die Kriterien hierzu sind extrem weit gefasst, werden die Rohdaten in das Verteilernetzwerk STONE GHOST eingespeist und stehen den „5 Eyes" sofort zur Verfügung.

Obwohl keine aktuellen Baupläne veröffentlicht sind, bestätigen Dokumente aus dem Jahr 2013 — veröffentlicht durch Edward Snowden und analysiert von Journalisten wie **Duncan Campbell** (https://www.duncancampbell.org/content/gchqs-middle-east-cable-tap-centre-revealed) —, dass die Abhörpraxis an den Landepunkten der Unterseekabel stattfindet, wo man optische Splitter eingebaut hat. In kommerziellen Systemen dienen diese Splitter oft der Redundanz, um das Signal auf zwei verschiedene Landestationen zu verteilen, falls eine Station ausfällt. Im Kontext der Überwachung wird diese physikalische Eigenschaft aber

genutzt, um eine identische Kopie des Signals an die Abhöreinrichtungen der Geheimdienste weiterzuleiten, ohne den ursprünglichen Datenstrom zu unterbrechen. Die Installation der Splitter erfolgt in Zusammenarbeit mit den Betreibern der Kabel, also den Telekommunikationsunternehmen, die als „Partner" in den Dokumenten unter verschiedenen Codenamen wie „REMEDY" oder **„GERONTIC“** (https://www.theregister.com/offbeat/2014/11/26/snowden-doc-leak-lists-submarined-cables-tapped-by-spooks/273338) geführt werden.

> ***In den 5-Eyes-Ländern und vielen Verbündeten sind Telekommunikationsanbieter sogar gesetzlich verpflichtet, ihre Netzwerke so zu konstruieren, dass Geheimdienste direkten Zugriff haben.***

Wo Hintertüren nicht gesetzlich eingebaut werden können, erfolgt der Zugriff indirekt, zum Beispiel über politischen **Druck** (https://www.securityweek.com/encrypted-services-providers-concerned-about-eu-proposal-encryption-backdoors/) zur Gesetzesänderung, bilaterale Geheimdienstkooperationen und das Abfangen von Datenströmen außerhalb der direkten Kontrolle der Telekom-Anbieter, zum Beispiel mittels PRISM.

PRISM kommt bei den großen Tech-Konzerne wie Google, Meta, Microsoft und Apple zum Einsatz, über die ein Großteil des Datenverkehrs läuft. Diese Firmen arbeiten oft „freiwillig” mit den Diensten zusammen und stellen Daten direkt bereit, ohne dass ein Provider im klassischen Sinne etwas davon mitbekommt. Wenn europäische Daten einmal im Besitz eines 5-Eyes-Dienstes sind, durch Abfangen an Seekabeln, durch PRISM oder durch die Weitergabe durch den eigenen Geheimdienst, können sie innerhalb der Allianz frei geteilt werden. Dieser sogenannte „Loophole Effect” (Schlupflocheffekt) umgeht das Verbot, die eigene Bevölkerung direkt zu überwachen.

STONE GHOST: Das Verteilernetzwerk

Um die Daten unter den Geheimdiensten zu teilen, kommt das private **Hochsicherheitsnetzwerk STONE GHOST** (https://en.wikipedia.org/wiki/Stone_Ghost) zum Einsatz. Dieses Netzwerk ist vom öffentlichen Internet separiert und wird von der US Defense Intelligence Agency (DIA) betrieben. Es stellt das Überwachungsrückgrat dar. STONE GHOST, zu dem bisher nur die „5 Eyes" Zugriff haben, dient dem Echtzeit-Austausch von abgefangenen und als relevant definierten **Rohdaten** (https://en.wikipedia.org/wiki/Signals_intelligence). Dabei kann es sich um abgefangene Telefonate, E-Mail-Inhalte, Chat-Protokolle, Standortdaten (GPS) oder auch Metadaten, also „wer verbindet sich wann mit wem" handeln. Beim Austausch gilt das Prinzip der „presumption of sharing" (Vermutung der Weitergabe). Dies bedeutet: Alles, was ein Land sammelt, ist standardmäßig für die anderen Partner sichtbar, es sei denn, es wird explizit als „nur nationale Relevanz" markiert.

Analysten in London können also dieselben Rohdaten in ihren Systemen sehen wie ihre Kollegen in den USA, Kanada, Australien und Neuseeland, ohne dass ein offizieller Antrag gestellt werden muss. Auf diese Weise werden die nationalen Gesetze zum Datenschutz ausgehebelt, denn die Daten landen zwar über STONE GHOST im eigenen System, gelten aber als „ausländische Aufklärung". Für den Einzelnen ist es zudem nicht nachvollziehbar, welcher Dienst ihn eigentlich abgehört hat, weil STONE GHOST so konzipiert wurde, dass der Ursprung der Daten verschleiert wird. Interessantes zu STONE GHOST steht auch auf der **Website Climateviewer** (https://climateviewer.org/history-and-science/government/maps/five-eyes-stoneghost-surveillance-network/).

2023 gab die US Defense Intelligence Agency (DIA) **bekannt**

(https://www.c4isrnet.com/cyber/2023/03/29/stone-ghost-secret-intel-network-may-expand-to-more-nations-dia/), das streng geheime System auch für andere Partner freigeben zu wollen. Das Upgrade werde im Jahr 2024 entwickelt, so der Chief Information Officer Doug Cossa. Vorgesehen ist ein Umbau des Systems, sodass Partner „on the fly" (ad hoc) hinzugefügt oder entfernt werden können. Das bedeutet, dass Partner der 9 Eyes oder 14 Eyes, also auch Deutschland, temporären Zugang erhalten könnten, wenn es um spezifische Bedrohungslagen ginge, zum Beispiel NATO-Einsätze oder Konflikte wie in der Ukraine. Die Erweiterung bedeute nicht, dass alle 14 Eyes automatisch Vollzugriff auf alle Rohdaten hätten, so Cossa. Vielmehr entstehe eine technische Möglichkeit, ausgewählte Datenströme sicher mit wechselnden Koalitionen zu teilen, ohne für jeden Fall ein separates Netzwerk aufbauen zu müssen.

SIGDASYS: Das STONE GHOST der 14 Eyes

Unabhängig von STONE GHOST betreiben die 14 Eyes — offiziell SIGINT Seniors Europe, SSEUR — seit Langem ihr dediziertes Kommunikationssystem **SIGDASYS (Signals Intelligence Data System)** (https://www.electrospaces.net/2020/05/maximator-and-other-european-sigint.html). Über dieses System werden abgefangene Kommunikationsdaten und Geheimdienstberichte ausgetauscht. Es wurde vom BND vorgeschlagen, um SIGINT-Daten an die NATO-Kommandeure an der Front weiterzuleiten.

Laut ***The Intercept*** (https://theintercept.com/2018/03/01/nsa-global-surveillance-sigint-seniors/), der sich auf die von Edward Snowden zur Verfügung gestellten Geheimdokumente der NSA stützt, werden SIGINT Seniors Europe and SIGINT Seniors Pacific von der NSA geleitet. Die Mitglieder der Gruppe stammen aus

Geheimdiensten, die die Kommunikation abhören. Über Geheimvereinbarungen werden die Rohdaten, zum Beispiel von Abhörstationen der jeweiligen Territorien, an die „5 Eyes" geliefert. Im Gegenzug werden ausgewertete Geheimdienstdokumente geliefert oder Zugang zu bestimmten Datenbanken wie **XKeyscore** (https://en.wikipedia.org/wiki/XKeyscore), einem Analysesystem der NSA, gewährt.

Das Maximator-Bündnis: Die europäischen 5 Eyes

Mit welchen miesen Methoden auch die Europäer schon lange Zeit arbeiten und wie verzahnt die westlichen Geheimdienste tatsächlich sind, thematisiert ein Artikel in **INTELLIGENCE AND NATIONAL SECURITY** (https://www.tandfonline.com/doi/full/10.1080/02684527.2020.1743538) von 2020. Die „5 Eyes Europa" bestehen seit 1976 unter dem Namen „Maximator", sie wurden auf Initiative des dänischen Geheimdienstes gegründet und schließen die Länder Dänemark, Frankreich, Deutschland, Schweden und die Niederlande ein. Der Name Maximator geht auf eine Biermarke der Augustiner Brauerei zurück.

Im Artikel heißt es: „Das Maximator-Bündnis vertieft unser Verständnis der kürzlich aufgedeckten Operation „Thesaurus/Rubicon": Die gemeinsame Beteiligung und Kontrolle der CIA und des BND am Schweizer Hersteller von Kryptografiegeräten, der Crypto AG, von 1970 bis 1993. Entscheidende Informationen über die Funktionsweise und Schwachstellen der von der Crypto AG und anderen Unternehmen verkauften Kryptografiegeräten wurden innerhalb des „Maximator"-Netzwerkes verbreitet. Dies ermöglichte es den Teilnehmern, abgefangene Nachrichten aus den mehr als hundert Ländern zu

entschlüsseln, die ab den 1970er Jahren kompromittierte Geräte gekauft hatten." Einen aufschlussreichen Artikel zum Maximator-Bündnis gibt es auch **hier** (https://www.electrospaces.net/2020/05/maximator-and-other-european-sigint.html).

Die Massenüberwachung in sieben Schritten

Um das System der Massenüberwachung transparenter zu machen, verfolgen wir den Weg einer E-Mail von Europa nach Nordamerika. Exakt den gleichen Weg nehmen auch Telefonate, Chats und Server-Anfragen. Die E-Mail muss über den großen Teich, also passiert sie einen der großen transatlantischen Knotenpunkte in UK oder an der Ostküste der USA, damit durchläuft sie die Überwachungsinfrastruktur der „5 Eyes".

1. Der physische Abgriff der Daten

Sobald die E-Mail den lokalen Provider in Europa verlässt und auf das globale Backbone-Netz trifft, passiert sie einen Landepunkt für **Glasfaserkabel** (https://paderta.com/karte-der-globalen-glasfaserkabel-in-der-tiefsee/), zum Beispiel in Cornwall, UK, oder New York, USA. An diesen Knotenpunkten sind die passiven Glasfaser-Splitter installiert. Diese kleinen optischen Geräte teilen nun das Lichtsignal in der Leitung, welches die Daten transportiert. Das Originalsignal läuft unverändert weiter zum Empfänger, eine Kopie wird in einen abgeschirmten Serverraum der Geheimdienste, beispielsweise des GCHQ oder der NSA, geleitet. In Hochleistungsservern wird nun der komplette kopierte Datenstrom, in dem sich auch die E-Mail befindet, digitalisiert und zur weiteren Verarbeitung vorbereitet.

2. Der Pufferspeicher

Bevor entschieden wird, ob die E-Mail interessant ist, muss sie zwischengespeichert werden. Dies geschieht mittels des TEMPORA-**Puffersystems** (https://en.wikipedia.org/wiki/Tempora), falls die E-Mail UK passiert, oder mit äquivalenten Programmen der NSA in den USA. In diesem temporären Datenspeicher, der von UK und USA gemeinsam betrieben wird, wird die Kopie der E-Mail etwa drei Tage lang gespeichert, während die Metadaten wie Absender, Empfänger, Betreff, Zeitpunkt und IP-Adressen 30 Tage lang aufbewahrt werden.

3. Die automatische Vorauswahl

Ein automatischer Filter entscheidet nun, ob die Daten „wertvoll" genug sind, um weitergeleitet zu werden. Dazu nutzen die Geheimdienste das System **TURMOIL** (https://robert.sesek.com/2014/9/unraveling_nsa_s_turbulence_programs.html), das den Datenstrom filtert. Im Falle der E-Mail analysiert **TURMOIL** (https://arstechnica.com/information-technology/2014/03/nsas-automated-hacking-engine-offers-hands-free-pwning-of-the-world/) nun, ob die E-Mail bestimmte „Selektoren" wie E-Mail-Adressen, Telefonnummern, IP-Adressen und Keywords enthält, die von Analysten zuvor eingegeben wurden und als verdächtig gelten. Wird die Software fündig, markiert sie die E-Mail und leitet sie an spezielle Analysesysteme wie **XKeyscore** (https://en.wikipedia.org/wiki/XKeyscore) weiter. Wird sie nicht fündig, werden nur die Metadaten extrahiert und langfristig gespeichert.

4. Die Tiefenanalyse

Wurde die E-Mail markiert, wird sie nun mit XKeyscore tiefer analysiert. Dazu durchsucht XKeyscore die riesigen Rohdatenbestände, inklusive des TEMPORA-Puffers. Ein

menschlicher Analyst kann hier die E-Mail im Klartext lesen, wenn er einen „Strong Selector", zum Beispiel die E-Mail-Adresse, eingibt. Damit dies funktioniert, muss XKeyscore die E-Mail aber zuerst aus den Datenpaketen rekonstruieren, damit Header, Text und eventuelle Anhänge angezeigt werden können. Die Software verknüpft diese Information auch mit anderen Datenpunkten, beispielsweise welche Webseiten der Absender zuvor besucht hat. Anschließend entscheidet entweder der Analyst oder ein automatischer Regel-Satz in XKeyscore: „Ist das relevant?" Wenn ja, speichert der Analyst die E-Mail oder ein automatischer Trigger von XKeyscore leitet die Daten vom flüchtigen Puffer in die langfristigen Archive weiter.

5. Die langfristige Archivierung

Wurde die E-Mail als relevant eingestuft, landet der Text der E-Mail und mögliche Anhänge in einer Datenbank wie PINWALE, wo sie fünf Jahre oder länger gespeichert werden. Die Metadaten der E-Mail werden bis zu fünf Jahre in einer Datenbank wie MARINA gespeichert. Wird der E-Mail-Absender während dieser Zeit besonders auffällig, kann sein gesamter Internetverkehr retrospektiv überprüft werden.

6. Der Datenaustausch mit den Partnern

Wurde die E-Mail als relevant eingestuft, wird sie zudem verschlüsselt über das Hochsicherheitsnetzwerk STONE GHOST mit allen Partnern geteilt. So können alle Analysten der Geheimdienste nun über STONE GHOST auf die Metadaten oder auf den gesamten Inhalt der E-Mail zugreifen. Dies umgeht mögliche nationale Beschränkungen, da die Daten offiziell von einem „ausländischen Geheimdienst" gesammelt wurden.

Dieser gesamte Prozess läuft für Milliarden von Kommunikationen täglich automatisiert ab.

> ***Der entscheidende Faktor ist oft nicht, ob Ihre E-Mail erfasst wird, das geschieht fast immer im ersten und im zweiten Schritt. Das entscheidende ist, ob Ihre E-Mail im dritten Schritt einen Filter auslöst. Wenn dies geschieht, wird Ihre Kommunikation im vierten Schritt für einen Menschen sichtbar, der Ihre privaten Daten liest, bewertet und darüber entscheidet, ob Sie als gefährlich eingestuft und überwacht werden.***

Wer sich eingehender mit den erwähnten Analyse- und Datenbanksystemen beschäftigen möchte, dem sei die **Power Point Präsentation** (https://www.aclu.org/files/natsec/nsa/NSA%20XKeyscore%20Powerpoint.pdf) der NSA von 2007 empfohlen.

7. Der Angriff auf unsere Geräte

Wird ein Individuum vom Algorithmus als auffällig markiert und nützt eine Verschlüsselung, kann eine automatisierte, heimliche Infiltration seines Geräts mittels der Werkzeuge TURMOIL, TURBINE und FOXACID stattfinden. Ziel ist es, die Verschlüsselung zu umgehen, indem man Malware direkt auf dem Gerät installiert. Gut erklärt werden diese Tools **hier** (https://www.linkedin.com/pulse/nsas-quantum-hacking-arsenal-how-works-why-matters-hasan-mahmud-tvjlc). Der Prozess der Infiltration läuft weitgehend unbemerkt in Millisekunden ab, während man eine normale Website lädt: Klickt man auf einen Link auf einer Seite, erkennt das System TURMOIL im Datenstrom, dass das Gerät eine bestimmte Schwachstelle hat. Das kann ein veralteter Browser oder ein bestimmtes Betriebssystem sein.

Bevor die eigentliche Webseite auf dem Gerät ankommt, leitet das System die Anfrage blitzschnell auf einen geheimen FOXACID-Server um. Da dieser Server schneller antwortet als die echte Website, „gewinnt" er das Rennen. Der Browser „denkt", er

kommuniziere mit der echten Seite. Der FOXACID-Server sendet aber keine Website, sondern einen Exploit, das ist ein kleines Programm, das die Sicherheitslücke im Gerät ausnutzt. Der Exploit installiert eine Malware, welche „Implant" genannt wird. Ab diesem Moment ist das Gerät infiziert und der Geheimdienst hat vollen Zugriff auf das Gerät. Er kann die Festplatte durchsuchen, Tastaturanschläge mitlesen (Keylogger), Mikrofon und Kamera aktivieren und sämtliche Daten noch vor der Verschlüsselung abgreifen. Dieser Angriff macht also die beste Verteidigung, das heißt Verschlüsselung, VPN, Tor, wirkungslos, denn die Malware liest den Text, bevor er verschlüsselt versendet wird. Der Geheimdienst sieht also den Klartext. Dies ist die Eskalationsstufe, wenn reine Überwachung des Datenverkehrs nicht mehr ausreicht, weil der Nutzer zu gut verschlüsselt.

Die Gefahr der Falsch-Positiven

> ***Die Systeme sind so gestaltet, dass Jeder durch komplexe Verhaltensmuster und Kontext-Analysen unschuldig in Verdacht geraten kann. Dabei geht es weniger um einzelne Wörter, die benutzt werden, obwohl auch diese existieren. Es geht primär um Anomalien.***

Systeme wie der **NSA-Algorithmus SKYNET** (https://en.wikipedia.org/wiki/SKYNET_(surveillance_program)) definieren alles als „wertvoll", was vom statistischen Durchschnitt abweicht. Wer plötzlich verschlüsselte Kommunikation nutzt, unregelmäßige Reisebewegungen hat oder Kontakte zu Personen in Krisengebieten pflegt, wird von KI als „anomal" eingestuft. Wer, aus welchem Grund auch immer, von seinem bisherigen Gewohnheiten abweicht, gerät in Verdacht und wird überprüft.
Der Journalist **Ahmed Zaidan** (https://www.aljazeera.com/opinions/2015/5/15/al-jazeeras-a-

zaidan-i-am-a-journalist-not-terrorist) wurde als Terrorverdächtiger markiert, nur weil er oft telefonierte, reiste und Verschlüsselung nutzte — typisches Verhalten für Reporter, aber eben auch für Kuriere. Oft reicht die Metadaten-Kombination: Wer spricht mit wem, wann, wo und wie oft, um ein Profil als „wertvoll" zu markieren. Dabei werden sogar unschuldige Menschen automatisiert **getötet** (https://arstechnica.com/information-technology/2016/02/the-nsas-skynet-program-may-be-killing-thousands-of-innocent-people/).

Fazit

Die Ausweitung der Überwachung und der Kontrolle im Internet dient dazu, die illegale Massenüberwachung langsam salonfähig zu machen und ihr den Anstrich von Legalität zu geben. Der so oft beschworene Datenschutz ist keinen Pfifferling wert, denn er wird schon seit geraumer Zeit mit Füßen getreten. Was bisher im Verborgenen geschah, das soll sich bald als „völlig normal" einbürgern. Denn Künstliche Intelligenz, die bald mehr steuern soll, als uns lieb ist, kann dies nur effizient tun, wenn sie Zugriff auf sämtliche verfügbaren Daten hat. Datenschutz ist in einer digitalen Welt ein Relikt der Vergangenheit. Die Daten, so Oracle-Gründer Larry Ellison, müssen frei fließen. Alles was wir tun, muss der KI in Echtzeit zur Verfügung stehen, nur so kann sie „gute" Entscheidungen treffen. Nur so kann sie eine möglichst perfekte Verteilungswirtschaft aufbauen und kontrollieren. Nur wenn das Individuum vollkommen gläsern ist, können seine Bedürfnisse ermittelt und ihm die Dinge seines täglichen Bedarfs zur Verfügung gestellt werden, wobei selbstverständlich sein Verhalten eine gewichtige Rolle spielen soll. Das von freien Entscheidungen geprägte Leben, das Leben, das wir alle zu kennen glaubten, war schon immer nur eine Illusion. Nun soll auch diese Illusion in der Mülltonne der Geschichte landen.

Simone Hörrlein ist Lebensmittelchemikerin und Wissenschaftsjournalistin. Nach ihrem Studium an der **TU München** war sie mehrere Jahre in der medizinischen Forschung tätig und arbeitete zuletzt in der Wissenschaftskommunikation des **Kompetenzzentrums für Ernährung**. Neben den Naturwissenschaften interessiert sie sich für Finanz- und Geopolitik. Aktuell lebt sie in Kanada.