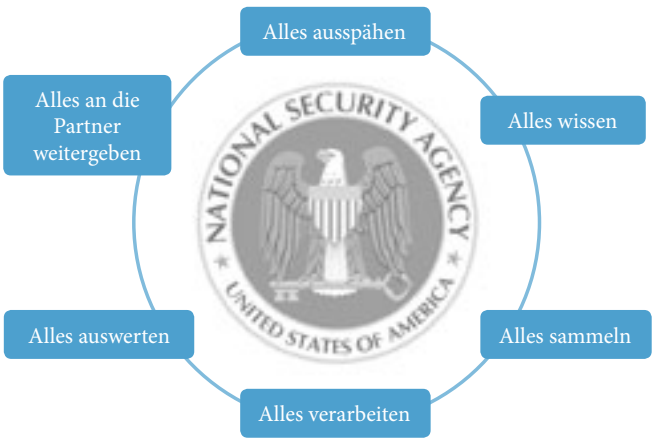
Weltgesellschaft

Überwachte Weltgesellschaft: Nachrichtendienste und die Bedrohung der Privatsphäre

Die Kontroversen, die durch die Weitergabe von Dokumenten der *US National Security Agency* (NSA) und des *British Government Communications Headquarters* (GCHQ) an die Medien durch Edward Snowden ausgelöst wurden, stehen im Zusammenhang mit zwei wichtigen Entwicklungen: Die Digitalisierung und die technischen Mittel, Daten zu sammeln, zu verarbeiten und zu speichern, haben zu einem Wandel in der Arbeit der Geheimdienste geführt. Zudem verstärkte ein neues Risikobewusstsein, insbesondere nach dem 11. September 2001, Forderungen, zu nachrichtendienstlichen Zwecken so viele Daten wie möglich zu sammeln.
Als größtenteils geschlossenes selbstreferenzielles System können Nachrichtendienste der Demokratie genauso schaden wie die Bedrohungen, vor denen sie die Bürger angeblich schützen sollen. Das massenhafte Sammeln von Daten bedroht zwar potenziell die bürgerlichen Freiheiten, die Reaktion der Öffentlichkeit darauf ist jedoch zweideutig. Es ist fraglich, ob eine globale Internet-Governance dazu beitragen kann, die Privatsphäre und die Freiheitsrechte der Bürger zu gewährleisten, solange das Engagement (von Teilen) der Zivilgesellschaft, bürgerliche Freiheiten zu schützen, nicht von den Nationalstaaten aufgegriffen wird.

Abbildung 1: Die Arbeit der Nachrichtendienste hat sich durch Digitalisierung und technische Möglichkeiten verändert

Die neue Haltung der NSA zum Sammeln von Daten: »So viele Daten wie möglich sammeln«



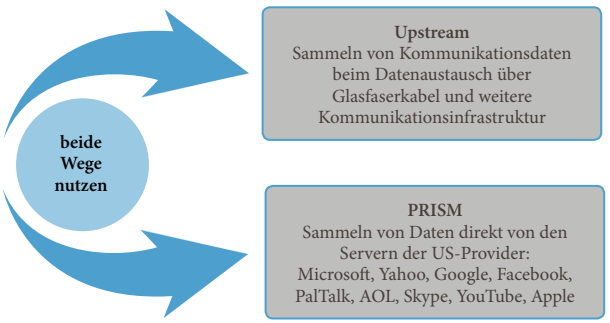
Quelle: Greenwald 2014, S. 97, modifizierte Fassung
Die Snowden-Dokumente können eingesehen werden unter: The Guardian, The NSA Files, http://www.theguardian.com/world/the-nsa-files?INTCMP=SRCH, 23.9.2014

Eine Revolution in der Arbeit der Nachrichtendienste

Jede kurze Geschichte der Nachrichtendienste bezeugt, dass Regierungen schon immer die Kommunikation ihrer Gegner, intern wie extern, abgehört haben. Im Laufe des 20. Jahrhunderts wurden immer ausgeklügeltere Abhörmethoden für den Telefon- und Funkverkehr entwickelt, und schließlich machten es Computer möglich, die gesammelten Daten zu durchsuchen, so z. B. das Echelon-System, mit dem »Schlüsselbegriffe« in der Satelliten-Kommunikation herausgefiltert werden können (Campbell 1999). Das digitale Zeitalter hat jedoch anscheinend die Möglichkeit, »alles zu wissen«, in Reichweite gebracht, wie es in der NSA-Präsentation von 2011 zum Ausdruck kommt [vgl. Abbildung 1].

Gleichzeitig stellten die Übertragung durch Glasfaserkabel und die kommerzielle Verfügbarkeit von Verschlüsselungssoftware wie beispielsweise *Pretty Good Privacy* (PGP) für staatliche Behörden wie NSA und GCHQ jedoch eine Herausforderung dar, übertragene Daten zu sammeln und anschließend zu entschlüsseln. Inzwischen geben die NSA/GCHQ-Akten jede Menge Aufschluss darüber, wie diesen Herausforderungen im nie endenden »Rüstungswettlauf« zwischen Datensicherung und Abhören von Kommunikation begegnet werden kann. Das Anzapfen von Glasfasernetzen (Upstream) und das Abgreifen von Daten direkt von den Servern der wichtigsten Kommunikationsdienstleister (*communication service providers*, CSPs) (PRISM) sind die wichtigsten Informationsquellen für die NSA, die die Analysten nutzen [vgl. Abbildung 2]. In anderen Fällen wird Ausrüstungsmaterial, das für Ziele im Ausland bestimmt ist, abgefangen und von der *Tailored-Access-Operations*-Einheit der NSA mit Sendern verändert. Das Material wird dann erneut verpackt und an die Zieladresse weitergeschickt, wo es dann per Fernzugriff zugänglich ist. Das gleiche Ergebnis kann erzielt werden, indem online *Malware* (Schadsoftware) einge-

Abbildung 2: Das Abfangen von Informationen ist hoch entwickelt
NSA: Zwei Arten, Informationen zu sammeln



Quelle: Greenwald 2014, S.108, modifizierte Fassung

schleust wird (Greenwald 2014, S. 116 ff., S. 148 f.).

Das Problem der Verschlüsselung macht ein zentrales Paradox der gegenwärtigen Situation deutlich. TOR, der *onion router* (ein dezentralisiertes Anonymisierungsnetzwerk für Netzwerkprotokoll-Verbindungen), ist beispielsweise eine öffentliche Open-Source-Methode zum Schutz der Online-Anonymität, die von vielen Unternehmen und Individuen genutzt wird, beispielsweise von Dissidenten in repressiven Regimen, zweifelsfrei aber auch von Kriminellen. Ursprünglich wurde TOR vom US-Verteidigungsministerium (*Department of Defense*, DoD) entwickelt, und bisher konnten die meisten Versuche der NSA – die ebenfalls Teil des DoD ist –, die Sicherheit von TOR im Kern zu gefährden, abgewehrt werden. Die Angriffe der Nachrichtendienste auf die Verschlüsselung sind stark kritisiert worden. Wenn sie beispielsweise *backdoors* in kommerzielle Software einbauen, um die Überwachung zu erleichtern, wird die Software dadurch für andere Hacker anfälliger und ihre Integrität für alle Computer-Nutzer bedroht. Der Gründer des World Wide Web, Tim Berners-Lee, verurteilt dies und bezeichnet ein solches Vorgehen als abstoßend und dumm, denn es widerspreche dem Kampf der Regierungen gegen Internet-Kriminalität und sei ein Verrat an der Technologieindustrie (Pilkington 2013a).

Nachrichtendienste: Zusammenarbeit, Vertrauen und »Ausspähen von Freunden«

Seit Ende des Kalten Krieges sind immer mehr miteinander verflochtene Netzwerke im staatlichen und im Unternehmenssektor entstanden. Diese entwickeln und produzieren Datenverarbeitungs-Hardware und -Software. Gleichzeitig sind private Sicherheitsunternehmen ebenfalls immer stärker in Bereiche involviert, die früher den gesamten Tätigkeitsbereich staatlicher Nachrichtendienste ausmachten (Priest/Arkin 2011, S. 184). Das mag besonders auf die USA zutreffen. Jedes Land jedoch, dessen nachrichtendienstliche Ambitionen die finanziellen Möglichkeiten übersteigen, kann darauf zurückgreifen, nachrichtendienstliche Aufträge »auszulagern«. In den Snowden-Dokumenten werden vielfältigste Wege der Zusammenarbeit von CSPs mit staatlichen Behörden beschrieben. In einigen Fällen werden diese gesetzlich dazu verpflichtet, in anderen Fällen sind damit finanzielle Anreize verbunden, um ihrem Patriotismus »auf die Sprünge zu helfen«. Wieder andere Fälle der Zusammenarbeit geschehen – zur Verärgerung der CSPs – völlig unfreiwillig, wenn Behörden Unternehmensserver »hacken« bzw. in die Unternehmenskommunikation eindringen. Nachdem etwa das deutsche Innenministerium seinen Vertrag mit *Verizon*, einem US-amerikanischen Telekommunikationsunternehmen, beendet hat, um die eigene Informationssicherheit zu verbessern, überrascht es nicht, dass viele Unternehmen damit drohen, ihre Zusammenarbeit mit der US-Regierung einzuschränken. Die Gefahr, dass einige US-Unternehmen weiter wirtschaft-

Das UKUSA-Abkommen

»Das zehnseitige streng geheime *British-U.S.-Communication Intelligence Agreement* wurde am 5. 6. 1946 unterzeichnet und verpflichtete beide Nationen, nachrichtendienstliche Erkenntnisse miteinander auszutauschen. Damit wurde eine Praxis fortgesetzt, die während des Zweiten Weltkriegs begonnen hatte. In dem später als UKUSA-Abkommen bezeichneten Dokument werden die Bedingungen für die Vereinbarung formuliert, die die Grundlage für die Zusammenarbeit im Bereich *Signals Intelligence* (SIGINT) während des Kalten Krieges bildete. In das Abkommen wurden später auch Kanada, Australien und Neuseeland einbezogen …«

Quelle: http://www.nationalarchives.gov.uk/documents/ukusa-highlights-guide.pdf, 27. 10. 2014

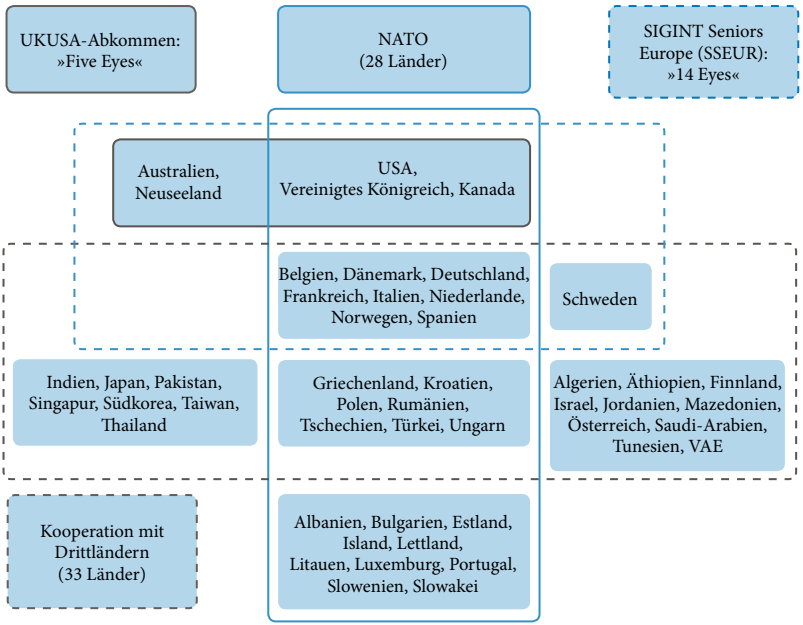
lichen Schaden erleiden werden, ist hoch, während andere, wie beispielsweise diejenigen, die spezielle verschlüsselte Mobilfunkdienstleistungen in Deutschland anbieten, vermutlich profitieren werden (Harris 2014).

Wenn die globale Kommunikationsinfrastruktur überwacht werden soll, kann dies nicht eine einzige Nation übernehmen, egal, wie mächtig sie ist; dies erfordert Zusammenarbeit. Die Zusammenarbeit von Nachrichtendiensten hat sich seit dem frühen 20. Jahrhundert entwickelt, am schnellsten zwischen den Alliierten. Im Westen wurden die relativ ad hoc zustande gekommenen Vereinbarungen zwischen zwei Weltkriegen zu Beginn des Kalten Krieges im sogenannten UKUSA-Abkommen formalisiert, das eine systematische Zusammenarbeit der Nachrichtendienste in den Bereichen Kommunikation und Sicherheit vorsah [vgl. Kasten]. Damals wie heute wird das Abkommen finanziell durch die »Hegemonialmacht« USA dominiert. Andere angelsächsische Länder tragen dazu bei, dass eine weltweite Überwachung gewährleistet werden kann. Die grundlegenden Dokumente im Hinblick auf das Abkommen wurden 2010 im Vereinigten Königreich offiziell veröffentlicht.

Neben UKUSA gibt es noch andere Übereinkommen zur nachrichtendienstlichen Zusammenarbeit, beispielsweise im Rahmen der *North Atlantic Treaty Organization* (NATO) und die *Signals Intelligence Seniors Europe* (SSEUR) [vgl. Abbildung 3]. Die nachrichtendienstliche Zusammenarbeit ist zwischen den *Five Eyes* – und in militärischen Angelegenheiten innerhalb der NATO – besonders umfassend. SSEUR besteht aus den wichtigsten europäischen Mitwirkenden bei der *Signals Intelligence* (SIGINT), der Fernmelde- und elektronischen Aufklärung. In der Region Ostasien/Pazifik gibt es ebenfalls eine entsprechende Gruppe. Eine Zusammenarbeit mit »Dritten« außerhalb dieser Gruppen findet bei speziellen Einsätzen statt. Die Zusammenarbeit von Nachrichtendiensten erfolgt meist bilateral und informell, da Vertrauen und der Grundsatz der Gegenseitigkeit wichtig sind, um Geheimhaltung zu gewährleisten. Die Abkommen beinhalten keinen nahtlosen, multilateralen Austausch nachrichtendienstlicher Erkenntnisse, sondern haben eher den Charakter von Netzwerken. Die USA

Abbildung 3: Die Kooperation der Nachrichtendienste erfolgt meist bilateral und informell, jedoch über verschiedene Netzwerke geteilt

Internationale Zusammenarbeit von Nachrichtendiensten unter Führung der USA



Quelle: »Top Level Communications«, www.electrospaces.net, 24.10.2014 modifizierte Fassung

haben sich seit dem 11. September 2001 für eine noch umfassendere Zusammenarbeit eingesetzt. Dies gilt auch für frühere Feinde, die nun im sogenannten »langen Kampf« gegen den Terrorismus mit herangezogen werden können.

Selbst innerhalb von UKUSA gibt es kein formelles Abkommen zwischen Ländern, welches Spionage untereinander verbietet. Es gibt jedoch eine Art »stilles Einvernehmen« zwischen langfristigen Verbündeten. Die USA kooperieren zwar mit anderen Ländern, sie spionieren sie jedoch auch aus, wenn sie glauben, dass dies im nationalen Interesse der USA liegt. Die ersten Meldungen, dass die NSA Deutschland überwacht und sogar das Telefon der Kanzlerin abhört, führten zu großen Kontroversen. Die Auseinandersetzung erreichte einen neuen Höhepunkt, als ein Mitarbeiter des deutschen Bundesnachrichtendienstes (BND) verhaftet wurde, weil der Verdacht bestand, dass er für die USA spioniert und Dokumente an die *Central Intelligence Agency* (CIA) verkauft hatte, darunter auch Unterlagen über den Untersuchungsausschuss des Bundestags zur NSA-Abhöraffäre. Natürlich betreibt auch der BND seine eigene Spionage: Als im August 2014 Berichte an die Öffentlichkeit gelangten, dass man die Türkei (einen NATO-Partner) über Jahre hinweg bespitzelt hatte, bezeichnete der türkische Außenminister dies als »absolut inakzeptabel« (Spiegel Staff 2014).

Dies hinderte die beiden Länder jedoch nicht daran, sich gleichzeitig darauf zu verständigen, die Zusammenarbeit ihrer Nachrichtendienste zu intensivieren, insbesondere im Hinblick auf die Bedrohung durch den »Islamischen Staat« (IS).

Netzwerke sind daher nicht immer nur Instrumente der Zusammenarbeit. Nicht nur arbeiten Staaten in einigen Zusammenhängen mit Unternehmen zusammen, während sie in anderen Bereichen versuchen, sie zu kontrollieren oder zu unterwandern. Auch Länder kooperieren auf einigen Gebieten, während sie auf anderen (unter anderem im Spionagebereich) intensiv miteinander konkurrieren (Bauman et al. 2014, S. 122). Eine Zusammenarbeit der Nachrichtendienste ist für diejenigen Länder, die echten Bedrohungen ausgesetzt sind, zwar eindeutig eine positive Entwicklung. Die Tatsache, dass diese Zusammenarbeit ohne jegliche wirksame Aufsicht stattfindet, bedeutet jedoch, dass immer die Gefahr von Menschenrechtsverletzungen besteht. Dies lässt sich anhand der gesamten Geschichte von Entführung und Folter aufzeigen, die in einer für die Öffentlichkeit bereinigten Form als »außerordentliche Auslieferung« bezeichnet wird (Sands 2008).

Nachrichtendienste bedrohen die Privatsphäre – doch wen kümmert das?

Das Internet selbst ist ein Netz Tausender unabhängiger Kommunikationsnetzwerke, und die Teilnehmer haben im Hinblick auf die individuelle Privatsphäre viele unterschiedliche Interessen. Um ihrem eigenen Ruf nicht zu schaden, werden z. B. medizinische und Finanznetzwerke die Privatsphäre ihrer Kunden wahren. Das zentrale Geschäftsmodell größerer CSPs und Nachrichtendienste besteht jedoch darin, die personenbezogenen Informationen der Bürger/Kunden zu eigenen Zwecken auszuwerten. Im Zuge der Snowden-Enthüllungen brachten Brasilien und Deutschland eine Resolution in der Generalversammlung der Vereinten Nationen ein, die im Dezember 2013 verabschiedet wurde [vgl. Kasten].

In einem Bericht vom Juni 2014 wies der Hohe Kommissar für Menschenrechte der UN erneut darauf hin, welche Bedingungen eine Überwachung durch den Staat erfüllen muss, um den Normen, die im Internationalen Pakt über bürgerliche und politische Rechte (*International Covenant on Civil and Political Rights*, ICCPR) festgelegt sind, gerecht zu werden. Diese Normen besagen, dass Überwachung niemals willkürlich oder ungesetzlich sein darf. Man könnte behaupten, dass massenhafte Überwachung willkürlich sei und dass es daher einen entscheidenden Widerspruch zwischen der internationalen Zusammenarbeit der Nachrichtendienste, wie sie sich inzwischen entwickelt hat, und dem ICCPR gebe. Dass eindeutig Besorgnis herrscht im Hinblick auf den Missbrauch privater Daten sowohl durch den Staat als auch durch Unternehmen, führt die rasch zunehmende Zahl an sozialen Netzwerken deutlich vor Augen. Die Einstellung zur angemessenen Grenzziehung zwischen Öffentlichem und Privatem verändert sich je nach

Die Resolution der UN-Generalversammlung »Das Recht auf Privatheit im digitalen Zeitalter« (UN Doc. A/Res/68/167)

»In dieser von 57 Mitgliedstaaten mit eingebrachten Resolution erklärte die Versammlung, dass die gleichen Rechte, die Menschen offline haben, auch online geschützt werden müssen, und forderte alle Staaten auf, das Recht auf Privatheit bei der digitalen Kommunikation zu achten. Sie forderte die Staaten ferner auf, ihre Verfahren, Praktiken und Rechtsvorschriften betreffend die Überwachung von Kommunikation, ihr Abfangen und das Sammeln personenbezogener Daten zu überprüfen, und sie betonte, dass die Staaten die vollständige und wirksame Umsetzung ihrer Verpflichtungen nach den internationalen Rechtsnormen sicherstellen müssen.«
Quelle: Bericht des Amtes des Hohen Kommissars der Vereinten Nationen für Menschenrechte: Das Recht auf Privatheit im digitalen Zeitalter, 30. Juni 2014, A/HRC/27/37, I. Einleitung, Abs. 5

Altersgruppe allerdings unterschiedlich. So »besitzen« beispielsweise EU-Bürger ihre personenbezogenen Daten. Wenn sie diese persönlichen Informationen jedoch benutzen, um sich Dienstleistungen wie Google oder Facebook zu »kaufen«, verlieren sie nicht nur die Kontrolle darüber, sondern liefern auch den Zugang zu den personenbezogenen Daten anderer, die mit ihnen in Kontakt stehen. Zur Verteidigung der Nachrichtendienste argumentieren einige Beamte, dass die Unternehmen (»Datenkraken«) eine größere Bedrohung der Privatsphäre darstellen. Das mag sich nach einer ungewöhnlichen Einlassung anhören, eine Umfrage des Marktforschungsunternehmens TNS im Vereinigten Königreich ergab jedoch, dass 55 % der Befragten »sehr/ziemlich« besorgt über die Aktivitäten von Suchmaschinen wie Google waren. 60 % äußerten dasselbe Unbehagen über soziale Medien wie Facebook. 43 % waren genauso besorgt über die Überwachung und das Sammeln von Daten durch britische Nachrichtendienste, 46 % im Hinblick auf die US-Geheimdienste (TNS 2014). Solche Gefühle könnten auch dadurch beeinflusst worden sein, dass Facebook ein Experiment gestartet hatte, die Nachrichten auf den Homepages von 689 000 Nutzern in eine positive oder negative Richtung zu manipulieren, um herauszufinden, ob man die Menschen dazu bringen kann, sich durch »emotionale Beeinflussung« mehr oder weniger positiv zu fühlen (Booth 2014).

Umfragedaten zeigen, dass das Ausmaß der gesammelten Informationen in den USA von der Mehrheit abgelehnt wird: Im Juni 2013 ergab eine Gallup-Umfrage, dass 57 % der Befragten »sehr« oder »ziemlich« besorgt waren, dass das Recht auf Privatsphäre verletzt worden war, 42 % dagegen waren »nicht allzu« oder »gar nicht« besorgt. 53 % lehnten das Sammeln von Telefon- und Internetdaten ab (37 % akzeptierten es) (Newport 2013). Ein Jahr später veröffentlichte das US-amerikanische Meinungsforschungsinstitut *Pew Research Center* die Ergebnisse einer umfangreichen globalen Umfrage, bei der etwa 48 000 Personen in 44 Ländern befragt wurden [vgl. Tabelle 1].

Tabelle 1: Globale Umfrage »Ist die Überwachung von ____ in den USA akzeptabel oder inakzeptabel?«

Prozentsatz	Bürgern Ihres Landes	Führungspersönlichkeiten Ihres Landes	US-amerikanischen Bürgern	Terrorverdächtigen
akzeptabel	12	20	31	64
inakzeptabel	81	73	62	29

Quelle: Pew Research 2014b

In fast allen Umfrage-Ländern war eine Mehrheit gegen eine Überwachung von E-Mails und Telefongesprächen ihrer Führungspersönlichkeiten oder Bürger durch die US-Regierung. Nicht überraschend tendieren dagegen die US-Amerikaner zu der Ansicht, dass das Abhören ausländischer Führungspersönlichkeiten eine akzeptable Praxis darstellt. Sie sind jedoch gespalten, ob diese Methode auch auf Bürger in anderen Ländern angewendet werden soll.

Einige andere Muster sind zudem erkennbar. Beispielsweise war die Ablehnung in den USA wesentlich größer, wenn es um das Sammeln von Daten im Inland ging. In den Altersgruppen gab es allerdings kaum Unterschiede hinsichtlich einer Befürwortung oder Ablehnung. Bei der Haltung zu Snowdens Aktivitäten gab es größere Unterschiede. Die Unterstützung war bei jüngeren Menschen im Allgemeinen größer (Pew Research 2014a). Dabei kommt ein großes Maß an Zynismus zum Vorschein: Nur einer von fünf Befragten in Kanada, dem Vereinigten Königreich und den USA glaubte, dass die gesammelten Informationen nur für Belange der nationalen Sicherheit genutzt würden, und fast die Hälfte war der Ansicht, dass die Regierung die Informationen für jeden beliebigen Zweck verwenden würde (Angus Reid 2013). Im Vereinigten Königreich glaubten nach einer Umfrage des Meinungsforschungsinstituts *YouGov* im Juli 2014 83 % der Befragten, dass sich die Nachrichtendienste unabhängig von der Gesetzeslage Zugang zu fast sämtlichen bzw. vielen Informationen über den Normalbürger verschaffen. Allerdings waren 64 % auch der Meinung, dass die Nachrichtendienste einen so umfassenden Zugriff ohne Gerichtsbeschluss haben sollten (Dahlgreen 2014).

Was Befragte bei Umfragen antworten, beeinflusst nicht notwendigerweise ihr Verhalten. Es gibt keine eindeutigen Belege dafür, ob und inwiefern Menschen nach den Snowden-Enthüllungen ihre Online-Gewohnheiten geändert haben. Eine Untersuchung der Google-Trend-Daten vor und nach dem 6. 6. 2013 ergab, dass die Suche nach »privaten« bzw. »problematischen« Ausdrücken statistisch signifikant zurückgegangen ist, insbesondere in Kanada, im Vereinigten Königreich und in den USA. Es konnte festgestellt werden, dass dieser Rückgang bei Google eventuell durch die verstärkte Nutzung anderer Suchmaschinen kompensiert wurde. Wenn dies so bleibt, könnte Google Schaden nehmen, wenn Werbung anderswohin verlagert wird (Stanganelli 2014). Es gibt jedoch keinerlei Hinweise, dass die sozialen Medien aufgegeben

werden: Von Juni 2013 bis Juni 2014 stieg die Zahl der monatlich aktiven Nutzer bei Twitter um 24 %, die der bei Facebook um 14 %. Ganz allgemein wirft diese Kontroverse grundlegendere Fragen der politischen Ökonomie und der Unterwerfung der Menschen unter Machtverhältnisse (öffentliche und private) mittels Überwachung auf als nur die typische Frage hinsichtlich der Rechte eines Bürgers auf Privatsphäre dem Staat gegenüber.

Können neue Formen globaler Internet-Governance die Privatsphäre der einzelnen Nutzer schützen?

Das »Netz der Netze« – das Internet – ist vielschichtig, es kombiniert physische und virtuelle Eigenschaften. Es gibt kein einziges einheitliches Regime für die Governance des Cyberspace, also die weltweite Regulierung des Internets, es gibt aber »eine Reihe locker miteinander verbundener Normen und Institutionen«, die irgendwo zwischen hierarchischer Integration und hoher Fragmentierung angesiedelt sind (Nye 2014, S. 7). Wie das Internet vor dem Hintergrund der Snowden-Enthüllungen reguliert werden kann, war bereits Gegenstand vieler Untersuchungen, u. a. der *Bildt Commission*, die vom Thinktank *Chatham House* im Vereinigten Königreich eingesetzt wurde, und des *Center for International Governance and Innovation* (CIGI).

Es überrascht nicht, dass in vielen Reaktionen auf Snowden die Dominanz der USA im Hinblick auf das Internet und die Unterwanderung durch die NSA kritisiert worden ist. Einige haben daher eine neue internationale Regulierung, beispielsweise durch die Vereinten Nationen, vorgeschlagen. Die Tatsache, dass beim UN-Menschenrechtsrat im September 2013 unter anderem ausgerechnet Länder wie Pakistan, Kuba, Simbabwe, Russland, Iran und China eine neue internationale multilaterale Regulierung vorschlugen, stimmt nachdenklich. Da Regierungen das Internet unilateral und in Zusammenarbeit überwachen, würde eine Umsetzung dieses Vorschlags die Situation ganz offensichtlich nicht verbessern.

Die Stärke des Internets besteht darin, dass es ein außerordentlich umfassendes, machtvolles Informations-»Gemeingut« bereitstellt; es ist jedoch, wie alle solche Gemeingüter, dem Missbrauch durch die Reichen und Mächtigen ausgesetzt. Das neoliberale »Multistakeholder«-Modell kann dafür kritisiert werden, dass es die Dominanz der größeren Internet-Unternehmen noch verstärkt und den reichsten Staaten ermöglicht, Regulierungs- und Besteuerungssysteme im eigenen Interesse zu etablieren. Da diese Unternehmen allerdings für die Bereitstellung der materiellen Infrastruktur des Internets von zentraler Bedeutung sind, ist es kaum machbar, sie auszuschließen. Ihnen sollte jedoch nicht die Führung übertragen werden. Staaten wiederum definieren ihre Sicherheitsinteressen aus einer realistischen Perspektive und nutzen das Internet für nachrichtendienstliche Zwecke, genauso wie sie schon immer alle anderen transnationalen Kommunikationskanäle ausgespäht haben. Wenn die Dominanz der großen Internet-Unternehmen einge-

schränkt werden soll, kann dies nur durch Initiativen wie NETmundial [vgl. Kasten] geschehen.

Es gab Warnungen, dass das Internet infolge der Enthüllungen durch Snowden und andere »balkanisiert« werden könnte. Tim Berners-Lee hat seine Besorgnis zum Ausdruck gebracht, dass durch jegliche Fragmentierung im Ergebnis eine abschreckende Wirkung für die Nutzung des Netzes und die »Interkreativität« (Brainstorming etc.) entstehen könnte (Pilkington 2013b). Kurzfristig spielen Regierungen, die von der US-Überwachung betroffen sind, mit dem Gedanken, ihre Kommunikationssicherheit zu erhöhen, indem sie neue Netzwerke entwickeln, die nicht über die USA laufen. Langfristig jedoch wären die ökonomischen und sozialen Kosten, sich aus dem globalen Netz auszuklinken – einmal angenommen, dies wäre möglich –, mit großer Sicherheit höher als eine nur marginale Erhöhung der Kommunikationssicherheit. Aus Sicht der Bürger könnte es durch eine Zersplitterung in regionale Netzwerke genauso viele Angriffe auf ihre Privatsphäre geben, wenn auch durch andere Staaten und Unternehmen (Bauman et al. 2014, S. 128 ff.). Es wird die »Informationsfreiheit« der russischen Bürger nicht fördern, wenn der Kreml seine Pläne weiterverfolgt, sich im Falle einer militärischen Konfrontation oder bei Protesten gegen die Regierung aus dem Internet auszuklinken und dem gemeinnützigen Internet-Unternehmen *Internet Corporation for Assigned Names and Numbers* (ICANN) mit Sitz in den USA die Kontrolle der .ru- und .su-Domains zu entziehen.

Es gibt ein äußerst breites Spektrum von Akteuren auf internationaler und

Die NETmundial-Multistakeholder-Stellungnahme, 24. April 2014, São Paulo, Brasilien

»Dies ist das nicht verpflichtende Ergebnis eines von unten initiierten, offenen und partizipatorischen Prozesses, an dem Tausende Menschen aus Regierungen, dem Privatsektor, der Zivilgesellschaft, dem Technikbereich und Akademiker aus der ganzen Welt teilgenommen haben. Die NETmundial-Konferenz war die erste ihrer Art. Sie wird hoffentlich zur Weiterentwicklung des Ökosystems der Internet-Governance beitragen …

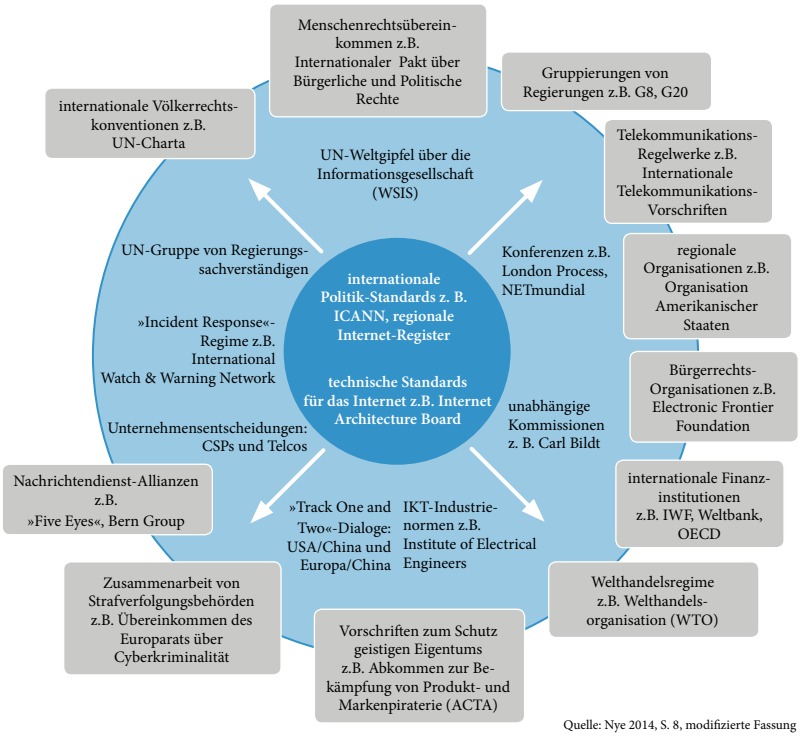
1. PRINZIPIEN DER INTERNET-GOVERNANCE

Bei der NETmundial-Konferenz wurden eine Reihe gemeinsamer Prinzipien und wichtiger Werte identifiziert, die zu einem inklusiven, wirksamen, legitimen und sich weiterentwickelnden Rahmen für die Internet-Governance beitragen können, der möglichst viele Stakeholder-Gruppen umfasst. Die Konferenzteilnehmer erkannten an, dass es sich beim Internet um eine globale Ressource handelt, die im öffentlichen Interesse verwaltet werden sollte …«

Quelle: http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf, 27. 10. 2014

Abbildung 4: Die Zivilgesellschaft kann das Netzwerk von Staaten und Unternehmen in der Internet-Governance nicht dominieren

Das Regelsystem zur Steuerung der weltweiten Cyber-Aktivitäten



Quelle: Nye 2014, S. 8, modifizierte Fassung

staatlicher Ebene, aus Unternehmen und der Zivilgesellschaft, die an der Entwicklung politischer und technischer Normen beteiligt sind [vgl. Abbildung 4]. Diejenigen, die die gegenwärtige Pseudo-Anarchie der Internet-Governance ändern wollen, sind mit der Herausforderung konfrontiert, dass Staaten und Unternehmen in Bereichen, in denen sie gemeinsame Interessen verfolgen, beispielsweise beim Internet-Bereichsnamensystem (*domain name system*, DNS), das durch das ICANN betreut wird, weiterhin intensiv zusammenarbeiten werden. Wenn es jedoch Interessenkonflikte gibt, gibt es kein Regelwerk mehr, sondern nur noch realistische Machtpolitik zwischen Staaten und Unternehmen, was auch dazu führt, dass die Überwachung unvermeidlich weitergeht. Der Zivilgesellschaft kommt bei der Internet-Governance eine Schlüsselrolle zu, sie kann allerdings die Netzwerke von Staat und Unternehmen nicht dominieren. Es gibt daher mittelfristig kaum Aussichten, dass die Internet-Governance einen stärkeren Schutz der Privatsphäre vor den jeweiligen Geschäftsmodellen der Staaten und Unternehmen bieten kann. Wie Berners-Lee anmerkt, ist ganz ein-

deutig ein neues System der Kontrolle und Überwachung erforderlich, um die Universalität des Webs zu schützen und gleichzeitig den Staaten zu ermöglichen, die notwendigen Ermittlungen durchzuführen (Pilkington 2013b). Außerdem müssen zivilgesellschaftliche Organisationen, deren einziges Interesse darin besteht, dass das Internet weiterhin als Gemeingut zur Verfügung steht, bei dem Versuch, ein Gegengewicht gegen die Macht von Staaten und Unternehmen zu bilden, eine zentrale Rolle spielen. Staaten stehen zwar in den gegenwärtigen Kontroversen über Massenüberwachung als die Hauptschurken da, nach wie vor haben jedoch nur demokratische Staaten die Ressourcen und die Legitimität, das allgemeine öffentliche Interesse gegen private Interessen und »unzivile« Organisationen zu verteidigen (Loader/Walker 2007).

Was kann gegen Massenüberwachung unternommen werden?

Das Kernproblem für Reformer ist, dass niemand das Recht von Staaten in Frage stellt, die Privatsphäre von Personen zu verletzen, die in dem Verdacht stehen, an illegalen, bedrohlichen Aktivitäten beteiligt zu sein. Viele bezweifeln jedoch, dass Massenüberwachung und das »Abfischen« von Daten angemessene Mittel dafür sind. Niemand hat bisher einen Weg gefunden, wie Staaten diese derzeit Unbekannten ohne irgendeine Form von Datenfilterung mit Hilfe von Suchbegriffen identifizieren können. Staaten akzeptieren in der Regel nicht, dass es Kommunikationswege gibt, die unter allen Umständen für Abhörmaßnahmen tabu sein sollten.

Es gibt drei mögliche Wege, auf diese Kontroverse zu reagieren: auf rechtlicher, technologischer und politischer Ebene. Ein Weg, der in Europa nach den Snowden-Enthüllungen verfolgt wurde, ist, zu verlangen, dass EU-Bürger in der US-Gesetzgebung denselben Schutz erhalten, den sie in Europa genießen. Eine Studie im Auftrag des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres des Europaparlaments kommt zu dem Ergebnis, dass dafür Änderungen in der US-Gesetzgebung erforderlich wären, die ursprünglich abgelehnt worden sind (Bigo et al. 2013, S. 9). Die Obama-Regierung verkündete jedoch im Juni 2014, dass ein Gesetz verabschiedet werden sollte, das EU-Bürgern viele der Rechte auf Schutz der Privatsphäre einräumt, wie sie für US-Bürger gelten. Dazu gehört auch das Recht auf gerichtlichen Rechtsbehelf bei absichtlicher oder mutwilliger Offenlegung geschützter Informationen bzw. bei versäumter Korrektur von Falschinformationen. Dieses Gesetz würde, wenn es verabschiedet wird, für die den USA zu Strafverfolgungszwecken zur Verfügung gestellten personenbezogenen Daten gelten. Das wäre ein Fortschritt, es gibt jedoch Grenzen für solche Maßnahmen; insbesondere findet Strafverfolgung in einem relativ transparenten Umfeld statt, unter Beteiligung von Polizei- und anderen Beamten, Staatsanwaltschaft und Gerichten. Daraus folgt, dass die Menschen wissen, ob und wann ihre personenbezogenen Daten benutzt (oder missbraucht) werden. Sie

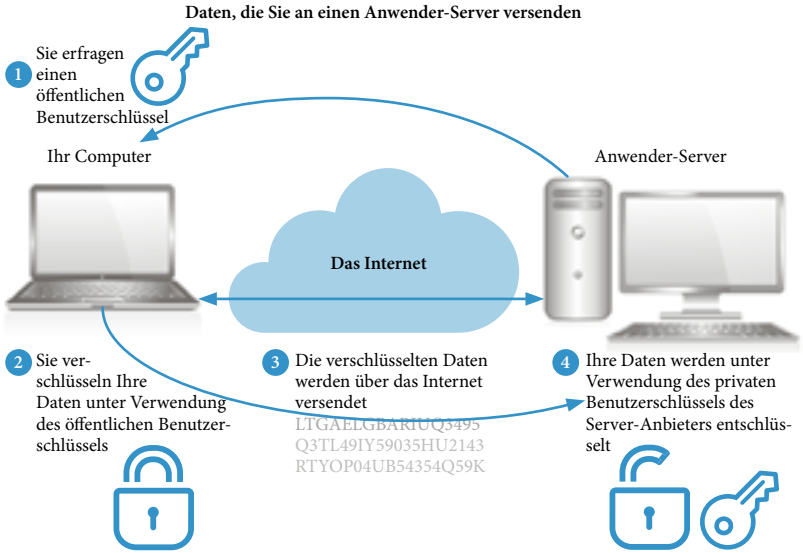
können dann Schritte unternehmen, sich davor zu schützen. Der Austausch nachrichtendienstlicher Informationen findet jedoch großenteils nicht in direktem Zusammenhang mit Strafverfolgung statt. Einige Informationen, die über überwachte Personen zusammengetragen werden, können eventuell dazu führen, dass Beweismaterial gesammelt wird, das zu einer Verhaftung und einem anschließenden Gerichtsprozess führt, für viele Informationen gilt dies jedoch nicht. Die Menschen merken oft gar nicht, dass sie überwacht werden. Die Datenschutzgesetzgebung nutzt ihnen deswegen oft nichts.

Das Potenzial für rechtliche Reformen ist daher begrenzt: Der internationale Austausch nachrichtendienstlicher Informationen vollzieht sich im Grunde außerhalb der Reichweite nationaler Gesetze. Die Grundlage ausländischer Geheimdienstaktivitäten besteht darin, die Gesetze anderer Länder zu brechen. Staaten, in denen die Nachrichtendienste eine große Reichweite haben, wie beispielsweise in den USA und im Vereinigten Königreich, stellen sicher, dass die Gesetzgebung für Nachrichtendienste diesen genauso viel Macht zubilligt wie auch Aktivitäten unterbindet. Staaten werden nicht freiwillig Macht abgeben, die ihrer Meinung nach (richtiger- oder fälschlicherweise) ihre Sicherheit erhöht, und sie werden ihre Gesetzgebung so gestalten, dass das Sammeln von Informationen »legal« geschieht. Zwischen der realistischen Basis für die nachrichtendienstlichen Aktivitäten des Staates und der kosmopolitischen Basis für den ICCPR gibt es heftige Konflikte, die nicht mit gesetzlichen Mitteln gelöst werden können. Es sollte jedoch weiter Druck ausgeübt werden, um größere Rechtssicherheit und Klarheit zu gewährleisten.

Insbesondere im Vereinigten Königreich sind die Gesetze im Hinblick auf die Internet-Überwachung sehr allgemein formuliert und teilweise unverständlich. Das Gesetz über Nachrichtendienste *(Intelligence Services Act)* von 1994 gesteht dem GCHQ breitgefächerte Machtbefugnisse zu, Kommunikation zu überwachen, zu sammeln, sie zu stören und bei der Verfolgung »nationaler Sicherheitsinteressen« Codes zu knacken. Im *Regulation of Investigatory Powers Act 2000* (RIPA) wird dies noch durch die Befugnis ergänzt, »alle Maßnahmen …, die notwendig sind« (RIPA, S. 5), zu ergreifen, um Informationen aus abgehörten Kommunikationen zu erhalten. Das RIPA ist an einigen Stellen allerdings ein durch und durch obskures Gesetz. Der Beauftragte für das Abhören von Kommunikation (*Interception of Communications Commissioner*, IoCC), ein früherer hoher Richter im Vereinigten Königreich, der mit der Aufsicht betraut ist, beschreibt einige Bestimmungen im RIPA als »für jedermann schwierig zu verstehen …« und stellt fest, dass »die Augen eines Lesers glasig werden, bevor er das Ende von Abschnitt 1 erreicht hat, vorausgesetzt, dass der Leser überhaupt anfängt zu lesen« (IoCC 2014, Abs. 6.5.3, 6.7.2). Dies ist von entscheidender Bedeutung – unabhängig davon, ob es sich dabei um bewusste Bemühungen handelt, das Gesetz im Interesse der Geheimhaltung möglichst undurchsichtig zu gestalten, ob es das Resultat gesetzlicher Regulierung eines technologisch komplexen Gebiets ist oder vermutlich eine Kombination aus beidem. Gesetzliche Regulierung der nachrichtendienstlichen Tätigkeit ist für demokratische Regierungsführung eine notwendige Voraussetzung, sie reicht jedoch nicht aus. Dass Gesetze allgemein,

Abbildung 5: Do it yourself! Überwachung durch die Anwendung von Verschlüsselung erschweren

Wie Verschlüsselung funktioniert



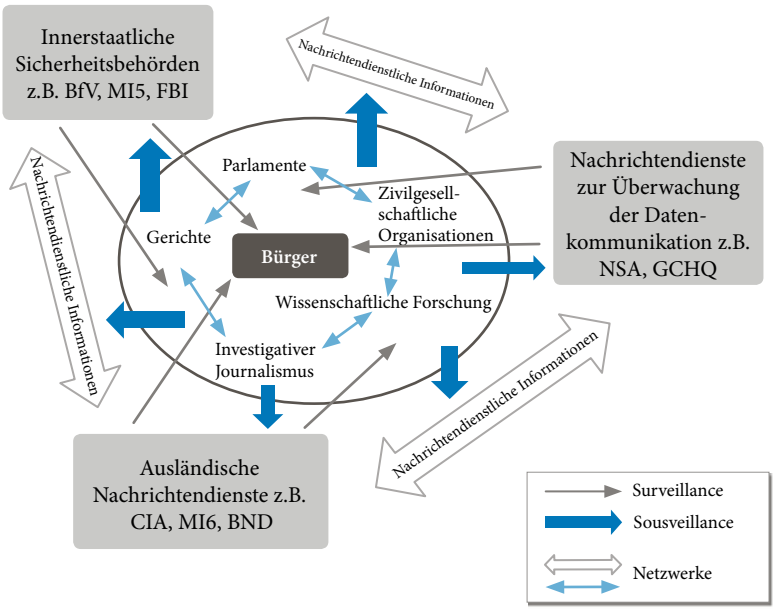
Quelle: http://technle.blogspot.de/2012/09/ssl-certificate-protection-for-your-data.html, 21.10.2014, modifizierte Fassung

wenn nicht sogar unklar formuliert werden, um Überwachung zu verschleiern, dient dem Zweck, die Geheimhaltung über Quellen und Methoden im Kern zu gewährleisten. Dadurch kommt wirksamen Kontrollmechanismen in diesem Bereich ein noch größerer Stellenwert zu als bei allen anderen Aktivitäten der Regierung. Welche gesetzlichen Neuregelungen auch immer auf diese Enthüllungen folgen – sie müssen der Öffentlichkeit wesentlich besser erläutert werden als die Regelungen, die derzeit gelten.

Auf technologischer Ebene können folgende Maßnahmen ergriffen werden: Snowden selbst hat empfohlen, dass Anwender mehr Verschlüsselungen nutzen sollten, um die Überwachung auszubremsen [vgl. Abbildung 5]. Außerdem gibt es Kampagnen wie »Reset the Net« (https://www.resetthenet.org), an denen sowohl Unternehmens- als auch zivilgesellschaftliche Organisationen beteiligt sind – unter anderem Google und die *Electronic Frontier Foundation* (EFF) –, die CSPs darin bestärken, Verschlüsselungsprotokolle und andere »bewährte Verfahren« im Sicherheitsbereich anzuwenden. Dazu gehören verschlüsselte Datencenter-Links, *Perfect Forward Secrecy* (PFS) und verschlüsselte Verbindungen mit den E-Mail-Diensten anderer Provider. Acht größere Internet-Unternehmen, unter anderem Google, Microsoft, Yahoo, Twitter und Facebook, haben die empfohlenen Sicherheitspraktiken der EFF bereits umgesetzt oder sind dabei, dies zu tun. Es bleibt fraglich, ob man damit

Abbildung 6: Die Überwacher überwachen

Hauptakteure in der Überwachung von staatlichen Nachrichtendienst-Netzwerken



Quelle: eigene Abbildung

mehr erreichen kann, als lediglich die nächste Stufe im »Wettrüsten« zwischen Bürgern und staatlichen Nachrichtendiensten auszulösen. Hinzu kommt die Dimension der »Ausrüstung«: Wie können sich Staaten und Unternehmen vor dem Einschleusen von *backdoors* in ihre Systeme im Fertigungsprozess oder auf dem Weg zwischen Hersteller und Kunden schützen?

Diese unvermeidliche Fortsetzung des alten Kampfes zwischen denjenigen, die die Regeln aufstellen, und denjenigen, die sie brechen, impliziert, dass es bei diesem Problem letztendlich um Politik und nicht um Technologie geht. Wenn, wie bereits erläutert, »das, was wir immer noch nationale Sicherheitsinteressen nennen, von einem neuen Adel der Nachrichtendienste dominiert wird, der in einem immer autonomeren transnationalen Feld agiert« (Bauman et al. 2014, S. 126), dann besteht das Problem darin, wie die nachrichtendienstlichen Netzwerke kontrolliert und überwacht werden können, um diese Autonomie zu reduzieren. Dafür sind nationale und internationale Mechanismen erforderlich, mit deren Hilfe der Missbrauch von Überwachungsmacht aufgedeckt werden könnte. Auf nationaler Ebene sind die Kontrollsysteme in vielen europäischen Ländern relativ neu und unterfinanziert. Gleichzeitig ist klar, dass nur wenige Kontrollbehörden mehr über die Komplexität der nachrichtendienstlichen Aufklärung verstehen als die Bürger, in deren Auftrag sie handeln. Das Problem

besteht darin, Strukturen zu entwickeln, die ausreichend widerstandsfähig und sachkundig sind [vgl. Abbildung 6].

Das Problem der Kontrolle wird noch durch die länderübergreifende Zusammenarbeit verstärkt. So wird beispielsweise der Kontrollbehörde der Zugang zu Informationen, die ein nationaler Nachrichtdienst von fremden Nachrichtendiensten erhalten hat, verweigert. Dies geschieht aufgrund des Grundsatzes der Kontrolle durch den Urheber (*originator control*, ORCON), der besagt, dass eine solche Information nicht ohne Zustimmung der Behörde, von der die Daten stammen, offengelegt werden kann. Auch supranationale Institutionen wie das Europaparlament und der Europarat können eine Offenlegung verlangen. Ihre Untersuchungen werden jedoch durch ihre fehlende Autorität nationalen Behörden gegenüber, die sie befragen wollen, unterminiert. Dies wurde während der Untersuchung des Europarats zur illegalen Auslieferung deutlich (Marty 2007). Selbst die nationalen Untersuchungen, die in Kanada, Deutschland und dem Vereinigten Königreich durchgeführt wurden, litten unter der Weigerung ausländischer Beamter zu kooperieren. In keiner der Untersuchungen erhielten Opfer die Möglichkeit, etwas über die geheimen Beweise zu erfahren, die für ihren Leidensweg verantwortlich waren (Wright 2011). Dass dieser Skandal überhaupt aufgedeckt wurde, ist der Arbeit eines informellen Kontrollnetzwerks von Journalisten, Rechtsanwälten, Forschern, Parlamentariern und zivilgesellschaftlichen Organisationen zu verdanken.

Bestehende Verbindungen zwischen nationalen Kontrollgremien in Gremien wie der alle zwei Jahre stattfindenden Konferenz der Kontrollausschüsse für die Geheimdienste *(International Intelligence Review Agency Conference)* sind zwar wichtig. Um eine wirkungsvolle transnationale Kontrolle zu gewährleisten, sind jedoch kreativere Verbindungen zwischen formellen und informellen Gremien erforderlich, um die knappen Ressourcen für die Kontrolle wirksam einzusetzen. *Über*wachung (oder französisch: *sur*veillance) ist fast schon eine falsche Bezeichnung für die Herausforderung, vor der eine Demokratie steht, die nachrichtendienstliche Aktivitäten kontrollieren muss, denn Kontrollbehörden sind im ungleichen Wettbewerb um die Kontrolle von Informationen den damit verbundenen Nachteilen ausgesetzt. Es wäre wahrscheinlich akkurater, das Ziel als *sous*veillance zu bezeichnen.

Literatur

Angus Reid 2013: More Canadians & Britons view Edward Snowden as »hero« than »traitor«. Americans split (http://angusreid.org/more-canadians-britons-view-edward-snowden-as-hero-than-traitor-americans-split/, 21. 1. 2015).

Bauman, Zygmunt/Didier Bigo/Paulo Esteves/Elspeth Guild/Vivienne Jabri/David Lyon/R. B. J. Walker 2014: After Snowden. Rethinking the Impact of Surveillance, in: International Political Sociology, Jg. 8/2, S. 121–144.

Bigo, Didier/Sergio Carrera/Nicholas Hernanz/Julien Jeandesboz/Joanna Parkin/Francesco Ragazzi/Amandine Scherrer 2013: National programmes for mass sur-

veillance of personal data in EU member states and their compatibility with EU law, Civil Liberties, Justice and Home Affairs Committee, European Parliament (http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET%282013%29493032_EN.pdf, 21. 1. 2015).

Booth, Robert 2014: Facebook reveals news feed experiment to control emotions, in: The Guardian, 30. 6. 2014 (http://www.theguardian.com/technology/2014/jun/29/facebook-users-emotions-news-feeds, 2. 12. 2014).

Campbell, Duncan 1999: Interception capabilities 2000. Report to European Parliament's Science and Technology Options Assessment Panel (STOA) 6. 5. 1999 (http://www.duncancampbell.org/menu/surveillance/echelon/IC2000_Report%20.pdf, 20. 6. 2014).

Dahlgreen, Will 2014: 47 % think security services have access to »almost everything« (http://yougov.co.uk/news/2014/07/12/47-think-security-services-have-access-almost-ever, 25. 7. 2014).

Greenwald, Glenn 2014: No place to hide. Edward Snowden, the NAS, and the U.S. Surveillance State, London.

Harris, Shane 2014: Snowdenfreude, in: Foreign Policy, 16. 7. 2014 (http://www.foreignpolicy.com/articles/2014/07/16/snowdenfreude_germany_us_spying, 20. 8. 2014).

IoCC 2014: 2013 Annual Report of the Interception of Communications Commissioner (http://www.iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf, 16. 9. 2014).

Loader, Ian/Neil Walker 2007: Civilizing security, Cambridge.

Marty, Dick 2007: Secret detentions and illegal transfers of detainees involving Council of Europe member states. Second report, Council of Europe, Parliamentary Assembly, Doc. 11302.

Newport, Frank 2013: Americans disapprove of government surveillance programs. Americans split on whether leaker did the right or wrong thing (http://www.gallup.com/poll/163043/americans-disapprove-government-surveillance-programs.aspx, 20. 6. 2014).

Nye, Joseph S. Jr. 2014: The regime complex for managing global cyber activities, Global Commission on Internet Governance, Paper Series Nr. 1, Mai 2014.

Pew Research 2014a: Most young Americans say Snowden has served the public interest (http://www.pewresearch.org/fact-tank/2014/01/22/most-young-americans-say-snowden-has-served-the-public-interest, 20. 8. 2014).

Pew Research 2014b: Global Attitudes Project. Global opinion of U.S. surveillance (http://www.pewglobal.org/2014/07/14/nsa-opinion, 30. 10. 2014).

Pilkington, Ed 2013a: Tim Berners-Lee: encryption cracking by spy agencies »appalling and foolish«, in: The Guardian, 7. 11. 2013 (http://www.theguardian.com/world/2013/nov/06/tim-berners-lee-encryption-spy-agencies, 21. 1. 2015).

Pilkington, Ed 2013b: Tim Berners-Lee: Spies' cracking of encryption undermines the web. World wide web inventor dismayed about US and UK attempts to undermine privacy and security, revealed by Edward Snowden, in: The Guardian: The Snowden Files, 3. 12. 2013 (http://www.theguardian.com/technology/2013/dec/03/tim-berners-lee-spies-cracking-encryption-web-snowden, 21. 1. 2015).

Priest, Dana/William Arkin 2011: Top secret America. The rise of the new American security state, New York.

RIPA (Regulation of Investigatory Powers Act) 2000 (http://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf, 29. 11. 2014).

Sands, Philippe 2008: Torture team. Deception, cruelty and the compromise of law, London.

Spiegel Staff 2014: Targeting Turkey: How Germany spies on its friends, Spiegel-

Online International (http://www.spiegel.de/international/germany/german-considers-turkey-to-be-official-target-for-spying-a-986656.html, 18. 8. 2014).

Stanganelli, Joe 2014: Post Snowden, Google users change habits, All analytics 2. 7. 2014 (http://www.allanalytics.com/author.asp?section_id=1437&doc_id=273952, 9. 9. 2014).

TNS 2014: Public Opinion Monitor: Britons give safeguarding security a higher priority than protecting privacy (http://www.tnsglobal.com/uk/press-release/public-opinion-monitor-britons-give-safeguarding-security-higher-priority-protecting-p, 9. 9. 2014).

Wright, Andrea 2011: Fit for purpose? Accountability challenges and paradoxes of domestic inquiries, in: Hans Born/Ian Leigh/Aidan Wills (Hg.), International intelligence cooperation and accountability, London, S. 170–198.

Peter Gill
Übersetzung: Angela Großmann