

## „Das Imperium schlägt zurück“

### Zur Lage der Menschenrechte im digitalen Zeitalter

Dieser Beitrag basiert auf meinem Vortrag auf der FfF-Jahrestagung, berücksichtigt aber auch neuere Entwicklungen. Er gibt meine persönliche Meinung wieder, die nicht notwendigerweise mit der Position von Amnesty International übereinstimmen muss.

„Mir ist nicht bekannt, dass ich abgehört werde.“

„Ich warte da lieber ab.“

„Es ist nicht meine Aufgabe, mich in die Details von PRISM einzuarbeiten.“

Zitate, die so manchem die Zornesröte ob der Untätigkeit der Bundesregierung im NSA-Spähskandal ins Gesicht getrieben haben. Es waren die Worte Angela Merkels im Sommer des vergangenen Jahres, als immer weitere Details zu den Überwachungsprogrammen der US-amerikanischen und britischen Geheimdienste NSA und GCHQ bekannt wurden. Die Kanzlerin, so die Botschaft, sieht keinen Handlungsbedarf.



Foto: Benjamin Kees

Im Oktober dann plötzlich ganz andere Töne: „Ausspähen unter Freunden, das geht gar nicht.“ Die Kanzlerin spricht von einem „gravierenden Vertrauensbruch“, die Überwachung sei „völlig inakzeptabel“ und müsse unverzüglich unterbunden werden. Botschafter werden einbestellt (im Fall der USA) oder jedenfalls zum Gespräch geladen (im Fall des Vereinigten Königreichs). Die Minister, die zuvor noch tönnten, Sicherheit sei ein „Supergrundrecht“ und „Die Vorwürfe sind vom Tisch“, fordern auf einmal eine Entschuldigung der USA, misstrauen allen früheren Zusicherungen der amerikanischen Freunde und versprechen eine lückenlose Aufklärung aller Vorwürfe. Das politische Berlin ist in Aufruhr.

Was war passiert? Ein Handy wurde abgehört. Nichts Neues? Doch. Denn es war das Handy der Bundeskanzlerin. Die Frage, weshalb das Menschenrecht auf Privatleben der Bundeskanzlerin soviel wichtiger und dringlicher sein soll als das der übrigen Menschen in Deutschland, blieb bei alledem unbeantwortet.

Das Online-Satiremagazin *Der Postillon* titelte: „Innenminister Friedrich erklärt Abhörsicherheit von Kanzlerinnenhandy zum Superdupergrundrecht“<sup>1</sup> – vor dem das Supergrundrecht auf Sicherheit natürlich zurücktreten muss. Und: „Angela Merkel empört, dass sie von USA behandelt wird, als wäre sie ein deutscher Bürger“.<sup>2</sup> Regierungssprecher Seibert wurde in dem

Artikel der Satz in den Mund gelegt: „Sie fragt sich sogar, wozu sie eigentlich Kanzlerin geworden ist, wenn ihre Privatsphäre genauso mit Füßen getreten wird wie die ihrer Wähler.“

Galgenhumor ist eine gesunde, aber nicht unbedingt die effektivste Strategie, dem Spähskandal und den Reaktionen der deutschen Politik zu begegnen. Denn es geht bei den Enthüllungen um die Zukunft eines Menschenrechts, das schon lange angezählt war, und im jetzigen Umfeld um seine nackte Existenz bangen muss.

### Menschenrechte im digitalen Zeitalter

Die Geschichte der Menschenrechte im Umfeld der IKT ist ambivalent.

Einerseits hat die Digitalisierung die Wahrnehmung von Menschenrechten vereinfacht, die Menschenrechtsarbeit effizienter gemacht:

„2010 wird möglicherweise als ein Jahr der Zeitenwende in die Geschichte der Menschenrechte eingehen: Menschenrechtsverteidiger und Journalisten bedienen sich zunehmend neuer Technologien, um die Mächtigen mit der Wahrheit zu konfrontieren und auf diese Weise auf eine stärkere Einhaltung der Menschenrechte zu dringen. Es war auch das Jahr, in dem einige repressive Regierungen damit rechnen mussten, dass ihre Tage gezählt sind.“<sup>3</sup> (Salil Shetty, Generalsekretär von Amnesty International, am Anfang des Amnesty Reports 2011)

Es war die Zeit der – zunächst friedlichen – Revolutionen in zahlreichen arabischen Ländern. Tunesien, Ägypten, Libyen, Bahrain, Syrien: Überall manifestierte sich Widerstand auf der Straße. Doch woher kam er? Die klassischen Medien berichteten kaum unabhängig. Wie konnten sich die Menschen so schnell organisieren? Die Machthaber waren überrascht von der Geschwindigkeit, mit der sich die Proteste verbreiteten. Zunächst schien alles nach Plan zu laufen: Eine Regierung nach der anderen stürzte. Das Internet hatte daran einen wesentlichen Anteil: Einfache Bürger konnten etwa in Blogs mit der Weltöffentlichkeit kommunizieren, in sozialen Netzwerken Aktivitäten planen und rechtswidriges Handeln der Konfliktparteien durch selbstgedrehte Clips auf Video-Plattformen belegen. Repressive Maßnahmen wie die zeitweise Kappung der Internet- und Mobilfunkanbindung Ägyptens konnten die Proteste nicht dauerhaft behindern – auch dank der Hilfe von Aktivisten aus dem Ausland, die alternative Kommunikationswege bereitstellten.





2010 war auch das Jahr von *WikiLeaks*: Die Enthüllungsplattform veröffentlichte binnen weniger Monate Hunderttausende Dokumente, die erstmals Menschenrechtsverletzungen und Verstöße gegen humanitäres Völkerrecht in den Kriegen in Afghanistan und im Irak belegten. Die US-Botschaftsdepeschen zeigten, wie wenig einigen westlichen Regierungen an Veränderung in den arabischen Staaten gelegen war, obwohl sie von den repressiven Methoden der dortigen Regierungen wussten.

Die Ereignisse vermittelten eine neue Hoffnung: dass das Internet die Kräfteverteilung nachhaltig zugunsten der Menschenrechte und ihrer Verteidiger verändern könnte.

Drei Jahre später scheint diese Hoffnung vergebens – die andere Lehre, die wir aus der technischen Entwicklung für die Menschenrechte ziehen müssen: *Julian Assange*, der Gründer von *WikiLeaks*, sitzt im ecuadorianischen Botschaftsasyll. Er befürchtet, das Strafverfahren in Schweden wegen Sexualdelikten diene als Vorwand, ihn wegen seiner Tätigkeit für *WikiLeaks* an die USA auszuliefern. *Chelsea Manning*, die *WikiLeaks* einen Großteil des oben beschriebenen Materials zur Verfügung gestellt hatte, war in den USA nach ihrer Festnahme zunächst zu Bedingungen inhaftiert, die nach Ansicht von *Amnesty* internationale Standards für die menschliche Behandlung von Untersuchungshäftlingen verletzen. Im August 2013 wurde sie von einem US-Militärgericht zu einer Freiheitsstrafe von 35 Jahren verurteilt, wegen der Weitergabe von eingestufteten Dokumenten und der Übergabe von Informationen über die nationale Verteidigung an nicht autorisierte Quellen. *Amnesty* hat sich mittlerweile für die Begnadigung *Mannings* ausgesprochen. Statt ein Exempel an ihr zu statuieren, solle die US-Regierung Menschenrechtsverletzungen im Zusammenhang mit ihrem *Krieg gegen Terror* untersuchen.<sup>4</sup>

Auch die Revolutionen des *Arabischen Frühlings* sind in vielen dieser Staaten – wie Ägypten oder Libyen – von schweren Rückschlägen bedroht. In Syrien haben sie zu einem jahrelangen Bürgerkrieg mit beiderseitigen Menschenrechtsverletzungen zwischen Regierungstruppen und einer zunehmend diffusen Gegenseite geführt, deren einziges gemeinsames Ziel der Sturz Assads zu sein scheint.

Die Enthüllungen *Edward Snowdens* schließlich zeigen, dass nicht nur bekannt repressive Regierungen wie die chinesische – die *ihren Teil* des Internet mit Hilfe der *Great Firewall of China* von kritischen Meinungsäußerungen freizuhalten sucht – die neuen Freiheiten der Menschen einschränken.

Wie sind diese Enthüllungen aus menschenrechtlicher Sicht zu bewerten, und welchen Schutz genießt der Enthüller?

### Das verschwundene Menschenrecht

In einer Resolution vom 5. Juli 2012 stellte der UN-Menschenrechtsrat fest, was vor dem Hintergrund der Universalität der Menschenrechte selbstverständlich sein sollte, aber offenbar einer Bekräftigung in diesem Gremium bedurfte: dass „*die gleichen Rechte, die Menschen offline haben, auch online geschützt werden müssen*“.<sup>5</sup> Dies gelte insbesondere für das Recht auf freie Meinungsäußerung, aber auch für die übrigen Menschenrechte.

Heute dürfte kein vernünftiger Zweifel daran bestehen, dass die Massenüberwachungsprogramme der NSA und des GCHQ – insbesondere *PRISM*, die *Upstream*-Programme, *Muscular* und *Tempora* –, jedenfalls so, wie sie in den Unterlagen *Snowdens* erscheinen, massiv eingreifen in das Menschenrecht auf Schutz des Privatlebens, wie es unter anderem in Artikel 12 der Allgemeinen Erklärung der Menschenrechte und Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte garantiert ist. Ein umfassenderer Eingriff als die nahezu vollständige Aufhebung des Privaten im Bereich der Telekommunikation erscheint kaum vorstellbar.

Wie jedes Menschenrecht ist auch das Recht auf Schutz des Privatlebens nicht schrankenlos gewährleistet. Voraussetzung für einen rechtmäßigen Eingriff ist eine gesetzliche Grundlage, mit der ein legitimer Zweck verfolgt wird, zu dem die gewählte Maßnahme nicht außer Verhältnis steht. Bei einigen bekannt gewordenen Programmen ist die gesetzliche Grundlage zweifelhaft; sie basieren teils auf einer eigenwillig weiten Interpretation des *FISA Amendment Act 2008*, die die Grenzen der Auslegung zu überschreiten scheint. Auch daran, dass der Zweck in allen Fällen ein legitimer ist, sind Zweifel angebracht. Mit nationaler Sicherheit oder dem Krieg gegen den Terror lassen sich die Bespitzelungen von diplomatischen Vertretungen und Unternehmen oder die Überwachung des Kanzlerinnenhandys kaum begründen.

Ganz sicher wird eine Rechtfertigung zumindest der Massenüberwachungsprogramme an der Verhältnismäßigkeitsprüfung scheitern. Die unterschiedslose Speicherung und Analyse sämtlicher Kommunikation, derer ein Nachrichtendienst mit seinen technischen Mitteln habhaft werden kann, ohne effektives rechtsstaatliches Verfahren, zeigt, dass hier keine ernsthafte Abwägung der beteiligten Interessen stattgefunden hat. Statt dessen wurde durch die Enthüllungen offenbar, dass die US-amerikanische und die britische Regierung nationalen Sicherheitsinteressen im Bereich der Telekommunikation absoluten Vorrang eingeräumt haben gegenüber einem Menschenrecht, dessen Bedeutung für die Würde und die Identität des Einzelnen im digitalen Zeitalter kaum überschätzt werden kann.

In einer von Brasilien und Deutschland initiierten, einstimmig verabschiedeten Resolution der UN-Generalversammlung<sup>6</sup> werden die Staaten aufgefordert, das Recht auf Privatleben zu achten und Verletzungen zu beenden, ihre Überwachungsmaßnahmen auf die Vereinbarkeit mit diesem Recht zu überprüfen und eine unabhängige Aufsicht über diese Maßnahmen sicherzustellen. Die gleichzeitige Bitte an die UN-Hochkommissarin für Menschenrechte, bis zum kommenden Herbst einen Bericht über die Lage des Menschenrechts auf Privatleben im Kontext staatlicher Kommunikationsüberwachung und -datensammlung vorzulegen, wird dafür sorgen, dass das Thema auf der internationalen Agenda bleibt.

*Amnesty* hat Menschenrechtsbeschwerde vor dem britischen *Investigatory Powers Tribunal* erhoben.<sup>7</sup> Sie richtet sich gegen das Überwachungsprogramm *Tempora* des GCHQ und dessen unzureichende Regulierung sowie gegen die Nutzung von NSA-Daten aus *PRISM* und den *Upstream*-Programmen durch das Vereinigte Königreich. Das Verfahren läuft parallel zu einer ähnlich lautenden Beschwerde mehrerer Organisationen vor dem *Europäischen Gerichtshof für Menschenrechte (EGMR)* in Straßburg.<sup>8</sup>

Beide Verfahren machen neben einer Verletzung des Rechts auf Privatheit auch einen Verstoß gegen das Recht auf Meinungsfreiheit geltend. Welch abschreckende Wirkung (*chilling effect*) das Wissen um eine Überwachung des eigenen Handelns auf die Wahrnehmung dieses Rechts haben kann, hat erst kürzlich eine Umfrage des Schriftstellerverbandes *PEN America* gezeigt: 24 % der befragten Schriftsteller vermieden es als Folge der *Snowden*-Enthüllungen, bestimmte Themen in Telefongesprächen oder E-Mails anzusprechen; weitere neun Prozent dächten ernsthaft darüber nach.<sup>9</sup>

### Schutz als Whistleblower?

Die öffentliche Bekanntgabe von Staatsgeheimnissen muss nicht zwangsläufig von der Meinungs- und Informationsfreiheit gedeckt sein. So ist anerkannt, dass nationale Sicherheitsinteressen einer Veröffentlichung im Einzelfall entgegenstehen können. Das bedeutet indes nicht, dass Staaten diesen Einschränkungsground missbrauchen dürfen, um die Veröffentlichung unliebsamer oder für sie unangenehmer Informationen zu verhindern. Geht es um Missstände, deren Bekanntgabe im öffentlichen Interesse liegt, wird eine Abwägung oft zugunsten der Veröffentlichung ausfallen, zumal wenn die aufgedeckten Handlungen gegen geltendes Recht verstoßen. In keinem Fall sollten Menschen dafür verfolgt werden, dass sie Informationen ans Licht bringen, die Menschenrechtsverletzungen belegen.

Die Rechtsprechung internationaler Gerichte zum *Whistleblower*-Schutz ist bislang dürftig. Der EGMR stützt die Beurteilung der Verhältnismäßigkeit einer Veröffentlichung interner Informationen (und damit die Frage, ob ein Verstoß gegen das Recht auf Meinungs- und Informationsfreiheit vorliegt) auf eine Reihe von Faktoren, die gegeneinander abzuwägen seien. Dazu zählen die Frage, ob alternative Wege bestanden und genutzt wurden, die Informationen bekannt zu machen (etwa auf dem internen Weg), das öffentliche Interesse an der Information, ihre Glaubwürdigkeit, der Schaden, den die staatliche Behörde durch die Veröffentlichung erleidet, und das Motiv des Whistleblowers. Aber auch die Schwere der gegen den Whistleblower verhängten Strafe kann eine Rolle spielen.<sup>10</sup>

All diese Kriterien scheinen für *Snowden* zu sprechen: Zumindest nach eigener Aussage hat er sich vor dem Gang an die Öffentlichkeit erfolglos an Vorgesetzte gewandt. An der Aufdeckung von Menschenrechtsverletzungen dürfte immer ein überragendes öffentliches Interesse bestehen, da es hier um gravierende Fehlentwicklungen und Völkerrechtsverstöße geht, so dass auch ein möglicher Schaden für den Staat im Verhältnis dazu in aller Regel zurücktreten muss. Die Authentizität der Informationen lässt sich angesichts der Menge und Detailgenauigkeit kaum bezweifeln. Ihr wurde auch von staatlichen Stellen bisher nicht grundsätzlich widersprochen. *Snowdens* Motivlage lässt die Anklageschrift<sup>11</sup> durchscheinen: Die Tatsache, dass *Snowden* nicht die „Übermittlung von Verteidigungsinformationen zum Nutzen einer ausländischen Regierung“ (18 U.S.C. § 794(a)) vorgeworfen wird, zeigt, dass zur Zeit nicht einmal die Strafverfolger davon ausgehen, dass *Snowden* dem Feind helfen wollte. (Dieser Tatbestand setzt voraus, dass der Täter in der Absicht oder begründeten Annahme gehandelt hat, die Informationen könnten zum Schaden der USA oder zum Vorteil eines anderen Staa-

### Artikel 8

#### Recht auf Achtung des Privat- und Familienlebens

(1) Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.

(2) Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.

### Artikel 10

#### Freiheit der Meinungsäußerung

(1) Jede Person hat das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben. Dieser Artikel hindert die Staaten nicht, für Hörfunk-, Fernseh- oder Kinounternehmen eine Genehmigung vorzuschreiben.

(2) Die Ausübung dieser Freiheiten ist mit Pflichten und Verantwortung verbunden; sie kann daher Formvorschriften, Bedingungen, Einschränkungen oder Strafdrohungen unterworfen werden, die gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sind für die nationale Sicherheit, die territoriale Unversehrtheit oder die öffentliche Sicherheit, zur Aufrechterhaltung der Ordnung oder zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral, zum Schutz des guten Rufes oder der Rechte anderer, zur Verhinderung der Verbreitung vertraulicher Informationen oder zur Wahrung der Autorität und der Unparteilichkeit der Rechtsprechung.

*Europäische Menschenrechtskonvention*

tes verwendet werden.) *Snowden* selbst hat eine entsprechende Motivation stets bestritten, seine bisherige Veröffentlichungsstrategie stützt dies.

*Amnesty* hat nach den ersten Berichten über die *NSA*-Dokumente betont, dass die Veröffentlichung von Informationen über Menschenrechtsverletzungen vom Recht auf Meinungsfreiheit geschützt sind, und dass ein Gerichtsverfahren gegen *Snowden* wegen dieser Enthüllungen politischer Verfolgung gleichkäme. Er dürfe nicht an die USA ausgeliefert werden, da er dort dem Risiko unmenschlicher Behandlung in Haft ausgesetzt wäre (wie der Fall *Manning* belegt). Auch dass er sich nach dem US-Spionagegesetz im Verfahren nicht auf das öffentliche Interesse berufen dürfe, sei ein Auslieferungshindernis. Daneben werde sein Recht auf Bewegungsfreiheit und sein Recht, Asyl zu beantragen, durch die Ungültigerklärung seines Reisepasses verletzt.<sup>12</sup>

### Nichts zu verbergen?

„Wer nichts zu verbergen hat, hat auch nichts zu befürchten“ – so lautet ein gängiges Argument von Sicherheitspolitikern, mit dem Bedenken gegen den Totalüberwachungsansatz hinter den Aktivitäten von *NSA* und *GCHQ* zerstreut werden sol-







len.<sup>13</sup> Auf die damit unterschwellig formulierte Frage beeilen sich auch hierzulande solchermaßen beruhigte Bürger zu versichern: „Ich habe nichts zu verbergen.“ Können solche erzwungenen (Selbst-)Beschwichtigungen der Maßstab in einer freiheitlichen Gesellschaft sein, die sich den Menschenrechten verpflichtet fühlt? Kann der Fortbestand von grundlegenden Rechten davon abhängig gemacht werden, ob der Einzelne durch ihre Beseitigung etwas zu befürchten hat?

Selbst für den abwegigen Fall, dass wir alle tatsächlich nichts zu verbergen hätten: Wer kann heute sagen, dass das auch morgen noch gilt? Wer kann sagen, dass die Daten, die sie oder er heute preisgibt, nicht morgen gegen sie oder ihn verwendet werden? Wer kann sagen, was die heute preisgegebenen Daten in Verbindung mit den morgen preisgegebenen Daten übermorgen vielleicht einmal über sie oder ihn aussagen werden?

Ein Staat, der im Geheimen abhorcht, was ihn nichts angeht, ohne wirksam von Gerichten oder vom Parlament kontrolliert zu werden, der ist schon heute keine Demokratie mehr. Was wird er morgen sein? Und wie werden die Daten vielleicht schon heute in diesen „postdemokratischen Zuständen“,<sup>14</sup> wie *Hans Magnus Enzensberger* es ausdrückt, gegen die Betroffenen verwendet? Wir werden das ganze Ausmaß wohl nie erfahren.

Erste Bedenken sind aber angebracht, wenn der deutsche Schriftsteller *Ilja Trojanow*, über den nicht bekannt ist, dass er sich irgendwelcher terroristischen Umtriebe verdächtig gemacht hat, der sich nichts zuschulden hat kommen lassen, außer sich kritisch über die Überwachungsaktivitäten der *NSA* zu äußern, trotz Visum ohne Angabe von Gründen nicht mehr in die USA einreisen darf.<sup>15</sup> Alarmiert sollte man sein, wenn Menschen aus Drittstaaten die Einreise in die USA verweigert wird, weil den US-Zoll- und Grenzschutzbehörden Gesundheitsinformationen vorlägen, die auf eine psychische Erkrankung hinwiesen.<sup>16</sup>

*Nichts zu verbergen?* So einfach ist es eben nicht. Für eine Woche, für ein Jahr, vielleicht für immer wird in großen Datensilos das Leben von Milliarden Menschen aufgezeichnet und analysiert, um es ihnen bei Bedarf vorhalten zu können. Jedenfalls dann, wenn sie sich in einem der Staaten aufhalten, die diese Überwachungsprogramme betreiben, oder dort einreisen wollen. Oder in ein Land, das mit diesen Staaten Daten austauscht – wie nach den Unterlagen von *Snowden* wohl die Mehrheit der EU-Mitgliedstaaten.

Vielleicht aber ist selbst das nicht einmal notwendig.

Wie ein Amnesty-Bericht vom Oktober 2013 belegt, führen die USA in einem strikt geheimgehaltenen Drohnenprogramm extralegale Hinrichtungen in pakistanischem Stammesgebiet durch.<sup>17</sup> Der Bericht untersucht neun der insgesamt 45 Drohnenangriffe, die die USA in der Zeit zwischen Januar 2012 und August 2013 in Pakistan durchgeführt haben und die zu zahlreichen zivilen Opfern geführt haben. Besonders verwerflich erscheinen dabei einerseits *secondary strikes* oder *rescuer attacks*, die sich gegen diejenigen zu richten scheinen, die Opfern vorangegangener Drohnenangriffe zu Hilfe eilen. Angriffe werden auch gegen Personen unbekannter Identität geflogen, deren Verhalten den die Stammesgebiete überwachenden US-Sicherheitsbehörden verdächtig erscheint (*signature strikes*). Doch auch in den übri-

gen Fällen außergerichtlicher Tötungen durch Drohnen operieren die USA nach Ansicht von *Amnesty* an menschenrechtlichen Standards und am Völkerrecht vorbei und begehen dabei unter Umständen sogar Kriegsverbrechen. Wie Berichte belegen, ist Pakistan nicht das einzige Land, in dem US-Kampfdrohnen Angriffe fliegen: Auch im Jemen oder in Somalia finden solche völkerrechtswidrigen Tötungen statt.<sup>18</sup> Die Daten für die Identifizierung und Lokalisierung der Zielpersonen stammen dabei häufig aus den Datenspeichern der *NSA* und *GCHQ*. Deren Personenprofile können direkt für Drohnenangriffe gegen den Betroffenen genutzt werden.<sup>19</sup> Auch der BND soll in mindestens einem Fall Telefondaten an die USA weitergegeben haben, die zur Tötung eines deutschen Staatsbürgers in Waziristan führten.<sup>20</sup>

Speicherung und Analyse der personenbezogenen Daten durch die Nachrichtendienste dienen zudem nicht nur dem Kampf gegen Terrorismus und organisierte Kriminalität, sondern auch dem *Cyberwar* um die Kontrolle über Gesellschaften und die Sicherung staatlicher Hegemonialstellungen.<sup>21</sup> Seitdem 2007 ein ganzes Land – Estland – lahmgelegt wurde, basteln die Militärstrategen an immer ausgefeilteren Cyber-Waffen, von denen *Stuxnet* die bekannteste sein dürfte.<sup>22</sup> Die Überwachungsprogramme der *Five Eyes*-Staaten und ihrer Partner verschaffen den Diensten dabei einen Informationsvorsprung, mit dem sie gesellschaftliche Entwicklungen weltweit früher als andere erkennen und im eigenen Sinne steuern können.

*Carl von Clausewitz* würde seinen bekannten Ausspruch vom *Krieg als Fortsetzung der Politik mit anderen Mitteln* heute vielleicht ergänzen um einen weiteren Satz: *Cyberwar* ist die Fortführung des kinetischen Kriegs mit anderen Mitteln. Der Kollateralschaden dieses virtuellen Krieges mit realen Folgen ist die weitgehende Vernichtung der unkörperlichen Integrität des Einzelnen: seiner Privatsphäre.

### Kooperation ist wichtig!

*Tim Berners-Lee*, der Erfinder des World Wide Web, wandte sich im Sommer 2013 an alle Amnesty-Mitglieder mit den Worten:

*„I believe we have reached a critical juncture where if we do not unite and fight for our rights to privacy, freedom of information, freedom of association, and freedom of expression in this new digital world, they will be taken away. [...] [H]uman rights defenders like Amnesty are critical to win the battle.“<sup>23</sup>*

In der deutschen Sektion nähern wir uns diesem Ziel: Die 2012 informell gegründete Arbeitsgruppe *Digital@Amnesty* will die bisherigen Aktivitäten von *Amnesty* zusammentragen, analysieren und eine Strategie für das weitere Vorgehen entwickeln. Mittelfristiges Ziel ist es, den Interessentenkreis zu einer vollwertigen Themenkoordinationsgruppe mit dem Fokus *Digitale Technologien und Menschenrechte* auszubauen. Auf dem Weg dahin suchen wir den Austausch mit auf diesem Gebiet bereits seit langem aktiven Bürger- und Menschenrechtsorganisationen wie dem *FIDH*. Der Spähskandal zeigt, wie eng westliche Geheimdienste in ihrem Bemühen kooperieren, auch ihre eigenen Bürger zu überwachen und zu kontrollieren. Wer diesem massiven Völkerrechtsbruch etwas entgegensetzen will, muss bereit sein,

sich ebenfalls mit Gleichgesinnten zu verbünden. Ich bin zuversichtlich, dass Amnesty als globale Bewegung ihren Teil dazu beitragen wird, gemeinsam mit anderen eine internationale Koalition der Verteidiger grundlegender Menschenrechte im digitalen Zeitalter zu bilden, und wünsche mir, dass die bereits geknüpften Kontakte zum FIF nicht abreißen werden.

## Anmerkungen

- 1 <http://www.der-postillon.com/2013/10/innenminister-friedrich-erklart.html>
- 2 <http://www.der-postillon.com/2013/10/angela-merkel-empfort-dass-sie-von-usa.html>
- 3 Amnesty International Report 2011: Zur weltweiten Lage der Menschenrechte, S. 7.
- 4 Amnesty International, USA: Commute Bradley Manning's sentence and investigate the abuses he exposed, 21.8.2013, <https://www.amnesty.org/en/news/usa-commute-bradley-manning-s-sentence-and-investigate-abuses-he-exposed-2013-08-21>
- 5 UN Human Rights Council, Resolution: The promotion, protection and enjoyment of human rights on the Internet, A/HRC/20/L.13, 29.6.2012 (angenommen am 5.7.2012), <http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement>
- 6 UN General Assembly, Resolution: The right to privacy in the digital age, A/RES/68/167, abgedruckt in A/68/456/Add.2, 10.12.2013 (angenommen am 18.12.2013), [https://www.un.org/ga/search/view\\_doc.asp?symbol=A/68/456/Add.2](https://www.un.org/ga/search/view_doc.asp?symbol=A/68/456/Add.2), S. 139 f.
- 7 Amnesty International, Amnesty International brings claim against UK over state surveillance, 9.12.2013, <https://www.amnesty.org/en/for-media/press-releases/amnesty-international-brings-claim-against-uk-over-state-surveillance-2013->
- 8 Beschwerdeführer in dem EGMR-Verfahren sind Big Brother Watch, English PEN, Open Government Partnership, und Constanze Kurz vom CCC; <https://www.privacynotprism.org.uk/news/2013/10/03/gchq-to-face-european-court-over-mass-surveillance/>
- 9 PEN America, Chilling effects: NSA Surveillance Drives U.S. Writers to Self-Censor, 12.11.2013, [http://www.pen.org/sites/default/files/Chilling%20Effects\\_PEN%20American.pdf](http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf)
- 10 So etwa in: EGMR, Guja gegen Moldawien, Appl. No. 14277/04, Urteil vom 12.2.2008, §§ 73 ff., <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-85016>
- 11 US District Court for the Eastern District of Virginia, USA v. Edward J. Snowden, Criminal Complaint, Case No. 1:13 CR 265 (CMH), 14.6.2013, <http://s3.documentcloud.org/documents/716865/snowden-complaint.pdf>
- 12 Amnesty International, USA must not persecute whistleblower Edward Snowden, 2.7.2013, <https://www.amnesty.org/en/news/usa-must-not-persecute-whistleblower-edward-snowden-2013-07-02>
- 13 Vgl. den britischen Außenminister William Hague wenige Tage nach der Veröffentlichung der ersten Snowden-Dokumente: <https://www.youtube.com/watch?v=IWam4EWI48M>
- 14 [http://www.daserste.de/information/wissen-kultur/ttt/sendung/hr/sendung\\_vom\\_18082013-102.html](http://www.daserste.de/information/wissen-kultur/ttt/sendung/hr/sendung_vom_18082013-102.html)
- 15 Spiegel Online, NSA-Kritiker Ilija Trojanow: Deutscher Schriftsteller darf nicht in die USA einreisen, 1.10.2013, <http://www.spiegel.de/kultur/gesellschaft/ilija-trojanow-nach-nsa-protest-einreise-in-die-usa-verweigert-a-925467.html>
- 16 Disabled woman denied entry to U.S. after agent cites supposedly private medical details, 28.11.2013, [http://www.thestar.com/news/gta/2013/11/28/disabled\\_woman\\_denied\\_entry\\_to\\_us\\_after\\_agent\\_cites\\_supposedly\\_private\\_medical\\_details.html](http://www.thestar.com/news/gta/2013/11/28/disabled_woman_denied_entry_to_us_after_agent_cites_supposedly_private_medical_details.html)
- 17 Amnesty International, Will I Be Next? US Drone Strikes in Pakistan, 2013, <http://www.amnesty.org/en/library/asset/ASA33/013/2013/en/041c08cb-fb54-47b3-b3fe-a72c9169e487/asa330132013en.pdf>. Auf der englischsprachigen Sonderseite zum Bericht, <http://drones-pakistan.amnesty.org>, hat Amnesty International Satellitenbilder, Videos und ausführliche Hintergrundinformationen zusammengestellt.
- 18 Vgl. „Schmutzige Kriege“, ARD-Dokumentation, gesendet im Programm Das Erste am 28.11.2013. Siehe auch den Bericht zur Geolokalisierung von Angriffszielen für Drohnenangriffe von CIA und JSOC, einer Kommandoeinheit der US-Armee, durch Handy-Metadaten aus dem NSA-Datenbestand: Jeremy Scahill/Glenn Greenwald, The NSA's Secret Role in the U.S. Assassination Program, 10.2.2014, <https://firstlook.org/theintercept/article/2014/02/10/the-nas-secret-role/>
- 19 Greg Miller/Julie Tate/Barton Gellman, Documents reveal NSA's extensive involvement in targeted killing program, 17.10.2013, [http://www.washingtonpost.com/world/national-security/documents-reveal-nas-extensive-involvement-in-targeted-killing-program/2013/10/16/29775278-3674-11e3-8a0e-4e2cf80831fc\\_story.html](http://www.washingtonpost.com/world/national-security/documents-reveal-nas-extensive-involvement-in-targeted-killing-program/2013/10/16/29775278-3674-11e3-8a0e-4e2cf80831fc_story.html)
- 20 Stefan Bucher/Hans Leyendecker, Unmut über BND-Chef Schindler, 10.8.2013, <http://www.sueddeutsche.de/politik/kooperation-mit-us-geheimdiensten-unmut-ueber-bnd-chef-schindler-1.1743505>
- 21 So auch „World Wide War: Der geheime Kampf um die Daten“, ZDF Zoom, Sendung vom 9.10.2013.
- 22 Vgl. die Veröffentlichungen zu den Aktivitäten der NSA-Abteilung Tailored Access Operations (TAO) u. a. in: Inside TAO: Documents Reveal Top NSA Hacking Unit, Spiegel Online, 29.12.2013, <http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html>; Jacob Appelbaum/Judith Horchert/Christian Stöcker, Shopping for Spy Gear: Catalog Advertises NSA Toolbox, Spiegel Online, 29.12.2013, [www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html](http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html)
- 23 <http://amnestyicm2013.wordpress.com/2013/08/22/the-greatest-threat-to-the-future-of-the-internet/>



Sebastian Schweda

**Sebastian Schweda** ist Rechtsanwalt mit Schwerpunkten im Datenschutz-, Telekommunikations- und Medienrecht und seit 2007 am Institut für Europäisches Medienrecht (EMR) in Saarbrücken tätig. Er ist aktives Mitglied bei Amnesty International und arbeitet derzeit am Aufbau einer neuen Koordinationsgruppe zum Themenkreis *Digitale Technologien und Menschenrechte* innerhalb der deutschen Sektion von Amnesty International. Die Gruppe ist erreichbar unter: [digital@amnesty.de](mailto:digital@amnesty.de).

