Bericht der Digitalen Gesellschaft

# Massenüberwachung durch die Geheimdienste:

# Wie ist die Schweiz betroffen, und welche Massnahmen sind notwendig?

20. Februar 2015

Digitale Gesellschaft
Marktgasse 3
5620 Bremgarten AG
https://www.digitale-gesellschaft.ch/

Die Digitale Gesellschaft ist ein offener Zusammenschluss netzpolitisch aktiver Gruppen und Einzelpersonen. Dazu gehören unter anderem der Chaos Computer Club Schweiz und Zürich, die Digitale Allmend, der Verein grundrechte.ch, die Piratenpartei Schweiz und die Swiss Privacy Foundation.

Version 1.01 vom 28. Juli 2015: Schreibfehler behoben

## Zusammenfassung

Seit Frühling 2013 wird nach und nach die wohl umfangreichste Überwachungsmaschinerie der Menschheitsgeschichte aufgedeckt. Die meisten Veröffentlichungen aus den Dokumenten von Whistleblower Edward Snowden gehen mittlerweile aber im täglichen Nachrichtenstrom unter. Die dringend notwendige Aufarbeitung der Massenüberwachung durch Geheimdienste und andere Sicherheitsbehörden – und deren Auswirkungen auf die Gesellschaft – findet deshalb kaum statt. Gerade auch viele Politikerinnen und Politiker scheinen sich mit dem Verlust von Privatsphäre und der Meinungsäusserungsfreiheit abgefunden zu haben, ebenso mit dem verlorenen Briefgeheimnis und den aufgehobenen Berufsgeheimnissen von Ärzten, Geistlichen und Rechtsanwälten.

Mit dem vorliegenden Bericht arbeitet die Digitale Gesellschaft die Massenüberwachung in der Schweiz auf:

Der Bericht fasst die bekannten Programme zur Massenüberwachung der NSA und des britischen GCHQ gemeinsam mit den Aktivitäten des schweizerischen Nachrichtendienstes zu einem Gesamtbild zusammen. Der Fokus liegt dabei auf der allgemeinen und universellen Betroffenheit sämtlicher Einwohnerinnen und Einwohner der Schweiz. Die Erkenntnisse werden abschliessend in sieben konkrete Massnahmen und Forderungen überführt.

# Inhaltsverzeichnis

# 1 Einleitung

Beinahe zwei Jahre sind seit den ersten Enthüllungen von Edward Snowden vergangen. In der Zwischenzeit belegen hunderte von Texten und Präsentationen die beinahe totale Unterwanderung des Internets durch die Geheimdienste der USA und Grossbritannien. Doch bereits die schiere Menge und die unterschiedlichsten Arten der Angriffe lassen einen oft sprachlos zurück: Zu keiner Zeit der Menschheitsgeschichte wurden die Privatsphäre, das Recht auf freie Meinungsäusserung, das Brief-, Post- und Fernmeldegeheimnis auf solch eklatante Weise verletzt.

Doch anstatt mit Nachdruck für grundlegende Menschenrechte einzustehen, scheint das politische Pendel bereits wieder zurückzuschlagen. Nicht erst seit den Anschlägen in Frankreich wird auch in der Schweiz am Ausbau der Vorratsdatenspeicherung und der Einführung der «Kabelaufklärung» gearbeitet – anstatt die Massenüberwachung, deren Nützlichkeit und vor allem deren Folgen für die Gesellschaft zu debattieren.

Die Digitale Gesellschaft veröffentlicht aus diesem Grund einen Bericht zur Massenüberwachung durch die Geheimdienste. Dieser klopft die Enthüllungen von Edward Snowden auf Bezüge zur Schweiz ab und fügt weitere Quellen zu einem umfassenden Bild zusammen. Es soll dabei die allgemeine und universelle Betroffenheit sämtlicher Einwohnerinnen und Einwohner der Schweiz aufgezeigt werden.

Im Fokus stehen jedoch nicht nur die National Security Agency (NSA) und der britische Geheimdienst «Government Communications Headquarters» (GCHQ), sondern es wird auch die Rolle des Nachrichtendienstes des Bundes (NDB) beleuchtet.

Der Text ist, in sich teilweise überlappende, sechs Kapitel eingeteilt:

- Einleitung
- Abhörstationen und -aktionen in der Schweiz
- Zugriffspunkte auf Datenkommunikation in der Schweiz
- Zugriffsmöglichkeiten auf Schweizer Datenkommunikation im Ausland
- Zusammenarbeit von ausländischen Geheimdiensten mit dem Nachrichtendienst des Bundes (NDB)
- Forderungen an die Politik

In jedem Kapitel werden zuerst die bereits bekannten Überwachungspraktiken zusammengefasst, bevor nochmals explizit auf die Betroffenheit für Personen in der Schweiz eingegangen wird. Das letzte Kapitel fordert dann sieben Massnahmen von der Schweizer Politik.

# 2 Abhörstationen und -aktionen in der Schweiz

## 2.1 Abhörstation Leuk, Verestar, nun Signalhorn AG

Bereits im Jahr 2000 beim Verkauf einer Satelliten-Bodenstation von Swisscom an die US-amerikanische Gesellschaft Verestar gab es Bedenken wegen möglicher Spionage. Diese Station in Leuk (Oberwallis) hat sich Gelände und Infrastruktur mit dem Abhörsystem Satos 3 geteilt, das vom VBS betrieben wird. Vom Verkauf betroffen waren auch kleinere Stationen in den Städten Genf, Basel und Zürich. Für den Sprecher des Eidgenössischen Datenschutzbeauftragten war schon damals klar, «dass auch der Schweizer Luftraum vom Lauschangriff der amerikanischen und britischen Geheimdiensten betroffen ist, egal ob jetzt die Satellitenanlage in Leuk von einem NSA-Ableger gekauft wurde oder nicht.»[1]

Eine Antwort vom Bundesrat auf eine Interpellation konnte 2001 nicht ganz überzeugen: «Die Firma Verestar betreibt jedoch nur Transit- und Access-Dienste in der Telekommunikation und hat daher keine Kenntnisse über den Inhalt der zu transportierenden Kundeninformationen. Die Gesellschaft arbeitet nicht mit so genannten klassifizierten Daten, weder für behördliche Institutionen noch für andere Kunden. Dies hat die Gesellschaft der Swisscom AG gegenüber versichert. Verestar [...] unterliegt [...] den Regeln des Fernmeldegesetzes (FMG).»[2]

Satos 3 heisst heute Onyx, und die Firma Verestar ist umfirmiert in Signalhorn AG – geblieben sind die Bedenken.

Gemäss einer Reportage der ZDF Sendung «Zoom» vom September 2013 hätte die NSA in Deutschland keinen Zugang mehr zu Daten mit Inlandsbezug. Diese Einschränkung sei jedoch kein Problem, denn Daten «mit Deutschlandbezug kann der NSA problemlos anderswo bekommen – von seinen Abhörstationen in Dänemark und der Schweiz».

Der Tages-Anzeiger vom 13.9.2013: «Trifft die Schilderung des ZDF zu, hätte dies in der Schweiz zweifellos ein politisches Erdbeben zur Folge, denn gemäss Schweizer Gesetz ist der Betrieb solcher Anlagen durch einen fremden Nachrichtendienst ebenso im höchsten Mass verboten wie fremder Direktzugriff auf eine Anlage, die durch die Schweiz betrieben wird und ihr gehört.»[3]

Die Rolle der Signalhorn AG bleibt jedoch im Dunkeln. Der NDB wiegelt ab: «In Leuk sind sie [die Infrastrukturen des Schweizer Satellitenabhörsystems] völlig getrennt von jenen des privaten Providers, der die übrigen Antennen auf dem angrenzenden Areal betreibt.» Und nein, «weder die NSA noch eine andere US-Behörde haben einen direkten Zugriff auf diese [unsere] Daten.»[4]

[1] http://www.heise.de/tp/artikel/4/4326/1.html
[2] http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20003629
[3] http://www.tagesanzeiger.ch/schweiz/Was-der-Schweizer-Geheimdienst-zum-ZDFBericht-sagt/story/14226857

Zwei Monate später greift «swissinfo» das Thema nochmals auf:

Der ehemalige Justizminister Christoph Blocher erklärte in der «Schweiz am Sonntag»: «Es ist eindeutig, dass die Schweiz mit amerikanischen Nachrichtendiensten zusammenarbeitet.»

Und: Doch auch wenn die Signalhorn AG effektiv die Datenübertragung für einen ausländischen Geheimdienst überwachen würde, könnten die Behörden nur dann eingreifen, wenn die Gespräche und Daten aus der Schweiz abgehen oder innerhalb des Landes ausgetauscht würden. Handle es sich lediglich um Daten aus dem Ausland, «würde das de facto kein Schweizer Gesetz verletzen», schreibt das VBS.[5]

Interessant hierzu ist auch der gegenteilige Bericht der Geschäftsprüfungsdelegation der Eidgenössischen Räte (GPDel) vom 10. November 2003 über das Projekt «Onyx»[6]. Dieser hält fest:

«Diese Sachlage mag paradox erscheinen. Während sämtliche Staaten die Spionage auf ihrem Territorium durch ihre Gesetzgebung im Allgemeinen verbieten – in der Schweiz ist dies mit Artikel 271–274 und Artikel 301 StGB der Fall –, wird die Frage der Rechtmässigkeit der Spionage zu Friedenszeiten im Völkerrecht weder auf der Vertrags- noch auf der Gewohnheitsebene geregelt. Diese Feststellung gilt auch für die Abhörung von Kommunikationen: In den meisten Staaten werden der Abhörung von Kommunikationen auf ihrem eigenen Hoheitsgebiet enge gesetzgeberische Grenzen gesetzt, jedoch scheinen die Abhörungen im Ausland von keiner internationalen Rechtsordnung verboten zu werden.»

Die GPDel kommt trotz Unbehagen jedoch zum Schluss:

«Die GPDel ist der Meinung, dass dieses Spannungsfeld zwischen den durch die Schweiz im Ausland realisierten Abhörungen einerseits und dem Grundsatz der nationalen Souveränität sowie dem Völkerrecht andererseits nicht mit normativen oder konventionellen Massnahmen gelöst werden kann; ansonsten müsste auf einen Auslandsnachrichtendienst verzichtet werden. Dieses Problem erfordert einen politischen Ansatz, der diese Fragen in Abhängigkeit der jeweils auftretenden Situation von Fall zu Fall regelt.»

Wenn die NSA via Signalhorn AG in Leuk spionierte – und selbst Informationen über Personen in der Schweiz gewinnen würde – würde dies der Schweizer Nachrichtendienst allenfalls sogar begrüssen. Hält die GPDel in ihrem Bericht doch auch das Überwachen von ausländischen Vorgängen für fremde Dienste für nützlich und nötig:

[4] http://www.tagesanzeiger.ch/schweiz/Was-der-Schweizer-Geheimdienst-zum-ZDFBericht-sagt/story/14226857

[5] http://www.swissinfo.ch/ger/die-grossen-ohren-von-leuk-und-die-us-geheimdienste/37285530

[6] http://www.admin.ch/opc/de/federal-gazette/2004/1499.pdf

«Die dank Onyx empfangenen Informationen bilden auch ein nützliches «Tauschmittel» mit den entsprechenden Dienststellen im Ausland. Diese Beziehungen basieren auf der Grundlage eines gegenseitigen Gebens und Nehmens, d.h. nach dem Prinzip des «do ut des». Die schweizerischen Dienste können nur dann hoffen, von ihren Partnern Informationen zu erhalten, wenn sie ihnen als Gegenleistung ebenfalls interessante Informationen anzubieten haben.»

## 2.2 «Botschaftsüberwachung»

Weltweit betreibt die NSA 80 Abhörstationen in diplomatischen Vertretungen der USA. In Genf dürfte sie sich auf dem Dach der amerikanischen UNO-Mission befinden. Die Station in Genf gehört zu den bemannten, d.h. es sind auch Einheiten des «Special Collection Service» (SCS) vor Ort, die Mobiltelefon, WLAN, Funk und Satellitenkommunikation abhören. Auch Edward Snowden gehörte einst zu diesem Team.[7] [8]

«Weitere Einheiten dürften sich in der US-Botschaft in Bern sowie beim US-Konsulat in Zürich befinden», sagte zudem ein ehemaliger NSA-Mitarbeiter zur «Schweiz am Sonntag». Speziell in Zürich soll auch Abhörtechnik zum Einsatz kommen, die möglicherweise im Konsulat selbst stationiert ist. Laut dem NSA-Mitarbeiter sind die Amerikaner in Zürich besonders an Informationen über den Finanzplatz interessiert: «Ziel ist auch das nahe Liechtenstein.» Zudem habe es die NSA von hier aus auch auf Zug abgesehen. Im Fokus stünden dort Rohstoffhandelskonzerne.[9]

## 2.3 Wirtschaftsspionage und geklaute Laptops in Genf

Der Schweizer Diplomat Nicolas Imboden gerät – wohl wegen seiner Tätigkeit für afrikanische Staaten, die er im Kampf gegen hohe US-Baumwollsubventionen vertreten hat – ins Blickfeld der NSA. Sein Name erscheint daraufhin auf einer Überwachungsliste der GCHQ[10]. Sein Notebook wird entwendet, die Kommunikation überwacht:

«Wenn [sogar] ich als Zielperson in der Datenbank auftauche, muss man davon ausgehen, dass die Überwachung offenbar sehr engmaschig ist.», zitiert die «Schweiz am Sonntag» den Diplomaten bereits im Dezember 2013.[11]

[7] http://magazin.spiegel.de/EpubDelivery/spiegel/pdf/118184380
[8] http://www.tagesanzeiger.ch/schweiz/standard/Wie-USSpione-in-Genf-Diplomaten-ueberwachen/story/29143106
[9] http://www.aargauerzeitung.ch/schweiz/us-geheimdienst-spioniert-auch-von-bern-und-zuerich-aus-127340850
[10] http://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner
[11] http://www.schweizamsonntag.ch/ressort/nachrichten/schweizer_ex-spitzendiplomat_von_britischen_spionen_abgehoert/

Ein Jahr später arbeitet die Rundschau den Fall nochmals auf[12]:

Erst auf Nachfrage orientierte der NDB Nicolas Imboden über das Resultat der Untersuchung: «Nach einer gründlichen Analyse stellten unsere Experten fest, dass Ihre Computer nicht mit aktiven Spähprogrammen infiziert sind. Das ist eine gute Nachricht, aber es schliesst leider nicht vollständig aus, dass sensible Daten abhanden gekommen sind.»

Und weiter: Die Politik in Bern hüllt sich in Schweigen über die Aktivitäten der NSA in der Schweiz. Paul Niederberger, Präsident der Geschäftsprüfungsdelegation und Nidwaldner CVP-Ständerat, erfährt erst durch die Rundschau-Recherchen vom Fall Imboden – und gibt keinen Kommentar dazu ab: «Die Frage ist: Was ist der Mehrnutzen, wenn man mehr Informationen bekäme. Es würde gar nicht viel mehr bringen, als was man bisher schon weiss.» […] Doch hat der Sicherheitsausschuss der Landesregierung in einem geheimen Beschluss die Akte Snowden anschliessend beiseite gelegt? Dies behauptet ein Insider. Es werde nicht untersucht, was die NSA gegenwärtig in der Schweiz mache. GPDel-Präsident Niederberger kann sich nicht an einen solchen Beschluss erinnern: «Wir erhalten so viele Akten, ich kann nicht sagen, ob wir das tatsächlich sahen oder nicht.»

## 2.4 Überwachung des Bankensektors

In einem Interview mit dem Tages-Anzeiger im Mai 2014 erklärt Glenn Greenwald: «US-Dienste zeigen – unter anderem – grosses Interesse an Banking und Geldflüssen. […] Es gibt Hinweise in den Dokumenten, dass die NSA das Schweizer Bankensystem ausspioniert. Erst muss man diese Unterlagen genauer auswerten.»[13]

## 2.5 Betroffenheit

Nicolas Imboden sieht seine Rolle als eher unbedeutend – und ist entsprechend überrascht, dass selbst er durch die NSA und GCHQ überwacht worden ist. Klar wird an seinem Beispiel auch, dass diese Geheimdienste zum Vorteil der Wirtschaft und nicht ausschliesslich aus Sicherheitsüberlegungen bespitzeln.

Auch die Überwachung aus den diplomatischen Vertretungen dient wirtschaftlichen oder politischen Zielen, während eine Gefahr durch Terroristen nicht erkennbar ist. Dasselbe gilt für den Bankensektor. Dass diesem Hinweis bis jetzt nicht weiter nachgegangen worden ist, erstaunt. Scheint doch neben der Kundschaft auch ein kompletter Wirtschaftszweig betroffen.

[12] http://www.srf.ch/news/schweiz/schnueffelt-die-nsa-aus-wirtschaftsinteressen-in-der-schweiz/

[13] http://www.tagesanzeiger.ch/ausland/amerika/Es-gibt-Hinweise-dass-die-NSA-die-Schweizer-Banken-ausspioniert/story/17225003

Für die Öffentlichkeit ist die Tätigkeit der Signalhorn AG aktuell unklar. Falls von Schweizer Territorium aus Kommunikation überwacht würde, wäre dies grundsätzlich eine strafbare Handlung:

- Verbotene Handlung für einen fremden Staat (Art. 271 StGB)
- Verbotener politischer Nachrichtendienst (Art. 272 StGB)
- Verbotener wirtschaftlicher Nachrichtendienst (Art. 273 StGB)
- Verbotener militärischer Nachrichtendienst (Art. 274 und 301 StGB)

# 3 Zugriffspunkte auf Datenkommunikation in der Schweiz

Tempora war eines der ersten Spionage-Prorgramme, das aus den Snowden-Dokumenten bekannt wurde. Dieses wird vom britischen Geheimdienst GCHQ betrieben und zapft die Kommunikation an, welche über Glaskabelverbindungen übertragen wird.

Im August 2013 hat die Süddeutsche Zeitung die Namen der Firmen und Programme bekannt gemacht, die mit den britischen Behörden kooperieren: Verizon Business (Programm «Dacron»), British Telecommunications («Remedy»), Vodafone Cable («Gerontic»), Global Crossing («Pinnage»), Level 3 («Little»), Viatel («Vitreous») und Interoute («Streetcar»).[14]

Einige dieser Firmen sind auch in der Schweiz tätig und bieten ihre Dienste lokaler Kundschaft an.

British Telecom etwa brüstet sich: «About 40 of Switzerland's top 100 companies rely on solutions from BT Global Services. Customers include: Credit Suisse, Novartis, UBS, Nestlé, Syngenta, Bank Julius Bär, SixGroup, Swatch, Glencore, Tetrapak, Clariant, UN, Triumph, Kuoni – to name only a few.»[15]

Verizon Business ist gar eine strategische Partnerschaft mit Swisscom eingegangen: «International tätige Geschäftskunden von Swisscom erhalten nahtlosen Zugang zum umfassenden globalen Netzwerk und zu den Lösungen von Verizon Business.»[16]

In Deutschland will die Bundesregierung die Verträge mit Verizon nicht erneuern. Auch die Schweiz hat Geschäftsbeziehungen zum Telekommunikationsunternehmen: Der Bund verlässt sich für die Kommunikation mit Botschaften und Konsulaten im Ausland auf die Dienste von Verizon. Das Bundesamt für Informatik und Telekommunikation (BIT) wiegelt dennoch ab: «Die Endgeräte und die Verschlüsselung werden durch das BIT bereitgestellt.»[17]

Auch Level3 spricht Schweizer Kundschaft an[18] und führt mehrere redundante Glasfaserverbindungen[19] durch die Schweiz. Genauso sind auch Interroute[20] und Viatel[21] vertreten.

[14] http://www.sueddeutsche.de/digital/internet-ueberwachung-snowden-enthuellt-namen-der-spaehenden-telekomfirmen-1.1736791
[15] https://www.globalservices.bt.com/hu/en/location/switzerland
[16] http://www.swisscom.ch/de/about/medien/press-releases/2008/05/20080528_01_Verizon.html
[17] http://www.schweizamsonntag.ch/ressort/nachrichten/auch_der_bund_ist_kunde_von_verizon/
[18] http://www.level3.com/en/global-reach/europe/switzerland/
[19] http://maps.level3.com/default/
[20] http://www.interoute.ch/de/wholesale
[21] http://www.viatel.com/media/35228/all_viatel_metro_maps.pdf

Die Weltwoche hat den oben erwähnten Artikel aus der Süddeutschen Zeitung aufgegriffen – und über die Lecks in der Schweiz berichtet[22]. Der Autor bringt dabei noch einen weiteren globalen Konzern zur Sprache: «Unter den US-Firmen mit Ableger in der Schweiz verfügt namentlich Equinix über eine herausragende Position. Equinix ist ein Gigant im globalen Datennetzwerk. [...] Weltweit verfügt die Firma über 99 Standorte. In der Schweiz sind es sieben, zwei in Genf und fünf in Zürich. In einem Zürcher Equinix-Datencenter wird auch der Server für den Aktienhandel der Schweizer Börse Six Swiss Exchange betrieben, wodurch diese zur schnellsten Börse der Welt aufgestiegen ist.»

Zudem betreibt Equinix einen der drei grossen Internet-Knotenpunkte in der Schweiz. «Eine der weltweit grössten Firmen, die durch die US-Regierung einfach ansprechbar ist – da ist praktisch garantiert, dass sie dazu angehalten wird, abzuhören», sagt ein IT-Experte, der über langjährige Berufserfahrung in und mit amerikanischen IT-Firmen verfügt, im selben Weltwoche-Artikel.

Ein Jahr später – im Sommer 2014 – setzt sich die Erkenntnis auch beim Bund an entscheidenden Stellen durch: Als Reaktion auf den US-Geheimdienstskandal will das Bundesamt für Bauten und Logistik (BBL) der Cablecom keine Aufträge mehr erteilen. Wie «Der Bund» schreibt[23], ist die Cablecom zwar rechtlich gesehen ein inländisches Unternehmen, eine GmbH mit Sitz in Zürich. Damit untersteht sie Schweizer Recht. Sie ist aber eine Tochter des britischen (früher US-amerikanischen) Konzerns Liberty Global und deshalb ausländisch beherrscht.

## 3.1 Betroffenheit

Personen, Unternehmungen und Behörden in der Schweiz sind mehrfach betroffen. Ob als Bankkunde (CS, UBS, SixGroup), Bezügerin von Internetzugang von Swisscom oder UPC Cablecom, Benutzer von überregionalen Datenverbindungen (zur Recherche, für das Online-Shopping, Kommunikation etc.) – die Zugriffsmöglichkeiten auf die Datenkommunikation in der Schweiz und aus der Schweiz sind kaum zu überblicken und geschehen über Firmen, die (auch) britischem oder US-amerikanischem Recht unterstehen. Entsprechende Spionagetätigkeiten müssten aber dennoch verfolgt und wirkungsvoll unterbunden werden (können). Es gehört eigentlich zu den Pflichten der Schweizer Behörden, in der Schweiz geltendes Recht durchzusetzen.

[22] http://www.weltwoche.ch/ausgaben/2013-34/spionage-wo-sind-die-lecks-im-schweizer-datenbunker-die-weltwoche-ausgabe-342013.html

[23] http://www.derbund.ch/schweiz/standard/Bund-traut-der-Cablecom-nach-NSAAffaere-nicht-mehr/story/30526870

# 4 Zugriffsmöglichkeiten auf Schweizer Datenkommunikation im Ausland

Moderne Smartphones sind beinahe permanent mit dem Internet und dem Hersteller verbunden. Dabei werden lokale Daten, wie Adressen, E-Mails, Fotos und Dokumente, in «die Cloud» synchronisiert, um von anderen Geräten darauf zuzugreifen oder sie als Backup zu sichern. Auch viele Apps senden als «Gegenleistung» zur kostenlosen Nutzung Adress- und Positionsdaten (GPS) zurück an die Entwickler. Den meisten BenutzerInnen sind diese Vorgänge nur vage bewusst.

Privatpersonen, Schulen[24], KMUs und auch Grossfirmen setzen zudem vermehrt auf Cloudservices. Anstatt lokal auf den eigenen Computer oder Servern installierte Programme werden Online-Dienste, wie Gmail, Office365, Salesforce etc. verwendet. Dabei geht meist vergessen, dass Anbieterinnen mit Sitz in den USA (und auch anderswo) gezwungen sind, mit den lokalen Behörden zusammenzuarbeiten. So hat bspw. der USA PATRIOT Act u.a. den Weg für das Prism-Programm gelegt. Dokumentiert ist, dass Microsoft, Yahoo, Google, Facebook, AOL und Apple gezwungen sind, der NSA und dem FBI Zugang zu laufender Kommunikation und sämtlichen gespeicherten Informationen zu verschaffen[25]. Diese Zugänge werden nicht etwa bei konkretem Verdacht auf eine Straftat verwendet. Sie werden vielmehr dazu benutzt, um die komplette Kommunikation in eigene Rechenzentren weiterzuleiten und die Daten für die Analyse aufzubereiten.[26]

In Grossbritannien hat sich parallel dazu die staatliche GCHQ zu mehr als 200 internationalen Glasfaserkabeln Zugang verschafft. Bereits 2012 konnte das Datenverarbeitungssystem des Geheimdienstes 600 Millionen «Telefon-Ereignisse» pro Tag verarbeiten. Im Rahmen dieses als Tempora bekannten Programms werden aber hauptsächlich Datenverbindungen abgehört – und deren Inhalte für 3 Tage und Metadaten sogar für 30 Tage gespeichert.[27] [28]

An einem einzigen der unzähligen Zugriffspunkte der GCHQ konnten 2008 in unter 10 Minuten ungefähr 70'000 E-Mails abgefangen werden. Bekannt ist, dass u.a. Nachrichten von BBC, Reuters, Guardian, New York Times, Le Monde, Sun, NBC und der Washington Post ausgesondert wurden. Investigative Journalisten werden vom Geheimdienst dann auch – gleich neben Terroristen und Hacker – als Gefahr eingestuft.[29]

[24] http://www.itreseller.ch/Artikel/75129/Microsoft_passt_Office-365-Bedingungen_Schweizer_Schulen_an.html
[25] https://de.wikipedia.org/wiki/USA_PATRIOT_Act
[26] https://de.wikipedia.org/wiki/PRISM
[27] http://www.taz.de/!118582/
[28] http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa
[29] http://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post

Von den 16 Unterseekabeln, welche die USA und Europa verbinden, führen nur gerade fünf Verbindung nicht über England. Vier davon sind Teil eines Rings oder eines Ausfallpaares, mit wiederum mindestens einem Andockpunkt in England. Es ist also praktisch unmöglich, an der GCHQ vorbei transatlantisch zu kommunizieren.[30]

In der Schweiz vermittelt das Safe Harbor-Abkommen mit den USA eine falsche Sicherheit: Da diese kein mit der Schweiz vergleichbares Datenschutzniveau besitzen, hat das Staatssekretariat für Wirtschaft (SECO) gemeinsam mit dem Eidgenössischen Datenschutzbeauftragten (EDÖB) und mit den USA dieses Regelwerk ausgearbeitet. Es bescheinigt, den darunter zertifizierten Unternehmen, ein ausreichendes Datenschutzniveau[31]. Auf der Liste der selbstzertifizierten Unternehmen sind weit über 3'000 Firmen[32] geführt, darunter Adobe, Amazon, Apple, Cisco, Dropbox, Evernote, Facebook, Google, Microsoft, SWIFT, Vodafone, Yahoo und Verint. Nicht dabei scheinen Level3 und UPS zu sein.

Das Safe Harbor-Abkommen steht jedoch nicht im direkten Widerspruch mit dem Patriot Act, da es entsprechende Ausnahmen für «national security, public interest, or law enforcement requirements» vorsieht[33]. Es verletzt hingegen Grundsätze des schweizerischen Datenschutzes.

Man könnte – und müsste – daher den räumlichen Anwendungsbereich des Datenschutzgesetzes anders auslegen: Eine global tätige Firma, die sich mit ihrem Angebot explizit auch an eine Kundschaft aus der Schweiz richtet (und sogar eine lokale Niederlassung hat), müsste sich an lokale Gesetze halten. Wie eine ausländische Fahrzeugmarke hiesige Abgasnormen zu erfüllen hat, müssten Internetdienstleister lokale Datenschutzbestimmungen befolgen. Der Europäische Gerichtshof hat in seinem Urteil zum «Recht auf Vergessenwerden» bereits festgehalten, dass die lokale Gesetzgebung derart anzuwenden ist[34].

Prism, Tempora und Safe Harbor sind nur drei Stichworte, die den Widerspruch zwischen «Staatsschutz» auf der einen und dem Recht auf Privatsphäre, dem Recht auf freie Meinungsäusserung, dem Schutz des Fernmeldegeheimnisses und des Redaktionsgeheimnisses auf der anderen Seite, aufzeigen. Einige weitere wären:

[30] http://www.submarinecablemap.com/
[31] http://www.edoeb.admin.ch/datenschutz/00626/00753/00970/index.html?lang=de
[32] https://safeharbor.export.gov/swisslist.aspx
[33] http://export.gov/safeharbor/swiss/eg_main_018500.asp
[34] http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1

- Neben XKeyscore[35] besteht mit ICREACH[36] eine zweite «Google-ähnliche» Suchmaschine, mit der zwei Dutzend Organisationen auf eine Billion Datensätze über Metadaten – und im Fall von XKeyscore auch auf Kommunikationsinhalte – zugreifen können.
- Die NSA scheint hunderttausende von Computern mit Malware infiziert und übernommen zu haben – während sich die GCHQ dem staatlichen Telekommunikationsunternehmen Belgacom bemächtigt hat.[37]
- Der Bundesnachrichtendienst BND hat am Datenknotenpunkt der Deutschen Telekom in Frankfurt am Main Leitungen angezapft und dupliziert. Die daraus gewonnen Informationen wurden unter dem Codenamen Eikonal an die NSA weitergegeben[38].
- Mit Regin[39] dürfte eine hochgefährliche Malware in den Händen westlicher Geheimdienste sein. Und auch diese ist darauf angewiesen, dass Sicherheitslücken in den zu infizierenden Systemen bestehen (bleiben).
- Zusätzlich arbeitet die NSA mit Standardisierungsgremien (wie dem NIST) und mit Firmen (wie bspw. RSA) zusammen, um Verschlüsselungsstandards schwächer und damit Kommunikation abhörbar zu machen.[40]
- Die Positionsbestimmung eines Mobilfunkgerätes kann aus der Ferne problemlos und international über das SS7-Protokoll[41] bewerkstelligt werden.

Es ist kaum möglich, eine Übersicht zu allen Veröffentlichungen und Programmen der NSA und ihrer verbündeten Organisationen zu behalten. Umfangreiche und eindrückliche Liste führen Cryptome[42] und Wikipedia[43]. Klar scheint, dass sich die Geheimdienste der USA und von Grossbritannien schlicht jeder Kommunikation bemächtigen wollen. Kollateralschäden, wie der Vertrauensverlust in die eigene Computerindustrie, werden hingenommen und dem vermeintlichen Sicherheitsbedürfnis untergeordnet.

[35] http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data
[36] https://firstlook.org/theintercept/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/
[37] https://firstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions-computers-malware/
[38] http://www.zeit.de/politik/deutschland/2015-01/nsa-untersuchungsausschuss-bnd-telekom/komplettansicht
[39] http://www.theguardian.com/technology/2014/nov/24/regin-malware-western-surveillance-technology
[40] http://www.zeit.de/digital/datenschutz/2013-09/rsa-bsafe-kryptografie-nsa
[41] http://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html
[42] http://cryptome.org/2013/11/snowden-tally.htm
[43] https://en.wikipedia.org/wiki/Global_surveillance_disclosures_%282013%E2%80%93present%29

## 4.1 Betroffenheit

Da eine Vielzahl der Überseekommunikation per Glasfaser über England verläuft, sind BenutzerInnen aus der Schweiz gleich mehrfach von der Überwachung betroffen: NSA und FBI erhalten beim Cloud-Anbieter in den USA Zugang, und die britische GCHQ schöpft die Daten bei der Übertragung ab. Es ist aber auch davon auszugehen, dass andere Staaten ähnlich verfahren. Als Beispiel sei hier noch Frankreich aufgeführt[44]. Zudem betreibt die Schweiz mit der Funkaufklärung und zukünftig wohl auch mit der Kabelaufklärung ähnliche Programme[45].

Dass der Datentransfer in die USA (über England) durch das Safe Harbor-Abkommen ausdrücklich genehmigt ist, begünstigt einen unbedarften Umgang mit sensiblen Daten durch Privatpersonen und insbesondere auch durch Firmen in der Schweiz. Diese verarbeiten dadurch nicht nur eigene Geschäftsdaten in Übersee, sondern auch die ihnen direkt oder indirekt anvertrauten (fremden) Personendaten.

Viele Funktionen und Programme (Updates, Synchronisation, etc.) kommunizieren automatisch und unbemerkt über US-amerikanische Server. Deswegen sind unwillentlich praktisch alle von der Überwachung betroffen. Selbst wer auf ein Smartphone verzichtet, findet seine sensiblen Daten in fremden Händen wieder, da Fotoalbum, Adressbuch oder eine andere Datensammlung einer Drittperson diese übertragen hat.

Damit die Geheimdienste Malware einschleusen können, sind sie darauf angewiesen, dass Sicherheitslücken bestehen (bleiben). Aus diesem Grund kauft die NSA Sicherheitslücken auf und hortet sie – anstatt die betroffenen Softwarefirmen zu informieren und mitzuhelfen, dass sie behoben werden.

Auch die willentliche Schwächung von Sicherheitsstandards trägt dazu bei, dass Systeme unsicher werden: Nicht nur die eigene Behörde kann diese Lücken dann für die vermeintlich «gute Sache» verwenden. Sie können auch vom politischen oder wirtschaftlichen Gegner gefunden – oder sogar von (anderen) Kriminellen ausgenutzt – werden.

[44] http://www.sueddeutsche.de/politik/abhoerskandal-frankreich-soll-massenhaft-internet-kommunikation-ueberwachen-1.1713094
[45] https://www.woz.ch/1449/nachrichtendienstgesetz/die-nsa-laesst-gruessen

# 5 Zusammenarbeit von ausländischen Geheimdiensten mit dem Nachrichtendienst des Bundes (NDB)

## 5.1 Abkommen mit der NSA, resp. den USA

Im Oktober 2013 behauptet Bundesrat Ueli Maurer an einer Pressekonferenz[46]: «Wir haben keine Kontakte mit der NSA. Es werden und wurden keine Daten mit der NSA ausgetauscht.» Ein Jahr später tönt es gegenüber der «Rundschau» aus dem NDB etwas anders[47]: «Der Nachrichtendienst des Bundes tauscht mit der NSA keine Daten direkt aus. Es existiert kein Abkommen NDB-NSA. (...) Letzte Kontakte waren Ende 2012.» Dass verschiedene US-Dienste «Partner» der Schweiz sind und Informationen ausgetauscht werden, scheint hingegen hinreichend belegt und ist auch nicht bestritten[48].

Nach den Anschlägen in New York vom 11.9.2001 wurden zudem zwei Abkommen «Operative Working Arrangement» (OWA) zwischen der Schweiz und den USA ausgehandelt. Dabei soll es «nicht um nachrichten- oder geheimdienstliche Tätigkeiten» gehen, wie der damals verantwortliche Bundesrat Christoph Blocher im Ständerat beteuerte. Gegenüber dem Tages-Anzeiger wollte er sich im Herbst 2013 hingegen nicht dazu äussern, ob eine solche Zusammenarbeit ausserhalb des Vertragswerks besprochen worden sei. Weiter zitiert der Tages-Anzeiger aus einem Interview mit der «Schweiz am Sonntag»: «Es ist eindeutig, dass die Schweiz mit amerikanischen Nachrichtendiensten zusammenarbeitet. Ob die NSA auch dabei ist, kann ich nicht sagen. Ich halte es aber nicht für ausgeschlossen.»[49]

Aus den Unterlagen von Edward Snowden geht zudem hervor, dass die Schweiz als «Tier B»-Land eine «Focused Cooperation» mit den USA resp. der NSA eingegangen ist. Dies ist, unmittelbar nach der Gruppe der «Five-Eyes» (USA, UK, Kanada, Australien und Neuseeland), die zweithöchste Stufe der Zusammenarbeit und umfasst 17 europäische Länder sowie Japan und Südkorea.[50]

Der Bundesrat gibt sich in der Antwort auf ein Postulat von Nationalrat Jean Christophe Schwaab zugeknöpft und will – unter Verweis auf die als vertraulich oder geheim klassifizierten Informationen – nur der Geschäftsprüfungsdelegation berichten.[51]

[46] http://www.tageswoche.ch/de/147/schweiz/599597/
[47] http://www.srf.ch/news/schweiz/schnueffelt-die-nsa-aus-wirtschaftsinteressen-in-der-schweiz
[48] http://www.tagesanzeiger.ch/schweiz/Die-USA-warnten-die-Schweiz-vor-Terrorzelle/story/23581899
[49] http://www.tagesanzeiger.ch/schweiz/standard/Blocher-verhandelte-mit-ExNSAChef/story/26432753
[50] http://www.steigerlegal.ch/2013/10/30/nsa-schweizerisch-amerikanische-zusammenarbeit/
[51] http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134069

Das zuerst von El Mundo veröffentlichte Dokument legt jedoch nahe, dass es sich dabei um «Computer Network Operations» Missionen und somit wohl um das Ausspähen von Computernetzwerken handeln dürfte.[52]

## 5.2 Datenaustausch mit Partnerdiensten – und die Überwachung ausländischer Kommunikation

Wie Markus Seiler, Direktor des Nachrichtendienstes, der NZZ anvertraut[53]: «Nachrichtendienst bedeutet ein ständiges Geben und Nehmen. Die Schweiz verfügt über einen kleinen, aber feinen Dienst. Wir haben unseren Partnern im Ausland durchaus etwas zu geben.»

Selbst wenn jeder Dienst «nur» die ausländische Kommunikation abhören würde, die Erkenntnisse jedoch mit den Partnerdiensten teilt, so werden schlussendlich doch alle auch vom «eigenen» Geheimdienst bespitzelt.

Wie auch der Hohe Kommissar der Vereinten Nationen für Menschenrechte in einem Bericht festgehalten hat, ist daher eine Unterscheidung zwischen In- und Auslandsüberwachung nicht zulässig: «To conclude otherwise would not only undermine the universality and essence of the rights protected by international human rights law, but may also create structural incentives for States to outsource surveillance to each other.» («Zu einem anderen Schluss zu kommen, würde nicht nur die Allgemeingültigkeit und den grundlegenden Charakter der internationalen Menschenrechte untergraben, sondern auch strukturelle Anreize für Staaten schaffen, die Überwachung gegenseitig auszulagern.»)[54]

Die Informationen, welche der Schweizer Geheimdienst seinen Partnern bietet, dürften mehrheitlich aus dem Abhörsystem Onyx stammen. Das Programm beschrieb die Weltwoche 2005 detailliert: Ausgearbeitet hatte den Plan, von Zimmerwald aus weltweit die Telefon-, Fax- und Mailverbindungen zu überwachen, der militärische Geheimdienst [...]. Die Landesregierung [der Bundesrat] stimmte erstens dem Vorhaben [...] zu, segnete zweitens die versteckte, also illegale Finanzierung und drittens die totale Geheimhaltung ab. Der Entscheid vom 13. August 1997 fehlt sogar im hochvertraulichen Verzeichnis der Beschlüsse des Bundesrates. Ein Protokoll existiert offenbar auch nicht; an die Öffentlichkeit drang nichts.[55]

Mit Bezug auf den bereits im zweiten Kapitel zitierten GPDel-Bericht von 2003[56] hielt die Weltwoche weiter fest: Das Abhören eines Kommunikationsteilnehmers

[52] http://electrospaces.blogspot.de/2014/09/nsas-foreign-partnerships.html
[53] http://www.nzz.ch/schweiz/wir-haben-weltrekordverdaechtig-viele-kontrolleure-1.18427615
[54] http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx
[55] http://www.weltwoche.ch/ausgaben/2005-10/artikel-2005-10-was-sagen-sie-je.html
[56] http://www.admin.ch/opc/de/federal-gazette/2004/1499.pdf

im Ausland auf fremdem Hoheitsgebiet stehe im Widerspruch zur territorialen Souveränität dieses Landes. Es sei zumindest denkbar, dass ein Staat oder eine Privatperson den Europäischen Menschenrechtsgerichtshof, den Menschenrechtsausschuss der Uno oder den Internationalen Gerichtshof anrufe, um die Schweizer Behörden anzuklagen.

## 5.3 Betroffenheit

Durch die Zusammenarbeit der verschiedenen Geheimdienste ist die Schweizer Bevölkerung in mehrfacher Hinsicht von der Überwachung betroffen:

Der NDB spioniert die Kommunikation im Ausland aus, um Informationen zum «Tausch» anbieten zu können. Um an diese Information zu gelangen, müssen die ausländischen Dienste wiederum wertvolle Informationen für und somit über die Schweiz besitzen. Was also liegt näher, als die Kommunikation der Schweiz abzuhören, um an Tauschware zu gelangen.

Die Überwachung ist (wohl aus diesem Grund) auch nicht strikt auf das Ausland beschränkt, darf der NDB doch Informationen über Personen im Inland bearbeiten, wenn sie für das Verständnis eines Vorgangs im Ausland notwendig sind.[57]

Der Schweizer Nachrichtendienst und die Bundesanwaltschaft wären auch für die Spionageabwehr, resp. die Verfolgung von fremden Nachrichtendiensten, zuständig. Da sie aber auf Informationen der Partnerdienste angewiesen sind, befinden sie sich in einem Interessenkonflikt.

[57] http://www.admin.ch/opc/de/classified-compilation/20080697/index.html

# 6 Forderungen der Digitalen Gesellschaft an die Politik

Nach der Zusammenstellung der allgemeinen und universellen Betroffenheit sämtlicher Einwohnerinnen und Einwohner der Schweiz durch die Überwachung der Geheimdienste werden im folgenden sieben Forderungen an die Politik – und somit mögliche Auswege – aufgezeigt:

## 6.1 Aufnahme der Tätigkeit der «Expertenkommission zur Zukunft der Datenbearbeitung und Datensicherheit»

Bereits anfangs Juni 2014 hat das Parlament einer Motion von Ständerat Paul Rechsteiner zugestimmt, welche den Bundesrat beauftragt, eine «Expertenkommission zur Zukunft der Datenbearbeitung und Datensicherheit in der Schweiz» einzusetzen:

«Die Enthüllungen von Edward Snowden zeigen, dass die Grundannahmen, von denen auch in der Schweiz auf dem Gebiet der Datenbearbeitung und Datensicherheit ausgegangen wurde, nicht mehr zutreffen.»[58]

Es müssen daher folgende Fragen beantwortet werden:

- Wie sind die technologischen und politischen Entwicklungen auf dem Gebiet der Datenbearbeitung zu beurteilen?
- Was bedeuten diese Entwicklungen für die schweizerische Wirtschaft, die Gesellschaft und den Staat?
- Wie ist der gegenwärtige Rechtsrahmen mit Blick auf diese Entwicklung zu beurteilen?
- Welche Empfehlungen ergeben sich daraus für die Schweiz: Auf nationaler Ebene und mit Blick auf mögliche Initiativen auf internationaler Ebene?

Der Bundesrat hatte die Ablehnung des Begehrens empfohlen und scheint es nun mit der Einberufung nicht allzu eilig zu haben. Die Defizite sind jedoch offensichtlich. Der vorliegende Bericht der Digitalen Gesellschaft versucht einige davon aufzuzeigen. Der Bundesrat ist aufgefordert, die Expertenkommission schnellstmöglich einzusetzen und den Schlussfolgerungen Beachtung zu schenken.

[58] http://www.parlament.ch/D/Suche/Seiten/geschaefte.aspx?gesch_id=20133841

## 6.2 Strafermittlung durch einen ausserordentlichen Bundesanwalt

Die Schweizerische Bundesanwaltschaft hat es im Herbst 2014 abgelehnt, ein Strafverfahren gegen die NSA & Co. zu eröffnen[59]. Eine entsprechende Strafanzeige gegen Unbekannt – insbesondere wegen verbotenem Nachrichtendienst – hatte die Digitale Gesellschaft kurz nach den ersten Enthüllungen von Edward Snwoden eingereicht. In der Zwischenzeit sind neben den Überwachungsprogrammen Prism und Tempora dutzende weitere Anhaltspunkte hinzugekommen, und der vorliegende Bericht versucht einige davon für ein Strafverfahren zusammenzutragen.

Die Bundesanwaltschaft ist nochmals aufgefordert, entsprechende Ermittlungen aufzunehmen und die Verantwortlichen zur Rechenschaft zu ziehen. Der Bundesrat hat das hierzu erforderliche Gesuch der Bundesanwaltschaft zur Aufnahme der Strafverfolgung gutzuheissen.

Nicht nur der Nachrichtendienst des Bundes scheint auf Informationen von Partnerdiensten angewiesen zu sein, sondern auch die Bundesanwaltschaft[60]. Um den rechtsstaatlichen Interessenkonflikt aufzulösen, muss die Strafermittlung vom Parlament einem ausserordentlichen Bundesanwalt übertragen werden.

Für die Strafverfolgung, aber auch für die Arbeit der Expertenkommission, scheint eine Aufarbeitung der Snowden-Dokumente entscheidend. Um weitere und konkretere Bezüge zur Schweiz zu erhalten, bietet sich eine Befragung von Edward Snowden oder Glenn Greenwald an. Einem Schweizer Rechercheteam dürfte aber auch der geplante Datenraum in New York offenstehen[61].

## 6.3 Evaluation des Safe Harbor-Abkommens

Das Safe Harbor-Abkommen ermöglicht, dass personenbezogene Daten aus der Schweiz in den USA, resp. durch US-amerikanische Firmen, bearbeitet werden dürfen. Es bescheinigt den Unternehmen ein Datenschutzniveau, wie es dem Schweizer Datenschutzgesetz entspricht. Der beinahe uneingeschränkte Zugriff auf sämtliche Meta- und Inhaltsdaten durch verschiedene US-Behörden widerspricht jedoch unseren Grundsätzen des Datenschutzes. Dies betrifft insbesondere die Prinzipen der Verhältnismässigkeit und der Transparenz.

Daher ist durch den Eidgenössischen Datenschutzbeauftragten zu prüfen, ob durch das Safe Harbor-Abkommen das notwendige Datenschutzniveau erreicht

[59] https://www.digitale-gesellschaft.ch/2014/10/15/bundesanwaltschaft-kein-strafverfahren-gegen-nsa-co-in-der-schweiz/
[60] http://www.tagesanzeiger.ch/schweiz/standard/Schweizer-ISZelle-soll-Anschlag-in-Berlin-geplant-haben/story/31048224
[61] http://www.spiegel.de/netzwelt/netzpolitik/graceenwald-will-snowden-dokumente-zugaenglich-machen-a-1006370.html

werden kann. Falls die anlasslose Massenüberwachung nicht verhindert werden kann, ist das Abkommen auszusetzen.

## 6.4 Überarbeitung des Datenschutzgesetzes

Damit das Datenschutzgesetz angemessen wirkt, muss es durchgesetzt werden können. Hier zeigen sich einige Schwächen, die in der anstehenden Revision verbessert werden müssen. Stichworte dazu sind:

- Bei schwerwiegender und/oder vorsätzlicher Verletzung der Sorgfaltspflicht müssen griffige Strafbestimmungen mit empfindlichen finanziellen Drohungen vorgesehen sein. Bussen sollen sich dabei am Geschäftsumsatz der Unternehmungen orientieren. Die Verfolgung muss von Amtes wegen geschehen.
- Da ein Gang durch die Instanzen langwierig und die Gegnerschaft (internationale) Konzerne mit eigenen juristischen Abteilung sein können, soll ein Verbandsbeschwerderecht eingeführt werden.
- Der räumliche Anwendungsbereich des Gesetzes soll ausdrücklich auch ausländische Firmen mit Geschäftstätigkeit (resp. Kundschaft) in der Schweiz umfassen.

## 6.5 Einsatz für internationale Abkommen zur Achtung der Privatsphäre und deren Durchsetzung (UNO, EMRK, ...)

Um die anlasslose Massenüberwachung eindämmen zu können, sind internationale Abkommen zur Achtung der Privatsphäre und deren Durchsetzung nötig. Die Schweiz setzt sich dazu in den geeigneten Gremien – wie der UNO, dem Europarat oder einer neu zu gründenden Organisation – für entsprechende Verträge ein.

In einem solchen Abkommen sind insbesondere folgende Punkte festzuschreiben:

- Keine (anlasslose) Massenüberwachung
- Keine Unterscheidung in in- und ausländische Kommunikationsvorgänge
- Keine Pauschalentscheide und keine Geheimgerichte

Darüberhinaus setzt sich die Schweiz für ein Abkommen gegen Cyber-Angriffe und für eine «Genfer Konvention gegen den Cyberwar» ein[62].

[62] http://www.balthasar-glaettli.ch/2015/01/19/eine-genfer-konvention-gegen-den-cyberkrieg/

## 6.6 Förderung von technischen Mitteln zum Schutz der Privatsphäre

Neben Abkommen auf politischer Ebene sind auch technische Massnahmen ein wichtiges Instrument, um das Recht auf digitale Privatsphäre, die Meinungs- und Versammlungsfreiheit und den ungehinderten Informationszugang wieder vermehrt zu gewährleisten.

Die Schweiz muss daher entsprechende Entwicklungen von Hardware, Software und Standards fördern. Diese müssten/sollten mindestens folgendes umfassen:

- Einsatz für Forschung und transparente Standardisierung von Verschlüsselungsalgorithmen, verwandten Techniken und darauf aufbauenden Applikationen
- Einsatz für die Erarbeitung, Verabschiedung und Umsetzung von sicheren Internet-Standards (RFCs)
- Entwicklung von Datenschutz- und Datensicherheitsstandards für Unternehmen
- Förderung von Open Source Software – nicht nur für Verschlüsselung und Signatur
- Realisierung von Programmen zum Aufspüren noch unbekannter Sicherheitslücken und konsequente Behebung von bekannten Fehlern / Verpflichtung zur Offenlegung der Informationen, d.h. keine Verwendung für den «eigenen (Geheimdienst-)Gebrauch»

## 6.7 Trennung von zivilem und militärischem Nachrichtendienst & Verzicht auf Überwachung ohne begründeten Verdacht

Damit die Schweiz die offensichtlichsten Interessenkonflikte ausräumen und sich Spielraum für internationale Verhandlungen schaffen kann, sind folgende Hausaufgaben zu erledigen:

- Trennung von zivilem und militärischem Nachrichtendienst
  - Beschränkung des militärischen Nachrichtendienstes auf militärische Ziele
  - Beschränkung des zivilen Staatsschutzes auf Spionageabwehr
  - Dafür eine Stärkung der Bundesanwaltschaft zur Verfolgung von terroristischen Aktivitäten, organisierter Kriminalität, Proliferation, verbotenem Nachrichtendienst und deren Vorbereitungshandlungen

- Keine Überwachung ohne begründeten Verdacht
  - Abschaffung der Vorratsdatenspeicherung («rückwirkende Überwachung»)
  - Verzicht auf die «Kabelaufklärung»

Diese Anstrengungen stärken als wesentlichen Nebeneffekt auch den Standort Schweiz: Rechtssicherheit, glaubwürdiger und in sich konsistenter Datenschutz, verlässliche und starke Datensicherheit verschaffen der lokalen IT-Industrie das nötige Umfeld, um für Wohlstand im 21. Jahrhundert sorgen zu können.