Rechtsanwälte in Bürogemeinschaft

RECHTSANWÄLTE SCHULTZ & FÖRSTER

HANS-EBERHARD SCHULTZ
Notar a. D.

CLAUS FÖRSTER
Fachanwalt für Sozialrecht
Fachanwalt für Strafrecht

Rechtsanwalt Claus Förster · Greifswalder Str. 4 · 10405 Berlin

Generalbundesanwalt
Postfach 2720
76014 Karlsruhe

Haus der Demokratie und Menschenrechte
Greifswalder Str. 4
10405 Berlin
Telefon: 030 43725028
Fax: 030 43725027

per Fax: 0721 8191590

Mein Zeichen (bitte stets angeben):

**Liga für Menschenrechte,**
**CC, Digitalcourage u.a.**
**(NSA)**

Berlin, 16. Juli 2014
cf

Sehr geehrter Herr Bundesanwalt Dietrich, sehr geehrte Damen und Herren,

wir kommen zurück auf unsere Strafanzeige vom 03.02.2014, den Schriftsatz vom 08.04.2014 mit drei Ordnern Anschlusserklärungen von fünf Organisationen und mehr als 1.800 Einzelpersonen sowie die Schriftsätze vom 08.04.2014 und vom 05.06.2014 und die dazu geführten Telefonate.

Mit Schriftsatz vom 05.06.2014 hatten wir noch einmal ausdrücklich um die Übersendung der Entscheidung gebeten, wonach einerseits ein Ermittlungsverfahren im Zusammenhang mit der Ausspähung eines Mobiltelefons der Bundeskanzlerin eingeleitet werden soll, aber andererseits die von unseren Mandanten angezeigte massenhafte Erhebung von Telekommunikationsdaten „weiter unter Beobachtung“ bleiben soll.

*I.*

Bis heute – mehr als einen Monat später (!) – haben wir weder die Entscheidung noch irgendeine Begründung dafür erhalten, warum aufgrund der Strafanzeige hinsichtlich der Totalüberwachung der gesamten Bevölkerung keine Ermittlungen aufgenommen werden, sondern nur im Fall der Bundeskanzlerin.

Die bevollmächtigten Rechtsanwälte einer derartigen Strafanzeige, die die Öffentlichkeit nach wie vor im erheblichen Maße beschäftigt, können nur über eine Pressemitteilung eine im Grunde nichts sagende pauschale Erklärung dafür zur Kenntnis nehmen. Der Generalbundesanwalt hält es aber offenbar nicht für nötig, die betroffenen Anzeigeerstatter über ihre bevollmächtigten Rechtsanwälte zu informieren und die Begründung mitzuteilen. Wir halten dies nicht nur für eine Frage des Stils. Vielmehr besteht hierauf im demokratischen Rechtsstaat ein Anspruch. Bevor wir eine förmliche Dienstaufsichtsbeschwerde erheben, geben wir hiermit Gelegenheit, eine entsprechende Begründung

**spätestens bis zum 25.07.2014**

nachzuholen.

*II.*

Unabhängig hiervon ist das Ermittlungsverfahren jedenfalls aufgrund einer Reihe neuer, bisher nicht bekannter Umstände einzuleiten. Hierzu im Einzelnen:

1. Es ist jetzt bekannt geworden, dass einer der Anzeigeerstatter, der Chaos-Computer-Club e. V. konkretes Angriffsziel des NSA war.

a) Am 3. Juli 2014 berichtete das ARD-Magazin Panorama, wie der US-amerikanische Geheimdienst NSA gezielt versucht, Knotenpunkte des Netzwerkes Tor auszuspähen. Laut dem Bericht werden alle Verbindungen mit diesen Knotenpunkten markiert und die Kommunikationsdaten in einer speziellen Datenbank gespeichert. Der Artikel ist abrufbar unter der URL
http://daserste.ndr.de/panorama/archiv/2014/Quellcode-entschluesselt-Beweis-fuer-NSA-Spionage-in-Deutschland,nsa224.html. Wir überreichen einen Abdruck des Artikels als

**- Anlage 1 -**

b) Bei Tor (The Onion Router) handelt es sich um ein Softwareprojekt, welches ursprünglich von der US Navy ins Leben gerufen wurde, um unbeobachte Internet-

zugriffe für eigene oder verbündete Truppen bei Undercover-Einsätzen zu ermöglichen. Mittlerweile wird das Projekt von der US-amerikanischen Nicht-Regierungsorganisation Electronic Frontier Foundation (EFF) unterstützt.

Tor ist momentan die einzig verlässliche Methode, um aus repressiven Staaten wie etwa China, Burma oder dem Iran verschlüsselt und anonymisiert mit der westlichen Welt kommunizieren zu können.

Prof. Michael Waidner vom Fraunhofer-Institut für Sichere Informationstechnologie in Darmstadt beschreibt in seinem Gutachten für den NSA-Untersuchungsauschuss über den technischen Schutz vor Überwachung den Einsatz von Tor folgendermaßen (S. 2):

> *„Um neben den Inhalts- auch die Metadaten (Verbindungsdaten) zu schützen, müssen Anonymisierungsdienste wie ‚Tor' [...] eingesetzt werden. Prinzipiell können solche Dienste einen guten Beitrag zum Schutz gegen Massen- und Einzelüberwachung leisten."*

Das Gutachten ist abrufbar unter der URL
http://www.bundestag.de/blob/285122/2f815a7598a9a7e9b4162d70173ecedb/mat_a_sv-1-2-pdf-data.pdf . Wir überreichen die Seiten 1-3 als

**- Anlage 2 -**

Tor wird weiter von Organisationen wie Amnesty International, Human Rights Watch oder Reporter ohne Grenzen zur Nutzung empfohlen, insbesondere in repressiven Regimes. Auch während der Olympischen Spiele in Peking wurde Tor von vielen Journalisten genutzt, um die chinesische Zensur ihrer Berichterstattung umgehen zu können. Wir überreichen einen Ausdruck einer Pressemitteilung des Chaos Computer Clubs zu diesem Thema, abrufbar als unter der URL
http://www.ccc.de/de/updates/2008/chinesewall als

**- Anlage 3 -**

Weiter spielte Tor eine große Rolle beispielsweise bei den Protesten im Iran gegen die umstrittene Regierung Ahmadinedschad. Die Software wurde hier zum einen zur Koordinierung der Protestierenden untereinander verwendet, zum anderen gelang es via Tor, Bilder und Videos von der gewaltsamen Niederschlagung der Protestbewegung vorbei an der iranischen Internetzensur in international zugängliche Video-Portale wie Youtube zu laden. Wir überreichen einen Ausdruck eines Blogbeitrages über die Nutzung von Tor im Iran, abrufbar unter der URL
https://blog.torproject.org/blog/measuring-tor-and-iran als

**- Anlage 4 -**

Auch während der Krise in Ägypten im Jahr 2011 spielte Tor eine wichtige Rolle, um die Bevölkerung mit unabhängigen Nachrichten und Informationen zu versorgen. Die Betreiber von Tor registrierten über 120.000 Downloads der Software aus diesem Land. Wir überreichen einen Ausdruck eines Beitrag der Onlineausgabe der Zeitung „The Boston Globe“, abrufbar unter der URL
http://www.boston.com/news/world/africa/articles/2011/01/30/mass_groups_software_helps_avoid_censorship/ als

**- Anlage 5 -**

c) Der Chaos Computer Club (CCC) betreibt seit einigen Jahren mehrere Knotenpunkte des Tor-Netzwerkes und engagiert sich zudem bei der Unterstützung der Weiterentwicklung der Software.

**Beweis:** Michael Hirdes, Vorstandsvorsitzender des Chaos Computer Clubs, zu laden über Chaos Computer Club e. V., Humboldtstraße 53, 22083 Hamburg.

Überdies betreibt der CCC eine der weltweit neun so genannten Tor Directories. Diese spielen in dem Zusammenspiel einzelner Tor-Server und dem Funktionieren des Netzwerkes eine zentrale Rolle. Die Directories verwalten innerhalb des Tor-Netzwerkes Listen aller momentan in dem Netzwerk verbundenen Knotenpunkte. Jeder Knotenpunkt ruft deshalb in regelmäßigen Abständen die Listen anderer Knotenpunkte ab, um Pakete innerhalb des Netzwerkes an andere Teilnehmer weiterleiten zu können. Das Tor Directory des CCC befindet sich auf dem Host *dannenberg.ccc.de* mit der IP-Adresse

**193.23.244.244**.

d) Das ARD-Magazin Panorama hat zwischenzeitlich die algorithmisch implementierten Filterregeln von XKeyScore, auf den es in seinem Bericht Bezug genommen hat, veröffentlicht. Diese Filterregeln sind abrufbar unter der URL
http://daserste.ndr.de/panorama/xkeyscorerules100.txt. Wir überreichen einen Abdruck als

**- Anlage 6 -**

Bei XKeyScore handelt es sich um das Interface, mit dem die NSA auf gespeicherte Daten zugreift und diese sichtbar macht. Hierbei kann sowohl auf bereits erhobene Daten (beispielsweise aus den Programmen PRISM oder TEMPORA) zugegriffen werden als auch in die Zukunft gerichtete Suchanfragen gestellt werden. Bei in die Zukunft ge-

richteten Anfragen werden alle Daten, die durch Knotenpunkte oder Leitungen geleitet werden, auf die die NSA Zugriff hat, gesondert gespeichert, sofern diese auf die eingegebenen Suchkriterien passen. XKeyScore ermöglicht dann den Zugriff auf diese so erhobenen Informationen.

Die deutschen Nachrichtendienste BND und BfV haben Zugriff auf XKeyScore, wie der Bundestagsdrucksache 17/14560 vom 14. August 2013 als Antwort auf eine parlamentarische Anfrage der SPD-Bundestagsfraktion zu entnehmen ist. Davon haben die Geheimdienste ihre jeweiligen Kontrollgremien im Bundestag in Kenntnis gesetzt. Die Unterrichtung der G10-Kommission erfolgte am 29. August 2013, die des Parlamentarischen Kontrollgremiums war bereits am 16. Juli 2013 durch das BfV erfolgt. Auf den Seiten 20 bis 23 der angegebenen Bundestagsdrucksache sind einige Details der Nutzung von XKeyScore durch die deutschen Nachrichtendienste angegeben. Die Drucksache ist abrufbar unter der URL

http://dipbt.bundestag.de/doc/btd/17/145/1714560.pdf . Wir überreichen einen Abdruck als

**- Anlage 7 -**

Auch Zeitungen, unter anderem „Die Zeit“ vom 9. August 2014, berichteten, dass der BND Zugriff auf XKeyScore hat. Ein entsprechender Artikel ist abrufbar unter der URL

http://www.zeit.de/politik/deutschland/2013-08/bnd-xkeyscore-nsa.

Wir überreichen einen Abdruck als

**- Anlage 8 -**

Auf XKeyscore können berechtige Personen sowohl über ein komfortables Such-Interface als auch über eine sogenannte Skriptsprache zugreifen. Die von der ARD veröffentlichten algorithmischen Filterregeln sind in einer solchen Skriptsprache geschrieben und erlauben dadurch komplexe Suchanfragen. Für eine genaue Beschreibung, wie diese Filterregeln zu lesen sind, verweisen wir auf folgende URL

http://blog.erratasec.com/2014/07/reading-xkeyscore-rules-source.html?m=1 .

Wir überreichen einen Abdruck als

**- Anlage 9 -**

Glenn Greenwald, einer der Journalisten der die Dokumente von Edward Snowden auswertet, beschrieb gegenüber ABC News die Fähigkeiten von XKeyScore wie folgt:

> *„It searches that database and lets them listen to the calls or read the emails of everything that the NSA has stored, or look at the browsing histories or Google*

*search terms that you've entered, and it also alerts them to any further activity that people connected to that email address or that IP address do in the future."*

Der Bericht ist abrufbar unter der URL http://abcnews.go.com/blogs/politics/2013/07/glenn-greenwald-low-level-nsa-analysts-have-powerful-and-invasive-search-tool/ . Wir überreichen einen Abdruck als

**- Anlage 10 -**

Für eine genaue Beschreibung der Funktionsweise von XKeyScore regen wir weiter an, den ehemaligen Mitarbeiter der NSA, Herrn Edward Snowden, als Zeugen zu vernehmen.

**Beweis:** Edward Snowden, zu laden über seinen Rechtsanwalt Wolfgang Kaleck, Immanuelkirchstraße 3–4, 10405 Berlin.

e) Die IP-Adresse „193.23.244.244" des vom CCC betriebenen Tor Directories ist in den veröffentlichten algorithmisch implementierten Filterregeln aus Anlage 6 explizit aufgeführt. In den Unterlagen heißt es wörtlich:

*// START_DEFINITION*

*/**

*Global Variable for Tor foreign directory servers. Searching for potential Tor clients connecting to the Tor foreign directory servers on ports 80 and 443.*

**/*

*$tor_foreign_directory_ip = ip('193.23.244.244' or '194.109.206.212' or '86.59.21.38' or '213.115.239.118' or '212.112.245.170') and port ('80' or '443');*

Neben der Variable *$tor_foreign_directory_ip* wird im weiteren Verlauf der Filterregeln die Variable *$tor_fvey_directory_ip* definiert. Diese Variable enthält alle Tor Directory Server, die sich in den sogenannten „5 Eyes Countries" (USA, Großbritannien, Kanada, Australien und Neuseeland) befinden und somit besonderen Beschränkungen bei der Überwachung unterliegen. Es ist deshalb davon auszugehen, dass sich die Überwachung schwerpunktmäßig auf die in *$tor_foreign_directory_ip* genannten Server und somit auch auf den Server des Chaos Computer Clubs konzentriert.

Wie aus Anlage 6 weiter hervorgeht, werden die Variablen in Filterregeln benutzt, die es erlauben, aus den in Internet-Austauschpunkten anfallenden Datenmengen gezielt diesen vorab definierten gefilterten Teil des Netzwerkverkehr auszuleiten und einer spezifischeren Analyse zuzuführen. Deren Ergebnisse lassen sich effizient in kompakter Form

in Datenbanken speichern. Können diese Datenpunkte von einer Vielzahl von Rechenzentren gewonnen werden, entsteht ein globales Bild von den Nutzern des Tor-Netzwerks und deren Nutzungszeiten.
Da diese Filterregeln auch routinemäßig die Version des Protokolls archivieren, hat der Betreiber dieses Systems ein Bild, welche Versionen der Tor-Software auf den Computern der Benutzer installiert sind – mithin eine gängige Vorbereitung für automatisiertes Ausnutzen von für einen bestimmten Stand der Software bekannt gewordene Implementierungsfehler.

f) Beim XKeyScore-System (XKS) handelt es sich um ein von der NSA, vom britischen GCHQ und auch deutschen Diensten [XKS_BfV][1] genutztes komplexes Such-, Erfassungs- und Zielfindungssystem, welches mit einem großen Teil der von NSA und GCHQ erfassten Kommunikationsinhalte und -Metadaten arbeitet. XKS ist als eine verteilte Suchmaschine strukturiert, welche die von den Analysten erstellten Suchmuster-Programme zu den 150 Abhör-Standorten der "Five Eyes"-Dienste (Stand 2008) verteilt [XKS-Präs[2], Seite 6]. An diesen Standorten fließen die Daten der angezapften Leitungen durch spezielle Computer, auf denen die XKS-Suchmuster-Programme laufen und den durchlaufenden Datenverkehr kontinuierlich durchmustern und Verbindungen, auf die die Suchkriterien zutreffen, vollständig archivieren und dem Analysten zur Kenntnis bringen. Zusätzlich dazu gibt es noch für einige Tage vorgehaltenen Zwischenspeicher des gesamten Datenverkehrs (besipielsweise das britische TEMPORA-Programm), die ebenfalls automatisch nach neu erstellten Suchmustern durchforstet werden. Zweck dieser Zwischenspeicher ist es, dass neu hinzugekommene Suchmuster auf die Vergangenheit angewendet werden können, und zwar auf dem gesamten abgezapften Verkehr am jeweiligen Standort.

Das Vorhandensein einer IP-Adresse in den XKS-Suchmuster-Programmen bedeutet, dass jeder Verkehr von und zu dem Computer, zu dem diese IP-Adresse gehört – und gegebenenfalls weiteren Kriterien genügt –, mitgeschnitten und archiviert wird. Dies ist ein sehr starkes Indiz dafür, dass Internet-Kommunikation, die von und zu der IP-Adresse des CCC "193.23.244.244" geschieht, durch NSA und GCHQ abgehört und erfasst werden.

---

[1] http://www.spiegel.de/international/germany/german-intelligence-agencies-used-nsa-spying-program-a-912173.html
[2] http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation

Aus einer weiteren NSA-Präsentation aus dem Snowden-Fundus [XKS-Tor][3] ist bekannt, dass spezifisch Tor-Server das Ziel der Erfassung von XKS sind. Das Vorhandensein der IP-Adresse "193.23.244.244", also einen Tor-Servers, in den Suchmuster-Programmen ist daher konsistent und logisch.
Weiterhin ist XKS so konzipiert, dass anhand der Suchkriterien aufgefundene Zielcomputer automatisiert auf ihre Angreifbarkeit durch die "Tailored Access Operations" (TAO) der NSA hin klassifiziert werden. [XKS-Präs, Seite 28] Die TAO-Abteilung ist innerhalb der NSA zuständig für – zum großen Teil automatisiert ablaufende – Angriffe gegen Computer zum Zwecke der Zugangs- und Informationsgewinnung. Aus anderen Snowden-Dokumenten (etwa [XKS-QUANTUM][4]) ist weiterhin bekannt, dass XKS routinemäßig für die Vorbereitung von Computerspionage-Angriffen genutzt wird.
Das Vorhandensein eines XKS-Selektors ist somit ein Indiz dafür, dass ein TAO-Angriff auf den Server mit der IP-Adresse des CCC "193.23.244.244" vorbereitet bzw. die dafür notwendigen Informationen gesammelt wurden.

g) Die Tatsache, wie die IP-Adresse in den algorithmisch implementierten Filterregeln von XKeyScore aufgeführt ist, lässt im Zusammenhang mit dem Wissen über die Funktionsweise von XKeyScore den Schluss zu, dass dieser Server des CCC direkt und aktiv von der NSA mit geheimdienstlichen Mitteln ausgespäht wurde. Dies hatte oder hat das Ziel, ein konkretes Abbild *aller* Kommunikationsvorgänge auf dem Server des Chaos Computer Clubs zu erlangen.

2. Der investigative Journalist, Jurist und Verfassungsrechtler Glenn Greenwald hat in seinen kürzlich erschienen Buch „Die globale Überwachung – Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen“ u. a. aufgrund seiner umfassenden Kenntnis des Materials von Edward Snowden ausgeführt:

> *„Alles in allem legt das Snowdenarchiv einen letztlich simplen Schluss nah: Die amerikanische Regierung hatte ein System aufgebaut, dessen Ziel die vollständige Abschaffung der elektronischen Privatsphäre war, und zwar weltweit. Es ist keineswegs übertrieben zu sagen, das es das erklärte Ziel des Überwachungsstaats ist, sicherzustellen, dass jegliche elektronische Kommunikation von und zwischen Menschen rund um den Globus von der NSA erfasst, gespeichert, überwacht und analysiert wird. Der Nachrichtendienst sieht*

[3] https://www.documentcloud.org/documents/894406-nsa-slides-xkeyscore.html
[4] https://www.aclu.org/sites/default/files/assets/menwith-hill-station-leverages-xkeyscore-for.pdf

*sich auf einer einzigartigen, allumfassenden Mission zu verhindern, dass sich auch nur der kleinste Brocken elektronischer Kommunikation seinem systematischen Zugriff entzieht." (S. 143)*

Hierzu werde ein umfassendes weltweites Kooperationssystem mit den Geheimdiensten anderer Länder durchgeführt. Aus einem vertraulichen Dokument aus dem Jahre 2013 mit dem Titel „Übersicht ausländischer Partner" ergibt sich, dass Deutschland auf der Kooperationsebene B geführt wird (S. 180), und zur Behauptung der amerikanischen Regierung, ein großer Teil der durch Snowden aufgedeckten Überwachung betreffe die Sammlung von Metadaten, nicht von Inhalten (weil damit die Privatsphäre nicht oder zumindest weniger verletzt sei) führt er aus, dass dies unzutreffend sei. Nach Ansicht von Experten verschafft die Massensammlung von Daten dem Staat nicht nur Informationen über mehr Menschen, sie offenbart auch private Dinge, auf die er bislang keinen Zugriff hatte (S. 195). Darüber hinaus enthüllten Snowdens Dokumente auch Elemente von Wirtschaftsspionage: Die Auswertung von E-Mails und das Belauschen von Telefonaten des brasilianischen Ölgiganten Petrobras, von Wirtschaftskongressen in Lateinamerika, von Chemieunternehmen in Venezuela und Mexiko, das Ausspähen des brasilianischen Bergbau- und Energieministeriums sowie von Energieunternehmen in mehreren anderen Ländern durch NSA-Verbündete (S. 195); darüber hinaus enthüllten Dokumente die Spionage auf diplomatischer Ebene. Unter anderem wurden 2001 zwei Lateinamerikaner ins Visier genommen. Das Dokument enthielt sogar „Auszüge aus abgefangenen SMS-Nachrichten von und an Nieto" und einen „engen Mitarbeiter" (S. 201). Schließlich bekräftigt und belegt er:

*„Aber XKeyscore erlaubt einem Analysten, genau das zu tun, was Snowden sagte: jeden User zu beobachten und auch, seine Emails zu lesen. Ein Analyst kann mit dem Programm nach allen E-Mails suchen, bei denen bestimmte User in der CC-Spalte oder im Text auftauchen." (S. 226)*

Weiterhin führte er aus, genauso einfach wie die E-Mail-Durchsuchung sei die Abschöpfung sozialer Netzwerke (S. 228).

Eine Bestätigung der eingangs dargelegten Überwachung von Servern des Anonymisierungsnetzwerks Tor befindet sich bei Greenwald, wenn er schreibt:

*„Auf der Liste der verschiedenen Bedrohungen gegen die Vereinigten Staaten führt die NSA erwartbare Elemente auf – ‚Hacker', ‚kriminelle Elemente' und ‚Terroristen'." (S. 241)*

**Neues Beweismittel:** Sachverständigengutachten des Journalisten Glenn Greenwald.

3. In einem kürzlich veröffentlichten Spiegelinterview hat der ehemalige DDR-Offizier Klaus Eichner zur schon damaligen bestehenden Ausrichtung der NSA u. a. ausgeführt:

> *„Die Ohren der NSA waren grundsätzlich nicht nur in Richtung Osten aufgestellt. Die NSA arbeitete im Westberlin und der Bundesrepublik in allen Richtungen. Es wurden Dossiers über die Spitzenpolitiker –Wirtschaftsmanager der BRD geführt."*

**Beweis:** Spiegelinterview „Geheimdienste wollen alles wissen", Spiegel 25, 16.06.2014 (S. 24 f).

Auf eine Anfrage der Opposition teilte die Bundesrepublik mit, der BND führe zwar keine Statistik darüber, wie viele Verbindungsinformationen über Telefonate, Mails und Kurznachrichten (Metadaten) er an die amerikanischen Dienste weitergibt. „Alle Metadaten" aber, die von der NSA-Filiale in Bad Aibling erfasst würden, würden aber auch „verfügbar gemacht". Bestätigt wird weiter, dass sowohl 2012, als auch 2013 jeden Monat mehr als 3 Millionen so genannte Inhaltsdaten übermittelt wurden, also abgehörte Gespräche oder Nachrichten.

**Beweis:** Antwort der Bundesregierung (BT-Drucksache Nr. +++++++).

Nach intensiven Recherchen des Spiegel und Dokumenten aus dem Bestand Edward Snowdens, die die Redaktion einsehen konnte, „ist der Austausch von Daten, Spähwerkzeugen Know-How viel intensiver, als es selbst Experten bekannt war. Zur Kooperation zwischen den Geheimdiensten wird aus einem Dokument zitiert, einem am 28.04.2002 unterzeichneten sechseitigen „Memorandum of Aggreement", das als „streng geheim" gestempelt sei, verständigen sich beide Seiten auf „gemeinsame Spionagethemen und Ziele, wie die Bekämpfung von Terrorismus, organisierter Kriminalität und der Verbreitung von Massenvernichtungswaffen".

**Beweis:** Spiegel 25/16.06.2014 (S. 26 ff, 27/28).

Zwar dürften danach keine Deutschen und Amerikaner ausgeforscht werden, jedoch gibt es Ausnahmen im Falle „terroristischer Aktivitäten": Auch wenn sich im Nachhinein herausstellt, dass die abgefangenen Signale brisanten Inhalts von einem Deutschen

stammen, können sie verwendet werden, wenn Partner informiert wird und seine Zustimmung erteilt; das gleiche gelte, wenn sich die „Endpunkte“ der belauschten Kommunikation im anderen Land befänden.
In einem anderen Dokument, einem Protokoll über die Zusammenarbeit und BND heißt es, Snowden hätte die Überwachungsergebnisse aus Afganistan, die der „BND täglich mit uns teilt“ hervorgehoben (S. 30). Mehrfach lobe die Agency über die NSA die Deutschen für ihre „Führungsrolle“ und dass sie zusätzliche Überwachungsziele ins Visier genommen haben: nämlich neben den militärischen auch zivile (S. 30).

*III.*

*1. Strafbarkeit der Ausspähung der Server des Anzeigeerstatters zu 3.*

Die angezeigten Personen sind verdächtig, sich wegen der im Schriftsatz vom 03.02.2014 aufgeführten Delikte strafbar gemacht zu haben, indem sie daran mitwirkten, die Server des CCC direkt und aktiv von der NSA mit geheimdienstlichen Mitteln auszuspähen mit dem Ziel, ein konkretes Abbild *aller* Kommunikationsvorgänge auf dem Server des Chaos Computer Clubs zu erlangen.

a) Dies stellt ein massenhaftes Erfassen von in Deutschland entstandenen Kommunikationsdaten dar, dessen Strafbarkeit im Schriftsatz vom 03.02.2014 ausführlich dargelegt wurde. Die Strafbarkeit liegt auch dann vor, wenn die Bemühungen, ein konkretes Abbild aller Kommunikationsvorgänge auf dem Server des Anzeigeerstatters zu 3., nicht zum Ziel geführt haben sollten.

b) Für die Strafbarkeit wegen geheimdienstlicher Agententätigkeit gemäß § 99 I StGB gilt dies, weil die Ausübung der geheimdienstlichen Tätigkeit unabhängig von einem Taterfolg strafbar ist.

c) Bei der Strafvereitelung ist die Vollendung nicht vom Erfolg der Ausspähungsbemühungen abhängig, da die Vereitelung des staatlichen Strafanspruchs durch das Unterdrücken von Tatspuren, Ermittlungsakten und Beweismitteln auch dann besteht, wenn die gegen den Anzeigeerstatter zu 3. gerichteten Ausspähungsbemühungen ihr Ziel nicht erreicht haben sollten.

d) Hinsichtlich der Verletzung der Vertraulichkeit des Wortes ist den Verdächtigen zumindest Versuch vorzuwerfen.

Der Versuch dieser Straftat ist gemäß § 201 IV StGB strafbar.

Die Verdächtigen haben gemäß § 22 StGB zur Verwirklichung dieser Tatbestände unmittelbar angesetzt. Ein unmittelbares Ansetzen liegt bei Handlungen des Täters vor, die nach dem Tatplan der Verwirklichung eines Tatbestandsmerkmals unmittelbar vorgelagert und im Falle ungestörten Fortgangs ohne Zwischenakte in die Tatbestandshandlung unmittelbar einmünden sollen.[5] Diese liegen vor, da das Programm, das die Ausspähung aller Kommunikationsvorgänge auf dem Server des Anzeigeerstatters zu 3. in Betrieb genommen wurde und dieses Programm nach der Vorstellung der Verdächtigen dies ermöglichen sollte.

*2. Kein Rechtfertigungsgrund aufgrund des Artikel-10-Gesetzes*

In der Strafanzeige vom 03.02.2014 wurde dargelegt, dass die Verwirklichung der Straftatbestände, auf die sich der Tatverdacht erstreckt, nicht zu rechtfertigen ist, insbesondere auch nicht durch § 19 III des Bundesverfassungsschutzgesetzes (BVerfSchG) und die entsprechenden Normen für die anderen Dienste. Die Vorschriften des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Art.-10-Gesetz, G10G) scheiden ebenfalls als Rechtfertigungsgrund aus.

a) Zwar sind gemäß § 1 I Nr. 1 G10G die Verfassungsschutzbehörden des Bundes und der Länder, der MAD und BND zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes einschließlich der Sicherheit der Deutschland stationierten Truppen von NATO-Mitgliedern berechtigt, die Telekommunikation zu überwachen und aufzuzeichnen. Der BND darf zu diesem Zweck auch dem Brief- oder Postgeheimnis unterliegende Sendungen öffnen einsehen. Zudem darf der BND dies gemäß § 1 I Nr. 2 G10G i. V. m. § 1 II des Gesetzes über den Bundesnachrichtendienst (BNDG) auch zur Abwehr weiterer, im Gesetz beschriebener Gefahren die Telekommunikation überwachen und aufzeichnen.

b) Die in § 1 I Nr. 1, §§ 3 ff. G10G geregelten „Beschränkungen in Einzelfällen“ dürfen gemäß § 3 I G10G angeordnet werden, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand in eine Tat aus dem dort genannten Straftatenkatalog plant, begeht oder begangen hat oder wenn Anhaltspunkte für den Verdacht bestehen, dass jemand Mitglied einer Vereinigung ist, deren Zweck oder deren Tätigkeit darauf gerichtet ist, Straftaten zu begehen, die gegen die freiheitliche demokratische Grundordnung oder gegen den Bestand oder die Sicherheit des Staates gerichtet sind.

---

[5] Fischer, StGB, § 22 Rn. 10.

Eine Anordnung darf sich gemäß § 3 II 2 G10G nur gegen den Verdächtigen oder gegen Personen richten, bei denen aufgrund bestimmter Tatsachen eine Kommunikation mit dem Verdächtigen oder die Nutzung ihres Anschlusses durch den Verdächtigen zu vermuten ist.

Da die massenhafte Ausspähung von Daten nicht an konkreten Einzelfällen ansetzt, sondern wie dargelegt ohne die genannten konkreten Anhaltspunkte bei einer Vielzahl von Personen angewandt wird, ist davon auszugehen, dass bei den meisten der Ausgespähten keinerlei Bezug zu dem in § 3 I G10G beschriebenen Verdacht besteht.

Sie kann sich daher nicht auf eine rechtmäßige Anordnung gestützt werden.

c) Die massenhafte Übermittlung ausgespähter Daten an ausländische Nachrichtendienste kann auch nicht als „strategische Beschränkung“ gemäß § 1 I Nr. 2, §§ 5 ff. G10G gerechtfertigt werden.

Die ohne Bezug zu einem konkreten Sachverhalt erfolgende massenhafte Ausspähung von Daten ist nicht mit der an konkrete Sachverhalten, die in Bezug zu in einem Katalog aufgezählten Tatbeständen schwerwiegender Gefahren stehen müssen, orientierten Regelung des § 5 I 3 G10G vereinbar. Selbst wenn man hiervon absieht, dürften so erhobene Daten jedenfalls nur nach einer Einzelfallprüfung anhand der Kriterien des § 7a I 1 G10G und nur mit Zustimmung des Bundeskanzleramts an ausländische öffentliche Stellen übermittelt werden. Dabei sind gemäß § 7a I 1 G10G die schutzwürdigen Interessen in die Abwägung einzubeziehen. Das Schaffen der automatisierten Zugriffsmöglichkeit ausländischer Nachrichtendienste ohne Abstellen auf den Einzelfall ist hiermit unvereinbar.

d) Zunächst ist aber festzuhalten, dass alle im G10G geregelten Maßnahmen gemäß § 9 G10G nur auf schriftlichen Antrag des Behördenleiters des jeweiligen Dienstes oder seines Stellvertreters angeordnet werden dürfen. Zuständig ist für die Anordnung gemäß § 10 I G10G bei Anträgen der Verfassungsschutzbehörden der Länder die oberste Landesbehörde, im Übrigen das Bundesministerium des Innern. Die verantwortlichen Personen haben die Kenntnis und Mitwirkung der von ihnen geleiteten Stellen an der bedingungslosen Massenüberwachung und dem Austausch der dabei gewonnenen Daten mit den Nachrichtendiensten der USA und anderer Länder stets bestritten. Demnach hätte es auch keine Anordnung gemäß §§ 9, 10 G10G gegeben, die diese Maßnahmen gerechtfertigt hätte. Sollte es sie dennoch geben, sind die vorzunehmenden Ermittlungen auch auf sie zu richten. Wenn – wovon im Hinblick auf die nachstehend skizzierte

Rechtslage auszugehen sein wird – der Unterzeichner einer solchen Anordnung davon ausgehen musste, dass sie rechtswidrig war, stellt diese ein wichtiges Beweismittel im Verfahren gegen ihn dar.

Im Ergebnis ist eine Rechtfertigung der Tatbestandsverwirklichung durch die Verdächtigen aufgrund des G10G ausgeschlossen.

Die Verdächtigen handelten daher rechtswidrig.

*3. Sachverständigengutachten des Untersuchungsausschusses*

Die Sachverständigengutachten des Untersuchungsausschusses des Deutschen Bundestags zum NSA-Skandal bekräftigen die Ausführungen der Strafanzeige (S. 35 ff) zum verfassungsrechtlich gebotenen Schutz des Rechts des Einzelnen, unkontrolliert zu kommunizieren, als unverzichtbare Grundvoraussetzung in einer demokratischen Gesellschaft.

Die Gutachten bestätigen, dass der BND verfassungswidrig handelt, wenn er mit Daten arbeitet, die er von der NSA bezogen habe; zudem haben Grundrechte wie das Fernmeldegeheimnis auch im Ausland für Ausländer zu gelten. Deshalb sind auch die für NSA und BND gemeinsam betriebenen Auslandsaufklärungen nicht grundgesetzkonform, so die Sachverständigen Hans Jürgen Papier, ehemaliger Richter am Bundesverfassungsgericht, sowie die Professoren Wolfgang Hoffmann, Riem und Matthias Bäcker.

So hat der Staatsrechtslehrer und ehemaliger Richter des Bundesverfassungsgerichts Wolfgang Hoffmann-Riem in seinem Gutachten ausgeführt:

> *„Würde der BND als deutscher Hoheitsträger durch Anzapfen eines im extraterritorialen Gebiet verlegten Glasfaserkabels, eines dort stationierten Servers oder unter Inanspruchnahme eines dort tätigen Providers abhören, wäre dies nicht nur dann ein Eingriff in Art. 10 GG, wenn er sich auf einen in Deutschland oder von oder nach Deutschland erfolgenden Kommunikationsverkehr bezöge, sondern auch, wenn die Spähaktionen im Ausland erfolgen.*
>
> *Eine solche Maßnahme wäre nach dem BNDG insoweit rechtswidrig, als sie nicht zur Erfüllung der gesetzlichen Zwecke erfolgte, insbesondere nicht der „Gewinnung von Erkenntnissen über das Ausland“ diente (Art. 1 Abs. 2 S. 1 BNDG), oder wenn sie nicht den Anforderungen der in Art. 1 Abs. 2 S. 2 BNDG in Bezug genommenen Normen entspräche.“*[6]

Zur Weitergabe von Daten aus Spähaktionen führt Hoffmann-Riem dann weiter aus:

[6] Gutachten Hoffmann-Riem für den Untersuchungsausschuss des Deutschen Bundestags, S. 11 f.

*„Derartige Daten dürften in der Folge auch nicht an andere Stellen weitergegeben werden. Ohnehin unterliegt die Weitergabe von Daten durch den BND strengen Anforderungen. Ihm ist es - und dann auch nur mit Zustimmung des Bundeskanzleramtes unter engen Voraussetzungen - erlaubt, die von ihm zulässigerweise erhobenen Daten an ausländische Stellen zu übermitteln. Vorausgesetzt ist, dass dies zur Wahrung außen- oder sicherheitspolitischer Belange der Bundesrepublik Deutschland erforderlich ist (§ 9 Abs. 2 Satz 1 BNDG).*

*Es gibt noch weitere Normen über die Weitergabe von Daten. So erlaubt Art. 3 des Zusatzabkommens zum NATO-Vertrag die Weitergabe, soweit die Sicherheit von NATO-Truppen in Deutschland betroffen ist. Ferner dürfen bei gemeinsamen Truppeneinsätzen - wie sie etwa in Afghanistan erfolgt sind - Daten übermittelt und es dürfen Daten, die von verschiedenen Diensten erhoben wurden, unter bestimmten Voraussetzungen verbunden werden, so etwa mit dem Ziel, ein Bild über die Lage in bestimmten Gegenden der militärischen Einsatzgebiete zu erstellen. Solche Ermächtigungen aber sind begrenzt. So erlauben sie nicht die pauschale Übermittlung von (Roh-)Daten, auch nicht von Daten, bei denen der Bezug auf die tatbestandlichen Voraussetzungen der Datenübermittlung noch gar nicht festgestellt worden ist oder bei denen der Zweck ihrer Auswertung die Weitergabe nicht rechtfertigt. Die Rechtsbindungen der Weitergabe entfallen für den BND, der ohnehin nur Auslandsaufklärung betreiben darf, auch nicht etwa dann, wenn keine Daten deutscher Staatsbürger betroffen sind.“*[7]

Mit freundlichen Grüßen

Schultz
-Rechtsanwalt-

Förster
-Rechtsanwalt-

[7] a. a. O., S. 12 f.