FIELD OF FOCUS 4
SELF-REGULATION AND REGULATION
INDIVIDUALS AND ORGANISATIONS

UNIVERSITÄT
HEIDELBERG
ZUKUNFT
SEIT 1386

Journal of Self-Regulation and Regulation

Volume 01 (2015)

Im Netz der Geheimdienste – strafrechtliche Aspekte der Massenüberwachung im Internet

Kai Cornelius

Abstract

Die anlasslose Ausspähung der Allgemeinheit im Internet ist aufgrund der Bedrohungsszenarien durch den internationalen Terrorismus und unterstützt durch die rasante technologische Entwicklung in einem bislang unvorstellbaren Maße ausgeufert. Dieser Beitrag untersucht anhand von drei Szenarien mit einem Bezugspunkt zu Deutschland, ob diesbezüglich eine Strafverfolgung in Betracht kommt. Dies betrifft die Vorbereitung des Eindringens in informationstechnische Systeme (mit einem Szenario zu *Treasuremap*), das Eindringen selbst (mit einem Szenario zu *Regin*) und die strategische Telekommunikationsüberwachung des Bundesnachrichtendienstes (BND) mit einem Szenario zu *Eikonal*. Außerdem wird anhand dieser Ausführungen die Frage erörtert, ob das geltende Recht neu auszurichten ist. Dabei werden einerseits sicherheitspolitische Aspekte, aber andererseits auch der Schutz des Bürgers vor einer allumfassenden Überwachung in einem angemessenen Ausgleich berücksichtigt.

Keywords

Telekommunikationsüberwachung, Fernmeldegeheimnis, Strafbarkeit, Rechtfertigung, Verbotsirrtum

DOI: 10.11588/josar.2015.0.23482

Im Netz der Geheimdienste – strafrechtliche Aspekte der Massenüberwachung im Internet

Kai Cornelius

1 Einleitung

Wer regiert das Internet? Im November 2014 wurde die Aufdeckung der Spionagesoftware Regin gemeldet. Diese wurde im laufenden Betrieb analysiert. Damit können Daten kopiert, Tastatureingaben protokolliert, die Kamera eingeschaltet oder gleich die vollständige Kontrolle über den Rechner übernommen werden (vgl. Symantec 2014: 14–15). Wer über ein so mächtiges Werkzeug verfügt, dem kommt aufgrund der nahezu allumfassend anmutenden Wissensherrschaft eine unerhörte Macht zu (vgl. Boehme-Neßler 2014: 825 unter Verweis auf das Francis Bacon 1597 zugeschriebene „scientia est potenzia"). Dieser Drang nach Wissen ist nichts Besonderes: Seit es Menschen gibt, gibt es Geheimnisse. Und genauso lange gibt es Menschen, die hinter die Geheimnisse der anderen kommen möchten, sei es aus wirtschaftlichen, militärischen oder politischen Gründen (vgl. Kloepfer 2002: § 1 Rn. 55 zum Einsatz von Informationen als Herrschaftsmittel). Ein Mittel dafür ist die Spionage. Nicht wenige Forscher bezeichnen die Spionage als „zweitältestes Gewerbe der Welt" (vgl. Stürmer 2006: 21; Reinhard 2007: 234). Dabei stellt sich in einem demokratischen Rechtsstaat immer wieder die Frage der Kontrolle und Rechtskonformität des verdeckten Erlangens der Informationen.

Dem wird sich der nachfolgende Beitrag unter zwei Aspekten widmen – einerseits der Massenüberwachung im Internet durch Geheimdienste, bekannt geworden durch *Edward Snowden,* jedoch noch weitgehender, wie das Aufdecken von *Regin* zeigt.[1] Andererseits wird untersucht, wie sich das Strafrecht dazu verhält. Dabei wird folgender Struktur gefolgt: Nach einigen einleitenden Worten zum rechtstatsächlichen Hintergrund der Massenüberwachung werden die verfassungsrechtlichen Vorgaben zum Fernmeldegeheimnis dargestellt. Daran schließt sich der Hauptteil mit den strafrechtlichen Implikationen an, die von der Vorgehensweise von Hackern (mit einem Szenario zu *Treasuremap*) über das Eindringen in informationstechnische Systeme (mit einem Szenario zu *Regin*) bis zur strategischen Telekommunikationsüberwachung des Bundesnachrichtendienstes (BND) mit einem Szenario zu *Eikonal* (vgl. zu diesem Szenario Cornelius 2015a: 693ff.) untersucht werden. Ein abschließendes Fazit rundet den Bei-

1 Eine begriffliche Unterscheidung zwischen Nachrichtendiensten und Geheimdiensten soll hier nicht erfolgen, zumal sie bezüglich der inländischen Geheimdienste keine Stütze in der deutschen Rechtsordnung findet (ebenso Lampe 2015: 363).

trag ab. Dabei sei betont, dass die strafrechtsdogmatische Analyse anhand der hier vorgestellten Szenarien erfolgt, da wegen der ungesicherten Faktenlage endgültige Aussagen über die Strafbarkeit einer erfolgten Massenüberwachung nicht möglich sind. Allerdings ist es auf diese Weise möglich, jene Grenzen aufzuzeigen, bei deren Überschreiten eine Strafbarkeit von Mitarbeitern der Nachrichtendienste gegeben ist.

2 Fakten zur Massenüberwachung

Die Enthüllungen von *Edward Snowden* im Juni 2013 haben zu einer „Globalen Überwachungs- und Spionageaffäre“ geführt. *Snowden* hatte von 2009 bis 2013 auf Top-Secret-Dokumente der NSA zugegriffen, er kopierte etwa 1,7 Mio. Dateien und begann diese an ausgewählte Presseorgane zu versenden. Dadurch wurde ein weltweites Netz von Spionagesystemen durch die NSA, das GCHQ und engste Partner (Nachrichtendienste Neuseelands, Kanadas und Australiens – die *Five Eyes*) aufgedeckt (Zeit Online 2015). Nach Aussage *Snowdens* handele es sich um die „größte verdachtsunabhängige Überwachung in der Geschichte der Menschheit“, die einen schwerwiegenden Verstoß gegen Menschenrechte und Verfassungen darstelle. Die betroffenen Geheimdienste wehren sich mit dem Argument, dass die Aktivitäten zum „Kampf gegen den internationalen Terror“ notwendig seien. Als Rechtsgrundlagen für die Massenüberwachung waren im Gefolge des Anschlags auf das World-Trade-Center am 11. September 2001 in den USA der Patriot Act und in Großbritannien der Regulation of Investigatory Powers Act geschaffen worden.

2.1 Echelon

Allerdings ist die Tatsache einer umfassenden Überwachung von Telekommunikation nicht neu. So wurde bereits im Jahr 2001 durch das *Europäische Parlament* ein Bericht zur Existenz eines globalen Abhörsystems erstellt (vgl. Schmid 2001). Darin wurde festgestellt, dass „es auf der Grundlage der durch den Nichtständigen Ausschuss eingeholten Informationen keinen Zweifel mehr daran gibt, dass ein globales Abhörsystem existiert, das unter Beteiligung der Vereinigten Staaten, des Vereinigten Königreichs, Kanadas, Australiens und Neuseelands im Rahmen des UKUSA-Abkommens betrieben wird“ (vgl. ebd.: 18).[2] Außerdem wird angenommen, dass „das System, oder Teile davon, zumindest für einige Zeit, den Decknamen ‚ECHELON‘ trugen“ (vgl. ebd.: 14). Zum Zweck des Echelon-Systems wird darüber hinaus festgehalten, dass „nunmehr kein Zweifel mehr daran bestehen kann, dass das System nicht zum Abhören militärischer, sondern zumindest privater und wirtschaftlicher Kommunikation dient“, wobei es insbesondere auf dem „globalen Abhören von Satellitenkommunikation aufbaut“ (ebd.). In Gebieten mit „hoher Kommunikationsdichte“ werde die Kommunikation allerdings

2 Als UKUSA-Abkommen wird ein 1948 unterzeichnetes Abkommen zwischen Großbritannien (United Kingdom, UK), den Vereinigten Staaten (USA) sowie Australien, Kanada und Neuseeland bezeichnet (hierzu ausführlich Schmid 2001: 63 ff.).

nur zu einem kleinen Teil mittels Satelliten vermittelt und so könne „der überwiegende Teil der Kommunikation nicht durch Bodenstationen […], sondern nur durch Anzapfen von Kabeln und Abfangen von Funk“ geschehen, was jedoch wiederum nur in eng gesteckten Grenzen möglich sei (ebd.: 14, 33–34.). Zusammen mit dem erheblichen Personalaufwand, der für eine Auswertung der Daten erforderlich sei, kommt der Echelon-Abschlussbericht daher zum Ergebnis, dass die UKUSA-Staaten letztlich nur auf einen geringen Teil der kabel- und funkgebundenen Kommunikation Zugriff haben und darüber hinaus eine gründliche Auswertung aller gewonnenen Daten nicht machbar erscheine (ebd.: 14). Dieser Bericht lässt damit bereits Strukturen der globalen Überwachungs- und Spionageaffäre erkennen, und es wird deutlich, dass weniger das Sammeln der Daten als eine entsprechende Auswertung derselben das Problem war. Konsequenzen wurden aus diesem Bericht nicht gezogen. Vielmehr fiel er den Zeitläuften nach den Terroranschlägen auf das World-Trade-Center am 11. September 2001 in New York zum Opfer, die im Rahmen der Terrorabwehr zu einer erheblichen Ausweitung nachrichtendienstlicher Befugnisse führten (siehe auch den Beitrag von Beckedahl in diesem Band).

2.2 PRISM, X-Keyscore und Tempora

Für die umfassende Überwachung der elektronischen Kommunikation stehen solche Programme wie PRISM, Boundless Informant, Xkeyscore, Tempora Mail Isolation Control and Tracking, FAIRVIEW, Genie, Bullrun und CO-TRAVELER Analytics. Das wohl bekannteste Programm PRISM soll einen direkten Zugang zu zentralen Servern von Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, Apple und anderen führenden US-Internetfirmen gewähren (vgl. Computerwoche 2013a). Dennoch wird dieses Phänomen nachfolgend nicht weiter verfolgt werden. Denn nach dem in § 3 StGB niedergelegten Territorialitätsprinzip gilt das deutsche Strafrecht für alle Taten, die im Inland begangen werden. Den Tatort bestimmt das Ubiquitätsprinzip des § 9 Abs. 1 StGB. Danach begründen sowohl der Handlungs- als auch der Erfolgsort eine Strafbarkeit (Cornelius 2013a: Rn. 56; Ambos 2011: § 9 Rn. 1). Bei PRISM ist jedoch nicht bekannt, dass die entsprechenden Überwachungshandlungen in Deutschland vorgenommen wurden oder der Erfolg eines Datenzugriffs in Deutschland eingetreten ist. Da außerdem – das wird hier einmal unterstellt – keine Strafbarkeit nach US-Recht vorliegt, ist die Anwendbarkeit deutschen Strafrechts auch nicht gem. § 7 StGB möglich. Denn die Voraussetzung hierfür ist, dass die Tat am Tatort mit Strafe bedroht ist (ebd.). Eine Anwendbarkeit deutschen Strafrechts kommt damit nur nach § 5 Nr. 4 StGB für Straftaten des Landesverrats und der Gefährdung der äußeren Sicherheit (§§ 94 bis 100a StGB) und nach § 5 Nr. 7 StGB bei der Verletzung von Betriebs- oder Geschäftsgeheimnissen in Betracht. Da insoweit eine umfassende strafrechtliche Betrachtung wegen der stark eingeschränkten Anwendbarkeit deutschen Strafrechts nicht möglich ist, soll PRISM hier nicht weiter verfolgt werden. Denn dieser Beitrag beschäf-

tigt sich explizit mit der *Massenüberwachung*. Damit geht es nicht um solche speziellen Szenarien, bei denen die Ausspähung von Staatsgeheimnissen oder von Wirtschaftsgeheimnissen verwirklicht wird, sondern um die Ausspähung der Allgemeinheit.

Bei *X-Keyscore* scheint diese auf den ersten Blick stärker betroffen. Dieses Tool dient der Auswertung der Datenmenge, die im Kommunikationsverkehr (Telefon und Internet) abgeschöpft wird. Mittels *X-Keyscore* können die großen Datenmengen gefiltert und in Echtzeit analysiert werden (Computerwoche 2013b). Es wurde auch an das *Bundesamt für Verfassungsschutz* weitergegeben, damit dieses die NSA unterstützen konnte (vgl. Spiegel Online 2014d). Damit kommt in Betracht, dass ein Tatort für potentiell strafbare Handlungen in Deutschland liegen kann. Dennoch soll auch dies hier nicht weiter verfolgt werden, da die eigentliche Erhebung der Daten durch die Massenüberwachung einer Auswertung durch *X-Keyscore* vorgelagert ist.

Ferner soll Berichten zufolge das Spähprogramm *Tempora* den Zugang zu bis dato 200 Glasfaserkabeln ermöglichen, die von Großbritannien aus ins Meer führen. Hierbei kann eine Komplettdatenspeicherung von Kommunikationsinhalten (aus dem weltweiten Telefon- und Internet-Verkehr) von bis zu drei Tagen und eine Speicherung von Metadaten von bis zu 30 Tagen vorgenommen werden (vgl. Spiegel Online 2013). Da das Anzapfen in internationalen Gewässern erfolgt und damit der Tatort nicht in Deutschland liegt, gelten die bereits bei *PRISM* dargestellten Einschränkungen zur Anwendbarkeit deutschen Strafrechts, so dass auch *TEMPORA* nicht weiter verfolgt werden soll.

2.3 Treasuremap, Regin und Eikonal

In einer internen Präsentation der NSA zu *Treasuremap* wird der Einsatzbereich dieser Datenbank wie folgt beschrieben: „Kartografiert das gesamte Internet, jedes Gerät, überall, jederzeit“ (vgl. Spiegel Online 2014c). Diese Karte soll von den groben bis hin zu den feinsten Strukturen des Netzes möglichst alles abbilden. Sie enthält Informationen darüber, wie Netzwerke aufgebaut sind, wo ihre Engpässe und Schwachstellen liegen und wie man Daten unauffällig von A nach B bringt. Das betrifft nicht nur Netzverbindungsstellen, sondern auch Router und Informationen über einzelne Endgeräte, verschlüsselte private Netzwerke (VPN-Netze) und WLAN-Netzwerke (vgl. The New York Times 2013). Eine wichtige Datenquelle ist dabei die Ablaufverfolgung für das Versenden von Datenpaketen über das Internet (sogenannte Traceroutes). Dies bedeutet, dass wie bei einem „roten Faden“ der Weg abgebildet wird, den die Datenpakete von Rechner eins zu Rechner zwei inklusive aller Zwischenschritte, also der dabei durchquerten Netzwerk-Knotenpunkte, nehmen (vgl. Spiegel Online 2014c). Wegen dieser kartografischen Darstellung wird *Treasuremap* auch als das „Google Earth für das Internet“ bezeichnet (vgl. Süddeutsche Zeitung 2014c). Dabei scheint Deutschland eine besondere Rolle zu spielen: Nach einem Dokument aus dem Fundus von *Edward Snowden* besteht die Möglichkeit, dass sich die NSA Zugriff auch auf Netzwerke der

Deutschen Telekom und des Kölner Providers *Netcologne* verschafft hat. Beide Anbieter sind auf einer Karte wie *Treasuremap*, die Verknüpfungen zwischen den Netzwerken einzelner Provider darstellt, mit einem roten Punkt markiert. Einem weiteren Dokument zufolge soll dieser rote Punkt bedeuten, dass es in diesem Netzwerk einen „Sigint collection point" gibt (vgl. Spiegel Online 2014c). Dieser lässt sich mit einem Spionagewerkzeug wie dem eingangs beschriebenen *Regin* nutzen, um in die Systeme einzudringen und Informationen zu sammeln. Ob dies stimmt, kann derzeit nicht verifiziert werden. Nachträgliche Untersuchungen der *Deutschen Telekom* und von *NetCologne* konnten dies nicht bestätigen (vgl. Süddeutsche Zeitung 2014c). Allerdings war genügend Zeit für die NSA, etwaige Spuren zu verwischen. Da die Datenströme nicht in den Grenzen des Nationalstaates kanalisierbar sind (bzw. dies zumindest nicht erfolgt ist), kann das Abgreifen der notwendigen Daten vielleicht auch außerhalb Deutschlands erfolgt sein, so dass sich jedoch wieder die Frage nach der Anwendbarkeit des deutschen Strafrechts stellen würde.

Anders sieht es bei dem in Köln ansässigen Unternehmen *Stellar* aus. In einem GCHQ-Dokument zu *Treasuremap* fand sich eine Tabelle, die zeigte, welche Stellar–Kunden über welchen Satellitentransponder kommunizierten; nach dem Bekanntwerden der Malware *Regin* ist vorstellbar, dass diese Daten über einen Zugriff auf das Firmennetzwerk erlangt wurden. Bei *Stellar* handelt es sich um ein Teleportunternehmen, das entlegene Orte, wie Ölplattformen, via Satellit mit Internet versorgt. Da für die Kommunikation über Satellitentransponder keine Glasfaserleitungen genutzt werden, ist es vorstellbar, dass entsprechende Angriffe bei *Stellar* selbst, also auf deutschem Boden, ausgeführt worden sind, so dass die Anwendbarkeit deutschen Strafrechts kein Problem darstellt. Die Staatsanwaltschaft Köln hat folgerichtig auch ein Ermittlungsverfahren gegen Unbekannt wegen des Verdachts auf das Ausspähen von Daten (§ 202a StGB) eingeleitet (vgl. Spiegel Online 2014b).

Für die deutschen Behörden selbst ist jedoch die „Operation Eikonal" von höchster Brisanz. Bei dieser arbeiteten die NSA und der BND jahrelang zur Überwachung von Telekommunikationsdaten zusammen (Süddeutsche Zeitung 2014a). Zwischen 2004 und 2008 zapfte der BND einen der wichtigsten Kommunikationsknotenpunkte der Welt, DE–CIX, in Frankfurt an und gab die so gewonnenen Rohdaten an die NSA weiter. Zwar sollte die Telekommunikation deutscher Personen vorher herausgefiltert werden, jedoch funktionierte der vom *BND* eingesetzte Filter DAFIS nur unzulänglich: So konnten 2003 nur 95 % der übermittelten Daten von deutschen Rohdaten bereinigt werden (Süddeutsche Zeitung 2014b). Dabei bemerkte der *BND* im Rahmen der Operation, dass durch die NSA auch nach Daten von Firmen wie der EADS (jetzt *Airbus Group*), *Eurocopter* (jetzt *Airbus Helicopters*) sowie von französischen Behörden gesucht wurde (Süddeutsche Zeitung 2014a).

Für die Betrachtung der strafrechtlichen Implikationen der Massenüberwachung bieten sich Szenarien in Anlehnung an *Treasuremap* (als „Karte des Internets") (vgl. Spiegel Online 2014c), *Regin* als Spionagetool zum Eindringen in Systeme und insbe-

sondere *Eikonal* (Süddeutsche Zeitung 2014a) als Beispiel für die Durchführung der strategischen Telekommunikationsüberwachung an. Anhand von *Treasuremap* und *Regin* lässt sich das Vorgehen bei einem „Einbruch“ in ein informationstechnisches System darstellen und *Eikonal* ist ein Paradebeispiel für die Massenüberwachung. Der direkte Bezug zu Deutschland ist auch gegeben, so dass die Anwendbarkeit deutschen Strafrechts uneingeschränkt möglich ist. Es gibt also mehr als nur vage Anhaltspunkte, dass wir es in der Praxis mit einer Massenüberwachung zu tun haben. Nachfolgend werden zunächst der verfassungsrechtliche Rechtsrahmen (Fernmeldegeheimnis sowie Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme) im Hinblick auf eine Massenüberwachung der Telekommunikation durch Geheimdienste dargestellt. Anschließend wird anhand von Szenarien zu Treasuremap, Regin und Eikonal eine strafrechtliche Bewertung vorgenommen.

3 Rechtsrahmen der Massenüberwachung

3.1 Fernmeldegeheimnis

Das Fernmeldegeheimnis ist unverletzlich. So sagt es unsere Verfassung (Art. 10 Abs. 1 GG). Einfachgesetzlich geregelt ist dann, was alles unter das Fernmeldegeheimnis fällt. Nach § 88 Abs. 1 TKG sind dies der Inhalt der Telekommunikation und ihre näheren Umstände. Das bezieht auch die Beteiligung an einem Telekommunikationsvorgang ein. Ein Eingriff in das Fernmeldegeheimnis liegt damit vor, wenn die öffentliche Gewalt vom Inhalt und den Umständen der geschützten Kommunikation Kenntnis nimmt (BVerfGE 67, 157 (172); 100, 313 (358); 125, 260 (309); 130, 151 (179); Gärditz et al. 2014: 217, damit sind auch die Verbindungsdaten umfasst; Cornelius, Kai 2013b: 167).

Warum gibt es überhaupt einen Schutz des Fernmeldegeheimnisses? Dies hat das *Bundesverfassungsgericht* treffend mit der Feststellung auf den Punkt gebracht, dass der Meinungs- und Informationsaustausch mittels Telekommunikationsanlagen nicht deswegen unterbleiben oder nach Form und Inhalt anders verlaufen soll, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten und Kenntnisse über die Kommunikationsbeziehungen oder Kommunikationsinhalte gewinnen (BVerfG 30.4.2007: 2752). Dies erfordert die Möglichkeit eines „privaten, vor der Öffentlichkeit verborgenen Austausches von Informationen“, zumal wenn die Telekommunikationsverbindung „wegen der räumlichen Distanz zwischen den Beteiligten auf eine Übermittlung durch andere angewiesen ist und deshalb in besonderer Weise einen Zugriff Dritter – einschließlich staatlicher Stellen – ermöglicht“ (BVerfGE 115, 166 (182).

Da es beim Fernmeldegeheimnis damit um den Schutz und die näheren Umstände der Telekommunikation geht, ist jetzt noch die Frage zu beantworten, was darunter – bei normativer Betrachtung – zu verstehen ist. Nach § 3 Nr. 22 TKG ist Telekommunikation der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen. Diese sind wiederum technische Einrichtun-

gen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können (§ 3 Nr. 23 TKG). Dieses Herunterbrechen auf die technische Ebene bedeutet, dass jeder Dienst (jede Nachrichtenübermittlung), der diese technische Ebene (durch Kommunikationsanlagen) benutzt, davon erfasst und vom Fernmeldegeheimnis geschützt ist. Deshalb werden alle Formen der Nachrichtenübermittlung unter Überwindung des Raumes in nicht körperlicher Weise und mittels technischer Einrichtungen unter dem Begriff der Telekommunikation subsumiert (Schwabenbauer 2013: 57; Cornelius 2015a: 697). Das bezieht also nicht nur Telefon, Telefax und E-Mail ein, sondern auch SMS, MMS, Skype, WhatsApp, Internetkommunikation über Satellit etc. (Roggan 2012: § 1 Rn. 11; Cornelius 2015a: 697).

Dieses nach Abs. 1 des Art. 10 GG eigentlich unverletzliche Fernmeldegeheimnis kann nach dem Gesetzesvorbehalt des Art. 10 Abs. 2: 1 GG aufgrund eines „einfachen" Gesetzes eingeschränkt werden. Nun wurde bereits dargestellt, dass die Gewährleistung des Fernmeldegeheimnisses unverletzlich ist und dass dazu nicht nur der Inhalt der Kommunikation, sondern auch die Umstände des Zustandekommens (also die Metadaten) zählen. Allerdings ist nach Art. 10 Abs. 2: 2 GG ein heimlicher Eingriff nur für den Schutz der freiheitlich-demokratischen Grundordnung oder den Bestand bzw. die Sicherung des Bundes oder eines seiner Länder zulässig (Cornelius 2015a: 697). Genau um diese Gemengelage geht es bei der Frage der strafrechtlichen Bewertung der Massenüberwachung.

3.2 Vertraulichkeit und Integrität informationstechnischer Systeme

Neben dem Fernmeldegeheimnis ist das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) in seiner Ausprägung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07) berührt, wenn die Kommunikation durch den Zugriff auf ein Endgerät des Telekommunikationsteilnehmers überwacht wird und die Daten nicht nur auf der Übertragungsstrecke abgefangen werden (Cornelius 2015a: 697). Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen (BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07). Diese Vorgaben des *Bundesverfassungsgerichts* hat der Gesetzgeber bei den Regelungen des § 20k BKAG zu Online-Durchsuchungen[3] berücksichtigt. Diese sind danach bei Vorliegen einer *konkreten Gefahr* für die enumerativ aufgeführten Rechtsgüter Leib, Leben oder Freiheit einer Person oder Güter der Allgemeinheit, deren Bedro-

3 Unter einer Online-Durchsuchung wird der heimliche staatliche Zugriff auf Datenbestände des Zielrechners durch Einschleusen von Überwachungssoftware wie Trojanern oder Backdoor-Programmen verstanden (vgl. Beulke et al. 2007: 60, 64; Cornelius 2007: 798; Soiné 2012: 1585, 1586; Jahn et al. 2007: 58).

hung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt, zulässig. Eine konkrete Gefahr liegt nach der Rechtsprechung des *Bundesverfassungsgerichts* und des *Bundesverwaltungsgerichts* dann vor, wenn die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ein Schaden für ein betroffenes Rechtsgut eintreten wird (BVerwG 1970: 1892; BVerwG 1991). Diese Wahrscheinlichkeitsprognose muss auf Tatsachen basieren, die über vage Anhaltspunkte oder bloße Vermutungen ohne greifbaren, auf den Einzelfall bezogenen Anlass hinausgehen (BVerfGE 100, 313 (395); 120, 274 (328); Soiné 2012: 1586). Eine anlassunabhängige Massenüberwachung der Telekommunikation im Internet kann diesen hohen Vorgaben des *Bundesverfassungsgerichts* nicht genügen (Cornelius 2015a: 697).

Allerdings ist eine Besonderheit zu beachten: Wenn der Zugriff auf das Endgerät ausschließlich auf die Überwachung einer laufenden Telekommunikation beschränkt und dies durch entsprechende technische Vorkehrungen und rechtliche Vorgaben sichergestellt ist, dann muss die hoheitliche Maßnahme „nur" den Anforderungen des Fernmeldegeheimnisses (Art. 10 GG) genügen (BVerfGE 120, 274). Obwohl bei dieser Quellen-TKÜ[4] wegen der Infiltration des Endgerätes der Schutzbereich des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme eröffnet ist, sind solche Eingriffe damit nicht an den hohen Vorgaben des „IT-Grundrechts" zu messen (Buermeyer 2013: 473; Hoffmann-Riem 2008: 1021–1022.). Deshalb sollen die Vorgaben des „IT-Grundrechts" hier nicht weiter vertieft werden. Dafür spricht auch ein weiteres Argument: Wenn schon die Messlatte des Art. 10 GG mit seinen geringeren Vorgaben gerissen wird, dann gilt dies erst recht für die höheren Vorgaben des „IT-Grundrechts".[5]

4 Szenario zu Treasure Map

Da es in der Natur der Sache liegt, dass geheimdienstliche Tätigkeiten regelmäßig nicht bekannt sind, werden für die nachfolgende strafrechtliche Bewertung ausschließlich Szenarien als Modelle der Abfolge von möglichen Ereignissen zugrunde gelegt, ohne dass damit die Aussage verbunden ist, dass der Sachverhalt *tatsächlich* so gegeben ist. Das heißt, es wird nicht behauptet, dass die Sachlage so war, sondern nur, dass es sich *möglicherweise* so zugetragen haben könnte.

Das Szenario zu *Treasure Map* besteht darin, dass ein Projekt zu analysieren ist, das sich mit der Kartografierung des gesamten Internets beschäftigt. So können nachfol-

4 Als Quellen-TKÜ wird die behördliche Überwachung von verschlüsselter Telekommunikation „direkt an der Quelle" – also noch vor der Verschlüsselung – durch Infektion des verwendeten Endgerätes mit einem Trojaner bezeichnet (vgl. Buermeyer 2013: 470).

5 An dieser Stelle sei jedoch ausdrücklich klargestellt, dass damit nicht eine Stellungnahme des Autors verbunden ist, dass eine Quellen-TKÜ nach den Vorschriften für eine Telekommunikationsüberwachung zulässig ist. Hierfür ist es nämlich nach den skizzierten Anforderungen notwendig, dass ein entsprechendes Infiltrationstool auch technisch dahingehend „beschränkt" ist, dass nur die laufende Telekommunikation und nicht etwa auf dem Endgerät gespeicherte Inhalte ausgespäht werden (instruktiv hierzu Buermeyer: 2013: 470ff.).

gende Computerangriffe, Spionageaktionen aber auch die Verteidigung von Computernetzwerken besser geplant werden. Die zu beantwortende Frage lautet dahin, ob mit der Planung von Angriffen verbundene Handlungen strafbar sind, wenn auch Netzwerke in Deutschland von dieser Kartografierung betroffen sind. Da das strategisch verfolgte Ziel letztlich das unberechtigte Eindringen in Computer- oder Netzwerksysteme ist, bietet sich hierbei ein Vergleich mit der Vorgehensweise von Hackern an.

Denn unter „Hacken" wird das unberechtigte Eindringen in Computer- oder Netzwerksysteme verstanden. Die ursprünglichen Hacker haben ihre Fähigkeiten dazu genutzt, die Stärke und Integrität von Computersystemen zu testen und zu verbessern. Nach und nach hat es sich eingebürgert, den Begriff „Hacker" für Eindringlinge zu verwenden, die illegal auf Computer(systeme) zugreifen (Ernst 2003: 3233).

Der Hacker wird – ebenso wie dies regelmäßig ein Einbrecher macht, bevor er in ein Objekt eindringt – zunächst Erkundigungen über das anzugreifende System einziehen. Hierzu wird er die Netzwerkinfrastruktur durch Zusammenstellung leicht erhältlicher Informationen (wie die Namen von Personen/Rechnern/Domänen, IP-Adressen) auskundschaften, um eine Abbildung des zunächst vollkommen unbekannten Systems zu erhalten.

Diese Informationen kann er beispielsweise durch Whois-Abfragen, die Nutzung von Internet-Verzeichnissen (www.arin.net), die Untersuchung des HTML-Quelltextes von Webseiten einschließlich der entsprechenden Kommentare erhalten. Die Nutzung solcher öffentlich verfügbaren Informationen – auch wenn sie mit dem Ziel eines späteren rechtswidrigen Eindringens in ein fremdes System erfolgen – sind zunächst nur Vorbereitungshandlungen und nicht strafbar (zu den Quellen zur Informationssammlung: vgl. Hadagny 2011: 58ff.). Dies ist – um das Bild des Einbrechers aufzugreifen – mit einer Sondierung der Lage und der Umgebung eines Gebäudes vergleichbar, in welches später eingebrochen werden soll.

Kritischer wird es, wenn die Angriffsvorbereitungen in die nächste Phase treten und nicht nur öffentlich verfügbare Informationen abgefragt, sondern Reaktionen von aktiven Systemen provoziert werden. So werden beim *Network Mapping* ganze Adressbereiche angepingt, um festzustellen, welche Systeme erreichbar sind. Wenn ein System aktiv ist, gibt es auf die Ping-Anfrage ein Echo, so dass die sendende Person die Adresse erkennen kann. Die Namensauflösung selbst kann Hinweise auf die Einsatzbereiche geben. Auch dies ist zunächst nur eine straflose Vorbereitungshandlung und – um bei dem Bild mit dem Einbrecher zu bleiben – mit dem Ablesen der Namensschilder vergleichbar.

Sobald das Zielsystem identifiziert ist, geht es darum, die Schwachstellen dieses Systems zu erkennen, um einen Zugriff darauf zu erleichtern. Hierfür kann beispielsweise die Methode des *Port-Scannings*[6] oder des damit verwandten *OS Fingerprinting*[7]

6 Unter dem Port-Scanning wird der Identifizierungsprozess offener Ports auf einem oder mehreren Hosts verstanden (vgl. Singh et al. 2010: 222).

genutzt werden. Auch hierbei wird das System durch PING-Anfragen gescannt, um festzustellen, welche Ports[8] offen sind. Eine bestimmte Kombination von offenen Ports lässt darauf schließen, welche Applikationen beziehungsweise auch welches Betriebssystem laufen. Sobald dies bekannt ist, ist es in einem zweiten Schritt möglich, eine Schwachstellenanalyse durchzuführen[9] und die beste Form des Eindringens zu finden (Rinker 2002: 663). Diese Vorgehensweise ist noch nicht mit einem Eindringen in das System verbunden, so dass es an dem Tatbestandsmerkmal des Überwindens einer Zugangssicherung fehlt, um zu einer Strafbarkeit wegen des Ausspähens von Daten (§ 202a StGB) gelangen zu können.[10] Vielmehr handelt es sich um das Erlangen von Informationen an der Außengrenze eines Systems, die noch nicht geschützt sind (Heghmanns 2012: Teil 6.1 Rn. 32). Bei einem Einbrecher wäre dies vergleichbar mit dem Schauen durch ein Schlüsselloch oder dem Rütteln an der Haustür oder dem Kellerfenster, um zu überprüfen, ob diese offen sind (Rinker 2002: 665). Zwar soll es nach – umstrittener (ablehnend: Hillenkamp 2007: § 22 Rn. 28, 99, 103) – Rechtsprechung bereits für eine Versuchsstrafbarkeit ausreichen, wenn der Täter die Tauglichkeit einer Sache für einen im *unmittelbaren* zeitlichen Anschluss beabsichtigten strafbaren Angriff untersucht (BGHSt 22, 80). Allerdings kann dies hier dahinstehen, da nach dem Szenario zu *Treaseuremap* nur eine Karte für *spätere* Angriffe angefertigt werden soll. Selbst nach dieser extensiven Rechtsprechung wäre diese Handlung noch eine straflose Vorbereitungshandlung, auch wenn sie mit dem Ziel durchgeführt wird, genaue Angriffsvorbereitungen zu ermöglichen. Dies ist hier nicht weiter zu vertiefen, da für das Ausspähen von Daten schon keine Versuchsstrafbarkeit angeordnet ist.

5 Szenario zu Regin

Anders verhält es sich, wenn es tatsächlich zu einem Eindringen *in* ein Computersystem kommt – also zu einem Hackerangriff. Für die strafrechtliche Betrachtung wird wieder wegen der fehlenden Verifizierungsmöglichkeiten bezüglich des tatsächlichen Geschehens von einem Szenario ausgegangen: Die Kunden eines Teleportanbieter nutzen das Internet über Satellit. Die Server der Firma stehen in Köln und sind durch eine

7 Von *OS-Fingerprinting* ist die Rede, wenn man ein Zielsystem anhand seiner spezifischen Eigenschaften auf Protokollebene identifizieren möchte. Anhand von kleinen Abweichungen gegenüber den Standards und weiteren einzigartigen Merkmalen, kann unter Umständen ein exakter „Fingerabdruck“ des Betriebssystems und evtl. dessen Version angelegt werden (vgl. Dirscherl 2010).

8 Ein Port ist ein virtueller Briefkasten zur Kommunikation eines Programms bzw. einer bestimmten Programmfunktion.

9 Beispielsweise kann nach – selbst dem Hersteller noch unbekannten – Schwachstellen gesucht werden. Für solche Zero-Day-Exploits existiert ein regelrechter Markt und es wird auch den Geheimdiensten immer wieder vorgeworfen, sich solche Schwachstellen nutzbar zu machen (vgl. Grüter 2013: 181 im Hinblick auf *Stuxnet*; Johnigk et al. 2014: 105 zur Entwicklung von Zero-Day-Exploits im Projekt *Quantum Insert* der NSA).

10 Zutreffend: Bär kommt zu einer Strafbarkeit nach § 202a StGB, sieht aber das Portscanning als Unterfall des Hackings, ohne sich damit auseinanderzusetzen, dass durch die Abfrage der Ports noch nicht in das System eingedrungen wird (vgl. Bär 2014: 14. Kap., Rn. 80; Marberth-Kubicki 2008: 17).

unternehmenseigene Firewall und Passwortabfragen gesichert. Ein ausländischer Geheimdienst verschafft sich Zugang zu dem System und erlangt die vollständigen Verbindungsdaten, die zeigen, welcher Kunde über welchen Satellitentransponder kommuniziert hat.[11] Die Firma stellt Strafantrag.

5.1 Materiell-strafrechtliche Betrachtung

Die Server des Teleportanbieters stehen in Deutschland, so dass die Anwendbarkeit deutschen Strafrechts bei diesem Szenario kein Problem darstellt. Obwohl der Schutz des Fernmeldegeheimnisses die Verbindungsdaten umfasst, liegt keine nach § 206 StGB strafbare Verletzung des Post- und Fernmeldegeheimnisses vor, da den Mitarbeitern eines ausländischen Geheimdienstes regelmäßig die Täterqualität für dieses Sonderdelikt fehlt. Gleichfalls liegt kein Verstoß gegen das Abhörverbot nach §§ 148, 89 TKG vor, da nicht die Telekommunikation durch Überwachung des Satelliten ausgeforscht wird, sondern leitungsgebunden in die Server eingedrungen wird (zu den Voraussetzungen des Abhörverbotes: vgl. Cornelius 2015a: 695). Ebenso scheidet eine Verletzung der Vertraulichkeit des Wortes nach § 201 StGB aus, da nicht die Gespräche selbst mitgeschnitten werden, sondern nur die Verbindungsdaten erlangt werden (zu den Voraussetzungen des § 201 StGB: vgl. ebd.).

Allerdings kommt eine Datenausspähung nach § 202a StGB in Betracht. Diese Vorschrift schützt die formelle Verfügungsbefugnis des Berechtigten, über die Zugänglichkeit der Daten zu bestimmen, also sein individuelles Geheimhaltungsinteresse (ebd.). Die Zuordnung von Daten an einen Berechtigten erfolgt dabei grundsätzlich danach, wer die Speicherung oder Übermittlung der Daten initiiert, also den Skripturakt vorgenommen hat (ebd.). Dagegen sind die Eigentumsverhältnisse oder der Personenbezug (hierfür ist § 43 BDSG einschlägig: Lenckner et al. 2014: § 202a Rn. 1.) unerheblich für die Bestimmung der Berechtigteneigenschaft. Bei der Zugrundelegung dieser Kriterien ist der Berechtigte im Sinne des § 202a StGB der Teleportanbieter, der die Daten auf seinem System speichert. Dieser kann darüber entscheiden, wer auf die Daten zugreifen darf. Das ist jedenfalls nicht der ausländische Geheimdienst, so dass die erlangten Verbindungsdaten nicht für ihn bestimmt sind (zu diesem Erfordernis: vgl. Kilian et al. 2013: Teil 10, Rn. 19).

Des Weiteren erfordert der Tatbestand der Datenausspähung, dass eine Zugangssicherung überwunden wird. Darunter ist jedes Hindernis zu verstehen, das den tatsächlichen Zugriff auf Daten nicht ganz unerheblich zu erschweren geeignet und dafür bestimmt ist (Cornelius 2015a: 695). Grundsätzlich ist davon auszugehen, dass eine Firma

11 Nach einem Dokument aus dem Fundus von *Edward Snowden* besteht die Möglichkeit, dass sich die NSA und GCHQ Zugriff auf Netzwerke der Deutschen Telekom und des Kölner Providers Netcologne verschafft haben (vgl. Spiegel Online 2014c). Die *Staatsanwaltschaft Köln* hat folgerichtig ein Ermittlungsverfahren gegen Unbekannt wegen des Verdachts des Ausspähens von Daten (§ 202a StGB) eingeleitet (vgl. Spiegel Online 2014b).

ihr Netzwerk gegen unberechtigte Zugriffe von außen sichert, wie es auch hier im Szenario vorgesehen ist. Damit ist auch dieses Tatbestandsmerkmal erfüllt.

Ferner muss sich der ausländische Geheimdienst den Zugang zu Daten verschafft haben, wobei ein erfolgreicher Systemeinbruch ausreichend ist. Das Verschaffen des Zugangs zu Daten ist in jedem Fall dann erfüllt, wenn der Täter die tatsächliche Herrschaftsmacht über die Daten erlangt (Kargl 2013: § 202a Rn. 12). Dies ist spätestens mit dem Abspeichern der Verbindungsdaten der Fall.

Das Verschaffen des Zugangs zu Daten ist dem tatsächlichen Verschaffen der Daten zeitlich vorgelagert. Deshalb ist es nach Überwindung der Zugangssicherung nicht mehr erforderlich, dass sich der Täter die Daten durch reproduzierbare Kenntnisnahme oder durch Erlangen der Herrschaftsmacht tatsächlich verschafft. Bereits die Möglichkeit hierzu ist ausreichend. Dann hat der Täter schon *Zugang* zu den Daten. Damit kommt es nicht mehr darauf an, dass die Strafverfolgungsbehörden dem Täter nachweisen müssen, dass er tatsächlich die Herrschaftsgewalt über Daten erlangt hat oder diese zumindest reproduzierbar zur Kenntnis genommen hat (Kilian et al. 2013: Teil 10, Rn. 31).

Das außerdem erforderliche Merkmal der Unbefugtheit ist gegeben, da weder ein Einverständnis des Berechtigten vorliegt noch ein Rechtfertigungsgrund greift. Strafprozessuale Ermächtigungsgrundlagen (wie §§ 94, 100a StPO) und Maßnahmen der präventiven Gefahrenabwehr scheiden für einen ausländischen Geheimdienst als Rechtfertigungsgrund bereits *per se* aus. Für eine Notwehr nach § 32 StGB ist ein „gegenwärtiger Angriff“ erforderlich. Dieser ist „als punktuelles Ereignis“ erst dann anzunehmen, wenn die Gefahr unmittelbar in eine Rechtsgutsverletzung umzuschlagen droht (Erb 2011: § 32 Rn. 105), wobei auch späte Vorbereitungsphasen einbezogen werden, wenn diese bereits den konkreten Lebensvorgang eingeleitet haben (ebd.: § 32 Rn. 108). Diese Gegenwärtigkeit liegt bei einer einzelfallunabhängigen[12] Überwachung der Allgemeinheit nicht vor, da dieses Konzept mit dem großflächigen Ansatz gerade keinen Überwachungsanlass benötigt (vgl. zu diesem Konzept: Bäcker 2014: 556; Cornelius 2015a: 696). Im Übrigen kann die Notwehr nur einen Eingriff in die Rechtsgüter des Angreifers rechtfertigen (vgl. Erb 2011: § 32 Rn. 122). Selbst für den Fall, dass der ausländische Nachrichtendienst Anhaltspunkt für einen unmittelbar bevorstehenden Angriff (beispielsweise einen terroristischen Anschlag) hat, könnte damit nur die gezielte Überwachung bestimmter Kommunikationsverbindungen, nicht aber die Erlangung sämtlicher Verbindungsdaten gerechtfertigt werden.

Die Voraussetzungen des § 34 StGB liegen gleichfalls nicht vor. Hierzu bedarf es einer gegenwärtigen, nicht anders abwendbaren Gefahr für ein Rechtsgut im Sinne des § 34 StGB. Selbst wenn die Gegenwärtigkeit der Gefahr teilweise schon dann bejaht

12 Wegen dieser Einzelfallunabhängigkeit scheitert selbst die Effizienzlösung, nach welcher eine Gegenwärtigkeit schon beim Verstreichenlassen der „letzten oder sichersten Abwehrchance“ vorliegen soll, ebenso ist die Möglichkeit einer Präventivnotwehr abzulehnen (vgl. Hillenkamp 1995: 152–153).

wird, wenn der Eintritt eines drohenden Schadens erst in der Zukunft zu erwarten ist, aber nur durch sofortiges Handeln abgewendet werden kann (Perron 2014: § 34 Rn. 17; Erb 2011: § 34 Rn. 85 lässt schon ein erhöhtes Fehlschlagsrisiko genügen), liegt dies bei der einzelfallunabhängigen umfassenden Telekommunikationsüberwachung gerade noch nicht vor. Denn die Überwachung der Telekommunikation erfolgt planmäßig und wird über einen längeren Zeitraum zur Informationsbeschaffung begangen, ohne dass ein Anlass dafür gegeben sein muss.[13]

5.2 Prozessuale Betrachtung

Die materielle Seite ist somit kein Problem – aber die Strafverfolgung. Ein Rechtshilfeersuchen wird keinen Erfolg haben, denn die Voraussetzung der gegenseitigen Strafbarkeit dürfte regelmäßig nicht gegeben sein. Der NSA-Mitarbeiter wird sich darauf berufen, dass seine Handlungen nach dem US-amerikanischen Recht zulässig sind (vgl. Wolf 2013: 1040ff.). Differenzierter gestaltet sich die Rechtslage mit Blick auf *Großbritannien*. Dieses ist ein Mitgliedsstaat der *Europäischen Union* und dort gibt es das besondere Instrument des Europäischen Haftbefehls. Grundsätzlich gilt auch für diesen das Prinzip der gegenseitigen Strafbarkeit, aber es gibt Ausnahmen, u.a. für Delikte der Cyberkriminalität – das ist die Datenausspähung – die im ausstellenden Staat im Höchstmaß mit einer Freiheitsstrafe von 3 Jahren bedroht ist. Auch diese Voraussetzung ist hier gegeben, da § 202a StGB einen Strafrahmen bis zu drei Jahren vorsieht. Damit käme also tatsächlich eine erfolgversprechende Strafverfolgung in Betracht, wenn entsprechend dem hier unterstellten Szenario ermittelt werden kann (vgl. Cornelius 2015a: 694). Das ist natürlich die schwierigste Aufgabe!

Außerdem gibt es ggf. noch eine andere Hürde. *Großbritannien* ist in einem Ablösungsprozess von der *Europäischen Union* begriffen (vgl. Brodowski 2013: 458). Dies führte u.a. dazu, dass das Vereinigte Königreich mit Schreiben vom 24. Juli 2013 zum 1. Dezember 2014 entsprechend einer im Rahmen der Verhandlungen zum Lissabon-Vertrag zugestandenen Ausstiegsklausel aus 133 Regelungen zur gemeinsamen europäischen Innen- und Justizpolitik ausstieg (Europäische Union 2012: Art. 10 Abs. 4: 322). 35 davon wollte die Regierung beibehalten und wieder einführen.[14] Darunter ist auch der Europäische Haftbefehl. Bei der Abstimmungsvorlage im Unterhaus waren aber nur 11 der 35 Regelungen (darunter auch nicht der Europäische Haftbefehl) enthalten, so dass sich die Frage stellt, ob dieser nun wiedereingeführt wurde oder nicht. Innenministerin *Theresa May* geht (zumindest noch) davon aus, dass die Abstimmung für alle 35 Regelungen und damit auch den Europäischen Haftbefehl gilt (vgl. Frankfurter Allgemeine Zeitung 2014).

13 Vgl. die Argumentation des OLG Düsseldorf 2013: 593 zur Einschleusung von Vertrauensleuten in kriminelle Organisationen, die im Hinblick auf die fehlende Gegenwärtigkeit einer Gefahr vergleichbar ist mit einer umfassenden anlasslosen Telekommunikationsüberwachung.

14 Diese Möglichkeit räumt Art. 10 Abs. 5: 1 ein (Europäische Union 2012: 322).

Dann stellt sich jedoch noch ein zusätzliches Problem: Grundsätzlich ist die Staatsanwaltschaft verpflichtet, bei Vorliegen eines Anfangsverdachts ein Ermittlungsverfahren einzuleiten und bei einem hinreichenden Tatverdacht Anklage zu erheben. Allerdings wird dieses Legalitätsprinzip eingeschränkt durch das Opportunitätsprinzip. So kann die Staatsanwaltschaft bei Taten, deren Erfolgsort zwar in Deutschland liegt, deren zum Erfolg führende (menschliche) Handlung aber außerhalb von Deutschland im Ausland vorgenommen wurde, auch das Verfahren einstellen (§ 153c III StPO) (Cornelius 2015a: 694). Voraussetzung hierfür ist, dass die Durchführung des Verfahrens die Gefahr eines schweren Nachteils[15] für die Bundesrepublik Deutschland herbeiführen würde oder wenn der Verfolgung sonstige überwiegende öffentliche Interessen[16] entgegenstehen.

6 Szenario zu Eikonal

In diesem Szenario wird davon ausgegangen, dass der *BND* zwischen 2004 und 2008 einen der wichtigsten Kommunikationsknotenpunkte der Welt, den DE–CIX, in Frankfurt anzapfte und die durch diese *strategische Telekommunikationsaufklärung* gewonnenen Daten an einen amerikanischen Geheimdienst weiterleitete. Zwar sollte die Telekommunikation deutscher Personen vorher herausgefiltert werden, jedoch funktionierte der vom *BND* eingesetzte Filter nur unzulänglich: Es konnten nur 95 % der übermittelten Daten von deutschen Rohdaten bereinigt werden.[17] Machen sich die Mitarbeiter des BND strafbar, wenn sie sich an einer solchen Aktion beteiligen? Die Antwort auf diese Frage ist: Ja![18]

6.1 Verwirklichte Straftatbestände

Zwar scheiden die Strafvorschriften des TKG (§§ 148 i.V.m. 89 TKG) nach diesem Szenario aus, da in den Schutzbereich dieser Vorschriften nur über Funk erfolgende Nachrichtenübermittlung fallen (Altenhain 2015: § 148 TKG Rn.; 6; Cornelius 2015a: 695). Ebenso wenig ist der Tatbestand des Ausspähens von Daten (§ 202a StGB) erfüllt. Freilich haben sich die Mitarbeiter des BND nach dem vorgestellten Szenario den Zugang zu Daten verschafft, die nicht für sie bestimmt waren. Es ist außerdem davon auszugehen, dass ein so bedeutender Internetknotenpunkt nicht ohne eine adäquate Zugangssicherung betrieben wird. Jedoch ist der Betreiber unter den Voraussetzungen des

15 Die Gefahr eines schweren Nachteils kann die äußere Sicherheit betreffen, aber auch das innere oder sonstige (z.B. das wirtschaftliche) Wohl, den inneren politischen Frieden etc.

16 Dies kann jedes sonstige öffentliche Interesse sein, so dass durchaus auch Erwägungen zur Verhinderung des Zusammenbruchs der Zusammenarbeit mit GCHQ oder NSA und den deutschen Geheimdiensten vorstellbar sind (vgl. zu diesen Erwägungen: Hettel et al. 2014: 349).

17 Zu den tatsächlichen Hintergründen für dieses Szenario vgl. Süddeutsche Zeitung 2014a, b.; Spiegel Online 2014a; Golem.de 2014.

18 Ausführlich wurde die Frage der Strafbarkeit bei der strategischen Telekommunikationsüberwachung untersucht (Cornelius 2015a: 693ff.), weshalb nachfolgend nur die wichtigsten Überlegungen widergegeben werden.

G10-Gesetzes verpflichtet, dem BND zur Durchführung der strategischen Telekommunikationsüberwachung den Zugriff zu gewähren, vgl. § 2 G 10 Gesetz und unterliegt diesbezüglich auch einem Mitteilungsverbot, § 17 G 10 Gesetz. Deshalb ist davon auszugehen, dass kein Überwinden einer entsprechenden Zugangssicherung vorliegt. Dies muss an dieser Stelle nicht weiter vertieft werden, denn selbst wenn keine Zugangssicherung überwunden wird und damit eine Strafbarkeit nach § 202a StGB ausscheiden würde, wären zumindest die Voraussetzungen des § 202b StGB (Abfangen von Daten) gegeben, da es sich bei privater Telekommunikation um eine nichtöffentliche Datenübermittlung handelt, die sich der BND unter Anwendung technischer Mittel verschafft. Das ist schon dann gegeben, wenn der Datenstrom in Gestalt einer Verdoppelung dem *BND* zugeleitet wird.[19] Je nach der Art der abgehörten Daten kommt daneben noch die Verletzung der Vertraulichkeit des Wortes (§ 201 StGB) in Betracht. Dies betrifft Sprachnachrichten (alle abgefangenen Telefonate), nicht dagegen Textnachrichten wie E-Mails. Da es sich bei den Mitarbeitern des BND regelmäßig um Amtsträger oder für den öffentlichen Dienst besonders verpflichtete Personen handeln wird, ist dann sogar die Qualifikation des § 201 Abs. 3 mit einem Strafrahmen von bis zu fünf Jahren Freiheitsstrafe gegeben (ausführlich: Cornelius 2015a: 695).

6.2 Keine strafrechtlichen Rechtfertigungsgründe

Die Verwirklichung eines Straftatbestandes ist jedoch nicht gleichzusetzen mit einer Strafbarkeit. Diese ist vielmehr dann ausgeschlossen, wenn sich der BND auf eine Berechtigung berufen kann, die Telekommunikation aufzeichnen und überwachen zu dürfen. Die allgemeinen Rechtfertigungsgründe kommen aus den bereits zur umfassenden Telekommunikationsüberwachung durch einen ausländischen Geheimdienst dargelegten Gründen auch für den BND nicht in Betracht. Bei der strategischen Telekommunikationsüberwachung wird es regelmäßig an der Gegenwärtigkeit eines Angriffs bzw. einer Gefahr fehlen (vgl. Erb 2011: § 32 Rn. 105, 108).

6.3 Keine Wahrnehmung amtlicher Befugnisse

Allerdings kann die rechtmäßige Wahrnehmung amtlicher Befugnisse die Verwirklichung von Straftatbeständen rechtfertigen. Dies wird im Grundsatz weder in der Rechtsprechung noch in der Lehre bestritten (Evers 1987: 155; Lampe 2015: 367–368; Rönnau 2007: Vor § 32 Rn. 21; Roxin 2006: § 14 Rn. 32; Lenckner et al. 2014: vor § 32 Rn. 4; Hoyer 2009: Vor §§ 32ff. Rn. 41), obgleich die Anforderungen im Einzelnen um-

19 Zu dieser Vorgehensweise im Rahmen der strategischen Telekommunikationsbeschränkung (vgl. BVerwG 2014: 1668, Rn. 24); bei diesem Vorgehen kommt es damit nicht mehr darauf an, welche Daten nach dem Einsatz von Suchworten für eine weitere Verarbeitung herausgefiltert werden (vgl. zur parallelen Erwägung für einen Eingriff in das Fernmeldegeheimnis: ebd.: 997., Rn.32; mit Anm. Gärditz 2014: 1000; der aber a.a.O. vor einer Individualisierung der im Rahmen der strategischen Überwachung gewonnenen Daten einen Grundrechtseingriff in Art. 10 Abs. 1 GG ablehnt (ebd.: 1002).

stritten sind (vgl. OLG Düsseldorf 2013: 591, wo das Gericht den Rechtfertigungsgrund der Wahrnehmung amtlicher Befugnisse prüft, § 3 BNDG i.V.m. § 8 Abs. 2 BVerfSchG letztlich aber nicht durchgreifen lässt; vgl. auch Frisch 2003: 200; Hofmann et al. 2014: 178–188). Nur wenn die in der öffentlich-rechtlichen Ermächtigungsnorm konkret genannten Eingriffsvoraussetzungen objektiv erfüllt sind, kommt eine Rechtfertigung in Betracht (Lenckner et al. 2014: Vor § 32 Rn. 84; Cornelius 2015a: 696).

6.3.1 Öffentlich-rechtliche Rechtswidrigkeit als notwendige Bedingung einer Strafrechtswidrigkeit

Dies soll jedoch nicht heißen, dass eine öffentlich-rechtliche Rechtswidrigkeit immer zu einer Strafrechtswidrigkeit eines Verhaltens führt. Im Gegenteil kann ein Verhalten in einer außerstrafrechtlichen Teilrechtsordnung rechtswidrig sein, ohne dass es auch strafrechtswidrig ist (Günther 1983: 73; Erb 2011: Vor §§ 32ff. Rn. 2–3; vgl. Lehleiter 1995: 97; vgl. auch Schenke et al. 2014: § 1 BNDG Rn. 12ff., § 3 BNDG Rn. 30 zum Grundsatz der differenzierten Rechtmäßigkeit bzw. Rechtswidrigkeit in unterschiedlichen Rechtsgebieten). Damit ist bei der strafrechtlichen Bewertung staatlicher Maßnahmen auf Grund öffentlich-rechtlicher Eingriffsbefugnisse gegenüber dem Bürger die öffentlich-rechtliche Rechtswidrigkeit eine notwendige, nicht aber hinreichende Bedingung für die Strafrechtswidrigkeit (Felix 1998: 306–307; Günther 1983: 101; Lehleiter 1995: 93).[20] Eine Verletzung von Straftatbeständen durch eine staatliche Maßnahme kann nur dann zulässig sein, wenn eine *hinreichend konkrete* Ermächtigungsgrundlage in Form einer Befugnisnorm einschlägig ist und die entsprechenden Anforderungen erfüllt sind (OLG Düsseldorf 2013: 591; Lampe 2015: 368, 371; vgl. Roxin 2006: § 14 Rn. 31–32, wonach eine öffentlich-rechtliche Erlaubnis die Strafrechtswidrigkeit eines Verhaltens ausschließt). Deshalb ist in einem ersten Prüfungsschritt zu untersuchen, ob die Telekommunikationsüberwachung nach dem *Eikonal*-Szenario durch öffentlich-rechtliche Erlaubnisvorschriften gedeckt ist oder nicht. Wenn dies gegeben ist, dann gilt die Rechtfertigung für die gesamte Rechtsordnung (Lampe 2015: 368). Nur wenn dies nicht der Fall ist, muss in einem zweiten Schritt untersucht werden, ob die öffentlich-rechtliche Rechtswidrigkeit auch zur strafrechtlichen Verantwortlichkeit des jeweils handelnden Beamten führt (vgl. zu dieser Vorgehensweise: Felix 1998: 307 unter Rückgriff auf BVerfGE 88, 203 (258)).

20 Lehleiter weist zu Recht darauf hin, dass dieser Rechtswidrigkeitsbegriff im Hinblick auf die Rechtsfolgen funktionsbestimmt rechtsdogmatisch zu verstehen ist. Da es im Rahmen dieses Beitrages um die strafrechtliche Rechtfertigung durch öffentlich-rechtliche Eingriffsbefugnisse geht, kommt es auf die Diskussion zur Verallgemeinerung des Stufenverhältnisses der Rechtswidrigkeitsbegriffe nicht an (vgl. beispielsweise zur Ungleichbehandlung des untauglichen Versuchs im Deliktsrecht und im Strafrecht: Hellmann 1986: 88).

6.3.2 Spezialgesetzliche Eingriffsbefugnisse

Der BND ist keine Ermittlungsbehörde, so dass er sich nicht auf die Ermächtigungsgrundlagen zur Strafverfolgung stützen kann (vgl. §§ 94, 100a StPO). Zwar soll er – wie die Polizei – auch zur Gefahrenabwehr tätig werden. Allerdings ist er nach dem verfassungsrechtlich nicht ausdrücklich normierten, aber vor den unterschiedlichen Aufgabenzuweisungen anerkannten Trennungsgebot eine selbständige nicht der Polizei zuordenbare Behörde (Schwabenbauer 2013: 17–18), was einfachgesetzlich in §§ 1 Abs. 2, 2 Abs. 3 BNDG zum Ausdruck kommt (Schenke et al. 2014: § 1 BNDG Rn. 12 ff., § 2 BNDG Rn. 33). Deshalb kann sich der *BND* auch nicht auf etwaige Ermächtigungen in den Polizeigesetzen (wie zum Beispiel die Generalklauseln) berufen (vgl. Pawlik 2010: 696; Zöller 2007: 767). Gleichfalls scheidet eine Berufung auf § 9 Abs. 1 i.V.m. § 8 Abs. 2 BVerfSchG für die geheime Erhebung von Telekommunikationsdaten aus. Denn für eine Ermächtigungsgrundlage in entsprechende Eingriffe des Art. 10 GG wäre es gemäß dem Zitiergebot des Art. 19 Abs. 2: 1 GG notwendig, dass die Möglichkeit von Einschränkungen des Fernmeldegeheimnisses explizit erwähnt wird, was wegen der abschließenden Regelung des G10-Gesetzes für die heimliche Post- und Telekommunikationsüberwachung nicht erfolgt ist (Schenke et al. 2014: § 8 BVerfSchG Rn. 39; Lampe 2015: 366).

Eine Rechtfertigung der Telekommunikationsüberwachung durch den BND käme damit nur nach den spezialgesetzlichen Vorschriften im Gesetz zur Beschränkung des Brief-, Post - und Fernmeldegeheimnisses (G10-Gesetz) bzw. dem BNDG in Betracht.

6.3.3 Überwachung inländischer Telekommunikation

Der BND ist ein Auslandsgeheimdienst. Konsequenterweise hat er keine Befugnis, die Telekommunikation zwischen zwei deutschen Teilnehmern im Rahmen der strategischen Telekommunikationsüberwachung zu überwachen (Bäcker 2014: 557; Cornelius 2015a: 698). Wenn – wie in diesem Szenario unterstellt – die Filter nicht ordnungsgemäß funktionieren und damit auch die Daten einer rein deutschen Kommunikation weitergegeben werden, ist keine Rechtfertigung – weder für die Erhebung noch für die Weitergabe – denkbar. Allerdings ist eine Strafbarkeit wegen fehlenden Vorsatzes solange ausgeschlossen, wie die Mitarbeiter des BND davon ausgingen, dass der Filter ordnungsgemäß funktioniert.

6.3.4 Überwachung internationaler Telekommunikation

Die Rechtslage gestaltet sich komplizierter bei Telekommunikationsbeziehungen zwischen einem Teilnehmer in Deutschland und einem zweiten Teilnehmer im Ausland. Die Überwachung solcher internationalen Telekommunikationsverbindungen soll unter bestimmten Voraussetzungen nach § 5 G 10 G zulässig sein (Huber 2013: 2573).[21] Da-

21 Mit Betonung auf der Beschränkung der Eingriffsermächtigung für Telekommunikationsverbindungen mit einem Bezugspunkt (Anfangs- oder Endpunkt) zu Deutschland.

bei geht es um die frühzeitige Erkennung von Gefahren für die Sicherheit der Bundesrepublik Deutschland, weshalb nicht die Identität der Kommunikationsteilnehmer, sondern die Inhalte der Telekommunikation im Vordergrund stehen (Schwabenbauer 2013: 62). Deshalb bedarf es für die strategische Telefonüberwachung keiner tatsächlichen Anhaltspunkte für eine konkrete Gefahr (BVerfGE 100, 313 (383)). Dennoch sind die verfassungsrechtlichen Vorgaben, welche das *Bundesverfassungsgericht* konkretisiert hat, streng. Danach ist eine Ermächtigung zur strategischen Überwachung internationaler Telekommunikation nur bei einschränkenden Vorgaben im Hinblick auf Gegenstand, Ausmaß und Modalitäten der Überwachung verfassungsgemäß (BVerfGE 100, 313 (376, 377, 384)). Es ist jedoch äußerst zweifelhaft, ob diese einschränkenden Vorgaben mit der weiten Formulierung des § 5 G 10 G erfüllt werden, weshalb tendenziell davon auszugehen ist, dass diese Vorschrift keine ausreichende Ermächtigungsgrundlage ist (ausführlich: Cornelius 2015a: 698–699). Da es in diesem Beitrag um die strafrechtlichen Verantwortlichkeiten geht, soll an dieser Stelle erst einmal die Feststellung ausreichen, dass die Rechtslage bezüglich der öffentlich-rechtlichen Bewertung höchst unklar ist.

6.3.5 Überwachung ausländischer Kommunikation

Der *Europäische Gerichtshof für Menschenrechte* hat sich mit der strategischen Überwachung ausländischer Kommunikation (d.h. beide Kommunikationsteilnehmer befinden sich im Ausland) befasst und hatte zu entscheiden, ob diese einen unerlaubten Eingriff in die Souveränität der ausländischen Staaten darstellt, in denen die überwachten Personen wohnen (EGMR 2007: 1433ff.). Dies hat er deshalb abgelehnt, da kein ausreichender Vortrag seitens der Beschwerdeführer erfolgte, dass ein Eingriff in die völkerrechtlich geschützte territoriale Souveränität ausländischer Staaten vorliege, zumal sich die Überwachungsanlagen auf deutschem Gebiet befanden und die Daten in Deutschland verwendet wurden (ebd.: 1435).

Bezüglich ausländischer Telekommunikationsüberwachung beruft sich der BND selbst auf die Aufgabenzuweisungsnorm des § 1 Abs. 2 BNDG (BT-Drs.17/9640: 6, 10; BT-Drs. 17/14739: 14; BVerfGE 100, 313 (337, 338); Huber 2001: 3298; Bäcker 2014: 560). Danach müsse die Datenerhebung lediglich dazu dienen, Erkenntnisse von außen- und sicherheitspolitischer Bedeutung zu beschaffen. Dieser Rechtsansicht hat die Bundesregierung in einer Stellungnahme vor dem *Bundesverfassungsgericht* dahingehend zugestimmt, dass diese Überwachung des „offenen Himmels“ nicht unter das G10-Gesetz falle (vgl. die Stellungnahme der Bundesregierung im Verfahren über das G10-Gesetz: BVerfGE 100, 313 (339)). Die Verletzung von Straftatbeständen durch diese Überwachungsmaßnahmen kann jedoch nicht auf eine allgemeine Aufgabenzuweisungsnorm ohne eine *hinreichend konkrete* Ermächtigung gestützt werden (vgl. OLG Düsseldorf 2013: 591; Lampe 2015: 368, 371), wenn die ausländische Kommunikation durch das Fernmeldegeheimnis des Art. 10 GG geschützt wird (Bäcker 2014: 560; Cor-

nelius 2015a: 699). Das *Bundesverfassungsgericht* hat in dem Verfahren zum G 10 bereits darauf hingewiesen, dass der Schutz des Fernmeldegeheimnisses jedenfalls bei einem territorialen Bezug zu Deutschland greift, der bereits dann besteht, wenn ausländische Telekommunikation mit Überwachungsanlagen aufgezeichnet wird, die sich auf deutschem Boden befinden (BVerfGE 100, 313 (363, 364). Dies ist bei unserem Beispiel zu Eikonal mit der Überwachung des DE-CIX gegeben. Der territoriale Bezug liegt vor, so dass der Schutzbereich des Fernmeldegeheimnisses eröffnet ist, also eine ausdrückliche Befugnisnorm als Ermächtigungsgrundlage erforderlich ist. Diese kann nicht in der allgemeinen Aufgabenzuweisungsnorm des § 1 Abs. 2: 1 BNDG gesehen werden (vgl. Huber 2013: 2575).[22]

6.3.6 Strafrechtswidrigkeit

Damit ist die notwendige Voraussetzung für eine Strafrechtswidrigkeit – nämlich eine mangelnde öffentlich-rechtliche Befugnisnorm – gegeben. Da weder die strafrechtlichen Rechtfertigungsgründe (§§ 32, 34 StGB) noch spezielle Eingriffsnormen greifen, ist nun in einem zweiten Schritt zu prüfen, ob diese öffentlich-rechtliche Rechtswidrigkeit auch zu einer Strafrechtswidrigkeit führt. Dies ist im Hinblick auf den einzelnen Mitarbeiter des BND dann ausgeschlossen, wenn er sich auf eine zwar rechtswidrige, aber verbindliche dienstliche Anordnung berufen kann.

Nach § 63 BBG ist eine Anordnung auch strafbaren Inhalts selbst dann verbindlich, wenn der konkrete Weisungsempfänger nicht erkannt hat und nach seinem Wissens- und Erfahrungshorizont auch nicht erkennen konnte, dass das, was von ihm verlangt wird, „strafbar“ ist (Lenckner 1993: 227). Bei dem hier zugrunde gelegten *Eikonal*-Szenario kann nicht davon ausgegangen werden, dass die Strafbarkeit so evident ist, dass der ausführende Beamte dies zumindest zweifelsfrei hätte erkennen können. Bei der Überwachung der internationalen Telekommunikation wurde herausgearbeitet, dass die Rechtslage unklar ist. Dies schließt die evidente Erkennbarkeit einer diesbezüglichen Strafbarkeit aus. Zwar stellt sich dies bei der strategischen Überwachung ausländischer Telekommunikation anders dar, da das Ergebnis einer fehlenden Ermächtigungsgrundlage eindeutig ist. Dennoch kann aus der Sicht eines BND-Mitarbeiters nicht von einem Evidenzfall ausgegangen werden, da sowohl die Rechtsabteilung des BND als auch die Bundesregierung der Auffassung sind bzw. waren, dass die strategische Überwachung ausländischer Telekommunikation allein aufgrund der Aufgabenzuweisungsnorm des § 1 Abs. 2 BNDG zulässig und damit eine entsprechende Strafbarkeit ausgeschlossen ist. Damit handelte es sich bei einer entsprechenden Weisung des jeweiligen Vorgesetzten an den ausführenden Mitarbeiter um eine verbindliche Anordnung, deren Durchführung dem jeweiligen Mitarbeiter nicht strafrechtlich zu

22 Huber weist darauf hin, dass die Aufzeichnung, Auswertung und die Entscheidung über die Weitergabe der Informationen auf deutschem Boden erfolgen.

einem Vorwurf gemacht werden kann (ausführlich zu diesen Erwägungen: Cornelius 2015a: 700–701).

Dies gilt jedoch nur für die Person des Ausführenden, nicht aber für das von dem Weisungsgeber zu verantwortende staatliche Handeln, welches im Außenrechtsverhältnis rechtswidrig bleibt (vgl. Lenckner 1993: 224–225; Erb 2011: § 34 Rn. 43; Paeffgen 2013: Vor §§ 32 Rn. 192). Das führt dazu, dass der Vorgesetzte, welcher sich nicht mehr auf eine verbindliche Weisung stützen kann, als mittelbarer Täter für die im Außenverhältnis begangene Tat haftet (Weißer et al. 2014: § 25 Rn. 34). Zumindest der Vorgesetzte, der den eigentlichen Einsatz von *Eikonal* angeordnet hat, kann sich nicht mehr auf die Verbindlichkeit einer rechtswidrigen Anweisung berufen.

6.3.7 Verbotsirrtum, § 17 StGB

Jedoch kommt in Betracht, dass eine strafrechtliche Verantwortlichkeit dieses Vorgesetzten wegen eines Verbotsirrtums nach § 17 StGB ausscheidet. Die herrschende Meinung geht davon aus, dass schon bei einem bedingten Unrechtsbewusstsein kein Verbotsirrtum vorliegt – also eine entsprechende Unrechtseinsicht vorhanden ist. Wenn es der Täter bei einer unklaren Rechtslage auch nur für möglich hält, dass sein Verhalten verboten sein könnte (vgl. BGH 1953: 431; OLG Karlsruhe 2000: 61) und er lediglich darauf hofft, dass sein Verhalten nicht gegen das Strafgesetz verstoße (Fischer et al. 2015: § 17, Rn. 9c), reicht dies also schon aus, um einen Unrechtsausschluss zu verneinen (Cornelius 2015a: 701; Cornelius 2015b: 106). Solche Zweifel müssten von den Juristen der Rechtsabteilung des BND bei einer sachgemäßen Prüfung der Rechtslage angesichts der G10-Entscheidung des *Bundesverfassungsgerichts* den verantwortlichen Mitarbeitern beim BND zur Kenntnis gebracht werden. Jedoch ist darauf hinzuweisen, dass die Rechtsprechung selbst – in Abkehr von den dogmatischen Grundsätzen zum Verbotsirrtum – eine Anwendung von § 17 StGB bei unbehebbaren Unrechtszweifeln zugesteht (ebd.; kritisch hierzu: Cornelius 2015b: 106 mit einem Lösungsvorschlag zur verfassungskonformen Auslegung). Ein solcher kommt in Anbetracht der unklaren Rechtslage zwar im Hinblick auf die Überwachung internationaler Telekommunikation in Betracht, ist aber angesichts der Rechtsprechung des Bundesverfassungsgerichts und auch der ganz herrschenden Meinung in der Literatur zur begrenzten Reichweite einer Aufgabenzuweisungsnorm bei der strategischen Überwachung ausländischer Telekommunikation ausgeschlossen.

7 Fazit

Die Herstellung einer Karte vom Internet wie *Treasuremap* ist selbst dann nicht strafbar, wenn das Angriffsvorbereitungen für ein späteres Eindringen in informationstechnische Systeme sind. Dagegen ist ein Vorgehen ausländischer Geheimdienste mit einem solchen Spionagetool wie *Regin* bereits von allgemeinen Vorschriften zur Computerkriminalität erfasst, ohne dass es – auf je nach Tatfrage ggf. auch mitverwirklichte –

Vorschriften zum Schutz von Staatsgeheimnissen oder von Betriebs- und Geschäftsgeheimnissen ankommt. Das eigentliche Problem besteht in der faktischen Unmöglichkeit der Strafverfolgung amerikanischer Geheimdienstbeamter. Bei den britischen ist dies wegen des fehlenden Erfordernisses der gegenseitigen Strafbarkeit im Bereich der Cyberkriminalität im Rahmen des Europäischen Haftbefehls leichter. Allerdings stellt sich dann die Frage, inwieweit tatsächlich ein Wille zur Strafverfolgung vorhanden ist, da nach dem Opportunitätsprinzip auch von einer Strafverfolgung abgesehen werden kann.

Im Hinblick auf die einzelfallunabhängige, anlasslose (strategische) Telekommunikationsüberwachung, die von den deutschen Geheimdiensten allein dem BND gestattet ist, ist die Überwachung inländischer und ausländischer Telekommunikation unzulässig. Nach dem Willen des Gesetzgebers soll dagegen die strategische Überwachung internationaler Telekommunikation zulässig sein. Diese normative Vorgabe aus § 5 G10-Gesetz ist technisch jedoch nicht umsetzbar. Allein deshalb ergibt sich schon dringend ein Neuordnungsbedarf im Bereich des Sicherheitsrechts.

Eine Rechtfertigung des staatlichen Handelns im Verhältnis zwischen betroffenem Telekommunikationsanbieter bzw. Bürger scheidet (im Außenrechtsverhältnis) aus. Jedoch kommt in Betracht, dass sich die ausführenden Beamten auf eine rechtswidrige verbindliche Anweisung eines Vorgesetzten berufen können mit der Folge, dass diese selbst kein strafrechtliches Unrecht verwirklicht haben. Der Vorgesetzte, der sich nicht mehr auf die Verbindlichkeit einer wenn auch rechtswidrigen Anweisung stützen kann, ist dagegen strafrechtlich verantwortlich. Eine dann zu erwägende Berufung auf einen Verbotsirrtum ist zwar Tatfrage, dürfte aber nur bei der Überwachung internationaler Telekommunikation in Betracht kommen. Aufgrund der Rechtsprechung des *Bundesverfassungsgerichts* und der damit übereinstimmenden weitaus herrschenden Meinung in der verfassungsrechtlichen Literatur, dass eine Überwachung auch ausländischer Telekommunikation von deutschem Boden ein Eingriff in das Fernmeldegeheimnis darstellt, dürfte er dagegen relativ geringe Chancen auf Erfolg im Hinblick auf die strategische Überwachung des „offenen Himmels“ haben. Denn daraus resultiert unmittelbar, dass konkrete Eingriffsbefugnisse für einen solchen Eingriff normiert sein müssen, die mit einer allgemeinen Aufgabenzuweisungsnorm wie § 1 Abs. 2:1 BNDG nicht vorliegen. Allerdings ist bei §§ 202a, b StGB zu beachten, dass diese relative Antragsdelikte sind. Dagegen ist die Qualifikation des § 201 Abs. 3 StGB im Hinblick auf das Abfangen von Sprachnachrichten ein Offizialdelikt, was ohne einen entsprechenden Antrag von der Staatsanwaltschaft zu verfolgen ist.

Unabhängig von der Strafverfolgung kommt der Feststellung einer nach deutschem Recht rechtswidrigen Erhebung für eine Verwendung der daraus gewonnenen Erkenntnisse in einem deutschen Strafverfahren Bedeutung zu (Gärditz 2014: 999; Gercke 2013: 754; Zöller 2007: 770–771). Das gilt sowohl für die Erkenntnisse ausländischer als auch inländischer Geheimdienste. Denn Strafverfolgungsbehörden können nur dann auf solche Erkenntnisse zurückgreifen, wenn die Daten durch eine vergleich-

bare Maßnahme in Übereinstimmung mit den strafprozessualen Vorschriften hätten erlangt werden können (vgl. BVerfGE 100, 313 (394); Schünemann 2008: 326; Zöller 2007: 771).

Der rechtstatsächliche Hintergrund der Massenüberwachung im Internet zeigt, dass es jetzt viel besser als früher möglich ist, jeden Einzelnen zu analysieren, zu vermessen und fast schon die Gedanken vorherzusagen. Damit scheint unsere Gesellschaft mittlerweile dem vom Jeremy Bentham entworfenen Panopticon – jener Vollzugsanstalt, deren ringförmige Bauweise die lückenlose Überwachung der Gefangenen ermöglicht – zu gleichen (vgl. zu diesem Gleichnis: Fischer-Lescano 2014: 965). Die Wirkung einer nicht sichtbaren Überwachung ist permanent, auch wenn ihre Durchführung nur sporadisch ist. Das Internet ist hervorragend geeignet, dieses Konzept einer durch die Architektur ermöglichten Überwachung zu verwirklichen (vgl. das Erfordernis von Technologien für den „hierarchischen Blick" bei: Foucault 1977: 221ff.). Die möglichen Auswirkungen hat das *Bundesverfassungsgericht* bereits im Volkszählungsurteil beschrieben: „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen" (BVerfGE 65, 1 (43)).

Was zur Verhinderung von Kriminalität vielleicht begrüßenswert erscheinen mag (vgl. Bayerisches Staatsministerium des Innern für Bau und Verkehr 2014),[23] ist mit Blick auf die Gedankenfreiheit des Einzelnen beängstigend. Hier ist eine Debatte notwendig! Abwehrmaßnahmen können nicht darin bestehen, die Zeit zurückzudrehen (vgl. Süddeutsche Zeitung 2014d).[24] Vielmehr sind die Rahmenbedingungen anzupassen. Dazu gehört einerseits die Neuausrichtung des Sicherheitsrechts. So ist die Unterscheidung zwischen Inlands- und Auslandsüberwachung nicht mehr zeitgemäß (Huber 2013: 2577; Schmahl 2014: 226). Andererseits ist die rechtspolitische Diskussion zu führen, wieweit eine Überwachung angemessen ist, um dadurch auch Terroranschläge zu verhindern.

Literatur

Altenhain, Karsten (2015): Telekommunikationsgesetz (TKG) Auszug: Normzweck, in: Heintschel-Heinegg, Bernd von (Hrsg.): Münchener Kommentar zum StGB. Nebenstrafrecht II, Bd. 7, C.H. Beck: München, 1377–1404.

Ambos, Kai (2011): § 9, in: Heintschel-Heinegg, Bernd von (Hrsg.): Münchener Kommentar zum Strafgesetzbuch: StGB, Bd 1: §§ 1-37 StGB, C.H. Beck: München, 261–277.

Bäcker, Matthias (2014): Strategische Telekommunikationsüberwachung auf dem Prüfstand, in: Kommunikation und Recht 33, 556–561.

23 Zum Einsatz der Prognosesoftware Precobs, um die Wahrscheinlichkeit der Begehung von Straftaten berechnen zu können.

24 Zu den Überlegungen im NSA-Untersuchungsausschuss, anstatt Computern mechanische Schreibmaschinen einzusetzen.

Bär, Wolfgang (2014): Computer- und Internetkriminalität, in: Wabnitz, Heinz-Bernd / Janovsky, Thomas (Hrsg.): Handbuch Wirtschafts- und Steuerstrafrecht, C.H. Beck: München, 813–908.

Bayerisches Staatsministerium des Innern für Bau und Verkehr 2014: Bayernweite Kontrollaktion gegen Diebes-banden, 26.11.2014, http://www.stmi.bayern.de/med/aktuell/archiv/2014/20141126sonderkontrollaktion/ (16.08.2015).

Beulke, Werner / Meininghaus, Florian (2007): Heimliche Online-Durchsuchung eines PC, in: Strafverteidiger 2, 60–65.

BGH (1953): Verbotsirrtum, in: Neue Juristische Wochenschrift 11, 431–433.

BGH (1968): Beginn der Gebrauchsentwendung durch Untersuchung des KfZ, in: BGHSt 22, 80–82.

Boehme-Neßler, Volker (2014): Das Recht auf Vergessenwerden – Ein neues Internet-Grundrecht im Europäischen Recht, in: Neue Zeitschrift für Verwaltungsrecht 13, 825–830.

Brodowski, Dominik (2013): Strafrechtsrelevante Entwicklungen in der Europäischen Union – ein Überblick, in: Zeitschrift für Internationale Strafrechtsdogmatik 8:11, 455–472.

Buermeyer, Ulf (2013): Zum Begriff der »laufenden Kommunikation« bei der Quellen-Telekommunikationsüberwachung (»Quellen-TKÜ«), in: Strafverteidiger 7, 470–476.

BVerfG (2007): Unzulässige Telefonüberwachung des Anwalts von El Masri, in: Neue Juristische Wochenschrift 38, 2752–2753.

BVerfGE 65, 1 (43); 67, 157 (172); 88, 203 (258); 100, 313 (337, 338, 339, 358, 363, 364, 376, 377, 383, 384; 394, 395); 115, 166 (182); 120, 274 (328); 125, 260 (309); 130, 151 (179).

BVerfG, Urteil vom 27.02.2008 – 1 BvR 370/07.

BVerwG (2014): Feststellungsklage gegen strategische Überwachung durch den BND, in: Neue Zeitschrift für Verwaltungsrecht 2014, 1666–1670.

BVerwG, Urteil vom 02.07.1991 – 1 C 21.89.

BVerwG (1970): Lagerung von Heizöl im engeren Schutzbereich eines Wasserschutzgebietes; nicht zu besorgende Verunreinigung des Grundwassers i.S. des § 34 Abs. 2 WHG, in: Neue Juristische Wochenschrift 42, 1890 – 1893.

Computerwoche (2013a): US-Regierung schnüffelt in Rechnern von Internet-Firmen, 07.06.2013, http://www.computerwoche.de/a/us-regierung-schnueffelt-in-rechnern-von-internet-firmen,2539842 (13.08.2015).

Computerwoche (2013b): Die Spionage-Werkzeuge der NSA, 01.08.2013, http://www.computerwoche.de/a/die-spionage-werkzeuge-der-nsa,2543728 (13.08.2015).

Cornelius, Kai (2015a): Strafrechtliche Verantwortlichkeiten bei der Strategischen Telekommunikationsüberwachung, in: Juristen Zeitung 70:14, 693–702.

Cornelius, Kai (2015b): Die Verbotsirrtumlösung zur Bewältigung unklarer Rechtslagen - ein dogmatischer Irrweg, in: Goltdammer's Archiv für Strafrecht 2, 101–124.

Cornelius, Kai (2013a): Besonderheiten des Strafrechts und Strafprozessrechts in der Informationstechnologie (Teil 10), in Leupold, Andreas / Glossner, Silke (Hrsg.): Münchener Anwaltshandbuch IT-Recht, C. H. Beck: München, 963–1080.

Cornelius, Kai (2013b): Zum strafrechtlichen Schutz des Fernmeldegeheimnisses und der Untreuerelevanz datenschutzrechtlicher Verstöße, in: Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht, 166–170.

Cornelius, Kai (2007): Verdeckte Online-Durchsuchung-Anmerkung zum Beschluss des BGH vom 31.1.2007 – StB 18/06, in: Juristen Zeitung, 62: 15–16, 796–800.

Deutscher Bundestag (2013): BT-Drs. 17/14739, http://dip21.bundestag.de/dip21/btd/17/147/1714739.pdf (16.08.2015).

Deutscher Bundestag (2012): BT-Drs.17/9640, http://dip21.bundestag.de/dip21/btd/17/096/1709640.pdf (16.08.2015).

Dirscherl, Hans-Christian (2010): Fingerprinting: Betriebssysteme identifizieren, 08.06.2010, http://www.pcwelt.de/ratgeber/Fingerprinting-Betriebssysteme-identifizieren-Netzwerk-Sicherheit-und-Nmap-171343.html (14.08.2015).

EGMR (2007): 29. 6. 2006 - 54934/00: Abhörmaßnahmen nach dem G 10-G, in: Neue Juristische Wochenschrift 20, 1433–1439.

Erb, Volker (2011): § 32 Notwehr, in: Heintschel-Heinegg, Bernd von (Hrsg.): Münchener Kommentar zum StGB. §§ 1 - 37 StGB, Bd. 1, C.H. Beck: München, 1435–1547.

Ernst, Stefan (2003): Hacker und Computerviren im Strafrecht, in: Neue Juristische Wochenschrift 45, 3233–3238.

Europäische Union (2012): Protokoll (Nr. 36) über die Übergangsbestimmung, in: Amtsblatt der Europäischen Union C 326, 55, 322–328, https://www.ecb.europa.eu/ecb/legal/pdf/c_32620121026de.pdf (15.08.2015).

Evers, Hans (1987): Sprengung an der Celler Gefängnismauer: Darf der Verfassungsschutz andere Behörden und die Öffentlichkeit täuschen?, in: Neue Juristische Wochenschrift 4, 153–159.

Felix, Dagmar (1998): Einheit der Rechtsordnung. Zur verfassungsrechtlichen Relevanz einer juristischen Argumentationsfigur, Mohr Siebeck: Tübingen.

Fischer, Thomas / Schwarz, Otto / Dreher, Eduard / Tröndle, Herbert (2015): Strafgesetzbuch: StGB mit Nebengesetzen, C.H. Beck: München.

Fischer-Lescano, Andreas (2014): Der Kampf um die Internetverfassung, in: Juristen Zeitung 69: 20, 965–974.

Foucault, Michel (1977): Überwachen und Strafen, Suhrkamp: Frankfurt am Main.

Frankfurter Allgemeine Zeitung (2014): Mit wehenden Frackschößen, 11.11.2014, http://www.faz.net/aktuell/politik/europaeische-union/london-heftige-debatte-im-unterhaus-13260875.html (15.08.2015).

Frisch, Peter (2003): V-Leute im Strafverfahren und im Verbotsverfahren, in: Deutsche Richterzeitung 81, 199–203.

Gärditz, Ferdinand (2014): Anmerkung, in: Juristen Zeitung 69: 20, 998–1002.

Gärditz, Ferdinand / Stuckenberg, Carl-Friedrich (2014): Vorratsdatenspeicherung à l'américaine – Zur Verfassungsmäßigkeit der Sammlung von Telefonverbindungsdaten durch die NSA, in: Juristen Zeitung 69:5, 209–219.

Gercke, Marco (2013): PRISM, TEMPORA und das deutsche Strafverfahren – Verwertbarkeit der Erkenntnisse ausländischer Nachrichtendienste, in: Computer und Recht 11, 749–754.

Golem.de (2014): Operation Eikonal: NSA wollte die DE-CIX-Daten des BND nicht mehr, 08.10.2014, http://www.golem.de/news/operation-eikonal-nsa-wollte-die-de-cix-daten-des-bnd-nicht-mehr-1410-109715.html (15.08.2015).

Grüter, Thomas (2013): Offline! Das unvermeidliche Ende des Internets und der Untergang der Informationsgesellschaft, Springer Spektrum: Berlin.

Günther, Hans-Ludwig (1983): Strafrechtswidrigkeit und Strafunrechtsausschluß. Studien zur Rechtswidrigkeit als Straftatmerkmal und zur Funktion der Rechtfertigungsgründe im Strafrecht, Carl Heymanns Verlag: Köln.

Hadagny, Christopher (2011): Kunst des Human Hacking: Social Engineering, mitp Verlags GmbH & Co. KG: Wachtendonk.

Heghmanns, Michael (2012): Straftaten gegen die betriebliche Datenverarbeitung, in: Achenbach, Hans / Ransiek, Andreas / Mosbacher, Andreas (Hrsg.): Handbuch Wirtschaftsstrafrecht, 741–816.

Hellmann, Uwe (1986): Die Anwendbarkeit zivilrechtlicher Rechtfertigungsgründe im Strafrecht, Carl Heymann: Köln.

Hettel, Alexander / Kirschhöfer, Max Phillip (2014): Aus aktuellem Anlass: Die Strafbarkeit geheimdienstlicher Spionage in der Bundesrepublik Deutschland, in: Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht 9, 341–349.

Hillenkamp, Thomas (2007): §§ 22 StGB, in: Laufhütte, Heinrich Wilhelm / Rissing-van Saan, Ruth / Tiedemann, Klaus (Hrsg.): Leipziger Kommentar zum StGB (LK-StGB), Bd. 1, de Gruyter: Berlin, Rn. 28, 99, 103.

Hillenkamp, Thomas (1995): In tyrannos - viktimodogmatische Bemerkungen zur Tötung des Familientyrannen, in: Kühne, Hans-Heiner (Hrsg.): Festschrift für Koichi Myazawa. Dem Wegbereiter des japanisch-deutschen Strafrechtsdiskurse, Nomos: Baden-Baden, 141–159.

Hofmann, Manfred / Ritzert, Silke (2014): Zur Strafbarkeit des Einsatzes nachrichtendienstlicher V-Personen in terroristischen Vereinigungen, extremistischen Organisationen und verbotenen Gruppierungen, in: Neue Zeitschrift für Strafrecht 4, 177–182.

Hoffmann-Riem, Wolfgang (2008): Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, in: Juristen Zeitung 63:21, 1009–1022.

Hoyer, Andreas (2009): Vorbemerkungen vor §§ 32ff. (Unrechtslehre), in: Wolter, Jürgen (Hrsg.): Systematischer Kommentar zum Strafgesetzbuch: SK-StGB, Carl Heymanns: Köln, Rn. 41.

Huber, Bertold (2013): Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite, in: Neue Juristische Wochenschrift 35, 2572–2576.

Huber, Bertold (2013): Das neue G 10-Gesetz, in: Neue Juristische Wochenschrift 45, 3296–3301.

Jahn, Matthias / Kudlich, Hans (2007): Die strafprozessuale Zulässigkeit der Online-Durchsuchung, in: Juristische Rundschau 2, 57–61.

Johnigk, Sylvia / Nothdurft, Kai (2014): Internet als Domäne von Militär und Geheimdiensten, in: Bittner, Peter / Hügel. Stefan / Kreowski, Hans-Jörg / Meyer-Ebrecht, Dietrich / Schinzel, Britta (Hrsg.): Gesellschaftliche Verantwortung in der digital vernetzten Welt, Lit Verlag: Berlin, 101–124.

Kargl, Walter (2013): § 202a Ausspähen von Daten, in: Kindhäuser, Urs / Neumann, Ulfrid / Paeffgen, Hans-Ullrich (Hrsg.): Nomos-Kommentar zum StGB (NK-StGB), Bd. 2, Nomos: Baden-Baden, 1402–1417.

Kilian, Wolfgang / Heussen, Benno / Cornelius, Kai (2013): Computerrechts-Handbuch, C.H. Beck: München.

Kloepfer, Michael (2002): Informationsrecht, C. H. Beck: München.

Lampe, Joachim (2015): Die Schwierigkeiten mit der Rechtfertigung nachrichtendienstlicher Tätigkeit, in: Neue Zeitschrift für Strafrecht 7, 361–372.

Lehleiter, Gunther (1995): Der rechtswidrige verbindliche Befehl. Strafrechtsdogmatische Untersuchung, demonstriert am Beispiel des militärischen Befehls, Peter Lang Verlag: Frankfurt am Main.

Lenckner, Theodor / Eisele, Jörg (2014): Verletzung des persönlichen Lebens- und Geheimbereichs (§§ 201–206), in: Schönke, Adolf / Schröder, Horst (Hrsg.): StGB. Kommentar, C.H. Beck: München, 1921–1996.

Lenckner, Theodor / Sternberg-Lieben, Detlev (2014): Vorbemerkungen vor § 32, in: Schönke, Adolf / Schröder, Horst (Hrsg.): StGB. Kommentar, C.H. Beck: München, RN 4.

Lenckner Theodor (1993): Der "rechtswidrige verbindliche Befehl" im Strafrecht - nur noch ein Relikt?, in: Küper, Wilfried (Hrsg.): Beiträge zur Rechtswissenschaft. Festschrift für Walter Stree und Johannes Wessels zum 70. Geburtstag, C.F. Müller: Heidelberg, 223–240.

Marberth-Kubicki, Annette (2008): Neuregelungen des Computerstrafrechts, in: IT-Rechtsberater, 17–19.

OLG Düsseldorf (2013): 6. 9. 2011 - 5 Sts 5/10: Vereinigungsmitglied als BND-Informant, in: Neue Zeitschrift für Strafrecht 10, 590–593.

OLG Karlsruhe (2000): 18. 10. 1999 - 2 Ws 51/99 : Gewerbliche Abgabe von Frischkäse in einer Gaststätte, in: Neue Zeitschrift für Strafrecht-RechtsprechungsReport 2, 60–62.

Paeffgen, Hans-Ullrich (2013): Notwehr und Notstand: Vorbemerkungen zu den §§ 32 ff, in: Kindhäuser, Urs / Neumann, Ulfrid / Paeffgen, Hans-Ullrich (Hrsg.): Nomos-Kommentar zum StGB (NK-StGB), Bd. 1, Nomos: Baden-Baden, 1247–1489.

Pawlik, Michael (2010): Zur strafprozessualen Verwertbarkeit rechtswidrig erlangter ausländischer Bankdaten, in Juristen Zeitung 65:14, 693–702.

Perron, Walter (2014): § 34 Rechtfertigender Notstand, in: Schönke, Adolf / Schröder, Horst (Hrsg.): StGB. Kommentar, C.H. Beck: München, 293–302.

Reinhard, Wolfgang (2007): Geheimnis und Fiktion als politische Realität, in: Reinhard, Wolfgang (Hrsg.): Krumme Touren – Anthropologie kommunikativer Umwege, Böhlau Verlag GmbH & Co. KG: Wien, 221–272.

Rinker, Mike (2002): Strafbarkeit und Strafverfolgung von „IP-Spoofing" und „Portscanning", in: MultiMedia und Recht 10, 663–665.

Rönnau, Thomas (2007): Vor § 32, in: Laufhütte, Heinrich Wilhelm / Rissing-van Saan, Ruth / Tiedemann, Klaus (Hrsg.): Leipziger Kommentar zum StGB (LK-StGB), Bd. 2, de Gruyter: Berlin, 1–352.

Roggan, Fredrik (2012): G-10-Gesetz, Nomos: Baden-Baden.

Roxin, Claus 2006: Strafrecht Allgemeiner Teil Band I: Grundlagen. Der Aufbau der Verbrechenslehre, C.H. Beck: München.

Schenke, Wolf-Rüdiger / Graulich, Kurt / Ruthig, Josef (2014) (Hrsg.): Sicherheitsrecht des Bundes. BPolG, BKAG, ATDG, BVerfSchG, BNDG, VereinsG, C.H. Beck: München 2014, § 1 BNDG Rn. 12 ff., § 3 BNDG Rn. 30.

Schmahl, Stefanie (2014): Effektiver Rechtsschutz gegen Überwachungsmaßnahmen ausländischer Geheimdienste?, in: Juristen Zeitung 69:5, 220–228.

Schmid, Gerhard (2001): Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem Echelon), EP, A5–0264/200,

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//DE (13.08.2015).

Schünemann, Bernd (2008): Prolegomena zu einer jeden künftigen Verteidigung, die in einem geheimdienstähnlichen Strafverfahren wird auftreten können, in: Goltdammer's Archiv für Strafrecht 155:5, 314–334.

Schwabenbauer, Thomas (2013): Heimliche Grundrechtseingriffe. Ein Beitrag zu den Möglichkeiten und Grenzen sicherheitsbehördlicher Ausforschung, Mohr Siebeck: Tübingen.

Singh, Himanshu / Chun, Robert (2010): Distributed Port Scan Detection, in: Stavroulakis, Peter / Stamp, Mark (Hrsg.): Handbook of Information and Communication Security, Springer: Heidelberg, 221–234.

Soiné, Michael (2012): Eingriffe in informationstechnische Systeme nach dem Polizeirecht des Bundes und der Länder, in: Neue Zeitschrift für Verwaltungsrecht 24, 1585–1589.

Stürmer, Michael (2006): Welt ohne Weltordnung, Murmann: Hamburg 2006.

Spiegel Online (2014a): Operation "Eikonal": Grüne und Linke verlangen Aufklärung über NSA-BND-Kooperation, 6.10.2014, http://www.spiegel.de/netzwelt/netzpolitik/eikonal-bnd-soll-daten-von-bundesbuergern-an-nsa-uebergeben-haben-a-995602.html (15.08.2015).

Spiegel Online (2014b): Britischer Geheimdienst GCHQ: Staatsanwaltschaft ermittelt nach mutmaßlichem Cyberangriff auf deutsche Firma, 21.09.2014, http://www.spiegel.de/netzwelt/netzpolitik/gchq-ermittlungen-nach-cyberangriff-auf-stellar-a-992903.html (13.08.2015).

Spiegel Online (2014c): NSA-System Treasuremap: "Jedes Gerät, überall, jederzeit", 17.09.2014, http://www.spiegel.de/netzwelt/netzpolitik/nsa-wie-der-geheimdienst-mit-dem-system-treasuremap-daten-sammelt-a-991496.html (13.08.2015).

Spiegel Online (2014d): Snowdens Deutschland-Akte: Die Dokumente im PDF-Format, 18.06.2014, http://www.spiegel.de/netzwelt/web/snowdens-deutschland-akte-alle-dokumente-als-pdf-a-975885.html (13.08.2015).

Spiegel Online (2013): Britische Internet-Überwachung: Freund liest mit, 22.06.2013, http://www.spiegel.de/netzwelt/netzpolitik/internetueberwachung-tempora-geheimdienst-zapft-glasfaserkabel-an-a-907283.html (13.08.2015).

Süddeutsche Zeitung (2014a): Codewort Eikonal - der Albtraum der Bundesregierung, 04.10.2014, http://www.sueddeutsche.de/politik/geheimdienste-codewort-eikonal-der-albtraum-der-bundesregierung-1.2157432 (13.08.2014).

Süddeutsche Zeitung (2014b): BND leitete Daten von Deutschen an NSA weiter, 03.10.2014, http://www.sueddeutsche.de/politik/spaeh-affaere-bnd-leitete-daten-vondeutschen-an-nsa-weiter-1.2157406 (13.08.2015).

Süddeutsche Zeitung (2014c): NSA kann offenbar direkt auf Telekom-Netz zugreifen, 13.09.2014, http://www.sueddeutsche.de/digital/neue-enthuellung-aus-snowden-dokumenten-nsa-kann-offenbar-direkt-auf-telekom-netz-zugreifen-1.2128313 (13.08.2015).

Süddeutsche Zeitung (2014d): Schreibmaschine soll für sichere Kommunikation sorgen, 14.07.2014, http://www.sueddeutsche.de/politik/nsa-untersuchungsausschuss-schreibmaschine-soll-fuer-sichere-kommunikation-sorgen-1.2045675 (16.08.2015).

Symantec (2014): Security Response. Regin: Top-tier espionage tool enables stealthy surveillance, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf (7.08.2015).

The New York Times (2013): N.S.A. Report Outlined Goals for More Power, 22.11.2013, http://mobile.nytimes.com/2013/11/23/us/politics/nsa-report-outlined-goals-for-more-power.html?hp=&pagewanted=all&_r=4 (13.08.2015).

Weißer, Bettina / Heine, Günter (2014): Täterschaft und Teilnahme (§§ 25–31), in: Schönke, Adolf / Schröder, Horst (Hrsg.): StGB. Kommentar, C.H. Beck: München, 478–570.

Wolf, Joachim (2013): Der rechtliche Nebel der deutsch-amerikanischen ,,NSA-Abhöraffäre“, in: Juristen Zeitung 68:21, 1039–1046.

Zeit Online (2015): Alles Wichtige zum NSA-Skandal. Welche Daten sammelt die NSA, was ist Prism und wie reagieren die Überwachten? Aktuelle Entwicklungen und ein Überblick über die Snowden-Enthüllungen seit Juni 2013, 02.07.2015, http://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal (13.08.2015).

Zöller, Mark (2007): Der Rechtsrahmen der Nachrichtendienste bei der „Bekämpfung“ des internationalen Terrorismus, in Juristen Zeitung 62:15/16, 763–771.

Autor

PD Dr. Kai Cornelius, LL.M.
Lehrstuhlvertreter an der Humboldt-Universität zu Berlin – Juristische Fakultät
Lehrstuhl für Strafrecht, Strafprozessrecht und Urheberrecht
Unter den Linden 6
D-10099 Berlin
cornelius@rewi.hu-berlin.de

DOI: 10.11588/josar.2015.0.23482

The **Journal of Self-Regulation and Regulation** is an open-access peer-reviewed journal serving as a potential outlet for edge-cutting interdisciplinary research on regulatory processes in individuals and organizations. It is published by the research council of Field of Focus 4 (FoF4) of Heidelberg University. The research council stimulates and coordinates interdisciplinary activities in research and teaching on self-regulation and regulation as part of the university's institutional strategy "Heidelberg: Realising the Potential of a Comprehensive University", which is funded by the Federal Government as part of the excellence initiative.

The *Journal of Self-Regulation and Regulation* publishes two volumes per year, regular volumes containing selected articles on different topics as well as special issues. In addition, the reader will be informed about the diverse activities of FoF4, uniting scientists of the faculty of behavioural and cultural studies, the faculty of social sciences and economics, as well as the faculty of law.

Imprint

Journal of Self-Regulation and Regulation Volume 01 (2015)

Research Council of Field of Focus 4, Heidelberg University
Forum Self-Regulation and Regulation
Hauptstr. 47–51
69117 Heidelberg, Germany

Fon: +49 (0)6221 / 54 – 7122
E-mail: fof4@psychologie.uni-heidelberg.de
Internet: https://www.uni-heidelberg.de/fof4

Publisher: Research Council of Field of Focus 4, Heidelberg University
Spokesperson: Sabina Pauen, Department of Psychology
Guest Editors: Wolf J. Schünemann, Department of Political Science
Sebastian Harnisch, Department of Political Science
Editorial Team: Melanie Bräunche, Sabine Falke

You can download the volumes of the *Journal of Self-Regulation and Regulation* free of charge at:
http://journals.ub.uni-heidelberg.de/index.php/josar/index