Ingo Ruhmann und Ute Bernhardt

IT-Sicherheitsrecht 2.0 – Einschränkungen statt Schutz von Grundrechten

Der Schutz von Persönlichkeitsrechten und des Grundrechts auf informationelle Selbstbestimmung war von Beginn an abhängig von adäquaten technischen und organisatorischen Schutzmaßnahmen gegen die missbräuchliche Nutzung von Daten und gegen Eingriffe in IT-Systeme. Spätestens mit dem 2008 definierten Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[1] ist die Exekutive in besondere Weise aufgefordert, technische, organisatorische und rechtliche Maßnahmen zu treffen, um digitale Schutzrechte zu gewährleisten. Zusammen mit dem Fernmeldegeheimnis gibt es einen klar formulierten Rahmen von Grundrechten, dem Rechtsetzung und die Praxis zur IT-Sicherheit folgen müssten. Die gegenwärtige Entwicklung wird dem nicht gerecht.

Die zunehmende Zahl von IT-Sicherheitsvorfällen, die sich nicht allein gegen Unternehmen und Privatpersonen richten, sondern auch gegen den Bundestag, Ressorts der Bundesregierung und internationale Einrichtungen, dokumentiert die Dringlichkeit, den Schutz der IT-Systeme zu verbessern. Die Untersuchung der Art und Intensität einiger Vorfälle hat verdeutlicht, dass die früher dominierenden Angreifer mit privatem oder kriminellem Hintergrund zunehmend durch staatliche Akteure ergänzt wurden, die über Ressourcen in vorher nicht gekanntem Ausmaß verfügen und diese auch intensiv – gegen Verbündete ebenso wie gegen Wettbewerber – einsetzen.

Die Bundesregierung hat 2015 darauf regulatorisch reagiert durch die Verabschiedung des IT-Sicherheitsgesetzes.[2] Nachgelegt wird nun das „*IT-Sicherheitsgesetz 2.0*“.[3] Nicht minder umfangreich fiel die Reaktion auf exekutiver Ebene aus. Die Aufgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI), des Bundesamtes für Verfassungsschutz (BfV), des Bundeskriminalamtes (BKA) und des Bundesnachrichtendienstes (BND) wurden erweitert und mit erheblichen Personalzuwächsen unterlegt. Mit der Errichtung der *Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITIS)* des Innenressorts und der *Agentur für Disruptive Innovationen in der Cybersicherheit und Schlüsseltechnologien (ADIC)* von Innen- und Verteidigungsressort wird die zielgerichtete Entwicklung und Bereitstellung von Werkzeugen für Cyber-Aktivitäten für Stellen des Bundes verfolgt, begleitet durch die Restrukturierung des ehemaligen *Kommandos Strategische Aufklärung* und dessen Migration in das *Kommando Cyber- und Informationsraum (KdoCIR)* der Bundeswehr. Die neuen Aufgaben von ZITIS, ADIC und KdoCIR, aber auch des BND und BfV sind allerdings keineswegs auf den Schutz der Integrität, Verfügbarkeit und Vertraulichkeit von IT-Systemen bezogen. Ihre Aufgabe ist es, Sicherheitslücken in IT-Systemen zu finden, neue Angriffsformen zu entwickeln und diese Hintertüren für staatliche Stellen nutzbar zu machen. Ihr Organisationszweck steht daher in einem starken Spannungsverhältnis zum verfassungsmäßigen Schutz von Grundrechten.

Wie viele andere Bereiche der IT-Sicherheit auch[4], so laufen Entwicklung, Einsatz und Nutzung von Angriffswerkzeugen sowie die dafür notwendigen Vorarbeiten nicht nur verfassungsmäßigen Grundsätzen zuwider. Wie im Folgenden nachgezeichnet wird, stehen viele der erforderlichen Arbeitsschritte in konkretem Widerspruch zum Strafrecht und zum internationalen Recht. Die aufgeworfenen Fragen sind komplex, vielfach neu und im deutschen Recht in keiner systematischen Weise in Beziehung zueinander gesetzt. Hier sollen daher vor allem die verschiedenen Dimensionen einer rechtlichen Bewertung unterzogen und mögliche Konsequenzen aufgezeigt werden. Ausgehend von einer Binnensicht des deutschen Rechts bei konkreten Eingriffen in IT-Systeme wird untersucht, welche rechtlichen Neuerungen geplant sind, um Ansätze für spezifische Eingriffe zu erhalten und auch die als „Hack-Backs“ bezeichneten Angriffe auf IT-Systeme außerhalb des deutschen Staatsgebiets vorzubereiten.

Das Recht

Staatliches Handeln basiert auf Gesetzen. Der Aufbau von Behörden und jede Verwendung öffentlicher Mittel sind abhängig von der Definition von Aufgaben, die sich aus den in den Verfassungen von Bund und Ländern vorgesehenen Rechten und Pflichten ableiten lassen müssen. Wenn exekutives Handeln in die Rechte Dritter – möglicherweise sogar Grundrechte – eingreift, so sind gesetzlich möglichst klar definierte Rechtsnormen erforderlich. Das darauf bezogene Exekutivhandeln sollte richterlich – oder wenn dies der Aufgabe nach nicht möglich ist, notfalls durch vergleichbare Konstruktionen wie parlamentarische Kontrollgremien – überprüfbar sein.

Das Grundrecht auf Unverletzlichkeit der Wohnung ist im Strafrecht nicht nur gegen die Entnahme von Wertgegenständen – Einbruchdiebstahl – geschützt, sondern beim Hausfriedensbruch auch gegen unerwünschtes Betreten. In der Strafprozessordnung ist formuliert, unter welchen Bedingungen durch staatliche Stellen in das Grundrecht auf Unverletzlichkeit der Wohnung eingegriffen und auf die Kompetenz von Schlossern für die nicht-konsensuelle Schaffung von Zugängen zurückgegriffen werden darf.

In der digitalen Sphäre werden solche im Analogen selbstverständlichen Grundsätze infrage gestellt. Schon beim Staatstrojaner wurde nicht ausgeschlossen, die Trojaner-Software bei Bedarf über einen physischen Zugang – d. h. den verdeckten Einbruch in die Räume der Zielperson – zu installieren.[5] Die Bundesregierung hatte bei der Reform des BSI-Gesetzes 2007 die Idee, dem BSI die Befugnis zu geben, ohne richterlichen Beschluss die Geschäftsräume eines Betreibers von Kommunikationstechnik zu betreten und sich „Zugang zu Gebäuden, Einrichtungen und informationstechnischen Systemen verschaffen“, „wenn dies zur Abwehr einer dringenden Gefahr für die Kommunikationstechnik des Bundes erforderlich sei“[6]. Davon nahm sie nur zögerlich Abstand. Diese Idee taucht nun modifiziert im *IT-Sicherheitsgesetz 2.0* wieder auf, eingeschränkt auf die Betriebsräume der Betreiber der von Bundesbehörden genutzten IT-Systeme. Anstatt also den Bundesbehörden Auflagen bei der Vergabe von Aufträgen an Rechenzentren zu machen, wird das BSI generell gesetzlich zum Eingreifen befugt. Noch weiter geht die Bundesregierung im „IT-Sicherheitsgesetz 2.0“ mit einem geplanten § 163g der Strafprozessordnung (StPO)[7], nach dem die Sicher-

heitsbehörden „auch gegen den Willen des Inhabers auf Nutzerkonten“ und die „Funktionen, die ein Anbieter eines Telekommunikations- oder Telemediendienstes dem Verdächtigen zur Verfügung stellt“ […] zugreifen“ können sollen. Dazu muss ein Nutzer den Sicherheitsbehörden die Zugangsdaten zu ihren Online-Diensten herausgeben, damit die Behörden die Online-Konten übernehmen und im Namen des Nutzers agieren können. Die Zulässigkeit der neuen Regelung wird an die Voraussetzungen des bestehenden § 100g StGB geknüpft. Der erlaubt die Abfrage von Verkehrsdaten wie etwa Funkzellen bei Verdacht auf schwere oder gemeingefährliche Straftaten, solchen gegen das Betäubungsmittelgesetz, bei Schleuser-Tätigkeit sowie bei Waffenhandel. Erlaubt würde danach die Identitätsübernahme durch den § 163g StPO aber – so § 100g STGB – auch bei „einer Straftat von auch im Einzelfall erheblicher Bedeutung“ oder wenn ein Verdächtiger eine Tat „in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat […] oder eine Straftat mittels Telekommunikation begangen hat“. Da alle Computer-Straftaten „mittels Telekommunikation“ begangen werden, ist die Folge, dass jeder Verdacht auf eine solche ausreichend wäre für eine Identitätsübernahme durch die Sicherheitsbehörden. Das ist nicht nur eine neue Dimension von Grundrechtseingriffen, sondern dürfte obendrein bei der Attribution von Cyberangriffen ganz neue Komplikationen aufwerfen. All dies sind Regelungsideen, die übertragen auf die analoge Welt als rechtswidriger Eingriff unmittelbar nachvollziehbar wären. Aber auch das Grundrecht auf informationelle Selbstbestimmung und das auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sind strafrechtlich in ähnlicher Weise gegen Einbruch in Systeme, Diebstahl oder Manipulation von Daten, gegen den Handel mit Einbruchswerkzeugen und einige Spezifika geschützt. Neu ist, dass die Bundesregierung die Entwicklung technischer Vorkehrungen zur Schaffung von Zugängen nun selbst in die Hand nimmt.

Der Austausch über Sicherheitslücken und die dazu verwendeten Mittel ist für IT-Sicherheitsexperten immer mit einem strafrechtlichen Risiko verbunden. Dem aktuellen Wortlaut des § 202c Strafgesetzbuch (StGB) nach macht sich bereits strafbar, wer Computerprogramme entwickelt, die Sicherungsmaßnahmen überwinden können und den Zugang zu geschützten Daten ermöglichen, oder sie „herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht“. Die Bundesregierung begründete die Einführung dieser Regelung: Die „Gefährlichkeit und Schädlichkeit von Hacking-Angriffen zeigen sich vor allem in jüngster Zeit auch in Deutschland (z. B. durch den Einsatz von Key-Logging-Trojanern, Sniffern oder Backdoorprogrammen)“[8]. Nun plant die Bundesregierung im *IT-Sicherheitsgesetz 2.0* überdies die Einführung eines § 200e StGB, um den „unbefugten Zugang zu einem Informationstechnischen System“ für sich oder einen Dritten unter Strafe zu stellen[9].

Neue Behörden und Befugnisse

Aufgabe von ZITIS ist, Zugangs- und Entschlüsselungswerkzeuge zu entwickeln bzw. einzukaufen und anderen zur Verfügung zu stellen. ZITIS hat also die Aufgabe, die technischen Mittel für genau die beiden hier beschriebenen Gesetzesverstöße zu entwickeln, zu beschaffen und anschließend anderen Behörden zu überlassen, ohne dass dafür gesetzliche Ausnahmen geschaffen wurden. Die Agentur für Disruptive Innovationen (ADIC) von Innen- und Verteidigungsressort setzt einen Schritt davor an und verfolgt die Entwicklung von IT-Sicherheitstechnik ebenso wie die von Angriffswerkzeugen für zivile Behörden und die Bundeswehr. Die Bundesregierung schließt zwar aus, Malware-Implantate in kritischen Infrastrukturen anderer Staaten „ohne die entsprechenden, insbesondere völkerrechtlichen, Rechtsgrundlagen einzusetzen“[10]. Nicht ausschließen will sie aber deren Entwicklung und auch deren Einsatz auf Rechtsgrundlagen, deren Prüfung sie noch nicht abgeschlossen hat.[11] Wohlgemerkt: Der Schutz von IT-Systemen ist Verfassungsauftrag und Grundrecht, eine Verbesserung des gesetzlichen Schutzes ist daher eindeutig zu begrüßen. Umso deutlicher ist dann aber der Bedarf, die Befugnisse der Behörden ebenso klar zu regeln.

Denn ZITIS kann sich auf kein Sonderrecht berufen. Die Spionagetätigkeit des BND bedeutet auch das Eindringen in fremde IT-Systeme. Auch die Bundeswehr soll im Kriegsfall in gegnerische IT-Systeme einbrechen. Das BSI entstammt zwar als Zentralstelle für das Chiffrierwesen dem BND,[12] prüft heute aber auf Basis eines eigenen Gesetzes IT-Sicherheitsaspekte und entwickelt und testet zivile Chiffriersysteme[13]. ZITIS soll der Bundesregierung zufolge die Behörden der Inneren Sicherheit mit informationstechnischen Fähigkeiten unterstützen. ZITIS sei kein Nachrichtendienst und habe keine Eingriffsbefugnisse und keine Sonderrechte.[14] ZITIS arbeitet somit entgegen strafrechtlicher Regelungen. Die Aufgabe der ADIC ist zwar abstrakter und in die Forschung vorverlagert; aber das Strafrecht sieht für Forschungsarbeiten aber keine Ausnahme vor. Die Tätigkeit der so Beschäftigten ist damit strafbar.

Um Sicherheitsvorfälle zu erkennen, müssen befallene Systeme forensisch untersucht werden bzw. die Datenkommunikation mit Hilfe von Auswertungssoftware – *Intrusion-Detection*-Systemen – auf Anomalien hin analysiert werden. Aufgabe der ZITIS-Abteilung TKÜV sind Arbeiten zur „Telekommunikationsüberwachung (u. a. Verbesserung des internationalen Datenaustauschs auf Grundlage der Europäischen Ermittlungsanordnung und der Auswertung von IP-Daten)“.[15] Aus rechtlicher Sicht stellt sich aber die Frage, woher die Daten für die Auswertung stammen. Für das auf Verdacht erfolgende Protokollieren und Auswerten von beliebigem, bei einem Provider durchlaufenden Datenverkehr (*Deep Packet Inspection*) wurde im § 100 Telekommunikationsgesetz (TKG) eine erweiterte Befugnisnorm nur für die Provider selbst geschaffen. Weder das BSI noch andere Behörden sind derzeit befugt, Kommunikationsdaten von Providern anzufordern und zu analysieren. Lediglich der BND kann bei der strategischen Kommunikationsüberwachung des Datenverkehrs mit dem Ausland Daten sammeln, die zur Analyse von Angriffen nutzbar sind. Strafverfolgungsbehörden dürfen derzeit nur Telekommunikations-*Verkehrsdaten* anfordern.[16] Die Weitergabe der von Fachleuten klassifizierten Kommunikationsinhalte bei IT-Sicherheitsvorfällen ist eine Straftat[17].

Der Schutz des Fernmeldegeheimnisses wird erst dann umgangen werden, wenn das BSI mit dem IT-Sicherheitsgesetz 2.0 durch eine Ergänzung an § 109 TKG Provider anweisen kann, protokollierte Kommunikationsdaten zu übergeben, um die Daten automatisiert auszuwerten – und sie 10 Jahre lang zu speichern[18]. ADIC oder ZITIS dürften aber auch dann nicht legal

über Kommunikationsdaten für IT-Sicherheitsanalysen verfügen. Diese können nur von einem Provider oder einer staatlichen Stelle stammen, die diese Daten unter Bruch des Fernmeldegeheimnisses weitergegeben hat.

Rechtliche Befugnisse und Aufgaben der alten und neuen Behörden zur IT-Sicherheit stehen also in einem wenig systematischen und widersprüchlichen Verhältnis zueinander.

Hack-Backs in Krieg und Frieden

Zu den neuen Operationsideen in der staatlichen IT-Sicherheit haben sich „Hack-Backs" gesellt, der offiziellen Darstellung zufolge die Beantwortung eines Cyberangriffs in der Regel aus dem Ausland durch gleichartige Gegenmaßnahmen. Lassen wir hier zunächst den Spannungs- und Verteidigungsfall beiseite, dann steht in einem an Recht und Gesetz gebundenen System auch diese Idee mit dem Strafrecht in einem nicht überbrückbaren Spannungsverhältnis.

§ 303 StGB stellt unter Strafe, Datenverarbeitungsanlagen oder Datenträger zu zerstören, zu beschädigen, unbrauchbar zu machen, zu beseitigen oder zu verändern. Nichts anderes ist das Ziel von Hack-Backs: Das Eindringen in fremde IT-Systeme, das Löschen von dort abgelegten Daten, das Hinterlegen und Installieren von Schadsoftware, die Außerbetriebnahme des gehackten Systems und andere Manipulationsformen.

Die Idee der Hack-Backs produziert einen ganz neuen Zielkonflikt. Zur Schadenminderung erlaubt das TKG in § 109 den Providern, Datenverkehre von und zu einer Störquelle einzuschränken, umzuleiten oder zu unterbinden. Das BSI soll nach dem *IT-Sicherheitsgesetz 2.0* Provider in Zukunft dazu anweisen können. Eine Störung oder ein Angriff wären damit zu beenden. Allerdings wäre ein von Providern – etwa durch Vorkehrungen in Routing-Tabellen – effektiv blockiertes IT-System auch für Hack-Backs der Sicherheitsbehörden nicht mehr direkt erreichbar. Wer Hack-Backs einsetzen will, wird den Angreifer also nicht einfach vom Internet-Datenverkehr aussperren wollen – oder muss seinerseits Zugangswege über Dritte suchen und die Auseinandersetzung über deren Wege führen – was eine Ausweitung des Angriffs nach sich ziehen dürfte.

Auch das Argument, die internationale Kooperation sei zu umständlich, trägt nicht. Die Bundesregierung hat sich mit der *Budapest Convention on Cybercrime* zur Kooperation und gegenseitigen Unterstützung bei Cyberattacken verpflichtet. Ausgenommen davon sind nach Art. 27 (4) der Konvention nur Fälle „nationaler Souveränität" und „essentieller Interessen". Unkooperatives Verhalten verrät implizit seine (sicherheits-) politischen Beweggründe und damit die Beteiligung staatlicher Stellen. Dies wiederum sieht das *Tallinn-Manual* – Ergebnis eines von der NATO beauftragten Expertenkreises – recht eindeutig: Von staatlichen Stellen nicht unterbundene Angriffe gegen IT-Systeme in einem anderen Staat stellen einen Bruch internationalen Rechts dar. Angriffe von staatlichen Stellen auf andere Staaten stellen Kriegshandlungen dar. Sie rechtfertigen sogar konventionelle militärische Gegenschläge, wenn die Schäden die Wirkung von Militärschlägen erreichen. Gegen IT-Systeme in anderen Staaten gerichtete Hack-Backs sind daher keine Lösung in transnationalen Cyber-Vorfällen, sondern ein Bruch internationalen Rechts oder gar der Weg zu Kriegshandlungen.[19]

Praxis der Hack-Backs sind präemptive Eingriffe

Doch damit nicht genug. Im Vorfeld der Cyber-Sicherheitskooperation zwischen den USA und der VR China 2015 sickerte durch, die US-Dienste würden das Abkommen nicht akzeptieren, wenn sie auf ihre Implantate in den Systemen der VR China verzichten müssten.[20] Prominente Datendiebstähle bei US-Behörden machten zugleich klar, dass die chinesischen Cyber-Akteure den USA nicht nachstehen. Zu den wenig beachteten Snowden-Enthüllungen gehört auch, dass der für elektronische Kriegsführung zuständige US-Geheimdienst NSA in Systeme gegnerischer Dienste einbricht, dort Implantate hinterlässt und sich Erkenntnisse von gegnerischen Aufklärungserfolgen auf dritter Seite und sogar vierter Seite beschafft. Die NSA weiß dadurch, dass und wie andere Dienste ihre Werkzeuge in allerlei fremden IT-Systemen einbauen – und dass konkurrierende Dienste dasselbe tun. Den Cyberkriegern dieser Welt ist also bekannt, dass alle Seiten ihre Cyberwaffen in den Infrastrukturen ihrer Zielländer in Stellung gebracht haben und bei Bedarf losschlagen können.

Hack-Backs sind keineswegs nur eine Notwehr-Maßnahme. Hack-Backs dienen dem Ausschalten der IT-Infrastruktur von vermuteten Gegnern, und zugleich der Vorbereitung solcher Cyber-Operationen. Dies hat die Bundesregierung als Handlungsoption nicht ausgeschlossen, wenn es die Rechtslage hergibt.[21] Dazu gehört, die Urheberschaft zu verschleiern und Fährten zu nichts ahnenden Dritten zu legen. Die Bundesregierung erklärte „False Flag"-Angriffe – zu Deutsch: das Kapern von Rechnern in Drittstaaten und deren Missbrauch für Cyberangriffe – zur zulässigen Kriegslist.[22]

Der russischen Seite wird vorgeworfen, Hacker für staatliche Zwecke als digitale Söldner einzusetzen.[23] Mit dem in Deutschland geplanten Zwang zur Herausgabe persönlicher Zugangsdaten zu Online-Diensten bei Straftaten, die „mittels Telekommunikation begangen werden", damit die Behörden die eigenen Online-Konten übernehmen und damit operieren können, entsteht eine ganz neue und eigene Form der Verwicklung von Hackern, IT-Sicherheitsfachleuten, Internetnutzern und staatlichen Stellen für Cyber-Operationen in einem Maße, das man bei Spionagefilmen für maßlos übertrieben halten würde.

Fazit

Wenn Behörden wie BND, BfV, ZITIS, ADIC und die Bundeswehr erst nach Sicherheitslöchern suchen, um dann in IT-Systeme einzugreifen und Hack-Backs durchzuführen, kompromittieren sie nicht nur die Sicherheit der IT-Infrastruktur, sondern setzen für ihr Eingriffshandeln voraus, dass die Missetäter ungestört weiter operieren können. Die meisten der beteiligten Behörden dürften nicht einmal über die Daten verfügen, die sie benötigen, um Gefährdungen aufzuspüren oder Angriffswege zu finden.

Mit der Entwicklung von Angriffsoptionen anstelle einer ausgebauten Kooperation mit staatlichen Stellen anderer Länder verstößt die Bundesregierung gegen internationales Recht. Hack-

Backs sind nicht nur keine Antwort auf IT-Sicherheitsvorfälle, sondern als Mittel zum Setzen von Implantaten in gegnerische IT-Systeme und Infrastrukturen essenzielle Voraussetzung für die Vorbereitung und Führung von Cyberkonflikten. Im Spannungsfall bringen Hack-Backs hoch riskante Eskalationsgefahren mit sich und geben angegriffenen Staaten einen völkerrechtlich legitimierbaren Grund, gegen Deutschland mit militärischen Mitteln vorzugehen. Mit dem *IT-Sicherheitsgesetz 2.0* sollen hierfür weitere Grundlagen geschaffen werden.

Vergleichbar zu den Zeiten des Kalten Kriegs haben wir bei Cyberwaffen ein Maß an gegenseitiger Abschreckung erreicht, das kooperative Maßnahmen dringend erforderlich macht, um eine schnelle und gefährliche Eskalation zu verhindern. Die notwendige Bedingung zur Bekämpfung von mehrstufigen Angriffen ist die Kooperation von Stellen in den verschiedenen betroffenen Staaten, um den Urhebern von Angriffen auf die Spur zu kommen. Die USA, Russland und die VR China hatten bis 2015 bereits eine dreiseitige Cyber-Sicherheitskooperation zuwege gebracht. Wer IT-Sicherheit erhalten will, muss als nächste Schritte auf den Ausbau von Kooperations- und Informationsstrukturen in internationalen Abkommen abzielen. Das setzt verantwortliches politisches Handeln voraus. Hack-Backs und die damit verbundenen Wege zur Schwächung der IT-Sicherheit sind das genau nicht.

Anmerkungen

1 *Bundesverfassungsgericht, Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07, 1 BvR 595/07*
2 *Bundesgesetzblatt, Teil I, Nr. 31, 17.7.2015, S. 1324*
3 *Am 3.4.2019 veröffentlicht von netzpolitik.org unter https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/#2019-03-27_BMI_Referentenentwurf_IT-Sicherheitsgesetz-2*
4 *Ingo Ruhmann, Ute Bernhardt: IT-Sicherheit, das EU-Recht und die Grundrechte: Neustart erforderlich; Gutachten des Netzwerks Datenschutz-Expertise, Mai 2016, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_eugh-itsig-2016.pdf*
5 *Vgl. etwa Dirk Fox in seinem Gutachten für das BVerfG, erschienen als Artikel: „Realisierung, Grenzen und Risiken der „Online-Durchsuchung“, DuD, Nr 31 (2007), S. 827-834, https://www.secorvo.de/publikationen/online-durchsuchung-fox-2007.pdf*
6 *Zitiert nach: http://www.dradio.de/dlf/sendungen/computer/849757/*
7 *Zitiert nach dem Entwurfstext bei netzpolitik.org, a.a.O.*
8 *So die Begründung der Gesetzesnovelle durch die Bundesregierung in Bt.-Drs. 16/3656, S. 9.*
9 *Auch dies zitiert nach dem Entwurfstext bei netzpolitik.org, a.a.O.*
10 *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Tobias Pflüger, Andrej Hunko, Michel Brandt, weiterer Abgeordneter und der Fraktion DIE LINKE: Rechtlich-organisatorischer Rahmen militärischer Cyber-Operationen, Bt.-Drs. 19/11920, Frage 9b*
11 *Ebd. Antwort auf die Fragen 3 bis 5*
12 *Ute Bernhardt; Ingo Ruhmann: Mutation einer Geheimdienststelle; in: Computerwoche, Nr. 12, 23. März 1990, S. 44–47*
13 *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) vom 14.08.2009*
14 *So die Bundesregierung in der Vorbemerkung und zu Frage 1 in der Antwort auf die Kleine Anfrage Struktur und Tätigkeit der Zentralen Stelle für Informationstechnik im Sicherheitsbereich, der Abg. Hahn u.a, Bt.-Drs. 19/6246*
15 *Ebd. Antwort auf Frage 22*
16 *Gemäß §100g StPO muss ein Provider Details der in Anspruch genommenen Telekommunikationsdienste und die Beteiligten an dem Telekommunikationsvorgang gemäß §96 TKG an Strafverfolgungsbehörden weitergeben.*
17 *Ingo Ruhmann, Ute Bernhardt: Der EuGH-Entscheid als Anstoß für mehr Rechtssicherheit in der IT-Sicherheit; DuD, Nr. 1, 2017, S. 34–38, S. 35f*
18 *So die geplante Änderung an §109 TKG im Entwurf des IT-Sicherheitsgesetz 2.0*
19 *Michael N. Schmitt (ed.): The Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge, 2013, S. 26ff*
20 *David E. Sanger: U.S. and China Seek Arms Deal for Cyberspace, New York Times, Sept. 19, 2015, http://www.nytimes.com/2015/09/20/world/asia/us-and-china-seek-arms-deal-for-cyberspace.html?_r=0*
21 *Vgl. Endnote 10, Antwort der Bundesregierung auf Frage 9b, Bt.-Drs. 19/11920*
22 *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan van Aken, Andrej Hunko, Christine Buchholz, weiterer Abgeordneter und der Fraktion DIE LINKE, „Elektronische Kampfführung der Bundeswehr“, BT-Drs. 18/3963, Antwort auf Fragen 30–33; Für die Nutzung ziviler IT-Systeme für solche Operationen siehe Plenarprotokoll der Fragestunde der 16. Sitzung des Deutschen Bundestages vom 19.2.2014, Antwort auf Frage 8, S. 1165 f.*
23 *So etwa beim Angriff auf den Bundestag: Wie russische Hacker Deutschland angriffen, Spiegel Online, 2.3.2018, https://www.spiegel.de/spiegel/spionage-wie-russische-hacker-deutschland-angriffen-a-1196180.html*

Ingo Ruhmann und Ute Bernhardt

Ingo Ruhmann ist Informatiker und arbeitet im Bereich Technikfolgenabschätzung, Forschungspolitik, IT-Sicherheit, Information Warfare, *Cyberwar*, Geschichte der Geheimdienste und Datenschutz. Er ist Lehrbeauftragter im Studiengang *Security Management* der Fachhochschule Brandenburg. Er ist Mitglied des FIfF und war Vorstandsmitglied von 1991 bis 1998.

Ute Bernhardt ist Informatikerin und beschäftigt sich seit Jahren mit Forschungspolitik, Datenschutz und IT-Sicherheit, dem Verhältnis von Wissenschaft und Frieden sowie der Beziehung von Informatik und Militär. Sie hat Lehraufträge an der Fachhochschule Bonn-Rhein-Sieg und der FernUni Hagen. Sie ist Mitglied des FIfF und war FIfF-Vorstandsmitglied von 1991 bis 1998.