Chaos Computer Club

Risiken für die innere Sicherheit beim Einsatz von Schadsoftware in der Strafverfolgung

Sachverständigenauskunft zum Änderungsantrag der Fraktionen CDU/CSU und SPD zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze (Ausschussdrucksache 18/11272)

Linus Neumann,
Constanze Kurz, Frank Rieger
Mittwoch, 31. Mai 2017

Abstract

Gefahr für die innere Sicherheit: Mit der Geheimhaltung von Sicherheitslücken, die zum Anbringen von Schadsoftware benötigt werden, geht eine Gefahr für die innere Sicherheit einher.

Unverhältnismäßiger Grundrechtseingriff bei niedriger rechtlicher Schwelle: Die rechtlichen Grenzen der sogenannten Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) lassen sich technisch kaum umsetzen, wodurch de facto eine Online-Durchsuchung geschaffen wird.

Fehlender Beleg der Notwendigkeit: Strafverfolgungsbehörden haben dank der fortschreitenden Digitalisierung aller Lebensbereiche bereits heute Zugriff auf eine nie dagewesene Fülle an Daten.

Fehlende technische Überprüfbarkeit und Nachvollziehbarkeit: Die technischen Rahmenbedingungen für den Einsatz von Schadsoftware sind nicht ausreichend spezifiziert, um Rechtssicherheit oder adäquate Kontrolle sicherzustellen.

Drohende Verletzung der Eckpunkte deutscher Kryptopolitik: Die unklare Definition der Mitwirkungspflichten sowie anstehende Änderungen der Regulierung im Telekommunikationsmarkt erschweren die Folgenabschätzung für Vertrauen, Sicherheit und Marktposition deutscher Anbieter von Verschlüsselungslösungen.

Einleitung

Im vorliegenden Änderungsantrag sollen die Ermittlungsmethoden der sogenannten „Quellen-Telekommunikationsüberwachung“ (Quellen-TKÜ) und der „Online-Durchsuchung“ im Rahmen der Strafprozessordnung geregelt werden.

Beide Maßnahmen bezeichnen das Anbringen einer Schadsoftware auf ein informationstechnisches System zum Zwecke der Ausleitung von Daten. Der Umfang der auszuleitenden Daten wird bei der Quellen-TKÜ rechtlich auf Kommunikationsinhalte begrenzt, während im Rahmen der Online-Durchsuchung das gesamte informationstechnische System übernommen werden darf. Für beide Methoden müssen vorab technische Systemparameter auf dem Zielsystem ermittelt und verifiziert werden.

Beide Maßnahmen sind aufgrund des hohen Grundrechtseingriffs bereits seit längerer Zeit Gegenstand öffentlicher und juristischer Debatten. Wichtige Ergebnisse dieser Diskussionen und der Beschwerdeverfahren vor dem Bundesverfassungsgericht müssen für den Änderungsantrag berücksichtigt werden und seien daher einleitend in Erinnerung gerufen:

Februar 2008: Der Erste Senat des Bundesverfassungsgerichts urteilt, dass das allgemeine Persönlichkeitsrecht gemäß Art. 2 Abs. 1 und Art. 1 Abs. 1 des Grundgesetzes auch ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst.[1]

Dezember 2008: Mit der Novellierung des BKA-Gesetzes erhält das Bundeskriminalamt (BKA) die Ermächtigungsgrundlage sowohl zur Quellen-TKÜ als auch zur Online-Durchsuchung.[2] Mehrere Verfassungsbeschwerden werden dagegen vorgebracht. Bereits am 27. Januar 2009 legt eine Journalistin Beschwerde ein, gefolgt von dem damaligen Herausgeber der Zeit, Michael Naumann, und dem Vorsitzenden der Humanistischen Union, Dr. Fredrik Roggan. Der ehemalige Innenminister Gerhart R. Baum und der Vorsitzende des Landesverbands Berlin des Deutschen Anwaltsvereins, Ulrich Schellenberg, sowie einige weitere Beschwerdeführer wenden sich ebenfalls mit umfangreichen Verfassungsbeschwerden gegen das Gesetz. Jede der Beschwerden befasst sich auch mit den Varianten des Staatstrojaners.

---

[1] BVerfG, Urteil des Ersten Senats vom 27. Februar 2008, 1 BvR 370/07, Rn. (1-333), http://www.bverfg.de/e/rs20080227_1bvr037007.html

[2] Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 25. Dezember 2008, http://www.bundesgerichtshof.de/SharedDocs/Downloads/DE/Bibliothek/Gesetzesmaterialien/16_wp/terrorismusabwehr_int_bka/bgbl108s3083.pdf;jsessionid=51B97D121F672E704ED6C241A4BB6BC6.1_cid368?__blob=publicationFile

Oktober 2011: Der Chaos Computer Club analysiert vom Landeskriminalamt Bayern eingesetzte Schadsoftware und deckt schwere technische Mängel und ein rechtswidriges Vorgehen auf.[3]

Februar 2016: Noch vor Abschluss der Prüfung durch das Bundesverfassungsgericht gibt das BKA bekannt, dass es über eine neue Schadsoftware zur Durchführung der Quellen-TKÜ verfüge. Das Bundesministerium des Innern (BMI) gibt die Software zur Nutzung frei, eine Billigung durch die Bundesdatenschutzbeauftragte wird nicht angestrebt.[4]

April 2016: Das Bundesverfassungsgericht kommt zu einem Urteil über das 2008 verabschiedete BKA-Gesetz und setzt darin erneut Grenzen für den Einsatz von staatlicher Schadsoftware.[5]

Zur Terrorismusabwehr sind seitens des BKA somit sowohl Quellen-TKÜ als auch Online-Durchsuchung bereits seit Dezember 2008 rechtlich zulässig, nach dem Urteil sind jedoch einige Regelungen für verfassungswidrig erklärt worden. Mit dem vorliegenden Änderungsantrag soll nun die Quellen-TKÜ ohne weitere Einschränkungen der einfachen Telekommunikationsüberwachung (TKÜ) gleichgestellt werden. Nur die Online-Durchsuchung soll auf schwerere Straftaten eingeschränkt bleiben.

Eine konventionelle Telekommunikationsüberwachung wird bekanntlich mit Hilfe des Telekommunikationsanbieters durchgeführt, der die Aufforderung erhält, die im Rahmen der Telekommunikationsvorgänge eines Verdächtigen anfallenden Daten an die Strafverfolgungsbehörden auszuleiten. Das Kommunikationsgerät der Zielperson bleibt dabei unberührt: Nur der Leitungsweg wird angezapft. Die gesetzlichen Schranken für diese Form der Überwachung nun auf eine weit komplexere, technisch anspruchsvolle und direkt in das betroffene Systeme eingreifende Methode anwenden zu wollen, zeugt von erheblicher Ignoranz für die damit einhergehenden Risiken.

Die im Jahr 2008 mit der Begründung der Terrorismusabwehr eingeführten Grundrechtseinschränkungen würden damit von der *ultima ratio* der inneren Sicherheit zum maximalinvasiven Alltagsinstrument der Strafverfolgung. Dabei konnten trotz des erheblichen Eingriffs in die Persönlichkeitsrechte und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme bisher die Notwendigkeit, Wirksamkeit und Effektivität dieser Maßnahmen nicht belegt werden. Die Infektion von Rechnern mit Schadsoftware ist keineswegs alternativlos, jedoch unbestritten mit zahlreichen Risiken verbunden. Keines dieser Risiken ist

---

[3] Chaos Computer Club (2011): *Analyse einer Regierungs-Malware,*
https://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf
Chaos Computer Club (2011): *0ZAPFTIS – Analyse einer Regierungs-Malware – Teil 2,*
https://www.ccc.de/system/uploads/83/original/staatstrojaner-report42.pdf

[4] Spiegel Online vom Mittwoch, 24.02.2016: *Innenministerium gibt umstrittenen Bundestrojaner frei,*
http://www.spiegel.de/netzwelt/netzpolitik/bundestrojaner-innenministerium-gibt-spaehsoftware-frei-a-1078656.html

[5] BVerfG, Urteil des Ersten Senats vom 20. April 2016, 1 BvR 966/09, Rn. (1-29),
http://www.bverfg.de/e/rs20160420_1bvr096609.html

jedoch mit einer konventionellen Telekommunikationsüberwachung verbunden, die rechtliche Gleichsetzung beider Maßnahmen verbietet sich daher auf technischer und rechtlicher Ebene.

Eine Ausweitung der Nutzung von Schadsoftware wird unweigerlich Folgen nach sich ziehen, die bereits in Staaten zu beobachten sind, deren Regierungen staatlichen Behörden eine Erlaubnis zum Hacken gegeben haben. Generell betreffen diese nachfolgend skizzierten Folgen sowohl konkrete technische Risiken als auch ökonomische Fragen, da die Ausnutzung von Sicherheitslücken und Schwachstellen mit einem Anbietermarkt in Zusammenhang steht. Angesichts der Tatsache, dass wir bereits heute vor erheblichen Problemen bei der technischen Beherrschbarkeit der Sicherheit von IT-Systemen stehen, ist eine weitere Destabilisierung der IT-Sicherheit durch staatliche Alimentierung dieses Marktes nicht anzuraten.

1. Gefahr für die innere Sicherheit

Für jeden Einsatz von Schadsoftware im Rahmen der Quellen-TKÜ oder Online-Durchsuchung wird (a) eine auf das Zielsystem spezifisch angepasste Softwarelösung sowie (b) ein Angriffspunkt auf diesem System benötigt, der zur Infektion genutzt werden kann. Im vorliegenden Änderungsantrag findet die technische Realität dieser Infektion eines informationstechnischen Systems keine Berücksichtigung. Zwar wird der gewünschte Funktionsumfang der anzubringenden Schadsoftware allgemein erläutert, jedoch bleibt die zentrale Frage außer Acht, wie die Schadsoftware auf dem Gerät der Zielperson angebracht werden soll. Auch die Vielzahl der verschiedenen Zielsysteme und -anforderungen bleibt unbeachtet.

Eine Infektion durch Dritte ist grundsätzlich nur bei fehlenden oder fehlerhaften Zugangsbeschränkungen oder durch Ausnutzung einer Software-Schwachstelle möglich. Da vollständig fehlende Zugangsbeschränkungen in den seltensten Fällen vorkommen und diese darüber hinaus direkten physischen Zugriff auf das Gerät voraussetzen würden, wären vorhandene Software-Schwachstellen für den größeren Teil der Einsätze Grundvoraussetzung.

➡ *Software-Schwachstellen werden zur Infektion eines informationstechnischen Systems benötigt. Sie sind separat von der Infektion selbst, in diesem Falle einer Schadsoftware zur Quellen-TKÜ oder zur Online-Durchsuchung, zu betrachten. Über eine vorhandene Software-Schwachstelle lassen sich andere Infektionen anbringen, und eine Infektion kann unter Inanspruchnahme unterschiedlicher Schwachstellen angebracht werden. Das Vorhandensein einer Schwachstelle ist jedoch Voraussetzung für die Infektion.*

Das Common Vulnerability Scoring System[6] (CVSS) bietet als de-facto-Branchenstandard eine Möglichkeit zur einheitlichen Betrachtung des technischen Risikos von Software-Schwachstellen. Der Wertebereich des Basiswerts reicht dabei von 0 (kein Risiko) bis 10 (kritisch).

Eine Schwachstelle, die bei physischem Zugriff die Infektion mit einer Schadsoftware (beispielsweise zur Quellen-TKÜ) ermöglicht, wird gemäß CVSS als mittleres Risiko (CVSS = 6.8) ausgewiesen.[7] Eine solche Schwachstelle würde jedoch immer noch voraussetzen, dass Ermittler des Zielgerätes temporär habhaft werden. Entsprechend aufwendig und auffällig wäre ihr Einsatz im Rahmen von Ermittlungsverfahren.

Um eine vom Nutzer des Gerätes unbemerkte Infektion vorzunehmen, wird eine Schwachstelle benötigt, die sich über das Netzwerk ausnutzen lässt. Sofern diese eine Nutzerinteraktion

---

[6] The CVSS Special Interest Group: *Common Vulnerability Scoring System v3.0: Specification Document,* https://www.first.org/cvss/specification-document

[7] Vgl. https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Die Einschränkung der Verfügbarkeit ist zwar nicht Ziel des Angriffs, jedoch im Rahmen der hypothetischen Schwachstelle ebenfalls im Rahmen der Möglichkeiten des Angreifers. Aus diesem Grund wird die Schwachstelle mit dem Wert 6.6 statt 5.9 bewertet.

voraussetzt, beispielsweise das Bestätigen einer Warnmeldung, wird die Schwachstelle mit einem Wert von 8.8 als „hoch“ eingestuft.[8] Ist eine Infektion ohne weitere Nutzerinteraktion möglich, so gilt die Schwachstelle mit einem CVSS-Wert von 9.8 als „kritisch“.[9]

➡ *Zur Infektion werden mindestens mittlere, im Regelfall sogar schwere bis kritische Schwachstellen benötigt.*

Um eine fortwährende Ausnutzung der Schwachstelle sicherzustellen, muss diese geheim gehalten werden, da sonst mit ihrer Beseitigung zu rechnen wäre. Dies bedeutet im Umkehrschluss, dass die Schwachstelle ausnahmslos auf allen betroffenen Geräten weltweit vorhanden sein muss. Damit geht zwingend das Risiko einher, dass die Schwachstelle von anderen interessierten Gruppen, insbesondere von Kriminellen oder anderen staatlichen Akteuren ebenfalls entdeckt und ausgenutzt wird.

Diese Abwägung gilt für jede einzelne Schwachstelle unabhängig von der Intention im Einzelfall. Dem möglicherweise berechtigten und legitimen Interesse zur Nutzung einer Schwachstelle zum Zwecke der Strafverfolgung steht somit unweigerlich das Risiko für die Allgemeinheit gegenüber, das sich aus dem Vorhandensein der Schwachstelle ergibt. Je öfter die Schwachstelle ausgenutzt wird, desto mehr erhöht sich auch das Risiko ihrer Entdeckung durch Dritte, die durch forensische Analyse und Reverse Engineering das Einfallstor entdecken und für eigene Zwecke missbrauchen können. Nicht zuletzt deshalb ist es geboten, die Anzahl der Schadsoftware-Einsätze gering zu halten. Eine Ausweitung wie im Änderungsantrag vorgesehen steht diesem Gebot jedoch entgegen.

Aus den offensichtlichen Erwägungen zur inneren Sicherheit ist es daher grundsätzlich falsch, das Wissen über Schwachstellen geheim zu halten und somit ihre Beseitigung zu verhindern oder aktiv zu verzögern. Entsprechend risikoarme und grundrechtsschonende Alternativen sind zu entwickeln.

➡ *Mit der Geheimhaltung von Wissen über Schwachstellen geht grundsätzlich ein Risiko für die innere Sicherheit einher, dessen Ausmaß proportional zur Anzahl und Kritikalität der betroffenen Geräte ist.*

Selbstverständlich wird regelmäßig argumentiert, dass staatliche Stellen mit dem Wissen über Schwachstellen verantwortungsbewusst und im strengen Rahmen rechtlicher Regulierung umgehen. Dabei wird außer Acht gelassen, dass Schwachstellen grundsätzlich agnostisch gegenüber Angreifer und Angriffsmotivation sind: Sie stehen allen, die Kenntnis darüber erlangen, gleichermaßen zur Verfügung.

So wurde der massenhafte Ausbruch der Schadsoftware „WannaCry“ durch eine kritische Schwachstelle (CVSS-Basiswert 8.1-9.3) ermöglicht,[10] über die der US-amerikanische Geheimdienst

---

[8] Vgl. https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

[9] Vgl. ebd.

[10] National Vulnerability Database: CVE-2017-0144 Detail, https://nvd.nist.gov/vuln/detail/CVE-2017-0144

NSA seit mindestens fünf Jahren Kenntnis hatte.[11] Zu den von WannaCry betroffenen Institutionen und Unternehmen gehörten zahlreiche Unternehmen, die den „Kritischen Infrastrukturen" zuzuordnen sind, unter anderem der spanische Telekommunikationskonzern Telefónica, das brasilianische Telekommunikationsunternehmen Vivo, der britische National Health Service (NHS) mit mehreren Krankenhäusern, das US-Logistikunternehmen FedEx, die Deutsche Bahn mit der Logistiktochter Schenker sowie das Russische Innenministerium (MWD), das Katastrophenschutzministerium sowie das Telekommunikationsunternehmen MegaFon.

Dieses Ausmaß an Schaden wurde erreicht, obwohl Microsoft zwei Monate zuvor einen Patch für die Schwachstelle bereitgestellt hatte, nachdem ein entsprechendes Angriffswerkzeug der NSA von Unbekannten gestohlen wurde. Zum Zeitpunkt der WannaCry-Angriffe war der größere Teil der betroffenen Systeme daher bereits „immun". Das Risiko, das die NSA durch das Geheimhalten der Schwachstelle für mehrere Jahre einging, war weitaus größer: Gemessen am möglichen Desaster-Ausmaß können die WannaCry-Angriffe als glimpflicher Ausgang bezeichnet werden. Allerdings ist die Veröffentlichung der Hacking-Werkzeuge der US-Behörden durch eine unbekannte Gruppe mit dem Namen „TheShadowsBrokers" zu diesem Zeitpunkt noch nicht abgeschlossen,[12] so dass weitere derartige Vorfälle nicht auszuschließen sind.

➡ *IT-Sicherheit ist ein kritischer Bestandteil der inneren Sicherheit. Kritische Infrastrukturen werden zu großen Teilen mit Standard-Software betrieben und verfügen über die gleichen Schwachstellen, die zur Infektion mit staatlicher Schadsoftware benötigt werden. Das Geheimhalten dieser Schwachstellen setzt somit die Kritischen Infrastrukturen einem direkten und unnötigen Angriffsrisiko aus.*

Zu der allgemeinen Frage, wie staatliche Stellen überhaupt Kenntnis von öffentlich nicht bekannten, zur Infektion informationstechnischer Systeme geeigneter Schwachstellen erlangen können, hat der Chaos Computer Club bereits 2016 Stellung genommen:[13]

> *„In den letzten Jahren ist international eine verstärkte Verbreitung kommerziell angebotener staatlicher Überwachungstrojaner zu verzeichnen. Diese Entwicklung ist problematisch, da das staatliche Ausnutzen von Schwachstellen einen Interessenkonflikt darstellt. Er besteht vor allem darin, dass aus wirtschaftlichen und Gemeinwohlerwägungen heraus ein hohes staatliches Interesse darin liegt, Computer-Schwachstellen schnell zu schließen, um Wirtschaftsspionage*

---

[11] The Washington Post, 16. Mai 2017: *NSA officials worried about the day its potent hacking tool would get loose. Then it did,* https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html

[12] Vgl. „TheShadowBrokers Monthly Dump Service – June 2017", https://steemit.com/shadowbrokers/@theshadowbrokers/theshadowbrokers-monthly-dump-service-june-2017

[13] Constanze Kurz, Linus Neumann, Frank Rieger, Dirk Engling (2016): *Stellungnahme zur „Quellen-TKÜ" nach dem Urteil des Bundesverfassungsgerichts vom 20. April 2016, 1 BvR 966/09,* https://ccc.de/system/uploads/216/original/quellen-tkue-CCC.pdf

> *zurückzudrängen und die grauen Märkte, in denen diese Sicherheitslücken gehandelt werden, nicht zusätzlich zu befeuern.*
>
> *Tritt der Staat als Käufer von Exploits auf, liegt es jedoch in seinem Interesse, die Sicherheitslücke möglichst lange selbst ausnutzen zu können und entsprechend nicht zu schließen. Generell wird der europäische Markt durch das Auftreten staatlicher Behörden als Käufer sowohl für die Verkäufer von ausnutzbaren Sicherheitslücken als auch für die spezialisierten Anbieter von Spionagesoftware attraktiver. Wenn die „Quellen-TKÜ" und damit der Einbruch in informationstechnische Systeme als Ermittlungsinstrument angestrebt wird, sollte zuvor eine Folgenabschätzung vorgenommen werden, um die Effekte auf diesen Markt abzuschätzen."*

Diese Situation besteht unverändert fort, weswegen diese Folgenabschätzung noch immer zu fordern ist.

2. Unverhältnismäßiger Grundrechtseingriff bei niedriger rechtlicher Schwelle

Gerade weil der Einsatz von Schadsoftware ein besonders schwerwiegender Grundrechtseingriff ist, hat das Bundesverfassungsgericht das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme überhaupt erst definiert. Diese wegweisende und weitsichtige Entscheidung wurde in einer Zeit getroffen, als die Digitalisierung aller Lebensbereiche noch weit weniger vorangeschritten war, als es heute der Fall ist.

Die Geschwindigkeit und die Dynamik, mit der diese Digitalisierung voranschreitet, erfordern eine behutsame und bedachte Politik, die der vorliegende Änderungsantrag vermissen lässt. Im Jahr 2008 war das Smartphone gerade erfunden worden, und die Entwicklung der digitalen Sphäre stand am Anfang der in ihrer Folge massiven gesellschaftlichen Veränderungen. Heute sind informationstechnische Systeme zum wesentlichen Ablagemedium für berufliche Informationen und private, sogar intimste Gedanken geworden.

Gleichermaßen stehen wir heute am Beginn der Digitalisierung aller Produkt- und Lebensbereiche. Die informationstechnischen Systeme einer Zielperson mögen heute noch weitestgehend auf Personal Computer und Smartphones beschränkt sein. In absehbarer Zeit wird eine Vielzahl an verschiedenen Produkten keinen Aspekt des Lebens mehr unerfasst lassen. Digitale Systeme werden zu weit mehr als Telekommunikationsmedien: zu unserem ausgelagerten Gehirn, das mehr über uns weiß, als wir selbst.

Technischer Kern sowohl der Quellen-TKÜ als auch der Online-Durchsuchung ist die erfolgreiche Manipulation des Rechners oder Smartphones und künftig weiterer, heute noch nicht typischer informationstechnischer Systeme, um die gewünschten Daten zu erlangen. Vor diesem Hintergrund ist zu betonen, dass – im Gegensatz zur Telekommunikationsüberwachung auf der Leitung oder einer Hausdurchsuchung – die Differenzierung in Quellen-TKÜ und Online-Durchsuchung eine rein virtuelle und willkürliche Unterscheidung ist, für die es keine reale technische Entsprechung geben kann: Informationstechnische Systeme sind universell programmierbar und einsetzbar. Entsprechend groß ist die Vielfalt an Kommunikationsmethoden und -applikationen, die eine Zielperson zum Einsatz bringen kann. Sie alle zielgerichtet erfassen zu können, ohne das informationstechnische System in der Vielzahl seiner weiteren Funktionen und Anwendungen zu erfassen, ist nicht möglich.

Dass die 2011 vom CCC analysierte staatliche Schadsoftware das Erfassen von E-Mail-Nachrichten und Chats durch das „Abfotografieren“ des gesamten Bildschirms realisierte, lässt sich nicht nur durch einen zufälligen oder nachlässigen Verstoß gegen die gesetzlichen Bestimmungen erklären: Es war auch Ausdruck der schieren Hilflosigkeit der Programmierer bei dem Versuch, in ihrer Software die schon damals kaum zu überblickenden verschiedenen Kommunikationsmöglichkeiten im Rahmen der Überwachungsmaßnahme zu erfassen. Eine der vielen Lehren aus diesem Skandal lautet daher auch, dass eine „reine“ Quellen-TKÜ praktisch nicht realisierbar ist.

Spionagesoftware leitet stets über die Überwachung der laufenden Telekommunikation hinausgehende Daten aus. Entsprechend stellte der Chaos Computer Club in seiner Stellungnahme 2015 fest:[14]

> *„De facto handelt es sich bei der Quellen-TKÜ um eine optische und akustische Wohnraumüberwachung, sowohl beim Benutzer des Systems als auch bei Kommunikationspartnern, die mit dem Tatvorwurf nichts zu tun haben könnten. Diese optische und akustische Überwachung wird nach der Plazierung der Computerwanze auf dem Zielsystem automatisch selektiv aktiviert, wenn eine der zu überwachenden Applikationen auf dem informationstechnischen System eine Kommunikation einleitet oder angeschaltet wird. Daß die betreffende Anwendung wirklich aktiv ist und sich die Überwachung primär auf den Kommunikationsvorgang erstreckt, ist nicht mit abschließender Sicherheit zu garantieren.“*

Daran hat sich auch 2017 nichts geändert.

➡ *Für die juristische Unterscheidung in Quellen-TKÜ und Online-Durchsuchung gibt es keine adäquate technische Entsprechung. Die Eingriffstiefe einer „Quellen-TKÜ“ ist nicht mit der einer Telekommunikationsüberwachung zu vergleichen.*

Das Bundesamt für Justiz berichtet für das Jahr 2015 eine Gesamtanzahl von

- **3.332** Anordnungen zur Überwachung von Festnetz-Telekommunikation,
- **21.905** Anordnungen zur Überwachung von Mobilfunk-Kommunikation,
- **7.432** Anordnungen zur Überwachung von Internet-Kommunikation.

Der Großteil dieser Anordnungen erfolgte im Rahmen der Überwachung von Ermittlungsverfahren wegen Verstoßes gegen das Betäubungsmittelgesetz.[15]

Durch die Gleichsetzung der rechtlichen Voraussetzungen von Quellen-TKÜ mit konventioneller Telekommunikationsüberwachung auf der Leitung erhält das bisher der Terrorismusabwehr und der Verfolgung schwerer Straftaten vorbehaltene Mittel Einzug in den Ermittlungsalltag.

➡ *Die Quellen-TKÜ würde von der „ultima ratio“ zum Standardinstrument der Strafverfolgung werden. Die Eingriffsschwere gebietet jedoch höhere rechtliche Hürden, um einen inflationären Einsatz zu verhindern.*

---

[14] Constanze Kurz, Dirk Engling, Frank Rieger, Thorsten Schröder (2015): *Stellungnahme an das Bundesverfassungsgericht zum BKA-Gesetz und zum Einsatz von Staatstrojanern, 1 BvR 966/09, 1 BvR 1140/09*, http://www.ccc.de/system/uploads/189/original/BKAG_Stellungnahme.pdf

[15] Bundesamt für Justiz, Referat III: Übersicht Telekommunikationsüberwachung (Maßnahmen nach § 100a StPO) für 2015, Stand 14.07.2016, https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/Uebersicht_TKUE_2015.pdf?__blob=publicationFile&v=2

3. Fehlender Beleg der Notwendigkeit

Zur Begründung der Ausweitung des schweren Grundrechtseingriffs der Quellen-TKÜ wird im vorliegenden Änderungsantrag angeführt:[16]

> *„Die Nutzung dieser mobilen Geräte ersetzt zunehmend die herkömmlichen Formen der Telekommunikation. Das Internet als komplexer Verbund von Rechnernetzen öffnet dem Nutzer eines angeschlossenen Systems nicht nur den Zugriff auf eine praktisch unübersehbare Fülle von Informationen, die von anderen Netzrechnern zum Abruf bereitgehalten werden. Es stellt ihm daneben zahlreiche neuartige Kommunikationsdienste zur Verfügung, mit deren Hilfe er über das Internet aktiv soziale Verbindungen aufbauen und pflegen kann, ohne herkömmliche Formen der Telekommunikation in Anspruch nehmen zu müssen."*

Es wird der Eindruck erweckt, die vielfältigen Möglichkeiten der Telekommunikationsüberwachung gemäß § 110 Telekommunikationsgesetz und Telekommunikations-Überwachungsverordnung, die bereits seit 2005 bestehen, sowie die vollumfängliche Internet-Metadaten-Überwachung gemäß dem 2015 erlassenen Gesetz zur Wiedereinführung der vorher bereits für verfassungswidrig erklärten Vorratsdatenspeicherung[17] stünden Strafverfolgungsbehörden gar nicht zur Verfügung. Mit der wieder eingeführten Vorratsdatenspeicherung wird ab 1. Juli 2017 (§ 150 Abs. 13 TKG) der Vollzugriff auf sämtliche Metadaten der Internetkommunikation der Bundesrepublik ermittlungstechnischer Alltag.

Ferner wird angeführt, dass das Ziel der Quellen-TKÜ primär die Erfassung verschlüsselter Kommunikationsinhalte ist:

> *„Im Bereich der Strafverfolgung ist umstritten, inwieweit die Überwachung insbesondere verschlüsselter Kommunikation über das Internet zulässig ist. Die Möglichkeit eines verdeckten Eingriffs in informationstechnische Systeme zum Zweck ihrer Durchsuchung besteht bislang für die Strafverfolgungsbehörden nicht."*

Es wird der Anschein erweckt, dass verschlüsselte Kommunikation Strafverfolgungsbehörden sämtlicher Ermittlungsansätze berauben und auf diese Weise eine Strafverfolgung oder Gefahrenabwehr verhindern würde. Diese unter dem Stichwort „Going Dark" bekannt gewordene

---

[16] Deutscher Bundestag, Ausschuss für Recht und Verbraucherschutz: Ausschussdrucksache 18(6)334: Formulierungshilfe der Bundesregierung für einen 15.05.2017 Änderungsantrag der Fraktionen CDU/CSU und SPD zu dem Gesetzentwurf der Bundesregierung – Drucksache 18/11272 – Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze, https://www.bundestag.de/blob/507632/c2362af32d325de93cc8342400d998bd/formulierungshilfe-data.pdf, dauerhaft verfügbar unter https://netzpolitik.org/2017/wir-veroeffentlichen-den-gesetzentwurf-der-grossen-koalition-zum-massenhaften-einsatz-von-staatstrojanern/#Formulierungshilfe

[17] Bundesrat Drucksache 492/15: Gesetzesbeschluss des Deutschen Bundestages – Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, http://dip21.bundestag.de/dip21/brd/2015/0492-15.pdf

Behauptung geht auf den ehemaligen FBI-Direktor James Comey zurück[18] und ist eine direkte öffentliche Reaktion zur Rechtfertigung der Enthüllungen Edward Snowdens, der eine bis heute fortdauernde Massenüberwachung durch US-Geheimdienste und Strafverfolgungsbehörden belegte.

Snowdens Enthüllungen zeigten das Gegenteil dessen, was als „Going Dark" bezeichnet wird: Ermittlungsbehörden verfügen trotz der zunehmenden Verschlüsselung von Gesprächsinhalten über mehr Daten und Ermittlungsansätze als je zuvor. Primär liegt dies an der Digitalisierung der gesamten Kommunikation an sich sowie an den heute typischen Online-Geschäftsmodellen und Zentralisierungstendenzen: Zugriff auf Nutzerdaten zum Zwecke der Auswertung ist treibender Wirtschaftsfaktor fast aller Online-Dienste. Für diese Geschäftsmodelle ist es unerlässlich, dass die Anbieter Einsicht in unverschlüsselte Daten ihrer Nutzer haben. Die Zentralisierungstendenzen lassen sich primär im Wandel von produktbasierten zu Dienstleistungsmodellen beobachten, die eine zentralisierte Erfassung begünstigen.

Auch bei verschlüsselten Kommunikationsinhalten fallen in der Regel Metadaten an, deren Analyse sehr genaue Einblicke in Bewegungsprofile, Gruppenzugehörigkeiten und Kommunikationsmuster ermöglicht und damit mannigfaltige Ermittlungsansätze liefert. Deutsche Strafverfolger sammeln diese Metadaten beispielsweise im Rahmen der sogenannten Funkzellenabfrage gemäß § 100g Abs. 3 StPO, der Telekommunikationsüberwachung gemäß § 110 TKG und zukünftig der sämtliche Internetkommunikation umfassenden Vorratsdatenspeicherung gemäß § 150 Abs. 13 TKG. Durch die Anwendung sogenannter „Stiller SMS" werden sogar eigens Metadaten erzeugt, Mobiltelefone regelmäßig als Ortungswanzen missbraucht und auf diese Weise eine Ausweitung der durch Telekommunikationsüberwachung erlangten Erkenntnisse erreicht. Die heute bereits existierende Fülle der Erfassungsmöglichkeiten lässt einzig einige Inhalte verschlüsselter Kommunikation außen vor: Für die Erfassung und Auswertung sämtlicher sonstigen Kommunikationsinhalte und Metadaten gibt es bereits eine Ermächtigungsgrundlage. Zusätzlich ist zu konstatieren, dass die Fülle an informationstechnischen Systemen, die Menschen heute in allen Lebenslagen umgeben, eine Menge an Datenspuren erzeugt, die noch vor wenigen Jahren kaum vorstellbar war. In dieser Konstellation entbehrt die Behauptung, man säße ermittlungstechnisch im Dunkeln, jeder Grundlage.

Doch auch unter der unzutreffenden Annahme, dass „Going dark" ein tatsächliches Phänomen wäre, existiert im Bereich der nationalen Sicherheit keine Schutzlücke, da die Mittel der Online-Durchsuchung und Quellen-TKÜ dem BKA bereits seit 2008 zur Verfügung stehen. Der vorliegende Änderungsantrag zielt jedoch darauf ab, diese als *ultima ratio* zum Schutz der nationalen Sicherheit begründeten Grundrechtseingriffe zu einem ermittlungstechnischen Alltag zu machen, ohne dass in diesem Bereich eine nennenswerte Schutzlücke belegt werden kann.

---

[18] James B. Comey, Director Federal Bureau of Investigation (2014): *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?,*
https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

4. Fehlende technische Überprüfbarkeit und Nachvollziehbarkeit

Informationstechnische Systeme sind universell programmierbar. Dies bedeutet, dass sie prinzipbedingt jede Funktion haben oder auch nicht haben können. Der genaue Funktionsumfang einer im Rahmen der Strafverfolgung zum Einsatz gebrachten Schadsoftware ist jedoch von fundamentaler Bedeutung für die Bewertung und Einordnung der auf diesem Wege erbrachten Indizien und Beweise sowie zur Beurteilung der Rechtmäßigkeit des Einsatzmittels.

Die im Jahre 2011 veröffentlichte Analyse des „Bundestrojaners" offenbarte beispielsweise Programmierfehler, die neben einer weiteren Schwächung der Integrität des Zielsystems auch noch eine beliebige Erweiterbarkeit der Funktionalität der Schadsoftware zufolge hatten – und das auch durch Dritte.[19]

Während die technischen Rahmenbedingungen einer Telekommunikationsüberwachung sich auch Laien vollständig erschließen können, handelt es sich bei einer Quellen-TKÜ um einen komplexen, intransparenten und nur durch Experten nachvollziehbaren und zu bewertenden Vorgang. Da auch digital erfasste Daten per se keinen Integritätsschutz haben, also zu jedem Zeitpunkt beliebig veränderbar sind, sind mehrere technische Anforderungen unabdingbar, um die Beweiskraft und Rechtmäßigkeit einer Online-Durchsuchung oder einer Quellen-TKÜ sicherzustellen.

Der vorliegende Änderungsantrag macht hierzu nur vage, daher nicht überprüfbare und rechtlich verbindliche technische Vorgaben:[20]

> *„Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen."*

Diese Vorgaben sind nicht ausreichend, um Rechtssicherheit und Überprüfbarkeit zu erreichen. Die parlamentarische Gruppe „Civici e Innovatori" der 17. Legislatur des italienischen Parlaments hat im

---

[19] Chaos Computer Club (2011): *Analyse einer Regierungs-Malware,* https://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf

[20] Deutscher Bundestag, Ausschuss für Recht und Verbraucherschutz: Ausschussdrucksache 18(6)334: Formulierungshilfe der Bundesregierung für einen 15.05.2017 Änderungsantrag der Fraktionen CDU/CSU und SPD zu dem Gesetzentwurf der Bundesregierung – Drucksache 18/11272 – Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze, https://www.bundestag.de/blob/507632/c2362af32d325de93cc8342400d998bd/formulierungshilfe-data.pdf, dauerhaft verfügbar unter https://netzpolitik.org/2017/wir-veroeffentlichen-den-gesetzentwurf-der-grossen-koalition-zum-massenhaften-einsatz-von-staatstrojanern/#Formulierungshilfe

Februar 2017 mehrere technische Anforderungen vorgeschlagen, die ein Mindestmaß an Rechtssicherheit und Überprüfbarkeit definieren.[21] Dazu gehören:

A. Der Quellcode muss hinterlegt und verifizierbar sein. Den Vorgang des Umwandelns des menschenlesbaren Quellcodes in ein ausführbares Programm wird als „Kompilieren" bezeichnet. Das resultierende Programm ist in seiner Funktionsweise sehr viel komplizierter und kaum abschließend zu erfassen. Erschwerend kommt hinzu, dass eine solche als „reverse engineering" bezeichnete Analyse bei Schadsoftware regelmäßig durch verschiedene Verschleierungsmaßnahmen erschwert wird, beispielsweise um den Schutz des Zielsystems durch Virenscanner auszuhebeln.

Für alle Betroffenen und auch für die zuständigen Datenschutzbehörden muss eine Einsichtnahme in den Quellcode zur Prüfung der rechtmäßigen Ausgestaltung der Spionagesoftware gesetzlich festgeschrieben werden. Zu diesem Schluss kam bereits der Bericht des bayerischen Landesbeauftragten für den Datenschutz, dessen Behörde als eine der wenigen staatlichen Kontrollbehörden überhaupt je Einblick in tatsächlich zum Einsatz gekommene staatliche Spionagesoftware nehmen konnte. Der Landesbeauftragte empfahl, sowohl bei konkretem Anlass als auch generell eine Quellcode-Sichtung zu ermöglichen:[22]

> *„Es wäre jedoch geboten, den jeweiligen Quellcode einzusehen, wenn hierzu ein konkreter Anlass besteht. Um verdeckte Funktionalitäten zuverlässig auszuschließen, ist auch die stichprobenartige Einsichtnahme in den Quellcode zu empfehlen."*

Ohne das Ergreifen besonderer Maßnahmen beim Kompilieren des Quellcodes zu einer ausführbaren Datei kommt es regelmäßig zu unterschiedlichen Ergebnissen. Dies erschwert eine Beweisführung, dass eine zum Einsatz gebrachte Schadsoftware tatsächlich dem zertifizierten Quellcode entspricht. Durch das Vorschreiben eines Vorgehens zur Sicherstellung reproduzierbarer Kompilierungsergebnisse[23] kann diese Schutzlücke geschlossen werden.

B. Jede Aktion muss vollständig, manipulationssicher und verifizierbar dokumentiert werden. Von der Infektion über die Datenextraktion bis zur Desinfektion muss der gesamte Vorgang der Quellen-TKÜ oder Online-Durchsuchung nachvollziehbar protokolliert sein, um es sowohl

---

[21] Civici e Innovatori: *Disciplina dell'uso dei captatori legali nel rispetto delle garanzie individuali,*

- Gesetzesvorschlag: http://www.civicieinnovatori.it/wp-content/uploads/2017/02/PDL-Captatori-Legali_DEFV3.pdf
- Technische Regeln: http://www.civicieinnovatori.it/wp-content/uploads/2017/02/DisciplinareTecnicoPropostadiLeggeCaptatore.pdf
- Begründung und Inhalt der technischen Regeln: http://www.civicieinnovatori.it/wp-content/uploads/2017/02/PDL-Captatori-Legali_DEFV3.pdf
- Zusammenfassung in englischer Sprache: *Rules governing the use of government trojan with respect for individual rights,* http://www.civicieinnovatori.it/wp-content/uploads/2017/02/Sintesi-PDL-captatori-EN.pdf

[22] Der Bayerische Landesbeauftragte für den Datenschutz (2012): *Prüfbericht Quellen-TKÜ*, S. 20f., https://www.datenschutz-bayern.de/0/bericht-qtkue.pdf

[23] Vgl. bspw. https://reproducible-builds.org

Richtern als auch Betroffenen zur Beweisführung zu ermöglichen, das Vorgehen der Ermittler nachzuvollziehen. Das Protokoll muss auf eine Weise angefertigt und gespeichert werden, die sowohl seine Umgehung als auch seine nachträgliche Veränderung verhindert. Kryptographische Hash-Funktionen eignen sich dabei zur beweissicheren Aufnahme von extrahierten Dateien, ohne deren Inhalte zum Teil des Protokolls werden zu lassen.

Weiterhin kann durch sogenannte Hash-Chains die Vorwärts-Integrität des Logs erhöht werden. Das Log sollte zwingend off-site und außerhalb des vom Angreifer kontrollierten Bereichs geführt werden, um die Manipulationswahrscheinlichkeit zu minimieren. Insbesondere sollten auf diese Weise auch die Löschvorgänge gemäß des geplanten § 100d (2) StPO inklusive der Prüfsummen-Hashes der gelöschten Dateien dokumentiert werden. Dies ermöglicht es, Eingriffe in den Kernbereich privater Lebensgestaltung auch im Nachhinein zu erkennen, und mindert damit unerkannten Missbrauch.

C. Die Schadsoftware darf nicht das allgemeine Sicherheitsniveau des Gerätes schwächen. Unter 1. wurde bereits dargestellt, dass vorhandene Schwachstellen Grundvoraussetzung für die Infektion eines Zielgerätes sind. Darüber hinaus verfügt eine steigende Anzahl informationstechnischer Systeme über Sicherheitsmaßnahmen, die eine Infektion verhindern oder erschweren sollen. Hierzu gehören insbesondere Maßnahmen der Integritätssicherung wie Code-Signing und Secure Boot. Das Umgehen derartiger Schutzmechanismen wird häufig als „*jailbreak*“ bezeichnet und ist bei vielen Geräten Voraussetzung für eine erfolgreiche persistente Infektion mit Schadsoftware.

Das *Jailbreaking* setzt jedoch dauerhaft die Sicherheitsmaßnahmen außer Kraft und erlaubt das Ausführen arbiträren Programmcodes. Das Ergebnis ist ein gemindertes Grundsicherheitsniveau des Zielgerätes, welches infolgedessen einfacher durch weitere Angreifer infiziert werden kann. Eine derartige Kompromittierung und Risikoerhöhung ist im Rahmen staatlich angeordneter Maßnahmen nicht hinnehmbar.

D. Die Entwicklung und der Einsatz der Schadsoftware muss mittels einer zentralen Erfassung nachvollziehbar sein. Analog zur oben dargestellten manipulationssicheren Aufbewahrung von extrahierten Daten müssen auch die unterschiedlichen Versionen und Varianten der zum Einsatz gebrachten Schadsoftware-Typen festgehalten werden, um zu jedem Zeitpunkt eine vollständige Untersuchung zu ermöglichen.

E. Eine unabhängige Zertifizierung der technischen und datenschutzrechtlichen Vorgaben muss regelmäßig erneuert werden. Den Vorgaben gemäß A. entsprechend, sollte jede zum Einsatz gebrachte Version der Schadsoftware durch eine unabhängige Stelle geprüft und zertifiziert werden, bevor diese zum Einsatz kommt: Die Feststellung jahrelanger rechtswidriger Praxis kann nicht zur Beweislast der im Strafverfahren Beschuldigten gemacht werden. Jede Änderung der Schadsoftware muss gemäß D. protokolliert und wesentliche Zusatzfunktionen neu zertifiziert werden.

Zudem kann bei der vorliegenden Eingriffsintensität auf eine Evaluation auch der richterlichen Beschlüsse, die eine Quellen-TKÜ oder Online-Durchsuchung anordnen, nicht verzichtet werden. Sie soll neben den technischen Vorgaben auch die Sinnhaftigkeit der Einsätze sowie langfristige Folgen unabhängig untersuchen.

F. Verschlüsselung und Integritätsschutz der erfassten Daten. Die mit Hilfe der Schadsoftware extrahierten Daten müssen nach dem Stand der Technik verschlüsselt und gegen Manipulation geschützt ausschließlich auf informationstechnischen System unter der Hoheit der Strafverfolgungsbehörden gespeichert werden.

G. Beschränkung hoheitlicher Aufgaben auf staatliche Stellen. Der Eingriff in die Vertraulichkeit und Integrität eines informationstechnischen Systems ist ein schwerer Grundrechtseingriff im Rahmen der hoheitlichen Aufgabe der Strafverfolgung. Ein Auslagern dieser Aufgabe auf privatwirtschaftliche Dienstleister ist daher grundsätzlich abzulehnen. Sämtliche Schadsoftware muss direkt von Strafverfolgungsbehörden angebracht und bedient werden.

Verstöße gegen dieses Gebot sind dabei kein theoretisches Konstrukt, sondern gängige Praxis in Ländern wie Bahrain, Äthiopien, Bangladesch, den Niederlanden, Estland, Australien, der Mongolei oder Nigeria, die Schadsoftware vom Zulieferer und Betreiber Gamma International einsetzen.[24] Das Bundeskriminalamt beschaffte die Software bereits im Oktober 2012.[25] Weder der in den seltensten Fällen in demokratischer Tradition stehende Kundenstamm des Unternehmens noch ein erfolgreicher Hacking-Angriff auf Gamma International/FinFisher wird vom Bundeskriminalamt als Hindernis für eine Zusammenarbeit gesehen, wie aus einem Bericht des Bundesrechnungshofs hervorgeht:[26]

> *„Die Analyse des Hacking-Angriffs auf einen Internet-Server der Firma FinFisher im Zeitraum vom 1. bis 3. August 2014, in dessen Folge ca. 40 Gigabyte interne Daten der Firma erlangt und im Internet veröffentlicht wurden, hat das BKA im November 2014 mit dem Ergebnis abgeschlossen, die Zusammenarbeit mit der Firma fortzusetzen.“*

---

[24] Ben Wagner, Claudio Guarnieri (2014): *Finfisher – Deutsche Firmen verdienen Millionen mit Überwachungstechnik,* in Zeit Online vom 5. September 2014, http://www.zeit.de/digital/datenschutz/2014-09/export-finfisher-gamma-gastbeitrag

[25] Andre Meister (2013): *Bundeskriminalamt bestätigt Anschaffung von Staatstrojaner Gamma FinFisher: „Wir haben die Software“,* https://netzpolitik.org/2013/bundeskriminalamt-bestatigt-anschaffung-von-staatstrojaner-gamma-finfisher-wir-haben-die-software/

[26] Der Bundesrechnungshof: Bericht zur Nr. 10 des Beschlusses des Haushaltsausschusses des Deutschen Bundestages zu TOP 20 der 74. Sitzung am 10. November 2011, öffentlich einsehbar unter: Andre Meister (2016): *Kritik vom Bundesrechnungshof: Das Bundeskriminalamt will gleich zwei Staatstrojaner einsetzen,* https://netzpolitik.org/2016/kritik-vom-bundesrechnungshof-das-bundeskriminalamt-will-gleich-zwei-staatstrojaner-einsetzen/

5. Drohende Verletzung der Eckpunkte der deutschen Kryptopolitik

Durch Änderung des § 100a soll eine konventionelle TKÜ zur Quellen-TKÜ erweitert werden dürfen:

> *„Die Überwachung und Aufzeichnung der Telekommunikation darf auch in der Weise erfolgen, dass mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen. Auf dem informationstechnischen System des Betroffenen gespeicherte Inhalte und Umstände der Kommunikation dürfen überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können."*

Hier stellt sich die Frage, ob damit auch Server-Systeme erfasst sein können. Ist dies der Fall, ließe sich aus dieser Ermächtigung eine Handhabe konstruieren, um beispielsweise für derartige Angriffe anfällige Systembetreiber zu zwingen, den Schlüsselaustausch einer sich aufbauenden Verschlüsselung zu beeinträchtigen, vergleichbar dem Vorgehen beim Abhören von Skype-Gesprächen. Praktisch würde dies bedeuten, dass der Dienstanbieter die Verschlüsselung umgeht.

Eine solche Ermächtigung zum Eingriff in informationstechnische Systeme wäre sehr weitreichend, jedoch unspezifisch formuliert, da der Betroffene nach dem Wortlaut der Regelung auch serverseitige Systeme seines Anbieters „nutzt". Damit würden Strafverfolgungsbehörden die Ermächtigung erhalten, auch auf Systemen der Dienstanbieter Manipulationen zur Absenkung des Sicherheitsniveaus vorzunehmen: etwa an den Servern, über die Nachrichten weitergeleitet werden oder über die der Schlüsselaustausch erfolgt, mit dem dann in der Folge Nachrichten verschlüsselt werden.

De facto ergäbe sich mit dieser Ermächtigung eine Verpflichtung von Dienstanbietern zur Duldung von staatlichen Hintertüren, die den auch vom BMI unterstützten Eckpunkten deutscher Kryptopolitik[27] klar widersprechen.

➡ *Mindestens muss eine deutliche Beschränkung auf die Manipulation von direkt vom Betroffenen genutzten Endgeräten und ein expliziter Ausschluss der Manipulation und Infiltration von Systemen der Dienstanbieter erfolgen, um eine uferlose Ausweitung der Eingriffsbefugnisse zu vermeiden.*

---

[27] Bundesministerium des Innern und Bundesministerium für Wirtschaft und Technologie vom 2. Juni 1999: *Eckpunkte der deutschen Kryptopolitik,* Quelle beim BMWI nicht mehr vorhanden, dauerhaft verfügbar unter, https://hp.kairaven.de/law/eckwertkrypto.html
Vgl. Deutscher Bundestag, Drucksache 14/1149, http://dipbt.bundestag.de/doc/btd/14/011/1401149.pdf und Deutscher Bundestag Drucksache 18/5144, http://dipbt.bundestag.de/dip21/btd/18/051/1805144.pdf

Die in der StPO definierte Mitwirkungspflicht der Anbieter von Telekommunikationsdiensten an Überwachungsmaßnahmen (neu: Absatz 4 § 100 StPO) wird durch die parallel zu diesem Gesetzgebungsverfahren angestrebte Ausweitung des Geltungsbereichs des TKG zum beweglichen Ziel in einem hochgradig kritischen Rechtsgebiet: Die vom Bundesrat geforderte Ausdehnung des TKG und damit des Kreises der gemäß dem vorliegenden Änderungsantrag zur Mitwirkung Verpflichteten auf alle Anbieter von „Messengerdiensten und standortbezogenen Diensten mit Telekommunikationsdiensten“[28] könnte in Kombination mit den hier angestrebten Änderungen der StPO ebenfalls zu einer Situation führen, in der Dienstanbieter zu einer Schaffung bzw. Duldung von Hintertüren für Behörden gezwungen werden können. Dies wäre erneut in direktem Widerspruch zu den Eckpunkten deutscher Kryptopolitik und würde zu einer erheblichen Verschlechterung von Vertrauen, Sicherheit und Marktposition deutscher Anbieter von Verschlüsselungslösungen führen.

➡ *Sämtliche derartige Gesetzesvorhaben müssen zwingend gemeinsam betrachtet werden.*

[28] Bundesrat Drucksache 88/16 vom 17.02.16: Entschließung des Bundesrates zur Anpassung des Rechtsrahmens an das Zeit- alter der Digitalisierung im Telekommunikationsbereich – Rechtssicherheit bei Messengerdiensten, standortbezogenen Diensten und anderen neuen Geschäftsmodellen,
http://www.bundesrat.de/SharedDocs/drucksachen/2016/0001-0100/88-16.pdf?__blob=publicationFile&v=1

Fazit

Mit dem Geheimhalten von Sicherheitslücken, die zum Anbringen von Schadsoftware genutzt werden können, geht ein hohes Risiko für die innere Sicherheit einher. Das Risiko für das Entdecken dieser Sicherheitslücken durch Dritte steigt mit der Häufigkeit ihrer Ausnutzung durch staatliche Stellen. Im Sinne der inneren Sicherheit ist eine Beseitigung sämtlicher Schwachstellen anzustreben und von deren Hortung und Geheimhaltung abzusehen.

Die Anwendung von Schadsoftware im Strafverfahren stellt einen schweren Grundrechtseingriff dar. Die rechtlichen Grenzen der sogenannten Quellen-Telekommunikationsüberwachung lassen sich technisch kaum umsetzen. Bei alltäglichen Strafverfahren gibt es keine Rechtfertigung derart schwerwiegender Grundrechtseingriffe.

Die Prämisse, dass Strafverfolgungsbehörden aufgrund von Verschlüsselung der Kommunikation keine Ermittlungsansätze oder Daten zur Verfügung stünden, hält der Empirie nicht stand. Das Gegenteil ist der Fall: Strafverfolgungsbehörden steht dank der fortschreitenden Digitalisierung aller Lebensbereiche eine nie dagewesene Fülle an Daten zur Verfügung.

Die technischen Rahmenbedingungen für den Einsatz von Schadsoftware sind sowohl für die generell abzulehnende gedankliche Konstruktion der Quellen-TKÜ als auch für die vollumfängliche Online-Durchsuchung nicht ausreichend spezifiziert: weder eine Rechtssicherheit noch adäquate Kontrollmöglichkeiten werden sichergestellt.

Eine Verletzung der Eckpunkte deutscher Kryptopolitik würde zu einer erheblichen Verschlechterung von Vertrauen, Sicherheit und Marktposition deutscher Anbieter von Verschlüsselungslösungen führen.

Der Änderungsantrag ist folglich in seiner Gänze abzulehnen.