Forum InformatikerInnen
für Frieden
und gesellschaftliche
Verantwortung e. V.

Technische und gesellschaftliche Kosten des verdeckten Zugriffs auf die Grundlagen der vernetzten Gesellschaft

Sachverständigenauskunft zu dem Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen – Drucksache 19/5412

Dipl. Inf. Rainer Rehak für das FIfF
rainer.rehak@fiff.de
0D66 63E5 70A3 964A EE60D927 4427 CFE5 8C19 AE19

Dienstag, 7.2.2018
Version 1.5

Inhaltsverzeichnis

„Gegeben die technische Entwicklung, wird Freiheit und Unbeobachtbarkeit des Denkens (etwa beim Erwägen von Äußerungen oder Handlungen) künftig untrennbar mit dem Schutz persönlichster Rechner, ihrer Anwendung und auch der Daten auf ihnen verknüpft sein. […] Der Zugriff auf gespeicherte Computerdaten auf persönlichsten Rechnern entgegen des Willens des Eigennutzers ist daher künftig weniger mit einer klassischen Hausdurchsuchung vergleichbar, als vielmehr mit der Verabreichung bewusstseinsverändernder Drogen zum Zwecke des Erlangens von Aussagen.“

Prof. Dr. Andreas Pfitzmann[1]

1 Prof. Dr. Andreas Pfitzmann, Rede vor dem Bundesverfassungsgericht als Sachverständiger zur Online-Durchsuchung, 10.10.2007, Seiten 3 und 4. Pfitzmann hatte den Lehrstuhl für Datenschutz und Datensicherheit an der Technischen Universität Dresden inne.

1 Zusammenfassung und Änderungsvorschläge

Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung nimmt gern zum vorliegenden Gesetzesentwurf DS-19/5412 Stellung.

Speziell die Paragraphen § 6 (Quellen-TKÜ) und § 8 (Online-Durchsuchung) beziehen sich auf eine technische Ermächtigung, mit der ein informationstechnisches System infiltriert werden kann. Welche Daten letztendlich ausgeleitet werden – Kommunikation oder nicht – ist technisch nicht automatisiert unterscheidbar und dementsprechend auch nicht sinnvoll einzuhegen. *QTKÜ und OD müssen daher die gleichen Eingriffshürden haben.*

Des weiteren gibt es technisch begründet wesentliche Zweifel an einer vertrauenswürdigen Protokollierbarkeit der Aktivitäten und Funde einer QTKÜ/OD auf einem infiltrierten Zielsystem. Die technischen Grundvoraussetzungen für verlässliches Logging und Signierung sind auf einem fremden System nicht gegeben. *Eine detaillierte Dokumentation jedes Zugriffs, mindestens in Form von kompletter Quellcodevorlage und -Auditierung, ist ebenso nötig, wie die rechtliche Eingrenzung auf bestimmte Zielsystemarten.*

Die heimliche Installation einer QTKÜ/OD-Software verlangt die Nutzung von Sicherheitslücken. Die dadurch entstehenden Anreize für Dritte, Sicherheitslücken nicht mehr zu melden, sondern zu verkaufen oder derartige Dienste anzubieten, schadet der allgemeinen IT-Sicherheit weltweit. Das greift langfristig die Grundlagen der vernetzten Gesellschaft an und korrodiert die digitale Infrastruktur. Zusätzlich vertreiben diese Dritten die gleichen Sicherheitslücken üblicherweise auch an Diktaturen weltweit, die damit ihre BürgerInnen kontrollieren, DissidentInnen/MenschenrechtsverteidigerInnen ausspähen und verfolgen. *Um auf eine sichere und menschenfreundliche IT-Landschaft hinzuwirken, dürfen keine Sicherheitslücken verwendet, gehandelt oder zurückgehalten werden – insbesondere keine bislang unbekannten Lücken (zerodays).*

Die These eines „Blindwerdens von Behörden“ durch Kryptographienutzung („Going-dark“) lässt sich nicht erhärten, physische Interaktionen von Kriminellen und allgemeine Effekte der Digitalisierung bieten nach wie vor hinreichende Ansatzpunkte für eine effektive Gefahrenabwehr.

Der Verfassungsschutz ist ein Geheimdienst und per definitionem ungleich intransparenter und schwerer demokratisch zu kontrollieren als etwa Polizeien. *Derartig eingriffstiefe und folgenschwere Ermächtigungen wie § 6 und § 8 dürfen ihm demnach grundsätzlich nicht erteilt werden.*

In der Konsequenz raten wir nachdrücklich dazu, die Paragraphen § 6 (Quellen-TKÜ) und § 8 (Online-Durchsuchung) ersatzlos zu streichen.

2 Vertrauen in die digitale Welt

In einer vernetzten Informationsgesellschaft,[2] die sich mehr und mehr auf digitale Infrastrukturen verlässt – vom Laptop bis zum Stromnetz – verlangt die enorme und immer größer werdende Komplexität dieser Zusammenhänge nach einem Kit, um überhaupt funktionsfähig zu bleiben. Dieser Kit ist Vertrauen, Vertrauen in technische Systeme, in deren Hersteller, in die Nutzerinnen und Nutzer und auch in staatliche Organe dahingehend, diesen neuen Umstand der Digitalisierung in der Breite sinnvoll zu nutzen, mit zu gestalten und auch, wo nötig, rechtlich einzuhegen. Dieses Vertrauen – gerade in üblicherweise als verlässlich empfundene behördliche Stellen – hat jedoch in jüngerer Vergangenheit wiederholt auf diverse Arten Schaden genommen. Dabei muss nicht über den Atlantik zur National Security Agency (NSA) geblickt werden, sondern ganz konkret auf deutsche Behörden des Sicherheitsbereichs.[3]

Angefangen bei den politischen Enthüllungen um die Operationen Glotaic[4] oder Eikonal[5], über die Nutzung der NSA-Programms XKEYSCORE durch den Verfassungsschutz[6] bis hin zum bundesweiten *Digitask*-Trojaner-Debakel[7] ist offensichtlich, dass ein erneuter Vertrauensaufbau dringend geboten ist. Und Projekte wie der gehackte „Hamburger Wahlstift“, das gescheiterte „De-Mail“ oder kürzlich das „besondere elektronische Anwaltspostfach“ (beA) zeigen, wie kompliziert es tatsächlich ist, sensible IT-Projekte zu stemmen und Vertrauen aufzubauen. Dafür sind behutsamer Technikeinsatz, reflektiertes Vorgehen und kontinuierliche Transparenz unablässig.[8]

3 Vertraulichkeits- und Integritätserwartung

Genau diese Aspekte hatte das Bundesverfassungsgericht im Blick, als es 2008 das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) formulierte. Es ist dabei kein Grundrecht auf die zwei Schutzziele der IT-Sicherheit „Vertraulichkeit“ und „Integrität“, sondern ein Grundrecht auf die *Gewährleistung* der beiden, also eine wesent-

2 Nach Prof. Wolfgang Coy in Anlehnung an die McLuhansche Gutenberg-Galaxis auch „Turing-Galaxis“ genannt.
3 Siehe Konferenzbeiträge der FIfFKon2014 „Der Fall des Geheimen – ein Blick unter den eigenen Teppich.“ 2014, TU-Berlin, https://2014.fiffkon.de.
4 Greis , Friedhelm: BND griff Daten offenbar über Tarnfirma ab, Golem.de, 24.2.2015, https://www.golem.de/news/operation-glotaic-bnd-griff-daten-offenbar-ueber-tarnfirma-ab-1502-112571.html.
5 Kehrhahn , Jobst-H.: Operation Eikonal: BND soll jahrelang Daten deutscher Bürger an NSA übermittelt haben, Heise.de, 05.10.2014, https://www.heise.de/newsticker/meldung/Operation-Eikonal-BND-soll-jahrelang-Daten-deutscher-Buerger-an-NSA-uebermittelt-haben-2411680.html.
6 Biermann , Kai: Wozu braucht der Verfassungsschutz Xkeyscore?, Zeit.de, 12.2.2016, http://www.zeit.de/digital/datenschutz/2016-02/verfassungsschutz-bfv-nsa-xkeyscore.
7 CCC: Chaos Computer Club analysiert aktuelle Version des Staatstrojaners, ccc.de, 26.10.2011, https://www.ccc.de/de/updates/2011/analysiert-aktueller-staatstrojaner.
8 Bundesamt für Sicherheit in der Informationstechnik (BSI, Hrsg): Broschüre Digitale Gesellschaft: smart & sicher, IT-Sicherheit aus Nutzer- und Expertensicht, 2017, S. 50.

liche Vorverlagerung des Schutzes. Um die zugrundeliegenden Überlegungen zu beschreiben, legte das Gericht in seiner Urteilsbegründung dar, dass der Wesensgehalt des Grundrechts der „Schutz der Vertraulichkeits- und Integritätserwartung“[9] an informationstechnische Systeme ist. Daraus lässt sich nach unserer Lesart eine klare präventive Handlungspflicht staatlicher Stellen – inklusive der gesetzgebenden – zum Schutze informationstechnischer Systeme ableiten.

3.1 Digitale Infrastrukturen

Dabei darf auch nicht nur die Privatsphäre der einzelnen Person[10] maßgeblich sein, sondern es muss immer auch die digitale Infrastruktur der vernetzten Gesellschaft mit in den Blick genommen werden, und das Vertrauen hierin. Der Begriff der „Vernetzung“ verweist hier hier keinesfalls nur auf direkte, technische Netzwerkverbindungen zwischen Geräten, sondern auch auf die vielgestaltigen Abhängigkeiten der verschiedenen Systeme und Akteure voneinander. Dies können gemeinsame Softwarehersteller sein oder aber der Einsatz bestimmter Softwarekomponenten oder Betriebssysteme an ganz verschiedenen Stellen der digitalen Landschaft. Wird also ein Hersteller oder Softwareprodukt durch bestimmte Maßnahmen und Regelungen geschützt, werden parallel dazu auch die anderswo eingesetzten Systeme, NutzerInnen und Nutzungsweisen mitgeschützt. Im Gegenzug bedeutet dies jedoch auch, dass Schädigungen oder Schwächungen von bestimmten Softwarekomponenten gleichermaßen auch alle anderen Einsatzweisen schwächt und unsicherer macht. Aus diesem Grunde war es beispielsweise möglich, dass die Schadsoftware „Wannacry“ sowohl private Laptops, als auch Krankenhaus-Eisenbahn- und Providersysteme[11] lahmlegen konnte: Millionen Systeme hatten ähnliche Softwarekomponenten – in diesem Falle das Betriebssystem Microsoft Windows – und waren damit gleichermaßen verwundbar.

Wenn wir also von einer vernetzten Gesellschaft mit „Cloud“, „Industrie 4.0“ und „smarten“ Infrastrukturen sprechen, muss immer auch die damit einhergehende gegenseitig Abhängigkeit und Verwundbarkeit mitgedacht werden.

4 Gegenstand der Stellungnahme

Wie kann eingangs beschriebene Vertrauen aufgebaut bzw. erhalten bleiben, wie können informationstechnische Systeme sicher gemacht und die Vertraulichkeits- und Integritätserwartung der BürgerInnen tatsächlich geschützt

9 Bundesverfassungsgericht: Bundesverfassungsgerichtsurteil zur Online-Durchsuchung, BverfG, 1 BvR 370/07, 27.2.2008, Abs. 206, http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html.

10 Seite 40 des Gesetzesentwurfes, Drucksache 19/5412.

11 Holland, Martin und Kannenberg, Axel: WannaCry – Angriff mit Ransomware legt weltweit Zehntausende Rechner lahm, heise.de, 12.5.2017, https://www.heise.de/newsticker/meldung/WannaCry-Angriff-mit-Ransomware-legt-weltweit-Zehntausende-Rechner-lahm-3713235.html.

werden? Diese sehr grundsätzlichen Fragen sollen hier in Bezug auf den anlassgebenden Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen angegangen werden.

Geheimdienste, also staatliche Behörden, die wesentlich auf verdeckte Maßnahmen, Tarnoperationen, „Vertrauensleute“ oder verdeckte MitarbeiterInnen setzen – sind inhärent auf Intransparenz angelegt und angewiesen, da Heimlichkeit das primäre Mittel ist, die ihnen übertragenen Aufgaben auszufüllen. Ermächtigungen derartiger Dienste müssen folglich besonders kritisch analysiert werden, da einmal freigegebene Maßnahmen und ermöglichte Methoden meist nur nach Skandalen erneut zur breiten Diskussion gestellt werden (können). Auch wenn laut dem flankierenden Entwurf eines neuen Verfassungsschutzkontrollgesetzes (VSKG) nun beispielsweise jedes einzelne Mitglied der Kontrollkommission gemäß VSKG § 4 Abs. 2 Akteneinsicht bekommen kann und zudem eigene MitarbeiterInnen zur Seite gestellt bekommt, besteht naturgemäß dennoch die übliche Geheimhaltungspflicht der Kommission nach VSKG § 2.

Besonderheit von Geheimdiensten

In der Stellungnahme werden wir uns unserer Expertise entsprechend vordringlich den im Gesetzesentwurf angesprochenen verdeckten technischen Maßnahmen und ihren gesellschaftlichen Implikationen zuwenden – konkret der sogenannten Quellen-Telekommunikationsüberwachung (QTKÜ) und der heimlichen Online-Durchsuchung (OD)[12]. Dabei ist hervorzuheben, dass diese Maßnahmen zwei Besonderheiten aufweisen, die sie gerade in den Händen von Geheimdiensten zusätzlich problematisch erscheinen lassen: Erstens sind es aktive Maßnahmen von immenser Eingriffstiefe für die Betroffenen und zweitens sind die langfristigen Konsequenzen des Einsatzes sehr schwer abzuschätzen, weil sich die Anreizstrukturen bestimmter IT-sicherheitsrelevanter Märkte dadurch ändern können.

Eine Evaluation und Diskussion der genauen Auswirkungen solcher Maßnahmen wird beim Einsatz durch Geheimdienste wesentlich erschwert oder sogar unmöglich gemacht. Auch wenn sich die Aufgabenbereiche von Polizeien und Geheimdiensten mittlerweile gefährlich überlappen, sind dennoch die Berichts- und Transparenzpflichen von polizeilichen Behörden – im Gegensatz zu verdeckt tätigen Organisationen – immer noch grundsätzlich auf Offenheit angelegt. Wegen dieses gewichtigen Unterschieds gehen die rechtfertigenden Referenzen auf die BKA-Gesetz-Entscheidung des Bundesverfassungsgerichts, wie etwa auf Seite 40 des vorliegenden Gesetzentwurfs

12 Im Text werden auch die Begriffe verdeckte Online-Datenerhebung bzw. verdeckte Online(-)Überwachung verwendet.

(Drucksache 19/5412), grundsätzlich fehl. Ein Geheimdienst ist keine Polizei und eine Polizei ist kein Geheimdienst.

Struktur der Stellungnahme

Zunächst werden einige technische Sachverhalte der Maßnahmen kommentiert und diskutiert, danach werden indirekte Auswirkungen des Einsatzes derartiger Maßnahmen auf die öffentliche Sicherheit erläutert sowie diskutiert und dann folgen resultierende Vorschläge, alternative Herangehensweisen und abschließende Überlegungen.

Ziel dieser Sachverständigenauskunft ist es, in Anlehnung an HVSG § 15 Abs. 2 (Verhältnismäßigkeit) erkennbar zu machen, wie sehr die Nachteile außer Verhältnis zu etwaigen Erfolgen der angesprochenen Maßnahmen stehen.

5 Direkte Auswirkungen technischer Eigenschaften

Im ersten Abschnitt soll es um die technischen Unterschiede und Gemeinsamkeiten der Maßnahmen QTKÜ und OD gehen, wonach eine Betrachtung der Protokollierungsmöglichkeiten sowie Vertrauenswürdigkeit der Funde solcher Maßnahmen erfolgt. In dieser Stellungnahme findet sich jedoch keine vollständige Diskussion des Lebenszyklus‘ einer QTKÜ- bzw. OD-Software und aller vorhandenen Risiken, da dies an anderer Stelle schon ausführlich beschrieben worden ist.[13]

5.1 Die technische Natur von QTKÜ und OD

Dieser Gesetzesentwurf geht, wie andere vor ihm auch, fälschlicherweise davon aus, dass QTKÜ (§ 6) und OD (§ 8) gänzlich verschiedene Maßnahmen sind, die demnach auch getrennt voneinander betrachtet und geregelt werden können. So wird die QTKÜ im Entwurf auf Seite 37 als spezielle Form der grundrechtlich vergleichsweise „leichtgewichtigen“ Telekommunikationsüberwachung beschrieben, die OD jedoch als „Sonderform“ einer eingriffsintensiven Wohnraumüberwachung. Dies zeigt sich u. a.daran, dass die OD in § 8 „nach Maßgabe des § 7“ ermöglicht wird und in § 9 das Verfahren bei Maßnahmen nach den §§ 7 und 8 in einem Rutsch geregelt wird.

Auch im Verfassungsschutzkontrollgesetz (VSKG) wird derartig unterschieden: So muss nach VSKG § 3 Abs. 3 Satz 2. ein jährlicher Lagebericht zur OD-Maßnahmen erstellt werden und auch dem Landtag muss laut VSKG § 6 über OD-Maßnahmen berichtet werden, all dies gilt für QTKÜ-Maßnahmen nicht. Weiterhin kann eine QTKÜ nach unserer Lesart auch schon zur Quellengewinnung nach HVSG § 5 Abs. 1 Satz 2 verwendet werden.

13 Rehak, Rainer: Angezapft – Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung, MV-Verlag Editon Wissenschaft, 2013.

Das ist juristisch betrachtet nachvollziehbar, doch technisch absolut nicht haltbar – mit schwerwiegenden Implikationen, denn im Entwurf wird betrachtet, was der gewünschte Zweck einer Maßnahme ist, aber ignoriert, was die tatsächliche Realisierung nach sich zieht: Alle Schritte – von der Aufbringung der Software auf das Zielsystem – also die Infiltration – über das versteckte Agieren darin, das Aktualisieren und Nachladen von Funktionalität bis hin zur Löschung – sind identisch.[14] Allein die Datensuche ist geringfügig unterschiedlich; sie ist jedoch nur abhängig von wenigen Konfigurationsparametern und selbst dieser Unterschied taugt nicht für eine Reduzierung der Eingriffstiefe, wie in 5.3 weiter ausgeführt wird. Die jeweils für die verschiedenen Maßnahmen eingesetzte Software ist also gleich mächtig und jederzeit gleichermaßen anpass- und erweiterbar. Nur ein kleiner Schalter macht aus einer QTKÜ eine OD, weil beide nach Aktivierung bereits tief im System verankert sind.

Diese Dynamik ist bei üblichen technischen Geräten nicht zu finden. Mit einem Fernseher kann man keinen Brief schreiben und mit einer Schreibmaschine kann man nicht fernsehen; die Nutzungsarten sind streng getrennt, weil sie mit unterschiedlichen Geräten realisiert werden. Ein Digitalcomputer jedoch ist eine sogenannte „Universalmaschine“, die allein durch die aktuell laufende Software bestimmt jegliche (berechenbare) Funktion ausführen kann. Im Gegensatz zu physischen Maschinen lässt sich Software jedoch sehr leicht verändern und bei so ähnlichen Funktionen wie sie QTKÜ und OD erfüllen, besteht der Unterschied tatsächlich nur in einer anderen Konfigurationsdatei.

Die grundlegende Unterscheidung zwischen QTKÜ und OD ist also juristisch gewünscht, aber technisch nicht abbildbar. In der Folge müssten die beiden Maßnahmen jedoch auch grundrechtlich ähnlich behandelt werden und nicht wie im aktuellen Entwurf fundamental unterschiedlich.

Eine erhellende Analogie

Das konzeptionelle Problem lässt sich gut mit einer Analogie beschreiben. Angenommen es gäbe eine sehr günstige, leichte, kleine, genaue Maschinenpistole, die nur mit einem kleinen Schalter zwischen langsamen Einzelschuss und Automatik umgeschaltet werden könnte. Nun ist die entscheidende Frage, warum nicht normale Polizeistreifen und Spezialkommandos einfach diese gleiche Waffen bekommen sollten; die ersteren mit dem Schalter auf „leicht bewaffnet“ und die letzteren mit dem Schalter auf „schwer bewaffnet“? Die Verneinung liegt in struktureller, staatlicher Selbstbeschränkung begründet. Staatliche Stellen sollen nur gerade so viel Macht zugewiesen bekommen, um

14 Ebd. Seite 16.

ihre Aufgaben zu erledigen; eine normale Polizeistreife hat eben keine Maschinenpistole.

Genau diese rechtsstaatlich gebotene Beschränkung ist mit einer QTKÜ technisch bedingt nicht umsetzbar, denn sie ist einer OD baugleich und somit gleichmächtig.

5.2 Die entscheidende Hürde

Diese „Unbeschränkbarkeit“ hat auch das Bundesverfassungsgericht 2008 in seinem Urteil zur heimlichen Online-Durchsuchung ausgeführt: „Wird ein komplexes informationstechnisches System zum Zweck der Telekommunikationsüberwachung technisch infiltriert („Quellen-Telekommunikationsüberwachung“), so ist mit der Infiltration die entscheidende Hürde genommen, um das System insgesamt auszuspähen. Die dadurch bedingte Gefährdung geht weit über die hinaus, die mit einer bloßen Überwachung der laufenden Telekommunikation verbunden ist.“[15]

Es ist demnach gänzlich unverständlich und entbehrt jeder technischen Grundlage, warum eine QTKÜ mit geringeren Eingriffshürden als die OD zur Anwendung kommen können soll. Die gleiche technische Fehleinschätzung liegt auch der StPO-Änderung von 22. Juni 2017 zugrunde, bei der die Möglichkeiten für Anwendung von QTKÜ und OD – mittels einer Formulierungshilfe – stark ausgeweitet worden sind.[16] Auch in der dortigen Anhörung hatten die technischen Sachverständigen auf dieses gravierende Problem hingewiesen – vergeblich.[17] Auch bei der Entscheidung zur Verfassungsbeschwerden gegen die Ermittlungsbefugnisse des BKA zur Terrorismusbekämpfung wurde dieser Umstand übersehen.[18]

Der Trojaner des Bundesverfassungsgerichts

Diese aus technischer Sicht rechtliche Fehlentwicklung ist in einem juristischen Winkelzug des Bundesverfassungsgerichts begründet. In einer abstrakten „Wenn-dann“-Formulierung platzierte es selbst einen Trojaner im eigenen Urteil: „Art. 10 Abs. 1 GG ist hingegen der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer „Quellen-Telekommunikationsüberwachung“, wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt

15 Bundesverfassungsgericht: Bundesverfassungsgerichtsurteil zur Online-Durchsuchung, BverfG, 1 BvR 370/07, 27.2.2008, Abs. 188.
16 FIfF-Pressemitteilung vom 23. Juni 2017: Entfesselter Staatstrojaner: Große Koalition verhöhnt IT-Sicherheit und Demokratie, https://www.fiff.de/presse/pressemitteilungen/entfesselter-trojaner-grosse-koalition-verhoehnt-it-sicherheit-und-demokratie.
17 Anhörung des Rechtsausschusses, Mittwoch, 31. Mai 2017 „Änderung StGB, JGG, StPO“. https://www.bundestag.de/ausschuesse/ausschuesse18/a06/anhoerungen/aenderung-stgb--jgg--stpo-2/507628
18 Gemeinsame Erklärung vom 20. April 2016, https://www.fiff.de/presse/pressemitteilungen/urteil-zum-bka-gesetz.

sein.“[19] Dieser Passus ist technisch unbegründbar und inkonsistent mit dem Rest des Urteils; entweder wurde das System unter Verletzung des IT-Gewährleistungsgrundrechts infiltriert oder aber nicht. Aus Sicht der IT-Sicherheit ist Datenauswahl nach einer gelungenen Infiltration zweitrangig, das System ist kompromittiert – und außer Kontrolle.

Nun stellt aber HVSG § 6 (Abs. 2) 1. genau auf diese Hintertür ab, wonach die QTKÜ anwendbar wird, wenn „sichergestellt ist, dass ausschließlich laufende Kommunikation überwacht und aufgezeichnet wird“. Ignorieren wir für einem Moment alle Konzepte und Erkenntnisse der IT-Sicherheit und folgen dem Bundesverfassungsgericht ist seiner Ausnahmeregelung: Das neue konkrete Problem besteht nun darin, dass diese Beschränkung auf laufende Kommunikation prinzipiell technisch nicht sichergestellt werden kann, die Bedingung also nie erfüllt wird und dieser Passus folglich immer nur abstrakt bleiben muss.

5.3 Beschränkung auf laufende Kommunikation

Eine QTKÜ soll die Klartextdaten einer verschlüsselt ablaufenden Kommunikation erlangen, welche einer normalen Telekommunikationsüberwachung (TKÜ) nur verschlüsselt zugänglich sind. Zusätzlich dürfen nur genau die Daten der aktuell laufende Kommunikation überwacht und aufgezeichnet werden – nichts weiter.

Zu diesem Zweck müssten die Kommunikationsdaten also direkt auf dem Endgeräten vor der Verschlüsselung (beim Versand) bzw. direkt nach der Entschlüsselung (beim Empfang) auf dem Endgeräten abgegriffen werden. Auf weitere Daten – etwa Daten aus vorherigen Kommunikationsvorgängen – darf nicht zugegriffen werden.

Eine gleichzeitige Umsetzung beider Anforderungen ist praktisch nicht leistbar, wie in der technischen Literatur bereits detailliert beschrieben worden ist.[20] Exemplarisch sollen hier nur einige wesentliche Probleme erläutert werden.

Transport- und normale Datenverschlüsselung

Technisch kann zwischen Transport- und normaler Datenverschlüsselung unterschieden werden. Im ersten Fall ist die Verschlüsselung Teil des Transport-, also Versendevorgangs; beispielhaft sei dafür die HTTPS-Verschlüsselung beim Webseitenzugriff genannt. Im zweiten Fall findet die

19 Bundesverfassungsgericht: Bundesverfassungsgerichtsurteil zur Online-Durchsuchung, BverfG, 1 BvR 370/07, 27.2.2008, Absatz 190.

20 Rehak, Rainer: Angezapft – Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung, MV-Verlag Editon Wissenschaft, 2013, Seite 44 ff.

Verschlüsselung direkt auf den lagernden Daten des Systems statt; beispielhaft seien hier passwortgeschützte ZIP-Dateien genannt.

Bei den am weitesten verbreiteten Standards für E-Mailverschlüsselung (PGP[21] und S/MIME[22]) und bei jeglichen Instant-Messenger-Anwendungen (Signal[23], Whatsapp, etc) wird normale Datenverschlüsselung verwendet. Dies leuchtet ein, da die Nachrichten zunächst zum Versenden vorbereitet werden und gegebenenfalls erst später, wenn eine Verbindung mit dem Internet besteht, tatsächlich versendet werden.

Der Prozess des Versendens einer verschlüsselten Nachricht gleicht also strukturell eher dem Schützen einer ZIP-Datei mit einem Passwort und dem späteren, eventuellen Verschicken. „Eventuell“ deshalb, weil etwa die meisten für Verschlüsselung konfigurierten E-Mailprogramme auch Entwürfe verschlüsselt speichern. Diese können dann später verschickt werden; oder auch nicht. Gleiches gilt für den Postausgang, aus dem noch nicht verschickte E-Mails wieder gelöscht werden können. Auch der normale Versendevorgang einer Nachricht kann abgebrochen werden, sei es weil etwas Wichtiges vergessen wurde oder weil man es sich einfach anders überlegt hat. In all diesen Fällen hat eine QTKÜ, die die Daten vor der Verschlüsselung kopieren muss, Daten überwacht und gespeichert, die nicht zu laufender Kommunikation gehören.

Ein weiteres, wesentliches Problem gerade bei mobilen Instant-Messengern ist der Zugriff auf eingehende und gespeicherte Nachrichten, denn dafür ist ein Vollzugriff auf die innerhalb der App gespeicherten Nachrichten nötig. Wenn allerdings dieser Zugriff erfolgreich ist, müssen die Daten beispielsweise nach Datum sortiert werden, was einen Zugriff auf alle Nachrichten impliziert. Wieder werden Daten überwacht, die nicht zu laufender Kommunikation gehören.

Ein Extremszenario muss noch erwähnt werden, weil es die grundrechtliche, immense Gefährdung der QTKÜ gut illustrieren kann. Um verschlüsselte Videotelefonie (Skype, etc) auszuleiten, wird von einer QTKÜ üblicherweise das Mikrofon und die Kamera angezapft, um dann anhand des System- und Softwareverhaltens zu detektieren, wann ein Gespräch stattfindet. Da die Kommunikationssoftware nicht kooperiert – der Zugriff soll ja heimlich stattfinden – ist die Erkennung laufender Kommunikation technisch nicht trivial umzusetzen. Schlägt sie fehl und es wird aufgezeichnet, obwohl keine Kommunikation stattfindet – weil etwa das Mikrofon softwareseitig stumm geschaltet ist oder ausschließlich Screensharing aktiviert ist, so ist aus der

21 OpenPGP Message Format, https://tools.ietf.org/html/rfc4880.
22 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification, https://tools.ietf.org/html/rfc5751.
23 Signal protocol family, Technical Specifications, https://signal.org/docs/.

„leichtfüßigen“ QTKÜ kurzerhand eine volle Wohnraumüberwachung mit Bild und Ton geworden.

Und all diese Funktionalität muss verdeckt gegen alle Abwehrmechanismen des Systems, sowie der einzelnen Softwarekomponenten durchgesetzt werden, sowie ohne selbst weitere Sicherheitslöcher im System zu erzeugen.

5.4 Detailgrad und Vertrauenswürdigkeit der Protokollierung

Der vertrauenswürdigen Protokollierung der Aktivitäten einer QTKÜ/OD kommt nicht nur wegen der Einschätzung und Verwertbarkeit der Ergebnisse eine große Bedeutung zu, sondern auch für den Schutz der Betroffenen, also der Wahrung ihrer Interessen und Rechte während der verdeckten Maßnahme.

Einerseits sollen die vorgenommenen Änderungen am System der Betroffenen detailliert protokolliert werden, sodass belegbar ist, dass diese Änderungen nach HVSG § 8 (Abs. 2) möglichst minimal waren und dass sie nach Beendigung der Maßnahme automatisiert rückgängig gemacht werden können. Andererseits muss daraus hervorgehen, dass die erlangten Daten und Hinweise tatsächlich auf dem System gefunden worden sind und nicht durch Softwarefehler der QTKÜ/OD selbst erzeugt worden, von dritten platziert oder gar ein falsches System infiltriert worden ist.

Ein objektives Mindestmaß an Detailgrad und Vertrauenswürdigkeit der Protokollierung sind daher essentiell für eine derartig eingriffsintensiven Maßnahme. Es verwundert daher sehr, dass die Protokollpflicht in HVSG§ 6 (Abs. 4) für QTKÜ/OD so unbestimmt formuliert ist. Festzuhalten ist nur „das zur Datenerhebung eingesetzte Mittel“ und „Angaben, die die Feststellung der erhobenen Daten ermöglichen“, doch was bedeutet dies? Alles ist denkbar von der Nennung des Firmen-/Produktnamens bis hin zur Dokumentation des Quellcodes der eingesetzten Software und der ausgenutzten Sicherheitslücken auf dem Zielsystem.

Die Vergangenheit hat gezeigt, dass sich Behörden durch den unvorbereiteten externen Einkauf von QTKÜ/OD-Software gänzlich von den Bedingungen der Hersteller abhängig machen.[24] Die Verweigerung der Einsichtnahme in den Quellcode oder zurückgehaltene Informationen zu ausgenutzten Sicherheitslücken beispielsweise sind ein unhaltbarer Zustand bei derartigen Maßnahmen und müssen von Anfang an rechtlich als Mindestforderung detailliert verhindert werden. Nur so können auch unabhängige Audits zur Sicherstellung der Funktion ermöglicht werden.

24 Meister, Andre: Staatstrojaner: DigiTask verweigert Datenschutzbeauftragten Einblick in Quellcode, netzpolitik.org, 11.9.2012, https://netzpolitik.org/2012/staatstrojaner-digitask-verweigert-datenschutzbeauftragten-einblick-in-quellcode/.

Wenn es keine kommerziellen Anbieter gibt, die den rechtsstaatlichen Anforderungen entsprechen, so bliebe vor diesem Hintergrund nur die Eigenentwicklung oder Unterlassung.

Vertrauenswürdigkeit

Der zweite relevante Aspekt ist die Vertrauenswürdigkeit der Protokollierung von Softwareaktivitäten. Dabei gibt es grundsätzliche Probleme, denn die Software legt die Protokolle an, während sie auf einem „fremden“ – dem infiltrierten – System agiert. Die Protokolle sind demnach stets mit Vorsicht zu interpretieren. Auch eine kryptographische Absicherung der Protokolle kommt nicht ernsthaft in Frage, da jegliches dafür nötige Schlüsselmaterial wiederum dem fremden System auch zugreifbar wäre.[25] Sobald also das fremde System die QTKÜ/OD-Software entdecken würde, könnte sie anfangen, gefälschte Protokolle zu erzeugen und kryptographisch korrekt abgesichert an die Behörden zu senden. Diese Fälschung ist im Betrieb praktisch unentdeckbar und kann auch durch nachträgliche forensische Untersuchungen kaum bemerkt werden. Diese auch nachträglich nicht aufzulösende Unkontrollierbarkeit der ohnehin schon verdeckten Maßnahme stellt eine derartig gravierende grundrechtliche Gefährdung der Betroffenen dar und sollte daher einem Geheimdienst nicht zur Verfügung stehen.

6 Auswirkungen auf die öffentliche Sicherheit

Jedes informationstechnische System enthält eine Reihe von Sicherheitsmaßnahmen, um die IT-Sicherheit des Systems zu gewährleisten, etwa dass nur Befugte Zugriff auf die dortigen Informationen haben; diese also lesen (Informationsvertraulichkeit) oder verändern (Datenintegrität) können. Wer befugt ist, entscheiden die BesitzerInnen der Systeme, und jegliche Software – vom Betriebssystem bis zum Browser – unterstützen sie bei der Durchsetzung dieser Entscheidung.

Externe Zugriffsversuche durch staatliche Akteure sind folglich aus Sicht des Systems die gleichen Angriffe, wie sie beispielsweise auch von Schadsoftware – Viren, Würmern und Trojanern – der (organisierten) Kriminalität kontinuierlich versucht werden.

Soll also ein externer Zugriff für eine QTKÜ oder OD durchgeführt werden, so müssen die systemeigenen Sicherheitsmechanismen umgangen werden, was alle Softwarehersteller wiederum nach Kräften zu verhindern suchen. Jedes hinreichend komplexe System hat jedoch auch Fehler, die, wenn sie Auswirkungen auf die Sicherheitsfunktionen des Systems haben, Sicherheits-

25 Rehak, Rainer: Angezapft – Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung, MV-Verlag Editon Wissenschaft, 2013, Seite 38 ff.

lücken genannt werden.[26] Kleine Softwareteile, die diese Lücken praktisch ausnutzen, um unbefugt Kontrolle über ein fremdes System zu erlangen, werden Expoits[27] genannt.

Sicherheit versus Sicherheit

Damit nun extern auf ein Zielsystem zugegriffen werden kann, so muss die QTKÜ/OD-Software solche Expoits nutzen, wodurch ein folgenreicher und gesellschaftlich hoch relevanter Zielkonflikt entsteht: staatliche Behörden brauchen funktionierende Exploits für Maßnahmen wie die QTKÜ und OD, doch die Sicherheit unserer IT-Infrastruktur hängt gerade davon ab, jegliche Sicherheitslücken schnellstens zu schließen. Alle informationstechnischen Systeme, von Privatgeräten, über Krankenhaus-, Eisenbahn-, Verkehrsleitsysteme bis hin zu Kraftwerkssteuerungen nutzen mittlerweile ähnliche vernetzte Softwarekomponenten, und diese müssen so sicher wie möglich gehalten werden, oder eben nicht.

Wenn der Verfassungsschutz auch im digitalen Zeitalter die „Sicherheit des Einzelnen“ effektiv und auch glaubwürdig schützen möchten, wie auf der ersten Seite des Gesetzesentwurfes zu lesen ist, so muss auch er sich uneingeschränkt für die Schließung von Sicherheitslücken einsetzen. Dazu gibt es keine Alternative, will man Konzepte wie „Cloudcomputing“, Datenschutz, „smart city“, „Internet of things“ oder „Industrie 4.0“ tatsächlich ernst nehmen. Diese Erkenntnis ist Konsens in der wissenschaftlichen und praktischen IT-Sicherheit.

Globaler Schwarzmarkt von Sicherheitslücken

Doch diese Frage hat noch weitreichendere gesellschaftliche Implikationen, denn woher kommen die für eine QTKÜ/OD nötigen, noch unentdeckten Sicherheitslücken – die sogenannten Zerodays? Diese Lücken können aufwändig selbst gesucht werden, was sehr viel behördeninterne IT-Kompetenz erfordert. Wenn dann Lücken gefunden werden, so ist das ein Beleg dafür, dass auch andere diese Lücken haben finden können und sie womöglich schon ausnutzen. Eine sofortige Übermittlung an den Hersteller und ggf. das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist im Sinne der (öffentlichen) Sicherheit dringend geraten. Gleiches gilt für schon bekannte Sicherheitslücken: diese dürfen nicht genutzt, sondern müssen so schnell wie möglich geschlossen werden. Das wohl bekannteste Beispiel für den Irrweg, Lücken zu behalten, war sicherlich der oben schon erwähnte Erpresserwurm „Wannacry“, der weltweit zehntausende Systeme infiltrierte und Sicherheitslücken nutze, die der US-Geheimdienst NSA seit Jahren für eine

26 Eckert, Claudia: IT-Sicherheit: Konzepte - Verfahren – Protokolle, De Gruyter Oldenbourg, 2014, Einführung.
27 Engl. für ausnutzen, ausbeuten, instrumentalisieren.

spätere Verwendung aufgehoben hatte – trotz diesbezüglicher interner Risikoabwägungsmechanismen.[28]

Die zweite Möglichkeit besteht darin Sicherheitslücken/Exploits auf dem globalen Schwarzmarkt zu kaufen und in eigene QTKÜ/OD-Software zu integrieren oder aber schon fertige Infiltrationssoftware von spezialisierten Firmen zu „mieten“. Der externe Kauf bzw. das Mieten derartiger Software haben jedoch gravierende Nebeneffekte, und das nicht nur auf die IT-Sicherheit. Gerade staatliche Akteure im Sicherheitsbereich sind oft finanziell gut ausgestattet, wodurch diese Exploit-Märkte ganz wesentlich erzeugt und auch erst legitimiert werden. In der Folge wird die gesamte IT-Infrastruktur unsicherer, weil Lücken zunehmend nicht mehr an Hersteller gemeldet, sondern auf den Märkten an die Meistbietenden versteigert werden.

Sowohl beim Lückenankauf, als auch beim externen „Mieten“ bleibt stets unklar, an wen die Lücken sonst noch verkauft werden. Auch wenn derartige IT-Firmen wie *Hacking Team*, zu deren Kunden beispielsweise spanische und US-amerikanische Behörden (CNI, FBI, DEA) gehören, stets bestreiten, mit Diktaturen zusammenzuarbeiten, kommt dennoch immer wieder das Gegenteil ans Licht. So verkaufte *Hacking Team* nachweislich an Behörden in Ägypten, Libanon, Aserbaidschan, Kasachstan, Sudan und Äthiopien. In veröffentlichten E-Mails an die Firma *Hacking Team* bedankten sich die staatlichen Stellen der Diktaturen dafür, „oppositionelle Ziele [nun] schnell identifizieren zu können“.[29]

Gleiches lässt sich über die aktuell vom Bundeskriminalamt (BKA) beauftragte[30] deutsche Firma Gamma/FinFisher berichten, die u. a. den *FinSpy-QTKÜ*-Trojaner herstellt, der nun eingesetzt werden soll.[31] FinSpy wurde damals auch von bahrainischen Behörden genutzt, um DissidentInnen zu verfolgen und den Arabischen Frühling niederzuschlagen.[32] Weitere Kunden der Firma sind Behörden in Diktaturen wie Dubai oder Katar, aber auch die Mongolei und Indonesien.[33] Dabei werden auch diese Firmen immer

28 Hay Newman, Lily: Feds Explain Their Software Bug Stash—But Don’t Erase Concerns, wired.com, 15.11.2017, https://www.wired.com/story/vulnerability-equity-process-charter-transparency-concerns/.
29 Borchers, Detlef: Überwachungssoftware: Aus Hacking Team wurde Hacked Team, heise.de 6.7.2015, https://www.heise.de/security/meldung/Ueberwachungssoftware-Aus-Hacking-Team-wurde-Hacked-Team-2736160.html.
30 Meister, Andre: Geheimes Dokument: Das BKA will schon dieses Jahr Messenger-Apps wie WhatsApp hacken, netzpolitik.org, 20.7.2017, https://netzpolitik.org/2017/geheimes-dokument-das-bka-will-schon-dieses-jahr-messenger-apps-wie-whatsapp-hacken/.
31 dpa/pbe: Grünes Licht für den gekauften Staatstrojaner, spiegel.de, 2.2.2018, http://www.spiegel.de/netzwelt/netzpolitik/smartphone-ueberwachung-bka-darf-gekauften-staatstrojaner-jetzt-einsetzen-a-1191112.html.
32 Meister, Andre: Gamma FinFisher: Überwachungstechnologie „made in Germany“ gegen Arabischen Frühling in Bahrain eingesetzt, netzpoltik.org, 8.8.2014, https://netzpolitik.org/2014/gamma-finfisher-ueberwachungstechnologie-made-in-germany-gegen-arabischen-fruehling-in-bahrain-eingesetzt/.
33 Meister, Andre: Gamma FinFisher: Neue Analyse des Staatstrojaners deutet auf weitere Kunden hin, Netzpoltiik.org, 9.8.2012, https://netzpolitik.org/2012/gamma-finfisher-neue-analyse-des-staatstrojaners-deutet-auf-weitere-kunden-hin/.

wieder gehackt und dann die Software, Sicherheitslücken und interne Dokumente veröffentlicht.[34]

Das ist der aktuelle, katastrophale Zustand der weltweiten IT-Sicherheit, und deutsche Behörden helfen mit, diesen Status quo aufrecht zu erhalten. Wir halten das wir für inakzeptabel.

In der wohlwollenden Interpretation unterstützen deutsche Behörden mit Steuergeldern nur derartig schäbige Geschäftsmodelle, im der besorgniserregenderen Deutung finanziert Deutschland Firmen, die direkt oder indirekt an der Verfolgung von DissidentInnen und MenschenrechtsverteidigerInnen in Diktaturen beteiligt sind.[35] Dies ist neben dem eigentlichen Skandal zudem eine denkbar schlechte Position, um auf eine Lösung des dringenden Problems der globalen IT-Sicherheit hinzuarbeiten

Es kann nicht im Interesse Deutschlands sein, international wirksame Anreize zu schaffen und zu stützen, die diametral dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme entgegenstehen, deswegen darf auch der Verfassungsschutz derartige Aktivitäten nicht unterstützen.

Wenn es tatsächlich um Sicherheit gehen soll, so muss die Suche nach Sicherheitslücken strukturiert, koordiniert und konsequent angegangen werden, ohne Ausnahme. Die globalisiert-vernetzte Informationsgesellschaft bedeutet mittlerweile eben auch: es gibt keine öffentliche Sicherheit mehr ohne IT-Sicherheit.

7 Alternative Ansätze zu staatlichem Hacking

In den USA und auch in Deutschland findet sich die Argumentation, dass das Aufkommen von Ende-zu-Ende-verschlüsselten Kommunikationskanälen die Arbeit von Sicherheitsbehörden zunehmend erschwert. Der Zweck von QTKÜ und OD ist die Aufklärung und Informationsbeschaffung zur Gefahrenabwehr, weil dies scheinbar nicht mehr ohne Direktzugriff auf Endgeräte geht. Doch einer tieferen Analyse hält dieses Argument nicht stand, wie unter anderem in einem Report des Berkman Center for Internet & Society der Harvard University zu lesen ist.[36] Darin wird ausgeführt, wie sich durch die technische Weiterentwicklung auch immer neue Informationsquellen auftun, angefange bei der Analyse von Metadaten bis hin zu Firmen, deren Geschäftsmodelle gerade davon abhängen, keine Ende-zu-Ende-Verschlüsselung zu nutzen. Dabei

34 Meister, Andre: Gamma FinFisher gehackt: Werbe-Videos von Exploits und Quelltext von FinFly Web veröffentlicht, Netzpolitik.org, 6.8.2014, https://netzpolitik.org/2014/gamma-finfisher-gehackt-werbe-videos-von-exploits-und-quelltext-von-finfly-web-veroeffentlicht/.

35 Amnesty International: A year ago, Ahmed Mansoor's iPhone was targeted using elite spyware only sold to governments, amnesty.org, 2017, https://www.amnesty.org/en/get-involved/take-action/free-ahmed-mansoor/.

36 Schneier, Bruce, et al: Don't Panic: Making Progress on the „Going Dark" Debate, Berkman Center for Internet & Society, Harvard University, 1.2.2016, https://cyber.harvard.edu/pubrelease/dont-panic/.

geht es uns bestimmt nicht darum, gewissen datenschutzaversen Firmen das Wort zu reden, sondern zu überlegen, wie die stetige Digitalisierung in anderer Weise zur Gefahrenabwendung genutzt werden kann, ohne dabei die eigene Infrastruktur zu kompromittieren. Auch ohne Verschlüsselung haben Menschen mit der zunehmenden Verlagerung ins Digitale neue Alternativen, sich vor QTKÜ und OD von Behörden zu schützen.[37]

Die Motivation der Gesetzesänderung verdient ebenso einen Kommentar, auch wenn sich diese Stellungnahme speziell mit QTKÜ und OD beschäftigt. An vielen Stellen im Entwurf ist von Terror die Rede, insbesondere durch den NSU, aber auch auf andere Taten wird Bezug genommen. An dieser Stelle sei jedoch die Frage gestattet, wo QTKÜ oder OD tatsächlich die primäre Lösung hätten sein können, es also keine anderen Erfolgsansätze hätte geben können? Drei Beispiele aus der aktuellen Terror-und-Verschlüsselung-Debatte seien hier einmal kurz kommentiert:

1) Gerade im skandalösen Fall des NSU und seiner (Nicht-)Aufklärung waren fehlende QKTÜ/OD-Fähigkeiten sicherlich das kleinste Problem im ganzen Debakel.[38]

2) Im Fall der rechtsextremen „Oldschool Society“ (OSS), weitläufig bekannt durch den höchst strittigen Telegram-Zugriff durch das BKA, waren die so erlangten Informationen vor dem Münchner Oberlandesgericht für die Verurteilung letztendlich gar nicht verwendet worden.[39]

3) Der weltweit berühmte Fall um die San-Bernadino-Bomber und ihr verschlüsseltes iPhone machte zwar gute Schlagzeilen für Apple, basierte jedoch auf einem Password-Reset-Fehler der Ermittler, der dann erst den extrem teuren Hack nötig machte. Das Öffnen des iPhones brachte im Übrigen gar keine nützlichen Informationen hervor.[40]

Insgesamt sehen wir die Begründung der neuen IT-Befugnisse in Bezug auf die im Entwurf benannten terroristischen Straftaten und Ereignisse also mit kritischer Vorsicht. Auch wenn der Zweck Terrorismusbekämpfung die volle Unterstützung verdient, scheinen uns die technischen Infiltrationsbefugnisse doch über das Ziel hinaus zu schießen. Gerade bei den im Entwurf genannten Ereignissen lohnt es sich, detailliert zu durchdenken, inwiefern eine QTKÜ/OD jeweils hilfreich und zwingend notwendig gewesen wäre, insbesondere weil in

37 Wood, Andrew Keane: Encryption Substitution, Hoover Institution, Stanford University, 18.7.2017, www.hoover.org/sites/default/files/research/docs/woods_encryption_substituteswebreadypdf.pdf.

38 Pichl, Maximilian: Von Aufklärung keine Spur: 20 Jahre NSU- Komplex, Blätter für deutsche und internationale Politik, 1/2018, https://www.blaetter.de/archiv/jahrgaenge/2018/januar/von-aufklaerung-keine-spur-20-jahre-nsu-komplex.

39 Braun, Sven: Bundeskriminalamt knackt Telegram-Accounts, netzpolitik.org, 26.08.2016, https://netzpolitik.org/2016/bundeskriminalamt-knackt-telegram-accounts/.

40 Ellen Nakashima: Comey defends FBI’s purchase of iPhone hacking tool, washingtonpost.com, 11.5.2016, https://www.washingtonpost.com/world/national-security/comey-defends-fbis-purchase-of-iphone-hacking-tool/2016/05/11/ce7eae54-1616-11e6-924d-838753295f9a_story.html.

einigen Fällen die Täter schon vorher bekannt waren und etwa der Anschlag am Breitscheidplatz in Berlin offenbar sogar mit Involvierung von V-Leuten durchgeführt worden ist.[41] Gleiches gilt für den NSU-Fall „Andreas Temme“.

Dieser Kommentar ist an dieser Stelle wichtig, da insbesondere die hier diskutierten verdeckten Methoden der Informationstechnik sehr, sehr teuer sind und es muss reflektiert werden, ob diese Mittel nicht gesellschaftlich weitaus sinnvoller angelegt werden können – von Polizeipersonal[42] bis Schulangebote, als auf den Konten zwielichtiger Schwarzmarkthändler, deren Geschäftsmodell die Unsicherheit unserer IT-Infrastruktur, die Festigung von Diktaturen und das ungehinderte[43] Verfolgbarmachen von Menschenrechts-verteidigerInnen ist.

In der ganzen Debatte ist noch viel Bewegung über den richtigen Weg zum gleichen Ziel. Wir jedenfalls sehen nicht, dass die Geheimdienste blind werden, wenn sie keine Telefone infiltrieren können. Kriminalstatistiken sowie Aufklärungsraten geben uns glücklicherweise auch keinen Anlass zur Sorge, diese Diskussion übereilt abschließen zu müssen.

8 Offensive Unsicherheit

Der aktuelle Vorstoß, Geheimdiensten wie dem Verfassungsschutz die Ermächtigung zu geben, informationstechnische Systeme zu infiltrieren, ist in in einen stetigen, sehr beunruhigenden Trend einzuordnen: Der schrittweise Ausbau von informationstechnischen Offensivfähigkeiten der Behörden im Sicherheitsbereich.

Sowohl der Bundesnachrichtendienst (BND) hat mit seiner „Strategische Initiative Technik“ die Fähigkeiten bekommen, technische Systeme verdeckt und offen angreifen können[44] als auch die Bundeswehr mit der „Strategische Leitlinie Cyber-Verteidigung“, die explizit – anders als der Name impliziert – auch „offensive Cyber-Fähigkeiten“ als „Wirkmittel“ vorsieht.[45]

Wie erwartet war die Kritik aus den Kreisen der Informatik für eine derartige Offensivausrichtung bei einem gleichzeitig so desaströsen Zustand der

41 Goll, Jo und Adamek, Sascha: V-Mann soll Gruppe um Amri zu Anschlägen aufgehetzt haben, rbb, 19.10.17, https://www.rbb24.de/politik/beitrag/2017/10/amri-von-v-mann-angestachelt-anschlag-berlin-breitscheidplatz.html.

42 „Die Stadt wächst seit Jahren, unser Personalbestand aber nicht, das schafft jede Menge Tatgelegenheiten“, aus Scheffer, Ulrike und Zawatka-Gerlach, Ulrich: Berlin ist die Hauptstadt des Verbrechens, tagesspiegel.de, 24.4.2017, http://www.tagesspiegel.de/politik/kriminalstatistik-2016-berlin-ist-die-hauptstadt-des-verbrechens/19711644.html.

43 Loll, Anna Catherin: Lieber ohne Menschenrechte exportieren, zeit.de, 17.9.2017, http://www.zeit.de/wirtschaft/2017-09/exporte-menschenrechte-dual-use-diktaturen/komplettansicht.

44 Meister, Andre: Strategische Initiative Technik: Wir enthüllen, wie der BND für 300 Millionen Euro seine Technik aufrüsten will, netzpolitik.org, 21.9.2015, https://netzpolitik.org/2015/strategische-initiative-technik-wir-enthuellen-wie-der-bnd-fuer-300-millionen-euro-seine-technik-aufruesten-will/.

45 Gebauer, Matthias: Von der Leyen rüstet an der Cyberfront auf, spiegel.de, 10.7.2015, http://www.spiegel.de/politik/deutschland/bundeswehr-ursula-von-der-leyen-ruestet-an-der-cyber-front-auf-a-1042985.html.

eigenen IT-Sicherheit immens.[46] Da werden viele hundert Millionen Euro in geheime IT-Angriffsstrategien investiert; und beispielsweise für das „Nationale Referenzprojekt zur IT-Sicherheit in Industrie 4.0“[47] – als Absicherung der Zukunft der deutschen Industrie – gibt es 33 Millionen Euro, ganze fünf Millionen Euro weniger, als für das krachend gescheiterte „besondere elektronische Anwaltspostfach“ (BeA) ausgegeben worden ist.[48]

Spätestens an dieser Stelle wird klar, dass es keine digitale Gesamtstrategie gibt, doch das Resultat dieser Flucht nach vorn ist eine selbst initiierte Korrosion der Grundlagen unserer vernetzten Gesellschaft. Und genau in diese Kerbe schlägt auch dieses Gesetz mit seinen Ermächtigungen.

Mit dieser Fahrtrichtung wird es stetig schwieriger, langfristig auf eine globale Ächtung des Handels mit Sicherheitslücken oder sonstige Beschränkungen der strukturellen Verminderung der IT-Sicherheit hinzuarbeiten; und das wäre langfristig die einzig vernünftige Grundlagenstrategie einer Digitalisierung. Wenn diese Position aber glaubhaft vertreten werden soll, so müssen konsequent alle Ressourcen in die Verbesserung und Absicherung der Technik investiert werden, denn ist langfristig die beste Investition in öffentlich (IT-)Sicherheit überhaupt.[49]

In diesem Lichte muss nun auch HVSG § 15 Abs. 1 verstanden werden, wodurch die Erläuterung zu § 6 Abs. 2, dass über technische Mittel gewonnene Informationen nicht die Problematik einer Mitarbeiter- bzw. Quellengefährdung bergen, wieder wesentlich relativiert wird: gefährdet wird dann eben die Allgemeinheit.

Differenzierungsmöglichkeiten

Dabei geht der Entwurf nicht einmal behutsam mit der Zielmaterie um. Es gibt keine Differenzierung nach Gerätearten, aktuell wäre die Ermächtigung gültig für PCs, Laptops, Tablets und Mobiltelefone, aber auch für Autos, Herzschrittmacher, Assistenzsysteme wie Alexa/Home/etc, Krankenhaussysteme, Hafenkrananlagen, Industriesteuerungen, „smarte“ Fernseher, Türsteuerungen, Heizungsthermostate, Fitnessarmbänder, „smarte“ Zahnbürsten bis hin zur vernetzten Spielzeugpuppe.[50] Immer nur theoretisch begrenzt vom abstrakten Verhältnismäßigkeitsparagraphen HVSG § 15, der jedoch bei QTKÜen in der aktuellen Ausgestaltung des Gesetzes gar nicht effektiv von

46 Meister, Andre, Geheime Cyber-Leitlinie: Verteidigungsministerium erlaubt Bundeswehr „Cyberwar“ und offensive digitale Angriffe, netzpolitik.org, 30.7.2015, https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/.

47 Dipl.-Ing. Simon Duque Antón, Deutsches Forschungszentrum Künstliche Intelligenz (DFKI), https://www.dfki.de/web/forschung/projekte?pid=945.

48 Böck, Hanno: Noch mehr Sicherheitslücken im Anwaltspostfach, golem.de, 4.1.2018, https://www.golem.de/news/bea-noch-mehr-sicherheitsluecken-im-anwaltspostfach-1801-131942.html.

49 Siehe unsere Kampagne „Cyberpeace“, https://cyberpeace.fiff.de.

50 Kühl, Eike: Vernichten Sie diese Puppe, zeit.de, 17.2.2017, http://www.zeit.de/digital/datenschutz/2017-02/my-friend-cayla-puppe-spion-bundesnetzagentur/komplettansicht.

der Kontrollkommission überprüft werden kann, weil es keine aktiven Lageberichte gibt.

Auch die Belehrung ausländischer Stellen über Zweckbindung der übermittelten Daten und ggf. zu verlangende Auskunft nach HVSG § 22 Abs. 3. klingen eher unbedacht. Zumindest der offizielle Fragekatalog der Bundesregierung an die USA nach den Snowden-Enthüllungen im Jahr 2013 ist bis dato unbeantwortet geblieben. Diese Möglichkeit muss vor einer Übermittlung an ausländische Stellen in Betracht gezogen und dann ggf. neu abgewogen werden.

8.1 Abschluss

Letztlich sind in diesem Entwurf bezüglich der QTKÜ und OD keinerlei wirksamen Grenzen zum Schutze des eigentlich „absolut geschützten Kernbereichs privater Lebensgestaltung“ erkennbar und auch keine Ansätze, die langfristigen gesamtgesellschaftlichen Auswirkungen der Maßnahmen auf die öffentliche (IT-)Sicherheit entgegen zu wirken.

Auch die Vorgaben für das IT-Gewährleistungsgrundrecht wurden verwässert. So wurde die verfassungsrechtliche Vorgabe für eine Infiltration zum Schutz von „Güter[n] der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt“[51] umgewandelt in den Schutz von „Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist.[52] Diese neue Formulierung ist unserer Ansicht nach viel zu weit auslegbar.

Diese Gründe, zusammengenommen mit der prinzipiell geringen Transparenz eines Geheimdienstes, sorgen dafür, dass wir dringend zu einer ersatzlosen Streichung dieser beiden Ermächtigungen HVSG § 6 und § 8 raten.

Abschließend sei noch angemerkt, dass die vom Bundesverfassungsgericht formulierten Leitsätze und Überlegungen grundsätzlich nur den allerletzten verfassungsmäßigen Rahmen aufzeigen sollen, in welchem sich der Gesetzgeber unbedingt bewegen muss. Es besteht überhaupt keine Pflicht und Notwendigkeit, diesen Rahmen immer zwingend auszuschöpfen. Es zeugt unserer Ansicht nach eben nicht von Wertschätzung dieser Werte und Grenzen, wenn sie vom Gesetzgeber auffallend oft berührt und leider auch regelmäßig überschritten werden. Genau zu dieser Abgrenzungsthematik schrieb das Bundesverfassungsgericht 2004 im Urteil zum großen Lauschangriff: „Inzwischen scheint man sich an den Gedanken gewöhnt zu haben, dass mit den mittlerweile entwickelten technischen Möglichkeiten auch deren grenzenloser Einsatz hinzunehmen ist. Wenn aber selbst die

51 Bundesverfassungsgericht: Bundesverfassungsgerichtsurteil zur Online-Durchsuchung, BverfG, 1 BvR 370/07, 27.2.2008, 2. Leitsatz, http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html.

52 HVSG § 7 Satz 3.

persönliche Intimsphäre [...] kein Tabu mehr ist, vor dem das Sicherheitsbedürfnis Halt zu machen hat, stellt sich auch verfassungsrechtlich die Frage, ob das Menschenbild, das eine solche Vorgehensweise erzeugt, noch einer freiheitlich-rechtsstaatlichen Demokratie entspricht.“[53] Im vorliegenden Fall ist eine Ablehnung der Befugnisse sogar im Namen der Sicherheit sinnvoll.

9 Über das FIfF

Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V. ist ein deutschlandweiter Zusammenschluss von Menschen, die sich kritisch mit Auswirkungen des Einsatzes der Informatik und Informationstechnik auf die Gesellschaft auseinandersetzen. Unsere Mitglieder arbeiten überwiegend in informatiknahen Berufen, vom IT-Systemelektroniker bis hin zur Professorin für Theoretische Informatik. Das FIfF wirkt in vielen technischen und nichttechnischen Bereichen der Gesellschaft auf einen gesellschaftlich reflektierten Einsatz von informationstechnischen Systemen zum Wohle der Gesellschaft hin. Zu unseren Aufgaben zählen wir Öffentlichkeitsarbeit, sowie Beratung und das Erarbeiten fachlicher Studien. Zudem gibt das FIfF vierteljährlich die „FifF-Kommunikation – Zeitschrift für Informatik und Gesellschaft“ heraus und arbeitet mit anderen Friedens- sowie Bürgerrechtsorganisationen zusammen.

53 Bundesverfassungsgericht: Bundesverfassungsgerichtsurteil zum großen Lauschangriff, BverfG, 1 BvR 2378/98, 3.3.2004, Absatz 373, http://www.bundesverfassungsgericht.de/entscheidungen/rs20040303_1bvr237898.html.

Für alle Links gilt: letzter Zugriff: 2.2.2018.