Goethe-Universität Frankfurt am Main
Fachbereich 03 Gesellschaftswissenschaften
Institut für Politikwissenschaften
Sommersemester 2018

Gefährdet der staatliche Einsatz von Spionagesoftware die Innere Sicherheit?

Eine Untersuchung anhand des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens

–

Abschlussarbeit zur Erlangung des akademischen Grades
Bachelor of Arts (B.A.)

vorgelegt von:
Frank Kuhn

Erstgutachter/Betreuer: Dr. Philipp Erbentraut
Zweigutachterin: Prof. Dr. Brigitte Geißel

Frankfurt am Main, den 02.07.2018

Inhaltsverzeichnis

Abkürzungsverzeichnis

BBP	„Bug-Bounty“-Programme
BKA	Bundeskriminalamt
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten / BKA-Gesetz
BMI	Bundesministerium des Innern, für Bau und Heimat
BND	Bundesnachrichtendienst
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT	Bundestag
BVerfG	Bundesverfassungsgericht
CVVS	Common Vulnerability Scoring System
DNC	Democratic National Committee
FBI	Federal Bureau of Investigation
IoT	Internet of Things / Internet der Dinge
ISP	Internet Service Provider / Internetanbieter
KRITIS	kritische Infrastrukturen
LEP	Lying Endpoint Problem
NHS	National Health Service
NSA	National Security Agency
ODS	Online-Durchsuchung
PKS	Polizeiliche Kriminalstatistik
RCIS	Remote Control Interception Software
StPO	Strafprozessordnung
TKÜ	Telekommunikationsüberwachung
VoIP	Voice-over-IP / IP-Telefonie
ZITiS	Zentrale Stelle für Informationstechnik im Sicherheitsbereich

Abbildungsverzeichnis

1 Einleitung

Am 22. Juni 2017 verabschiedete der Deutsche Bundestag (BT) das *„Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens"*. Die Reform der Strafprozessordnung (StPO) schafft unter anderem die Rechtsgrundlagen für die sogenannte Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) und die Online-Durchsuchung (ODS). Die Quellen-TKÜ ermöglicht den Strafverfolgungsbehörden neben dem Abhören von unverschlüsselter Kommunikation nun auch das Abhören von verschlüsselter Kommunikation. Außerdem dürfen sie im Rahmen einer ODS über das Internet auf informationstechnische Systeme von Tatverdächtigen und die darauf gespeicherten Daten zugreifen. Damit sollen die Befugnisse der Strafverfolgungsbehörden an den technischen Fortschritt im Bereich der Telekommunikation angepasst werden (Deutscher Bundestag 2017). Diese Befugnisse zur Strafverfolgung stellen ein Novum dar, denn bislang durften Quellen-TKÜ und ODS nur zur Gefahrenabwehr auf Rechtsgrundlage der Polizeigesetze der Länder und des Bundes eingesetzt werden. So ist es z. B. dem Bundeskriminalamt (BKA) gestattet, zur Abwehr von Gefahren des internationalen Terrorismus auf die besagten Maßnahmen zurückzugreifen (§§ 49, 51 BKA-Gesetz).

Die Begriffe Quellen-TKÜ und ODS weisen zwar eine begriffliche Nähe zu etablierten Ermittlungsmaßnahmen wie der klassischen TKÜ (§ 100a StPO in seiner alten Fassung) und einer Durchsuchung (§§ 102, 103 StPO) auf, unterscheiden sich auf technischer Ebene jedoch grundlegend von ihren begrifflichen Verwandten (Freiling et al. 2017: S. 16). Denn sowohl bei einer Quellen-TKÜ als auch bei einer ODS werden die informationstechnischen Systeme der Tatverdächtigen zunächst aktiv mit einem Überwachungsprogramm infiltriert. Diese Infiltration ist „ein aktiver Vorgang, der das Zielsystem verändert" (ebd.).

In Bezug auf diese aktive Infiltration macht *Roggan* einen interessanten Zielkonflikt aus: Möchte der Staat die informationstechnischen Systeme von Tatverdächtigen infiltrieren, dann erfolgt die Infiltration beispielsweise über Sicherheitslücken in den IT-Systemen der Zielpersonen. Um diese Sicherheitslücken für sich zu nutzen, hat der Staat ein begründetes Interesse daran, dass etwaige Schwachstellen, die den jeweiligen Software- und Computerherstellern unbekannt sind, nicht geschlossen werden. Für deutsche Behörden ist also eine unsichere IT-Infrastruktur von Vorteil (Roggan 2017: S. 828–829). Software-Schwachstellen, die alle Benutzer betreffen und dem Staat bekannt sind, werden also nicht an die jeweiligen Hersteller weitergegeben, damit Einzelpersonen im Rahmen eines Strafverfahrens überwacht

werden können (Roggan 2017: S. 828–829). Dieses Vorgehen kollidiert mit dem staatlichen Auftrag, die Sicherheit in der Informationstechnik zu fördern (ebd.). Bei der StPO-Reform geht es also um „die Vertiefung einer latenten Gefahr für die innere Sicherheit bzw. die Allgemeinheit" (ebd.: S. 829), weil die IT-Sicherheitslücken auch von Cyberkriminellen genutzt werden können (ebd.).

Die Bundesregierung betrachtet diese Problematik aus einem anderen Blickwinkel. Der Stärkung und Anwendung von Verschlüsselungstechnologie steht das Gebot effektiver Strafverfolgung gegenüber. Darum müssen die Ermittlungsmaßnahmen dem technischen Fortschritt angepasst werden (BT-Drucksache 18/12785: S. 48–49).

Diese Thematik ist aus politikwissenschaftlicher Sicht hochinteressant. Schließlich ist es die Aufgabe des Staates, „die Sicherheit und innere Ordnung eines Gemeinwesens zu garantieren und Unsicherheit zu vermeiden" (Glaeßner 2003: S. 145). Der ehemalige Bundesinnenminister Hans-Peter Friedrich erklärte Sicherheit gar zum „Supergrundrecht" (Bewarder/Jungholt 2013). Darum stellt sich in Anbetracht der obigen Ausführungen *Roggans* und der Gesetzesbegründung der Bundesregierung die Frage, in welchem Maße der Staat dieser Aufgabe beim Einsatz von Spionagesoftware zur Strafverfolgung überhaupt nachkommt.

Mit dieser Problemstellung hat sich jedoch noch niemand ausführlich beschäftigt. Dies mag sicherlich damit zusammenhängen, dass Forschungsarbeiten im Politikfeld der Inneren Sicherheit grundsätzlich Mangelware sind (Preuß 2012: S. 226) und sich eher mit den Akteuren und Institutionen auseinandersetzen (Wenzelburger 2015: S. 676). Außerdem stammen die Untersuchungen oftmals von Kriminologen (ebd.: S. 663). Deshalb besteht im Regelfall eine explizit rechtswissenschaftliche Sichtweise auf die Ermittlungsmaßnahmen, bei der zwar auf die verschiedenen Möglichkeiten der Infiltration von informationstechnischen Systemen eingegangen wird, nicht aber auf mögliche Risiken für die Innere Sicherheit bei Anwendung dieser Möglichkeiten (siehe dazu Weiß 2009: S. 15–20 sowie Kohlmann 2012: S. 23–51 und Bunzel 2015: S. 35–47). Auch etwaige Verbesserungen der Inneren Sicherheit durch Quellen-TKÜ und ODS sind nicht Teil der rechtswissenschaftlichen Betrachtung.

Diese Forschungslücke soll unter Zuhilfenahme der folgenden Forschungsfrage untersucht werden:

> *„Schafft die Bundesregierung mit dem „Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens" vermeidbare Risiken für die Innere Sicherheit?"*

2 Methodisches Vorgehen

Um die Forschungsfrage zu beantworten, werden die folgenden drei Hypothesen überprüft:

> *H1: Die Strafverfolgungsbehörden müssen für die Erfüllung ihrer Aufgaben auf verschlüsselte Kommunikation sowie verschlüsselte Daten zugreifen können. Dafür benötigen sie die Ermittlungsinstrumente der Quellen-TKÜ und Online-Durchsuchung.*
>
> *H2: Infiltriert der Staat informationstechnische Systeme zum Zwecke der Strafverfolgung, so schafft er Risiken für die Sicherheit informationstechnischer Systeme (IT-Sicherheit).*
>
> *H3: Zwischen der effektiven Strafverfolgung und der Sicherheit informationstechnischer Systeme (IT-Sicherheit) besteht ein Zielkonflikt.*

In Bezug auf die Problemstellung dieser Arbeit stellt die vage Definition des Begriffes „Innere Sicherheit" beziehungsweise des Sicherheitsbegriffes selbst ein weiteres Problem dar. Lange Zeit beschäftigte sich die politische Philosophie mit dem Sicherheitsbegriff nur in Abgrenzung zum Freiheitsbegriff (Wenzelburger 2015: S. 664). Wenn in der Öffentlichkeit von „Sicherheit" die Rede ist, dann geht es meistens darum, welche rechtlichen oder politischen Maßnahmen zu einem bestimmten Zeitpunkt nötig sind, um Sicherheit zu gewährleisten – nicht aber um die Bedeutung des Konzeptes selbst (Waldron 2006: S. 455–456). Die Definition von „Sicherheit" in Abgrenzung zu „Freiheit" ist für diese Forschungsarbeit allerdings wenig hilfreich. Schließlich geht es hier gerade *nicht* um den vielfach behandelten Zielkonflikt zwischen Freiheit und Sicherheit, sondern darum, ob Sicherheitsgesetze selbst ein Risiko für die Innere Sicherheit darstellen können. Hierfür ist eine eigenständige Definition von „Sicherheit" unabdingbar.

Aus diesem Grund sollen zu Beginn der Arbeit zunächst die zentralen Begriffe erarbeitet werden. Neben der *Sicherheit* und der *Inneren Sicherheit* sind dies außerdem noch die *IT-Sicherheit* sowie das *Sicherheitsrisiko*. Weiterhin muss hierbei auch festgestellt werden, inwiefern Sicherheitslücken in IT-Systemen ein Sicherheitsrisiko darstellen. Außerdem erscheint es unerlässlich, kurz die technischen Grundlagen von Quellen-TKÜ und Online-Durchsuchung darzulegen.

Im Anschluss folgt die Untersuchung des *„Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens"*, wobei hier nur Quellen-TKÜ und ODS betrachtet werden. Andere im Gesetz enthaltene (Neu-)Regelungen wie das Fahrverbot als Nebenstrafe (Deutscher Bundestag 2017) sind in Bezug auf die Forschungsfrage nicht relevant. Das BKA-Gesetz

beinhaltet zwar ebenfalls die Ermittlungsmaßnahmen Quellen-TKÜ und ODS, wird aber trotzdem nicht in die Untersuchung miteinbezogen. Dies liegt darin begründet, dass sich die Befugnisse des BKA auf die vergleichsweise geringe Fallzahl des internationalen Terrorismus beschränken und die Ermittlungsmaßnahmen im Zeitraum von 2009–2016 laut BKA-Präsident Holger Münch ohnehin nur fünf Mal zum Einsatz kamen (ZEIT Online 2016).

Um die oben aufgestellten Hypothese zu überprüfen, werden Quellen-TKÜ und ODS hinsichtlich Verbesserung und Verschlechterung der Inneren Sicherheit untersucht. Als Orientierung kann dabei die Evaluation des Verfassungsschutzgesetzes von Nordrhein-Westfalen dienen, die zu Beginn des Jahres 2011 durchgeführt wurde; der Verfassungsschutz NRW war die erste Sicherheitsbehörde in Deutschland, welche die ODS einsetzen durfte. So ist in Bezug auf die Verbesserung der Inneren Sicherheit zu prüfen, ob die Ermittlungsmaßnahmen geeignet sind, mehr Sicherheit zu schaffen und ob die Behörden die Befugnisse überhaupt benötigen (vgl. Wolff 2015: S. 50). In Bezug auf die Verschlechterung sind insbesondere die unbeabsichtigten Wirkungen zu prüfen (vgl ebd.: S. 51). Im Anschluss lässt sich einschätzen, ob die entstandenen Risiken vermeidbar sind und ob die Zuwächse an Sicherheit diese Risiken rechtfertigen können (vgl. ebd.). Nicht vermeidbar wären die Risiken z. B. dann, wenn die Strafverfolgungsbehörden die neuen Befugnisse zur Quellen-TKÜ und ODS unbedingt benötigen, um ihren Auftrag erfüllen zu können. Vermeidbar wären die Risiken, wenn die Behörden z. B. auf andere Ermittlungsmaßnahmen zurückgreifen könnten. Gewissermaßen kann hier auch von einer Gesetzesfolgenabschätzung gesprochen werden, die im Wesentlichen auf Basis einer Literaturauswertung erfolgen soll.

Aus methodischer Sicht stellt die Betrachtung eines Gesetzes im Rahmen einer qualitativen Fallstudie dabei eine bewährte Methode dar, um die Politik der Inneren Sicherheit in einem Land zu bewerten (Wenzelburger 2015: S. 668). Ein Nachteil bei der Analyse eines Gesetzes ist freilich, dass das Verhalten der Akteure im Justizsystem ausgeblendet wird (ebd.). Dieses Problem betrifft auch die Untersuchung von Quellen-TKÜ und ODS, schließlich müssen die Ermittlungsmaßnahmen auf Antrag der Staatsanwaltschaft von einem Ermittlungsrichter angeordnet werden (siehe dazu § 100e StPO). Allerdings fehlt es derzeit wohl an einer ausreichend großen Datengrundlage für eine derartige Betrachtung, da das Gesetz noch relativ neu ist. Folglich erscheint eine derartige Analyse zu diesem Zeitpunkt ohnehin wenig sinnvoll.

Als Materialquellen für die Forschungsarbeit werden unter anderem die ausführlichen Gesetzesbegründungen aus den Bundestagsdrucksachen mitsamt den Stellungnahmen zahlreicher Sachverständiger aus dem Ausschuss für Justiz und Verbraucherschutz verwendet. Um die für eine wissenschaftliche Arbeit benötigte Objektivität sicherzustellen, kommen zudem Artikel aus wissenschaftlichen Journals und Forschungsarbeiten rund um die Thematik Quellen-TKÜ, ODS und staatliches Hacking zur Strafverfolgung hinzu. Denn in der Regel ist davon auszugehen, dass die Bundestagsfraktionen nur Sachverständige zur öffentlichen Anhörung einladen, die auch in ihrem Sinne argumentieren.

3 Zentrale Begriffe und theoretische Konzepte

Wie in der Einleitung dargestellt, sind präzise Definitionen der Begriffe *Sicherheit*, *Innere Sicherheit, IT-Sicherheit* und *Sicherheitsrisiko* essenziell, um die Forschungsfrage zu beantworten. Deshalb widmet sich dieser Teil der Arbeit eben diesen zentralen Begriffen.

3.1 Der Sicherheitsbegriff

Sicherheit hat sich zu einem zentralen Begriff in der Politik und der Gesellschaft avanciert – trotzdem bleibt die Bedeutung oftmals unklar (Daase 2010: S. 1). Wer einen Blick in ein Wörterbuch wirft, bekommt eine erste Vorstellung über den Sinngehalt des Begriffes. So schlägt der Duden unter anderem die folgenden Bedeutungen vor: „Zustand des Sicherseins, Geschütztseins vor Gefahr oder Schaden; höchstmögliches Freisein von Gefährdungen" (Duden Online o.J.).

Leider erlaubt die deutsche Sprache hier keine genauere Differenzierung, wie es im Englischen der Fall ist. Dort wird für gewöhnlich zwischen *Safety* und *Security* unterschieden. Dabei meint Safety so etwas wie „Betriebssicherheit", also „Strukturen und Prozesse[…], die möglichst gefahrenfrei sein sollten" (Frevel 2018: S. 2). Es handelt sich z. B. um Safety, „wenn die rutschige Teppichkante am Boden festgeklebt oder das kippelige Regal an die Wand gedübelt wird" (ebd. S. 3). Folglich ist unter Safety der Schutz vor Verletzungen und Gefahren zu verstehen (OED Online 2018). Bei Security hingegen steht die „Angriffssicherheit" im Fokus (Frevel 2018: S. 2). Gemeint ist damit der Schutz vor (externen) Bedrohungen oder Gefahren wie zum Beispiel Terrorismus, Kriminalität oder Spionage (OED Online 2018). Selbstverständlich ist der Unterschied zwischen Safety und Security nicht unbedingt trennscharf – beispielsweise geht der Schutz vor Terrorismus oftmals mit dem Schutz vor Verletzungen einher. Dennoch lässt sich feststellen, dass für diese Arbeit in erster Linie Sicherheit im Sinne von Security relevant ist. Schließlich beschäftigt sich die Forschungsfrage mit neuen Ermittlungsinstrumenten für die deutschen Strafverfolgungsbehörden, die für die Bekämpfung von Kriminalität und Terrorismus eingesetzt werden sollen.

Allerdings ist die Definition von Sicherheit als Zustand des Geschütztseins vor Angriffen (also Security) noch zu sehr vereinfacht, um eine adäquate Antwort zu geben, was unter Sicherheit zu verstehen ist. Vor demselben Problem steht auch das „pure safety"-Konzept von *Waldron*, der eine sehr basale, vom Freiheitsbegriff losgelöste Definition von Security basierend auf der Angst vor Terrorangriffen entwickelt hat. Demnach könne unter Security

die *individuelle Safety*, also der Schutz vor Verletzung oder gar dem (gewaltsamen) Tod, im Besonderen durch eine bestimmte Art von Angreifern (Terroristen), verstanden werden (Waldron 2006: S. 461–462).

Das „pure safety"-Konzept vernachlässigt materielle Verluste (z. B. den Verlust von Eigentum oder ökonomischem Wert) sowie die Verbindung zwischen Sicherheit und dem Bestand der gesellschaftlichen Ordnung (ebd.: S. 462). Darum erscheint es sinnvoll, das „pure-safety"-Konzept durch den Sicherheitsbegriff im juristischen Sinne, also die „Unversehrtheit von Rechtsgütern" (Glaeßner 2003: S. 19) zu erweitern – unter anderem auch deshalb, weil sich diese Forschungsarbeit mit einer Reform des Strafprozess*rechts* beschäftigt. Die Nähe zu den Rechtswissenschaften lässt sich somit nur schwer ausblenden. Dabei ist unter Rechtsgütern folgendes zu verstehen:

> „Als Rechtsgüter bezeichnet man die Lebensgüter, Sozialwerte und rechtlich anerkannten Interessen des Einzelnen oder der Allgemeinheit, die wegen ihrer besonderen Bedeutung für die Gesellschaft Rechtsschutz genießen. Rechtsgüter des Einzelnen sind zB [sic!] das Leben, die körperliche Unversehrtheit, die persönliche Freiheit, die Ehre, das Eigentum, das Vermögen **(Individualrechtsgüter)**. Rechtsgüter der Allgemeinheit sind zB [sic!] der Bestand des Staates und seiner freiheitlich-demokratischen Grundordnung, die Wahrung von Staatsgeheimnissen, die Rechtspflege, die Unbestechlichkeit von Amtsträgern, die Sicherheit des Straßenverkehrs, die Zuverlässigkeit von Urkunden im Rechtsverkehr **(Universalrechtsgüter)**." (Wessels et. Al 2016: S. 3, Hervorhebungen im Original)

Mit dieser Ergänzung sind nicht nur die körperliche Unversehrtheit und das Leben, sondern auch materielle Verluste, z. B. durch Diebstahl, sowie der Bestand der gesellschaftlichen Ordnung und unseres „way of life" (Waldron 2006: S. 462) Teil der Sicherheitsdefinition für diese Arbeit.

Ein weiteres Problem von *Waldrons* Konzept: Der subjektive Aspekt von Sicherheit wird komplett ignoriert (ebd.). Dies ist insofern problematisch, als dass jeder Mensch selbst festlegt, wie er die objektive Sicherheitslage interpretiert – daraus ergibt sich dann das subjektive Sicherheitsgefühl (Horning 2009: S. 82). Zwischen der objektiven Sicherheitslage, die in Deutschland zum Beispiel durch die vom BKA herausgegebene Polizeiliche Kriminalstatistik (PKS) gemessen werden kann, und dem subjektiven Sicherheitsgefühl auf der individuellen Ebene lassen sich bemerkenswerte Diskrepanzen beobachten. Selbst ein signifikanter Rückgang der Kriminalitätsrate geht nicht zwangsläufig mit einer geringeren Furcht vor Kriminalität einher (Glaeßner 2003: S. 18). Zusätzlich erfasst das Sicherheitsgefühl nicht nur die Kriminalitätsfurcht (also die Angst, selbst Opfer von Kriminalität zu werden), sondern auch „mittelbare Beeinträchtigungen" wie zum Beispiel die „Besorgnis anlässlich massenhafter Kleinkriminalität" (Schewe 2006: S. 322).

Besonders interessant ist darüber hinaus, dass zwischen der objektiven Gefährdung des Einzelnen und seinem subjektiven Sicherheitsgefühl kein proportionaler Zusammenhang besteht. Personen, die statistisch nicht besonders gefährdet sind, Opfer von (Gewalt-)Kriminalität zu werden, fürchten sich besonders stark. Gleichzeitig fürchten sich Menschen, die statistisch besonders häufig Opfer von Kriminalität werden, am wenigsten (Schewe 2006: S. 323). In Anbetracht der Tatsache, dass zwischen der objektiven Sicherheitslage und dem subjektiven Sicherheitsgefühl kein Zusammenhang ausgemacht werden kann, ist hier auch vom „Kriminalitätsfurchtparadox" die Rede (ebd.). Auf die Ursachen und Erklärungen dieses Phänomens soll an dieser Stelle nicht weiter eingegangen werden, denn für die Definition des Begriffes Sicherheit genügt zunächst das Wissen über die Diskrepanz zwischen objektiver Sicherheitslage und subjektivem Sicherheitsgefühl. [1]

Wichtig ist allerdings, dass das subjektive Sicherheitsgefühl zunehmend als Begründung für staatliche Maßnahmen angeführt wird. Insbesondere nach den Terroranschlägen am 11. September 2001 wurden demnach viele Maßnahmen ergriffen, die kaum darauf abzielten, die objektive Sicherheitslage zu verbessern. Vielmehr sollte der Bevölkerung das Gefühl vermittelt werden, dass alles Mögliche für ihre Sicherheit unternommen werde, was wiederum das subjektive Sicherheitsgefühl der Bürger stärken sollte (ebd: S. 324–325). Folglich darf sich die Betrachtung von Quellen-TKÜ und ODS nicht ausschließlich auf den objektiven Aspekt von Sicherheit beschränken. Das subjektive Sicherheitsgefühl muss ebenfalls berücksichtigt werden – ob die Ermittlungsmaßnahmen das subjektive Sicherheitsgefühl der Bevölkerung verbessern können, ist durchaus ein relevanter Aspekt der Fragestellung.

Die erarbeiteten Erkenntnisse zum Begriff Sicherheit lassen sich abschließend noch in einer griffen Arbeitsdefinition zusammenfassen:

> *Sicherheit im Sinne von Security meint den Schutz des Lebens und der körperlichen Unversehrtheit im Besonderen, sowie den Schutz von weiteren Rechtsgütern des Einzelnen und der Allgemeinheit vor externen Bedrohungen oder Gefahren. Sicherheit besteht zum einen aus der objektiven Sicherheitslage und zum anderen aus dem subjektiven Sicherheitsgefühl, welches durch die individuelle Interpretation der objektiven Sicherheitslage entsteht.*

[1] Für die Erklärung des Kriminalitätsfurchtparadoxes sei hier trotzdem auf Schewe 2006, S. 323–324 verwiesen.

3.2 Innere Sicherheit

Im Folgenden soll, ergänzend zu den obigen Ausführungen, auf den Begriff der *Inneren Sicherheit* eingegangen werden. Dabei ist anzumerken, dass die soeben erarbeitete Definition von Sicherheit aufgrund der verwendeten Literaturquellen bereits einen starken Fokus auf die Innere Sicherheit legt.

Zunächst einmal lässt sich feststellen, dass Innere Sicherheit in keinem Gesetz geregelt und in erster Linie ein politischer Begriff ist (Frevel 2018: S. 3). Eine Annäherung gelingt am besten über die Abgrenzung zur Äußeren Sicherheit. Bei der Äußeren Sicherheit geht es um die Gefährdung des Staates und seiner Bürger durch andere Staaten oder nichtstaatliche Akteure wie z. B. die Terrormiliz Islamischer Staat (ebd.: S. 5). Um dem entgegenzuwirken, bildet der Staat unter anderem Systeme der kollektiven Sicherheit, kooperiert mit anderen Staaten und ergreift militärische Maßnahmen wie z. B. den Aufbau von Streitkräften (ebd.: S. 5–6). Ein Politikfeld also, welches vorrangig im Bereich der Internationalen Beziehungen untersucht wird.

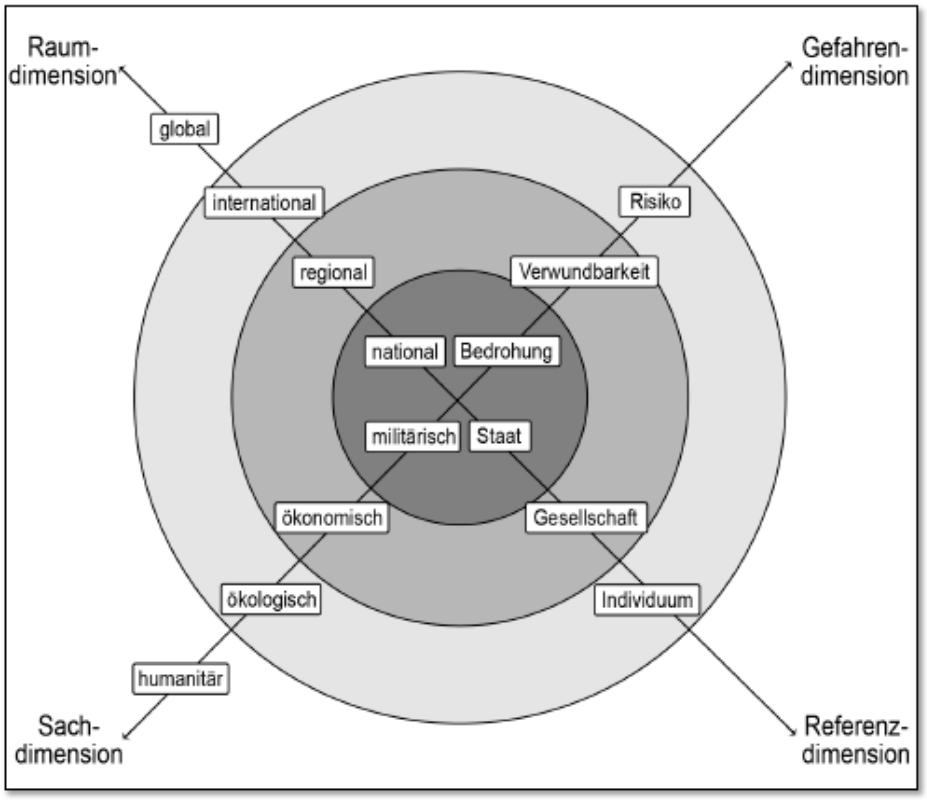
Die Eingrenzung des Begriffes Innere Sicherheit gestaltet sich leider nicht so einfach wie bei der Äußeren Sicherheit, denn die Gefährdungen sind wesentlich vielfältiger (ebd.: S. 9). Laut *Glaeßner* umfasst die Innere Sicherheit „die öffentliche Sicherheit und Ordnung und den Schutz der Individuen vor Gefahren, die ihnen durch Andere drohen“ (Glaeßner 2003: S. 145). Dies beinhaltet „den Schutz von Leib und Leben, der Gesundheit, der Freiheit und des Besitzes, gegen Kriminalität und andere unzulässige Eingriffe in das persönliche Leben“ (ebd.). *Frevel* ergänzt diese Ausführungen um den Schutz der freiheitlich-demokratischen Grundordnung der Bundesrepublik vor politischem Extremismus, den Schutz von Struktur und Ordnung des wirtschaftlichen Systems vor Wirtschaftskriminalität und den Schutz vor der Beeinflussung der Gesellschaft durch organisierte Kriminalität wie z. B. die Mafia (Frevel 2018: S. 7–8). Dabei fällt auf, dass die im vorherigen Gliederungsabschnitt erarbeitete Definition von Sicherheit bereits ziemlich nah an diese Anführungen heranreicht beziehungsweise größtenteils deckungsgleich ist. Insofern ist noch eine genauere Eingrenzung erforderlich, um dem vagen Begriff der Inneren Sicherheit habhaft zu werden.

Dies gelingt, wenn man wie *Frevel* auf die vier Dimensionen des erweiterten Sicherheitsbegriffes nach *Daase* zurückgreift (vgl. ebd.: S. 9–11).

Der erweiterte Sicherheitsbegriff zielt darauf ab, dass sich in der Zukunft vollkommen neue Gefahren entwickeln können. Darunter sind nicht nur neue Formen von Terrorismus, die

beispielsweise mit dem Einsatz von Massenvernichtungswaffen einhergehen können, zu verstehen. Auch Hackerangriffe, der Zerfall von Staaten und ganzen Regionen, sowie ökologische Katastrophen durch Wassermangel oder den Klimawandel fallen unter den erweiterten Sicherheitsbegriff (Lange 2006a: S. 287).

Abbildung 1: Die vier Dimensionen des erweiterten Sicherheitsbegriffs



Quelle: Daase 2010: S. 3

Um diese neuen Gefahren abzudecken, unterscheidet *Daase* zwischen vier verschiedenen Dimensionen des erweiterten Sicherheitsbegriffs. Wie an der obigen Abbildung unschwer zu erkennen ist, sind das die Sachdimension, die Referenzdimension, die Gefahrendimension und die Raumdimension. Die Sachdimension beschäftigt sich mit der Frage, in welchem Problembereich sich die Sicherheitsgefahren befinden. Die Referenzdimension fragt, wessen Sicherheit gewährleistet werden soll. Bei der Raumdimension geht es um das geografische Gebiet, für das Sicherheit angestrebt wird, und die Gefahrendimension beschäftigt sich mit der Konzeptualisierung des Sicherheitsproblems (Daase 2010: S.2).

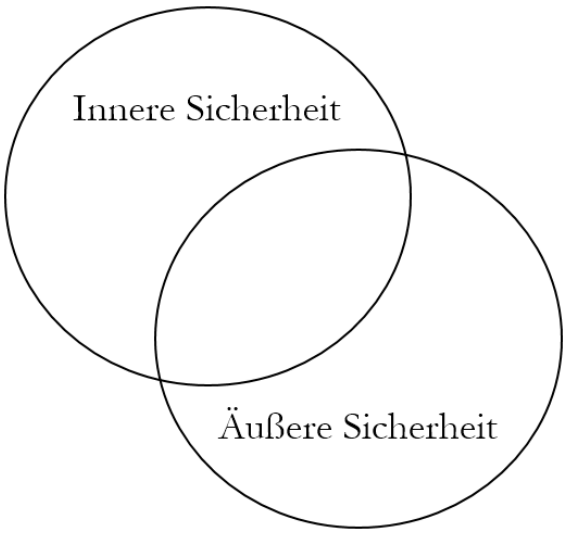
Frevel erweitert die Raumdimension noch um die lokale Ebene (Frevel 2018: S. 10) und definiert Innere Sicherheit mit Hilfe der von *Daase* entwickelten vier Dimensionen des erweiterten Sicherheitsbegriffs folgendermaßen:

> „**Innere Sicherheit** kann mit Bezug auf die sprachlichen Ursprünge und unter Nutzung der Dimensionen nach Daase beschrieben werden als (angestrebter) Zustand der Angriffssicherheit (security) von Individuen, Staat und Gesellschaft (Referenz) auf der lokalen bis nationalen Ebene (Raum) vor Bedrohungen (Gefahrendimension) mit kriminellem, extremistischen oder terroristischen Hintergrund (Sachdimension)." (Frevel 2018: S. 11, Hervorhebung im Original)

Da diese Definition von *Frevel* überaus stimmig erscheint und den Begriff der Inneren Sicherheit gut eingrenzt, soll sie im weiteren Verlauf dieser Arbeit Verwendung finden.

Es muss allerdings angemerkt werden, dass die Grenzen zwischen Äußerer und Innerer Sicherheit zunehmend miteinander verschwimmen und die beiden Politikfelder nicht mehr streng voneinander getrennt analysiert werden können. Grund dafür ist, dass sich transnationale Bedrohungen wie internationaler Terrorismus zunehmend auf die Innere Sicherheit auswirken (Wenzelburger 2015: S. 664–665).

Abbildung 2: Das Verhältnis der Inneren Sicherheit zur Äußeren Sicherheit



Quelle: In Anlehnung an Wenzelburger 2015: S. 666

Darüber hinaus sind Wirtschaftskriminalität, organisierte Kriminalität wie auch Cyberkriminalität Phänomene, die vor den Staatsgrenzen keinen Halt machen und sich somit nicht ausschließlich auf die Innere Sicherheit beziehen (Frevel 2018: S. 12). Auch wenn sich diese Forschungsarbeit mit der Inneren Sicherheit auseinandersetzt, sollte dieser Aspekt nicht gänzlich außer Acht gelassen werden.

3.3 IT-Sicherheit

Da im Laufe dieser Arbeit die *Sicherheit informationstechnischer Systeme (IT-Sicherheit)* eine tragende Rolle spielen wird, ist die Definition dieses Begriffes unabdingbar. Deswegen soll in diesem Abschnitt kurz dargestellt werden, was IT-Sicherheit bedeutet und wie sich die IT-Sicherheit zur Inneren Sicherheit verhält.

Als Ausgangspunkt für die Definition können die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebenen IT-Grundschutz-Kataloge dienen. Dort wird der Begriff wie folgt definiert:

> „IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind" (BSI 2016: S. 103).

Aus der Definition des BSI lassen sich drei sogenannte Schutzziele herauslesen: die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik. Die Vertraulichkeit meint, dass niemand unautorisiert an Informationen gelangt (Eckert 2008: S. 8). Informationsintegrität meint, dass Daten nicht ohne Autorisierung und unbemerkt manipuliert werden können (ebd.: S.7). Ein informationstechnisches System ist verfügbar, wenn alle autorisierten Benutzer stets Zugriff auf das System haben und hierbei nicht unberechtigt beeinträchtigt werden (ebd.: S. 10). Unter einem IT-System zu verstehen sind weiterhin „technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden" (BSI 2016: S. 104). Darunter fallen Computer und Mobiltelefone, aber auch Server, Clients, Router, Verteiler und Sicherheitsgateways (ebd.).

In Bezug auf die Definition des BSI erscheint es zudem erforderlich, den Ausdruck „Bedrohungen" der IT-Sicherheit noch weiter zu präzisieren. Vorliegend soll es in dieser Arbeit nämlich *nicht* um Bedrohungen gehen, die durch das Fehlverhalten des IT-Systems selbst entstehen und z. B. durch Programmierfehler hervorgerufen werden. Solche Bedrohungen „von innen" fallen unter den Aspekt der Betriebs- oder Funktionssicherheit, also unter die Safety (Eckert 2008: S. 6).

Stattdessen ist IT-Sicherheit auch hier im Sinne der Angriffssicherheit (Security) zu verstehen. Es geht also um „Konzepte und Maßnahmen zur Abwehr von Bedrohungen, die durch

unberechtigte Zugriffe auf die zu schützenden Güter des IT-Systems entstehen und im Wesentlichen von außen erfolgen“ (Eckert 2008: S. 6). Im Rahmen des Angriffes werden bestehende Schwachstellen des IT-Systems ausgenutzt (ebd.: S. 13–14). Als mögliche Angreifer-Typen kommen unter anderem Hacker, Internetkriminelle oder auch Unternehmen, die aus Gründen der Wirtschaftsspionage in fremde IT-Systeme eindringen, in Frage (ebd.: S. 19–20). Die Ausnutzung von Schwachstellen ist möglich, weil sich Software grundsätzlich nicht fehlerfrei herstellen lässt (Pohl 2009: S. 114). Etwaige Sicherheitslücken können zufällig entdeckt oder systematisch mit speziellen Tools gesucht werden (ebd.). Durchschnittlich kommen auf 1.000 Zeilen Software-Code 0,3 Fehler, was bei gängigen Betriebssystemen mit ca. 10 Millionen Zeilen Code rund 3.000 Fehler ergeben würde. Manche davon können für Angriffe auf IT-Systeme verwendet werden (Pohlmann/Riedel 2018: S. 38).

Deshalb soll im Folgenden diese Arbeitsdefinition zum Einsatz kommen:

> *IT-Sicherheit meint den Schutz von informationstechnischen Systemen vor Angriffen von außen, die bestehende Schwachstellen mit dem Ziel ausnutzen, unautorisiert auf Daten zuzugreifen, unbemerkt und ohne Berechtigung Daten zu verändern oder die Verfügbarkeit von IT-Systemen ohne Autorisierung zu beeinträchtigen.*

Nun bleibt noch zu klären, wie sich die IT-Sicherheit zum Konzept der Inneren Sicherheit verhält. Dafür werden zunächst einmal mögliche Gefährdungslagen zur Kenntnis genommen. Sogenannte kritische Infrastrukturen (KRITIS) wie Energie- und Wasserversorger, aber auch Telekommunikations- und Verkehrsunternehmen sowie Krankenhäuser sind immer stärker von funktionierenden IT-Systemen abhängig, was die Verwundbarkeit in Bezug auf Cyberangriffe drastisch erhöht (BSI 2017: S. 9). So führten 2015 und 2016 mehrere Cyber-Angriffe in der Ukraine zu mehrstündigen Stromausfällen, im November 2016 legte ein Angriff den Interzugang von rund 900.000 Telekom-Kunden in Deutschland lahm (ebd.: S. 11). Ebenfalls im Jahr 2016 drangen Hacker in das Netzwerk eines deutschen Industriekonzerns ein, konnten sich dort zwei Monate unbemerkt ausbreiten und teilweise technologische Daten stehlen (ebd.).

Darüber hinaus erfreuen sich insbesondere spezielle Erpressungs-Trojaner (sogenannte „Ransomware“) bei Cyberkriminellen gesteigerter Beliebtheit. In einer Umfrage des BSI gaben ein Drittel der befragten deutschen Unternehmen an, dass sie in den letzten sechs Monaten von Ransomware betroffen waren (Könen 2017: S. 50). Mit dieser Schadsoftware verschlüsseln die Täter Dateien auf dem System der Betroffenen und fordern ein Lösegeld, damit die Daten wieder entschlüsselt werden. Für besondere Aufmerksamkeit sorgte dabei der

Ransomware-Angriff auf das Lukaskrankenhaus in Neuss, infolge dessen das komplette IT-System der Klinik vollständig ausfiel (Ludwig 2016).

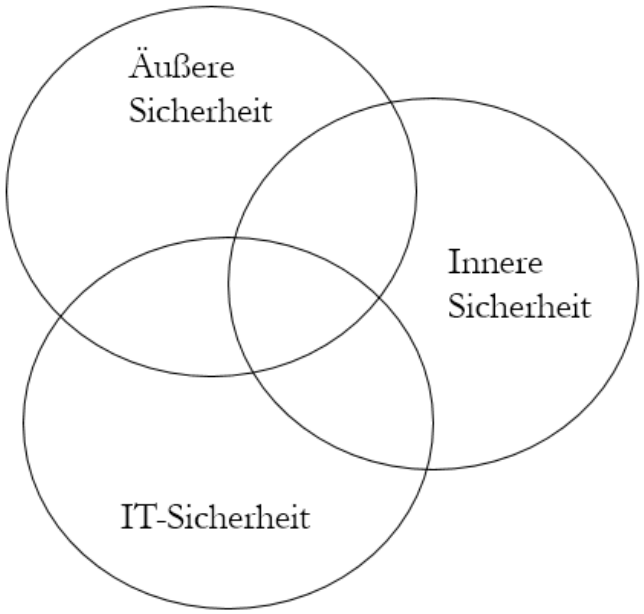
Auch die Gesellschaft selbst ist durch die tägliche Nutzung von Informationstechnik gefährdet. Smart-Home-Komponenten können von Kriminellen manipuliert werden, um sich Zutritt in Wohnhäuser zu verschaffen, bestimmte Authentifizierungsverfahren beim Online-Banking lassen sich durch Schadsoftware auf dem Endgerät missbrauchen (BSI 2017: S. 15–17). Wenn intelligente Stromzähler („Smart Meter") angegriffen werden, können sogar großflächige Stromausfälle („Blackouts") herbeigeführt werden (Wenzel 2018). Selbst staatliche Institutionen sind vor Hackerangriffen nicht mehr sicher, wie der Angriff auf das Datennetz der oberen Bundesverwaltung Ende 2017 zeigt (Brühl/Tenriverdi 2018).

Oftmals zielen solche Angriffe darauf ab, einen wirtschaftlichen Vorteil zu erlangen. Sollten Strom- und Wasserversorgung für einen längeren Zeitraum ausfallen, wären jedoch sogar Gefahren für Leib und Leben denkbar. Darüber hinaus können Cyberangriffe auch die gesellschaftliche Ordnung gefährden. Etwa dann, wenn das Eindringen in informationstechnische Systeme wie im Falle des Angriffes auf das Democratic National Committee (DNC) darauf abzielt, Wahlen zu beeinflussen (National Intelligence Council 2017: S. 1).

Mit diesem Wissen zur IT-Sicherheit und der im vorherigen Abschnitt dargelegten Definition der Inneren Sicherheit nach *Frevel* (vgl. Frevel 2018: S. 11) lassen sich beide Konzepte in Relation setzen. Eine lückenhafte IT-Sicherheit und daraus resultierende Angriffe (Gefahrendimension) können Individuen, Staat und Gesellschaft bedrohen (Referenzdimension), und zwar auf der lokalen bis nationalen Ebene (Raumdimension). Sofern der Angriff vor einem kriminellen, extremistischen oder terroristischen Hintergrund erfolgt (Sachdimension), lässt sich die IT-Sicherheit damit unter der Inneren Sicherheit subsumieren.

Wenn der Angriff allerdings von einem anderen Staat ausgeht, quasi in Form eines kriegerischen Akts, ist das Phänomen der IT-Sicherheit wohl eher der Äußeren Sicherheit zuzuordnen, auch wenn natürlich gleichzeitig die Innere Sicherheit betroffen sein kann. Folglich hängt die Einordnung von der etwaigen *Sachdimension* des Sicherheitsbegriffs ab. Die IT-Sicherheit ist somit Teil der Inneren Sicherheit und der Äußeren Sicherheit zugleich, was die folgende Abbildung noch einmal verdeutlichen soll:

Abbildung 3: Verhältnis der IT-Sicherheit zur Inneren und Äußeren Sicherheit



Quelle: eigene Darstellung, in Anlehnung an Wenzelburger 2015: S. 666

Auch wenn sich diese Arbeit – wie bereits weiter oben ausgeführt – auf die Innere Sicherheit beschränken soll, wird bei Betrachtung der IT-Sicherheit abermals deutlich, dass sich Innere Sicherheit und Äußere Sicherheit nicht trennscharf voneinander unterscheiden lassen.

3.4 Sicherheitsrisiken

Das letzte zentrale Konzept der Forschungsfrage ist das Sicherheitsrisiko. Leider ist auch der Risikobegriff ähnlich unbestimmt wie der Sicherheitsbegriff. Nicht ohne Grund schreibt *Luhmann*: „fragt man also nach einem Begriff des Risikos, stößt man in Nebel" (Luhmann 2005: S. 127).

Es lässt sich allerdings feststellen, dass Sicherheit der passende Gegenbegriff zum Risiko ist und das Risiko eine gewisse Nähe zum Begriff der Gefahr aufweist (ebd.: S. 128). Das leuchtet insbesondere im Hinblick auf die vier Dimensionen des erweiterten Sicherheitsbegriffs ein, schließlich wird das Risiko dort der Gefahrendimension zugeordnet. Das Risiko ist demnach eine mögliche Definition von Unsicherheit (Daase 2010: S. 15). Dabei beziehen sich Risiken nicht etwa auf territorial begrenzte Räume oder auf bestimmte kollektive Güter, sondern auf gesellschaftliche Funktionszusammenhänge. Mögliche Beispiele für Risiken sind laut *Daase* neben nuklearer Profileration auch organisierte Kriminalität, Drogenhandel sowie

Migration (Daase 2010: S. 17). Was im Genauen nun unter dem Begriff Sicherheitsrisiko zu verstehen ist, können diese Ausführungen jedoch nicht beantworten. Auch *Frevel*, der eine äußerst überzeugende Definition der Inneren Sicherheit entwickelte, gelingt keine geeignete Konzeptualisierung des Begriffes, mit der es sich arbeiten ließe. Laut *Frevel* bezieht sich der Begriff des Risikos auf „die Bewertung der Eintrittswahrscheinlichkeit und des Ausmaßes von möglichen Schädigungen" (Frevel 2018: S. 11). Hier wird ebenfalls nicht klar, was denn nun unter einem Risiko zu verstehen ist.

Eine bessere Erklärung des Risikobegriffs gelingt durch die Abgrenzung zum Gefahrenbegriff. Im Polizei- und Ordnungsrecht ist eine Gefahr dann gegeben, wenn ein Schaden für ein Schutzgut mit *hinreichender Wahrscheinlichkeit* eintreten wird (Kugelmann 2012: S. 95). In Bezug auf die unter 3.1 erarbeitete Definition von Sicherheit lässt sich der Begriff „Schutzgut" dabei durch „Rechtsgut" ersetzen.

Beim Risiko hingegen reicht die Eintrittswahrscheinlichkeit eines Schadens von der Schwelle unterhalb der hinreichenden Wahrscheinlichkeit bis hin zur bloßen Möglichkeit (Preuß 1996: S. 529). Definitionen außerhalb der Rechtswissenschaften zielen auf andere Unterscheidungen ab. So unterscheidet *Luhmann* zwischen der Selbstzurechnung von Schäden, dem Risiko, und der Fremdzurechnung, den Gefahren (Luhmann 2005: S. 140). Angesichts der Tatsache, dass es in dieser Arbeit um eine Reform der Strafprozessordnung geht, wird hier jedoch die rechtswissenschaftliche Definition angewendet.

Nur weil die Einschätzung eines Schadeneintritts beim Risiko unterhalb der hinreichenden Wahrscheinlichkeit liegt, bedeutet dies jedoch nicht, dass der Schaden objektiv weniger wahrscheinlich ist als im Falle einer Gefahr (Preuß 1996: S. 529). Das liegt in der subjektiven Bewertung eines möglichen Schadeneintritts begründet. Denn wie wahrscheinlich eine Gefahr, also der „Kausalzusammenhang zwischen einer gegenwärtigen Lage und einem zukünftigen Schadensereignis" (ebd.: S. 527) ist, entscheidet ein Mensch auf Basis seiner Erkenntnisfähigkeit (ebd.: S 527, 529).

Wenn es dem Menschen jedoch an einer verlässlichen Datengrundlage – oder, anders gesagt, an „hypothetische[m] Wissen" (Preuß 1996: S. 530) fehlt, so ist eine Einschätzung der Eintrittswahrscheinlichkeit auf Basis der Lebenserfahrung nicht mehr ohne Weiteres möglich (ebd.). Dies trifft insbesondere dann zu, wenn es um neue Schadensmöglichkeiten geht, die durch technologischen Fortschritt geschaffen werden und bis weit in die Zukunft reichen – also z. B. auf Umweltkatastrophen oder Epidemien. In diesen Fällen sind die Schadensmög-

lichkeiten und Schadensquellen bekannt, nicht aber der Verursachungszusammenhang. Damit lässt sich die Schadensmöglichkeit auch nicht mehr einem individuellen Verursacher zuordnen, was für das Recht der Gefahrenabwehr jedoch von zentraler Bedeutung ist (Preuß 1996: S. 530).

Deswegen kann bei neuartigen Gefährdungen auch von „schleichenden Katastrophen" gesprochen werden, weil sie „irgendwo", „irgendwie" und „irgendwann" (ebd.: S. 531) auftreten. Dabei bleiben Entwicklungsparameter, Ursachen und Urheber teilweise unbekannt (ebd.). Diese Ausführungen beschränken sich nicht nur auf die soeben genannten Beispiele biologischer Systeme (Krankheiten und Umweltschäden), sondern auch auf soziale Systeme. So kann der Zusammenbruch der Sowjetunion als Beleg dafür gewertet werden, dass gesellschaftliche Entwicklung ebenfalls unvorhersehbare Ereignisse erzeugen kann (ebd.: S. 534)

Auf Basis dieser Erkenntnisse lässt sich eine Risikodefinition entwickeln, mit der es sich im Fortgang dieser Arbeit arbeiten lässt:

> *Unter dem Begriff Sicherheitsrisiko sind in die Zukunft gerichtete Schäden für ein Rechtsgut zu verstehen, die durch gesellschaftlichen oder technologischen Fortschritt entstehen und deren Eintrittswahrscheinlichkeit sich aufgrund von unzulänglichem Wissen nicht feststellen lässt. Bei einem Sicherheitsrisiko kann der Bedrohung oftmals weder ein individueller Verursacher zugeordnet werden, noch sind Ursachen und Ausmaße der Bedrohung vollständig bekannt.*

Unter diese Definition fallen auch Angriffe auf IT-Systeme durch die Ausnutzung von etwaigen Schwachstellen. Dass durch Cyberattacken Schäden für ein Rechtsgut entstehen können, wurde bereits unter 3.3 dargelegt. Darüber hinaus treffen die weiteren Merkmale der Risikodefinition ebenfalls auf das Phänomen zu. So ist die Bedrohung durch den technologischen Fortschritt entstanden, denn die Digitalisierung schafft mit der fortschreitenden Vernetzung immer neue Gefährdungspotenziale (BSI 2017: S. 9–19).

Weiterhin ist es äußerst schwer, Cyberattacken einem Urheber zuzuordnen. Die Angreifer sind nicht nur in der Lage, ihre eigene Identität zu verschleiern, sie können ihre Angriffe auch von Rechnern aus verschiedensten Jurisdiktionen starten und gehen oftmals mit einer enorm hohen Geschwindigkeit vor. Dies alles macht die Identifizierung der Drahtzieher und ausführenden Personen einer Cyberattacke äußerst schwierig (Tsagourias 2012: S. 233). In Fachkreisen ist dabei vom Problem der Attribution die Rede (ebd.: S. 229).

Auch die Ursachen der Angriffe, also die Schwachstellen in den IT-Systemen, sind selten vollständig bekannt. Zwar existieren Datenbanken für öffentlich bekannte Schwachstellen,

doch diese können selbstredend wenig über nichtöffentliche oder gar noch unentdeckte Schwachstellen aussagen (BSI 2017: S. 21). Wenn der Öffentlichkeit unbekannte Schwachstellen ausgenutzt werden, liegt es in der Natur der Sache, dass die Ursache frühestens nach Beginn des Angriffs bekannt wird. Diese geradezu eklatante Wissenslücke verdeutlicht zudem, warum sich die Eintrittswahrscheinlichkeit von Angriffen auf informationstechnische Systeme nicht feststellen lässt. Wenn schon die Schwachstellen unbekannt sind, so stellt jede Prognose über die Eintrittswahrscheinlichkeit eines Schadens, der durch diese Schwachstellen entstehen könnte, praktisch ein Ding der Unmöglichkeit dar.

Davon einmal abgesehen bleiben auch die Ausmaße einer Cyberattacke oftmals im Unklaren. Zwar existiert für KRITIS-Betreiber eine Meldepflicht von IT-Sicherheitsvorfällen (BSI 2017: S. 10), allerdings gilt diese Meldepflicht nur für einen vergleichsweise geringen Anteil von Einrichtungen. So hat das Bundesinnenministerium (BMI) lediglich einen Bruchteil aller Krankenhäuser als KRITIS einstuft (Rest 2016). Darüber hinaus betreffen Cyberangriffe natürlich nicht ausschließlich umfangreiche IT-Systeme, sondern auch Privatrechner. Die PKS erfasst solche Straftaten im Bereich der Computerkriminalität allerdings nur teilweise, da Formen der digitalen Erpressung auch im Tatbestand der Erpressung erfasst werden, nicht aber unter Computerbetrug. Dazu kommt eine Dunkelziffer, die vom BKA als „sehr hoch" eingestuft wird (Krüger 2014: S. 4). Insofern erscheint es problematisch, die Ausmaße von Cyberangriffen überhaupt präzise zu erfassen. Folglich fallen Angriffe auf IT-Systeme durch die Ausnutzung von etwaigen Schwachstellen vollumfänglich unter die obige Risikodefinition.

In diesem Teil der Forschungsarbeit wurden nun die theoretischen Konzepte Sicherheit, Innere Sicherheit, IT-Sicherheit und Sicherheitsrisiko geklärt. Es wurde aufgezeigt, dass die IT-Sicherheit Teil der Inneren Sicherheit ist und Angriffe auf IT-Systeme unter die Definition des Sicherheitsrisikos fallen. Diese Theoriearbeit ist zwar umfangreich, aber auch notwendig, um die Begriffe auf die Ermittlungsmaßnahmen Quellen-TKÜ und ODS anzuwenden.

4 Technische Grundlagen zu Quellen-TKÜ und Online-Durchsuchung

Bevor die im Theorieteil erarbeiteten Begriffe auf die Ermittlungsmaßnahmen angewendet werden sollen, erscheint es angemessen, kurz auf die technischen Grundlagen von Quellen-TKÜ und Online-Durchsuchung einzugehen. Ohne ein gewisses Basiswissen dürfte es sonst schwerfallen, der Argumentation im Analysekapitel zu folgen.

Zunächst einmal geht es bei einer Quellen-Telekommunikationsüberwachung grundsätzlich darum, die Telekommunikation von Beschuldigten, z. B. in Form von Kurznachrichten oder Telefonaten, im Rahmen eines Strafverfahrens zu überwachen. Die Überwachung der Telekommunikation war selbstverständlich bereits vor der StPO-Reform durch das „Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens“ möglich und wurde in den §§ 100a, 100b StPO geregelt. Bei einer „klassischen TKÜ“ hören die Strafverfolgungsbehörden gewissermaßen passiv „im Netz“ mit (Freiling et. al 2017: S. 16). Das passive Mithören erfolgt über eine Ausleitung der Kommunikationsdaten durch die jeweiligen Telekommunikationsdienstleister (Bode 2012: S. 353). Die Telekommunikationsdienstleister leiten dabei die entsprechenden Daten an die Ermittlungsbehörden weiter. Somit können Polizei und Staatsanwaltschaft die Kommunikationsdaten verwalten, auswerten und speichern. E-Mails und Kurznachrichten können dadurch gelesen, Telefongespräche zeitversetzt angehört werden. Für gewöhnlich erfolgt diese Art der Telekommunikationsüberwachung jedoch nicht in Echtzeit (ebd.).

Im digitalisierten Zeitalter läuft Telekommunikation allerdings immer weniger über SMS und Telefon ab. So berichtet die Bundesnetzagentur (BNetzA) von einem starken Rückgang der SMS-Nutzung seit 2013 – Mobilfunknutzende ersetzen die Kurznachrichten zunehmend durch Messaging-Apps (BNetzA 2018: S. 60). Auch die Sprachkommunikation erfolgt mittlerweile überwiegend über das Internet und nicht mehr über klassische Telefonanschlüsse (ebd.: S. 54–55). Sprachtelefonie über das Internet firmiert in der Regel unter der Bezeichnung „Voice-over-IP“ (VoIP) oder IP-Telefonie.

Sowohl bei Messaging-Apps als auch bei VoIP-Anwendungen kommen zunehmend Verschlüsselungstechnologien zum Einsatz, was der IT-Sicherheit zu Gute kommt (Pohlmann/Riedel 2018: S. 37). Dabei handelt es sich in der Regel um eine sogenannte „Ende-zu-Ende“-Verschlüsselung, bei der die Kommunikationsdaten auf dem Ausgangsgerät verschlüsselt werden, *bevor* sie ins Internet gelangen. Auf dem Zielgerät angekommen lassen sich

die Daten dann wieder entschlüsseln. Die kryptografischen Schlüssel selbst verbleiben dabei auf den jeweiligen Geräten. Dadurch sind die Kommunikationsdaten auf dem gesamten Übertragungsnetz im Internet verschlüsselt (Freiling et. al 2017: S. 17). Zwar können die Internetanbieter (Internet Service Provider, kurz ISP) auch bei Kommunikation über das Internet verpflichtet werden, den Strafverfolgungsbehörden die entsprechenden Daten zur Verfügung zu stellen (Buermeyer 2007: S. 160). Durch die Verschlüsselung sind diese Kommunikationsdaten allerdings komplett unverständlich (Freiling et. al 2017: S. 17). Die Verschlüsselungsalgorithmen selbst gelten als sehr sicher – wenn Verschlüsselungsprogramme geknackt werden, liegt das meist an Fehlern in der Software-Implementierung, nicht aber an den Algorithmen selbst (Schulze 2017a: S. 24).

Darum setzt eine Quellen-TKÜ direkt an der „Quelle", also am Endgerät der Tatverdächtigen, an. Dort ist es möglich, auf die unverschlüsselten Kommunikationsinhalte zuzugreifen (Bunzel 2015: S. 64). Der Zugriff auf die Kommunikation erfolgt also vor der Verschlüsselung beziehungsweise nach der Entschlüsselung (BKA 2016: S. 1). Erlaubt ist ausschließlich der Zugriff auf sogenannte „laufende Telekommunikation", also z. B. Telefonate über VoIP-Anwendungen oder Messenger-Nachrichten (Singelnstein 2017). [2]

Wie genau die unverschlüsselten Kommunikationsdaten erhoben werden, ist im vorliegenden Fall nicht bekannt. Die Leistungsbeschreibung des BKA verweist lediglich darauf, dass die Daten „an geeigneten Kommunikationsschnittstellen des Zielsystems" (BKA 2016: S. 7–8) erfasst werden sollen. Denkbar wäre z. B. das Erstellen von Bildschirmabbildern („Screenshots") in regelmäßigen Zeitabständen oder der Einsatz eines sogenannten „Keyloggers", der sämtliche Tastatureingaben mitschneidet (Bode 2012: S. 360–361). Erstere Lösung kam bereits im Jahr 2009 beim Bayerischen Landeskriminalamt zum Einsatz (ebd.: S. 3–4), also noch bevor eine entsprechende Rechtsgrundlage für die Quellen-TKÜ in der StPO existierte.

Bei der Online-Durchsuchung besteht eine solche Beschränkung auf die laufende Telekommunikation nicht – prinzipiell dürfen aus dem entsprechenden Zielsystem *alle gespeicherten Daten* erhoben werden, sofern diese als Beweismittel für das jeweilige Strafverfahren in Betracht kommen (Singelnstein 2017).

[2] Die Beschränkung auf „laufende Telekommunikation" hat rechtliche Gründe, die mit dem Urteil des Bundesverfassungsgerichts (BVerfG) zur Online-Durchsuchung aus dem Jahr 2008 zusammenhängen (siehe BVerfGE 120, 274 – 350). Für diese Arbeit sind die rechtlichen Details dazu nicht relevant, es sei aber auf Singelnstein 2017 für die genauen Ursachen der Beschränkung verwiesen.

Sowohl bei der Quellen-TKÜ, als auch bei der ODS muss zur Installation der Spionagesoftware eine aktive Infiltration des Zielsystems erfolgen, „und zwar mit potenziellem Vollzugriff auf dessen Ressourcen“ (Freiling et al. 2017: S. 16). Davon ist insbesondere deshalb auszugehen, weil die Überwachungssoftware selbstverständlich nicht entdeckt werden soll (BKA 2016: S. 9). Diese Anforderungen erfordern sogenannte „Rootkit“-Techniken, die besonders tief in das Betriebssystem des Zielsystems eingreifen, sodass spezifische Programme und Dateien für Nutzerinnen und Nutzer gar nicht mehr sichtbar sind (Buermeyer 2007: S. 157–158).

Für die Installation der Spionagesoftware kommen dabei grundsätzlich mehrere Varianten in Betracht. Zum einen könnte das Programm manuell aufgespielt werden, z. B. im Rahmen einer Routinekontrolle am Flughafen (Bode 2012: S. 3) oder, indem in die Wohnräume der Zielperson eingedrungen wird (Kohlmann 2012: S. 44). Denkbar wäre auch die Installation durch infizierte E-Mail-Anhänge, Internetseiten oder Datenträger (ebd.: S. 44–45). Darüber hinaus ist es möglich, Schwachstellen im IT-System mit einem sogenannten „Exploit“ auszunutzen (ebd.: S. 30–31). Exploits sind dabei Programme, die derartige Schwachstellen automatisiert ausnutzen können (Pohlmann/Riedel 2018: S. 39).

Aus technischer Sicht unterscheidet sich das Vorgehen der Strafverfolgungsbehörden also praktisch nicht von den Methoden, die im Bereich der Internet- und Computer-Kriminalität zum Einsatz kommen. Darum firmieren Quellen-TKÜ und ODS auch unter den Bezeichnungen „Bundestrojaner“ (Pohlmann/Riedel 2018: S. 39–40) oder „Staatstrojaner“ (Meister 2017). Die Bundesregierung selbst lehnt diese Bezeichnung sowie den Begriff „Spionagesoftware“ allerdings mit der Begründung ab, dass Trojaner widerrechtlich eingesetzt werden, der Einsatz von Quellen-TKÜ und ODS jedoch auf einer entsprechenden Rechtsgrundlage basiert. Dies geht aus einer Kleinen Anfrage der Fraktion Bündnis90/Die Grünen aus dem Bundestag hervor (BT-Drucksache 19/1434: S. 5,7).

Jedenfalls lässt sich schon einmal feststellen, dass der Einsatz von der Spionagesoftware für die Quellen-TKÜ und ODS per se die IT-Sicherheit auf dem System der Betroffenen bedroht, da zumindest die Schutzziele der Datenintegrität und -Vertraulichkeit verletzt werden. Dies ist allerdings auch so beabsichtigt, selbst wenn die Änderungen am Zielsystem so gering wie möglich ausfallen sollen (BKA 2016: S. 8). Gleichzeitig stellt der Eingriff in das IT-System von Tatverdächtigen *keine Bedrohung* der Inneren Sicherheit dar, weil der Eingriff nicht aus kriminellem, extremistischen oder terroristischen Hintergrund erfolgt (Sachdimension). Vielmehr soll der Eingriff ja gerade dazu dienen, Kriminalität zu bekämpfen.

5 Auswirkungen auf die Innere Sicherheit

In diesem Kapitel soll nun untersucht werden, wie sich der Einsatz von Quellen-TKÜ und ODS auf die Innere Sicherheit allgemein auswirkt – im Positiven wie im Negativen. Dabei sind die Auswirkungen auf die IT-Sicherheit besonders relevant, schließlich ist die IT-Sicherheit, wie bereits in 3.3 dargestellt, auch Teil der Inneren Sicherheit. Von Interesse ist dabei nicht nur, *ob* diese beiden Ermittlungsmaßnahmen eine Auswirkung auf die Innere Sicherheit haben, sondern auch, *wie stark* die jeweiligen Auswirkungen sind. Die Messung erfolgt anhand der Einschätzung von Sachverständigen.

Selbstredend gestaltet es sich dabei jedoch schwierig, die tatsächlichen Auswirkungen festzustellen. Dies liegt unter anderem darin begründet, dass die Befugnisse erst seit kurzer Zeit bestehen. So erfolgt der Einsatz von Software zur Quellen-TKÜ und ODS auf Basis der neu geschaffenen Rechtsgrundlage bislang wohl nur in einem sehr begrenzten Umfang, wenn überhaupt. Die *Süddeutsche Zeitung* berichtete Ende Januar 2018, dass entsprechende Software zur Quellen-TKÜ bereits in laufenden Ermittlungsverfahren durch das BKA eingesetzt werde – in wie vielen Fällen der Einsatz erfolgte, bleibt jedoch unbekannt (Pinkert/Tanriverdi 2018). Nur wenige Tage später hieß es in der *WELT*, das BKA habe die Software noch nicht eingesetzt (Flade 2018). Welcher Medienbericht nun korrekt ist, lässt sich schwer sagen. Es ist allerdings auch möglich, dass sich beide Artikel auf zwei unterschiedliche Abhör-Programme beziehen (Biselli 2018).

Darüber hinaus existieren kaum öffentliche Daten über den Einsatz von Software zur Quellen-TKÜ und ODS, weil die Bundesregierung derartige Informationen als vertraulich oder sogar als geheim einstuft (BT-Drucksache 18/13566: S. 4–10). Von öffentlicher Seite ist darum weder bekannt, von welchem Hersteller die Software stammt, noch ob es verschiedene Software-Typen und Hersteller gibt, wie die Programme funktionieren und wie oft „Staatstrojaner" bereits zum Einsatz kamen (ebd.). Lediglich für den Zeitraum 2007–2011 existiert eine Auflistung der Bundesregierung, der zufolge das BKA und der Zollfahndungsdienst in 23 Fällen Software zur Quellen-TKÜ im Rahmen eines Strafverfahrens einsetzten (BT-Drucksache 17/7760: S. 11–13). [3]

[3] Mangels Rechtsgrundlage nutzten die Strafverfolgungsbehörden die Ermittlungsmaßnahmen in diesen Fällen wohl illegal. Damals erfolgte die Quellen-TKÜ auf Basis des §100a StPO in seiner alten Fassung, also vor der Reform durch das „Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens". Laut eines Gutachtens der Bundesanwaltschaft aus dem Jahr 2010 stellt diese alte Fassung jedoch keine Rechtsgrundlage für den Einsatz der Quellen-TKÜ dar (Generalbundesanwalt 2010).

Nichtsdestotrotz soll nun eine Abschätzung der zu erwartenden Auswirkungen von Quellen-TKÜ und ODS auf die Innere Sicherheit basierend auf relevanter Literatur, entsprechenden Gutachten von Sachverständigen der Bundestagsausschüsse und Medienberichten erfolgen.

5.1 Optimierung der Inneren Sicherheit durch Quellen-TKÜ und ODS

Bezugnehmend auf die in 3.1 und 3.2 dargestellten Begriffe von „Sicherheit" und „Innerer Sicherheit" können positive Auswirkungen auf die Innere Sicherheit als Verbesserungen des Schutzes

> „von Individuen, Staat und Gesellschaft (Referenz) auf der lokalen bis nationalen Ebene (Raum) vor Bedrohungen (Gefahrendimension) mit kriminellem, extremistischen oder terroristischen Hintergrund (Sachdimension)" (Frevel 2018: S. 11)

beschrieben werden.

Diese Art der „Sicherheitsoptimierung" (Lange 2006b: S. 126) wäre im vorliegenden Fall dem Bereich der Kriminalpolitik zuzuordnen, denn sie hat „das Ziel einer verbesserten Strafermittlung und -verfolgung zum Inhalt" (ebd.: S. 127). Dies deckt sich mit der Gesetzesbegründung:

> „Eine effektive […] Strafverfolgung muss sich diesen technischen Veränderungen [den Verschlüsslungstechnologien, Anmerkung d. Verf.] stellen und ihre Ermittlungsmaßnahmen dem technischen Fortschritt anpassen" (BT-Drucksache 18/12785: S. 48).

Grundsätzlich kann Strafverfolgung als repressive Maßnahme nicht unmittelbar Sicherheit gewährleisten, weil sie Bedrohungen nicht direkt abwehrt, sondern auf die Verfolgung bereits begangener Straftaten abzielt (Stoll 2003: S. 15–16). Strafe und Strafverfolgung können gemäß den Straftheorien allerdings vorbeugend wirken, z. B. indem die Gesellschaft vor Tätern geschützt wird (Frevel 2018: S. 164). Darum soll im Folgenden angenommen werden, dass mit einer effektiveren Strafverfolgung auch eine Verbesserung der objektiven Sicherheitslage einhergeht – z. B. indem durch aussagekräftigere Beweismittel die Verurteilung einer Täterin oder eines Täters erreicht werden kann und die Gesellschaft damit vor weiteren Straftaten dieses Individuums geschützt wäre (negative Spezialprävention, siehe Frevel 2018: S. 164).

Folglich muss in diesem Kapitel geprüft werden, inwiefern Quellen-TKÜ und ODS eine verbesserte Strafermittlung und -verfolgung ermöglichen können. Dafür ist – in Anlehnung an die Evaluation des Verfassungsschutzgesetzes NRW – zunächst einmal von Interesse, ob die Maßnahmen überhaupt geeignet sind, dieses Ziel zu erreichen (Wolf 2015: S. 50). Im Anschluss stellt sich die Frage nach der Notwendigkeit der Maßnahmen (ebd.). Sollten die Ermittlungen auch auf andere Weise mit gleicher Effizienz möglich sein, so würden die

neuen Ermittlungsmaßnahmen kein signifikantes „Plus“ an Sicherheit im Sinne einer Verbesserung der objektiven Sicherheitslage darstellen. In einem solchen Fall wären die positiven Auswirkungen von Quellen-TKÜ und ODS auf die Innere Sicherheit dann auch eher als vernachlässigbar einzustufen.

Zuletzt ist zu prüfen, inwiefern die Ermittlungsmaßnahmen geeignet und notwendig sind, um das subjektive Sicherheitsgefühl in der Bevölkerung zu verbessern, damit beide Aspekte von Sicherheit entsprechend berücksichtigt werden.

5.1.1 Geeignetheit – Nutzen von Staatstrojanern für die Strafverfolgung

Wie bereits unter 4 ausgeführt, sind die vom ISP im Rahmen einer klassischen TKÜ ausgeleiteten Daten für die Strafverfolgungsbehörden praktisch wertlos, da sie verschlüsselt sind. Derzeit nutzen weniger als 15 Prozent der Beschuldigten in einem Strafverfahren vollständig unverschlüsselte Kommunikation, zudem setzen laut BKA zwei Drittel der Täter bewusst verschlüsselte Kommunikation zur Tarnung ein (Greven 2017: S. 3). In den verbleibenden Fällen kann die Nutzung von Verschlüsselungstechnologie darauf zurückgeführt werden, dass Instant-Messenger und andere Anwendungen zur Kommunikation zunehmend von Haus aus mit etwaigen Verschlüsselungstechnologien ausgestattet sind (Greven 2017: S. 3). Dadurch kommt es laut BKA zu „teils erheblichen Überwachungslücken“ (Henzler 2017: S. 4), welche unvollständige Ermittlungsergebnisse oder eine mangelhafte Beweislage zur Folge haben. Zudem erschweren diese Überwachungslücken die Ermittlungen der Kommunikations- und Organisationsstrukturen von Tatverdächtigen (ebd.). Ein Staatsanwalt bei der Bundesanwaltschaft, der im Bereich der Spionage und der Proliferation ermittelt, führt an, dass TKÜ-Maßnahmen in den von ihm geführten Verfahren mittlerweile entweder geringe oder gar keine Erkenntnisse mehr zu Tage bringen (Greven 2017: S. 5). Unter Kriminellen habe es sich herumgesprochen, dass Messenger wie Whatsapp nicht überwacht werden könnten, sodass sensible Inhalte oftmals nicht über ein Telefongespräch, sondern per Instant-Messenger ausgetauscht würden (Greven 2017: S. 5–6).

Sofern sich Tatverdächtige mit ihrem mobilen Endgerät über einen offenen WLAN-Hotspot anonym ins Internet einwählen, anstatt über den ihnen zugeordneten Festnetz- oder Mobilfunkanschluss, läuft eine klassische TKÜ ebenfalls ins Leere (Henzler 2017: S. 1–2). In diesem Fall erfolgt die Kommunikation schließlich nicht über den ISP der Zielperson, sondern über einen den Ermittlungsbehörden unbekannten Anschluss (ebd.). Demzufolge werden

die Kommunikationsdaten bei der Schaltung einer TKÜ beim ISP der Zielperson auch nicht erfasst.

Darüber hinaus ist durch moderne Verschlüsselungstechnologien auch die Auswertung von beschlagnahmten Datenträgern nicht mehr gewährleistet (Krauß 2017: S. 3). Dies ist immer dann der Fall, wenn die Daten durch Kryptografieverfahren vor unbefugtem Zugriff geschützt sind (Henzler 2017: S. 2). Bei iPhones des US-Herstellers Apple ist dies seit 2014 werksmäßig der Fall, Android-Smartphones bieten bei neueren Geräten eine optionale Verschlüsselung an. Zudem existieren Verschlüsselungsprogramme auch für alle modernen Computerbetriebssysteme (Schulze 2017a: S. 23).

Die Problematik, dass Verschlüsselungstechnologien den Zugriff auf Beweismittel erschweren oder unmöglich machen, wird von den Strafverfolgern als „Going Dark" bezeichnet. James B. Comey, ehemaliger Direktor des US-amerikanischen Federal Bureau of Investigation (FBI), beschreibt dieses Phänomen folgendermaßen:

> "Unfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem. We call it 'Going Dark," and what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so." (Comey 2014)

Mit den Ermittlungsmaßnahmen der Quellen-TKÜ und der ODS wäre es zweifelsfrei möglich, gewissermaßen „Waffengleichheit" zwischen den Ermittlungsbehörden und den Kriminellen zu schaffen, indem der Zustand vor der technischen Weiterentwicklung quasi wiederhergestellt wird (Greven 2017: S. 3). Während die Quellen-TKÜ die Verschlüsselung von laufender Kommunikation auf dem Übertragungsweg umgehen kann (siehe auch Kapitel 4), vermag die ODS den Zugriff auf verschlüsselte Datenträger zu gewährleisten. Dies funktioniert, indem auf die unverschlüsselten Daten zugegriffen wird, während das IT-System gerade verwendet wird und mit dem Internet verbunden ist. Folglich sind die Maßnahmen also schon einmal geeignet, um die objektive Sicherheitslage und damit auch die Innere Sicherheit zu verbessern.

Weiterhin erscheinen Quellen-TKÜ und ODS auch als geeignet, das subjektive Sicherheitsgefühl von Teilen der Bevölkerung zu verbessern. So betonen die Strafverfolgungsbehörden, dass „mittelfristig damit zu rechnen [ist], dass die Telekommunikationsüberwachung im herkömmlichen Sinn nur noch unzureichende Ergebnisse bringen wird" (Huber 2017: S. 2). In der Politik ist die Rede davon, dass die Ermittler bei einer klassischen TKÜ „gerade noch

mitkriegen, wer gerade welche Pizza bestellt“ (Elisabeth Winkelmeier-Becker aus der Unionsfraktion, siehe Deutscher Bundestag 2017). Solche Aussagen wirken sich natürlich negativ auf das subjektive Sicherheitsgefühl aus. In gewisser Weise wird der Bevölkerung damit vermittelt, dass der Staat nicht mehr in der Lage ist, Kriminalität effektiv zu bekämpfen. Das subjektive Sicherheitsgefühl lässt sich allerdings stärken, indem die Regierung der Bevölkerung gegenüber kommuniziert, dass „alles für ihre Sicherheit unternommen [wird]“ (Schewe 2016: S. 325). Wenn der Staat mit Quellen-TKÜ und ODS die zuvor bemängelten Überwachungslücken schließt, so dürfte dies zumindest in der Theorie eine positive Auswirkung auf das subjektive Sicherheitsgefühl der Bevölkerung haben.

5.1.2 Notwendigkeit – alternative Mittel zum Einsatz von Staatstrojanern

Nur weil Quellen-TKÜ und ODS geeignet sind, die Innere Sicherheit positiv zu beeinflussen, sagt dies jedoch noch nichts über die Notwendigkeit der Maßnahmen für eine positive Beeinflussung der Inneren Sicherheit aus.

Ob die Strafverfolgungsbehörden Quellen-TKÜ und ODS auch dringend benötigen, um das „Going Dark“-Problem zu lösen, ist umstritten. *Singelnstein* führt an, „dass die Notwendigkeit des heimlichen Zugriffs auf informationstechnische Systeme keineswegs so drängend ist, wie die Polizei dies in der Debatte darstellt“ (Singelnstein 2017).

So kann auf die überwiegende Mehrheit der Daten im Rahmen einer offenen Durchsuchung gemäß der §§ 102 ff. StPO und einer Beschlagnahme nach §§ 94 ff. StPO zugegriffen werden (ebd.). Die Informationen, welche mittels Quellen-TKÜ oder ODS erhoben werden sollen, könnte man also auch direkt von den physischen Datenträgern auslesen – mit der Einschränkung, dass die Informationsgewinnung in diesem Fall nicht heimlich und auch nicht bereits früh im Ermittlungsverfahren erfolgt (Buermeyer 2017: S. 25). Prinzipiell würde der Zugriff auf die Kommunikationsdaten dann wie im Falle der Quellen-TKÜ und ODS vor der Verschlüsselung bzw. nach der Entschlüsselung geschehen.

Ein solches Vorgehen hätte allerdings drei entscheidende Nachteile. Zum einen lässt sich bei einer Beschlagnahme nur die bereits erfolgte, nicht die „laufende“ Kommunikation auslesen, zum anderen wären die Verdächtigen bei einer offenen Durchsuchung quasi „vorgewarnt“. Außerdem könnten die Kommunikationsdaten wohl kaum ohne Weiteres ausgelesen werden, wenn der Datenträger des Endgerätes selbst verschlüsselt ist. Insofern kann diese Argumentation nur teilweise überzeugen.

Es gibt allerdings noch andere Methoden, mit denen schon heute auf Kommunikation via Instant-Messenger zugegriffen werden kann, ohne vorher das IT-System der Zielperson infiltrieren zu müssen. So lassen sich zahlreiche Messenger-Apps auf mehreren Geräten gleichzeitig verwenden. Diesen Umstand macht sich das BKA bereits seit 2015 zu Nutze, um über den als besonders sicher geltenden Messenger „Telegram" versendete Kurznachrichten mitlesen zu können (Hoppenstedt 2018). Hierbei melden die Ermittler einfach ein neues Gerät auf dem Benutzerkonto der tatverdächtigen Zielperson an und fangen die Bestätigungs-SMS über den ISP ab. So lässt sich nicht nur die laufende Telekommunikation überwachen, vielmehr besteht sogar Zugriff auf bereits erfolgte Telekommunikation in Form von alten Chatverläufen. Laut Medienberichten setzte das BKA diese Methode erfolgreich in neun abgeschlossenen Strafverfahren ein, unter anderem gegen die Rechtsterroristen der „Oldschool Society". In den Jahren 2015 und 2016 kam die Methode insgesamt 43 Mal zum Einsatz (ebd.). Es ist also durchaus möglich, Instant-Messenger mit relativ simplen Methoden zu überwachen, wobei es in diesem Fall einige Einschränkungen gibt. So scheitert diese Abhörmethode, wenn die Verdächtigen eine sogenannte „Zwei-Faktor-Authentifizierung" aktiviert haben, bei der die Geräteanmeldung auf einem zweiten Gerät bestätigt werden muss. Außerdem kommt die Methode ebenfalls an ihre Grenzen, wenn die Chats Ende-zu-Ende-verschlüsselt sind (ebd.).

Es lässt sich also zunächst einmal schlussfolgern, dass Verschlüsselungstechnologien tatsächlich „impenetrable barriers" (IACP 2015: S. 2) für die Beschaffung von digitalen Beweismitteln darstellen.

Nichtsdestotrotz erscheint die Metapher „Going Dark" unpassend, um den aktuellen Zustand und die Zukunft der technischen Entwicklung in Bezug auf den Datenzugriff von Strafverfolgungsbehörden zu beschreiben (Zittrain et. al. 2016: S. 9). Zwar sorgen Verschlüsselung und Internetdienstleistungen von unbekannten Providern dafür, dass die Überwachung in einigen Fällen komplizierter wird. Gleichzeitig muss jedoch auch festgestellt werden, dass manche Bereiche wesentlich stärker „ausgeleuchtet" sind als in der Vergangenheit (ebd.).

So fallen auch bei verschlüsselter Kommunikation eine Vielzahl an sogenannten Metadaten wie z. B. Standortpositionen, Anrufprotokolle und Header-Informationen in E-Mails an. Diese Informationen stellen für die Ermittlungsbehörden enorme Datenmengen dar, die vor der Verbreitung von Smartphones und anderen Geräten schlichtweg nicht existierten (ebd.: S. 3).

Insbesondere nach den Enthüllungen Edward Snowdens aus dem Jahr 2013, welche in der globalen Überwachungs- und Spionageaffäre mündeten, ist die Bedeutung von Metadaten zur staatlichen Überwachung hinreichend bekannt. So äußerte sich Stewart Baker, der frühere General-Counsel der National Security Agency (NSA), folgendermaßen zu Metadaten: „Metadata absolutely tells you everything about somebody's life. If you have enough metadata you don't really need content" (zitiert nach Rusbringer 2013). Somit dürfte die Kombination von verschiedenen Metadaten in Zukunft eine größere Rolle bei Ermittlungen spielen (Schulze 2017a: S. 28).

Vor diesem Hintergrund erscheint die Notwendigkeit von Quellen-TKÜ und ODS für eine verbesserte Innere Sicherheit fraglich. Außerdem lassen sich drei Trends ausmachen, welche den staatlichen Zugriff auf Daten fördern: Daten als Geschäftsmodell, Cloud-Computing und das Internet der Dinge (Internet of Things, IoT) (Zittrain et al.: S.10).

Zunächst einmal würde eine konsequente Ende-zu-Ende-Verschlüsselung mit dem Geschäftsmodell von Unternehmen wie Google oder Facebook kollidieren. Diese finanzieren ihre kostenlosen Inhalte und Dienstleistungen nämlich in der Regel durch Werbung. Um den lukrativen Markt mit möglichst zielgerichteten Werbeanzeigen auch weiterhin bedienen zu können, benötigen die Unternehmen unbeschränkten Zugang zu Nutzerdaten (ebd.). Daher ist es unwahrscheinlich, dass alle Internetfirmen Verschlüsselungstechnologien für alle Applikationen und Dienstleistungen anbieten. Folglich können die Unternehmen den Strafverfolgungsbehörden auch weiterhin Zugang zu Kommunikationsdaten ihrer Benutzer zur Verfügung stellen (ebd.: S. 10–11).

Zweitens werden Produkte zunehmend als Service angeboten. Software und Daten müssen nicht mehr auf dem Endgerät des Benutzers installiert werden, stattdessen werden diese durch die „Cloud" zur Verfügung gestellt oder dort gespeichert. Somit lässt sich von überall auf die Daten oder den Service zugreifen. Eine Verschlüsselung der Daten wäre hier wenig praktikabel, da dies die Funktionalität der Dienste einschränken würde (ebd.). So benötigt die Volltext-Suche von Google für in der Cloud gespeicherte Dokumente verständlicherweise Zugriff auf den Klartext. Der Softwarehersteller Apple beispielsweise speichert die Sicherheitskopien seiner Nutzer zwar verschlüsselt in der „iCloud", besitzt aber trotzdem den Schlüssel. Verliert ein Apple-Kunde nun sein Endgerät oder sein Passwort, sind die Daten nicht verloren, da Apple sie entschlüsseln kann. Folglich kann Apple gesetzlich verpflichtet werden, den Strafverfolgungsbehörden diese Daten zur Verfügung zu stellen (Zittrain et. al 2016: S. 11). Dies trifft freilich auch auf andere Technologieunternehmen zu.

Drittens sind immer mehr alltägliche Objekte mit dem Internet verbunden. Dies beinhaltet nicht nur Fernseher und Uhren, sondern auch Glühbirnen, Toaster, Autos und Türschlösser (Zittrain et. al 2016: S. 13). Insbesondere die Audio- und Videosensoren der IoT-Geräte dürften den Strafverfolgungsbehörden dabei zahlreiche Wege eröffnen, auf Echtzeit-Kommunikation oder entsprechende Aufnahmen zuzugreifen (ebd.). Da diese IoT-Geräte meistens nur eine limitierte Rechenleistung und eine geringe Batteriekapazität besitzen, werden Spracheingaben zudem oftmals an ein Rechenzentrum des Anbieters gesendet und dort verarbeitet (ebd.).

Folglich ist zu konstatieren, dass einige der durch Verschlüsselungstechnologien entstandenen Überwachungslücken durch andere technische Entwicklungen oder Marktgegebenheiten wieder geschlossen werden und ein kommendes „Going-Dark"-Szenario unwahrscheinlich ist (Zittrain et. al 2016: S. 15). Insbesondere die Analyse von Metadaten dürfte in der Praxis vielversprechende Ermittlungsansätze liefern und ist in Deutschland heute schon möglich (Neumann et al. 2017: S. 13). Zudem verändern sich IT-Systeme ständig, sodass sich Kriminelle jederzeit der staatlichen Überwachung entziehen können, sofern sie nur entsprechend gut informiert sind (Singelnstein 2017). Beispielsweise lässt sich das nicht-persistente Betriebssystem „Tails" nutzen, um die Effektivität von Staatstrojanern zu mindern (Schulze 2017b: S. 4). Eine Verbesserung der objektiven Sicherheitslage durch eine effektivere Strafverfolgung, welche die entstandenen „Überwachungslücken" ausgleicht, lässt sich also wohl auch durch andere – bereits vorhandene – Methoden verwirklichen. Quellen-TKÜ und ODS sind dafür nicht dringend notwendig.

Die beiden Ermittlungsmaßnahmen sind demnach auch nicht dringend notwendig, um das subjektive Sicherheitsgefühl der Bevölkerung zu stärken. Dies könnte stattdessen durch Hinweise von Strafverfolgern und Politikern auf alternative Ermittlungsmethoden und die hier dargelegten Trends erfolgen. Anstatt zu bemängeln, dass durch Verschlüsselung ein „strafverfolgungsfreier Raum" (Henzler 2017: S. 4) entsteht, ließen sich auch die neuen Möglichkeiten, z. B. durch die Analyse von Metadaten hervorheben. So bekämen die Bürgerinnen und Bürger nicht den Eindruck, dass der Staat den Kriminellen, Terroristen und Extremisten (Sachdimension der Inneren Sicherheit) machtlos gegenübersteht, sondern durchaus über wirkungsvolle Ermittlungsmaßnahmen verfügt, welche die Überwachungslücken ausgleichen können.

Gleichzeitig soll hier jedoch auch anerkannt werden, dass die beiden Ermittlungsmaßnahmen im Verschlüsselungszeitalter in der Tat wesentliche Verbesserungen bei der Erlangung von

Beweismitteln darstellen können (Greven 2017: S. 3–4) und daher sicherlich nicht vollkommen entbehrlich sind. Da es an verlässlichen Daten fehlt, in wie vielen Fällen Ermittlungen wegen durch Verschlüsselungstechnologien bedingten Beweislücken eingestellt werden mussten, ohne dass alternative Ermittlungsmethoden erfolgversprechend gewesen wären (Schulze 2017b: S. 4), wird im Ergebnis dieses Kapitels vorläufig angenommen, dass Quellen-TKÜ und ODS zumindest eine geringe Effektivitätssteigerung der Strafverfolgung darstellen.

Unter der Prämisse, dass eine effektivere Strafverfolgung vorbeugend vor der Bedrohung von Individuen, Staat und Gesellschaft durch Kriminalität, Extremismus und Terrorismus auf lokaler bis nationaler Ebene schützt, lässt sich also durchaus von einer zumindest geringen „Optimierung" der Inneren Sicherheit durch Quellen-TKÜ und ODS sprechen.

5.2 Quellen-TKÜ und ODS als Risiko für die Innere Sicherheit

Im folgenden Kapitel soll nun betrachtet werden, inwiefern Quellen-TKÜ und ODS eine negative Auswirkung auf die Innere Sicherheit haben. Um diese negativen Auswirkungen zu konzeptualisieren, kann ebenfalls die Begriffsdefinition der Inneren Sicherheit nach Frevel herangezogen werden. Demnach wären unter negativen Auswirkungen auf die Innere Sicherheit die Verschlechterung des Schutzes

> „von Individuen, Staat und Gesellschaft (Referenz) auf der lokalen bis nationalen Ebene (Raum) vor Bedrohungen (Gefahrendimension) mit kriminellem, extremistischen oder terroristischen Hintergrund (Sachdimension)" (Frevel 2018: S. 11)

zu verstehen.

Es geht also nicht um Sicherheit, sondern vielmehr um das genaue Gegenteil davon, nämlich Unsicherheit. Hier soll unter Unsicherheit das Risiko von Angriffen auf IT-Systeme durch die Ausnutzung von Sicherheitslücken verstanden werden. Die Gefahrendimension ist in diesem Fall also gewissermaßen eine unzureichende, bzw. zu schwache IT-Sicherheit. Darum soll hier nun dargestellt werden, welche Risiken für die IT-Sicherheit beim Einsatz von Quellen-TKÜ und ODS entstehen oder verstärkt werden.

5.2.1 Verwendung von „Less-Than-Zero-Day"-Exploits wahrscheinlich

Wie zu Beginn des Kapitels dargelegt, liegen aus Geheimhaltungsgründen keine offiziellen Informationen zu der verwendeten Software oder den Infiltrationsmethoden vor. Laut Medienberichten existieren zwei verschiedene Programme für die Quellen-TKÜ und ODS.

Zum einen ist das die vom BKA entwickelte Remote Control Interception Software (RCIS), welche allerdings nur das Programm „Skype“ auf Windows-PCs überwachen kann und deshalb eher von geringem Nutzen ist (Flade 2018). Zum anderen hat das BMI im Februar 2018 ein zweites Programm für die Quellen-TKÜ freigegeben. Dabei handelt es sich offenbar um das kommerzielle Produkt „FinSpy“ der Firma „FinFisher“ aus München, welche sich auf Überwachungstechnologie spezialisiert hat (ebd.).

Welche der unter 4 aufgeführten Möglichkeiten zur Infiltration des Zielsystems zum Einsatz kommen sollen, ist leider nicht bekannt. Das Wissen über die Installationsmethode der Spionagesoftware ist allerdings wichtig, um die Risiken für die IT-Sicherheit abschätzen zu können. Sofern das Programm auf ein spezifisches System zugeschnitten und auch nur dort installiert wird, besteht grundsätzlich keine Bedrohung für die allgemeine IT-Sicherheit (Fox 2007: S. 833–834). Dies trifft dann zu, wenn die Behörden den Staatstrojaner getarnt per E-Mail versenden („kriminalistische List“) oder das Programm bei einer Grenzkontrolle auf das Endgerät der Zielperson aufspielen (Buermeyer 2017: S. 21). Erfolgt die Installation hingegen durch die Ausnutzung einer System-Schwachstelle, so hat diese Infiltrationsmethode durchaus negative Implikationen auf die Sicherheit von Millionen IT-Systemen (Fox 2007: S. 833–834).

Aufgrund von praktischen Erwägungen ist davon auszugehen, dass die präferierte Methode zur Infiltration des Zielsystems die Ausnutzung von Sicherheitslücken durch einen Exploit ist. Diese Variante führt nur in seltenen Fällen nicht zum Erfolg, zudem weisen die beiden anderen Methoden (manuelle Installation „vor Ort“ und die Installation über infizierte Websites/E-Mails/Dateien) ein erhebliches Entdeckungsrisiko auf und erfordern zumindest ein fahrlässiges Fehlverhalten des Systemnutzers (Pohl 2007: S. 686).

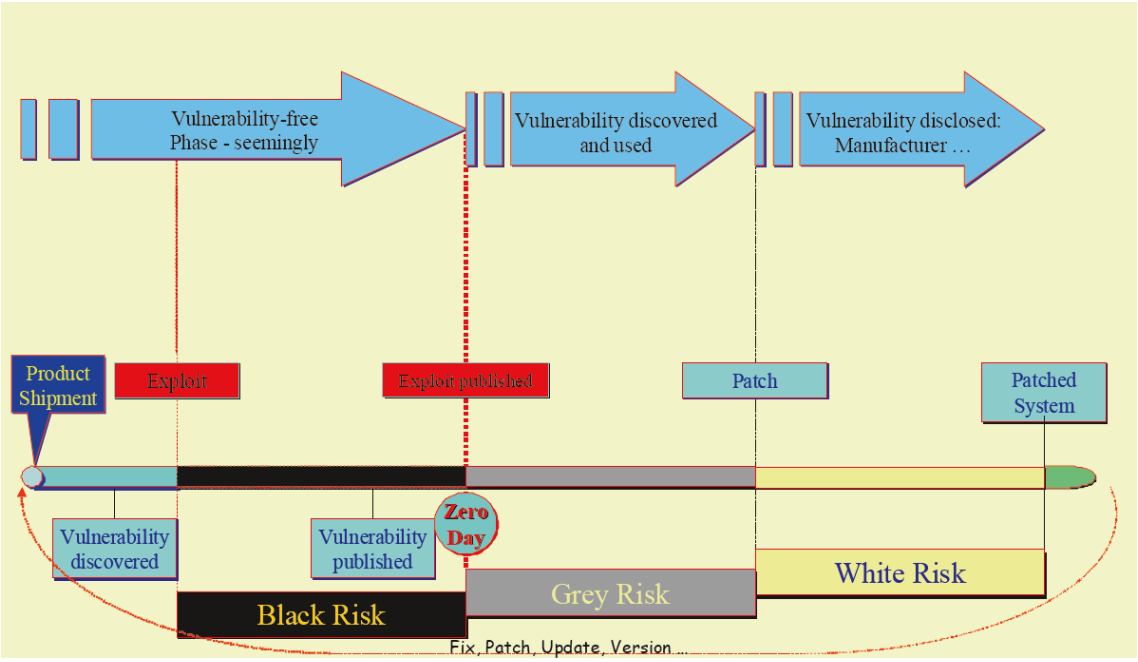
Abbildung 4: Methoden zur Infiltration in der Übersicht

Installationsmethode	Fehlverhalten erforderlich	Eindringen in Wohnraum erforderlich	Entdeckungsrisiko	Erfolgssausichten
manuell "vor Ort"	nein	ja	sehr hoch	mittel
infizierte E-Mail/Datei/Website	ja	nein	hoch	mittel
Ausnutzung von Sicherheitslücken	nein	nein	gering	hoch

Quelle: eigene Darstellung auf Basis von Pohl 2007: S. 686, Fox 2007: S. 829

Die Ausnutzung von bereits bekannten Sicherheitslücken, sogenannter „Zero-Day"-Vulnerabilitäten[4], kommt dabei jedoch nicht in Frage. Hier besteht für die Strafverfolgungsbehörden grundsätzlich ein zu hohes Risiko, dass die Sicherheitslücke während der Durchführung einer Quellen-TKÜ oder ODS durch ein Software-Update seitens des Herstellers, einen sogenannten „Patch", behoben wird (Pohl 2007: S. 685). In einem solchen Fall wäre der Ermittlungserfolg wohl akut gefährdet, denn die heimlichen Überwachungsmaßnahmen der Behörden könnten von der Zielperson möglicherweise entdeckt werden.

Abbildung 5: Lebenslauf von Sicherheitslücken



Quelle: Pohl 2009, S. 114

Aus diesem Grund dürften für die Quellen-TKÜ und ODS sogenannte „Less-Than-Zero-Day"-Exploits zum Einsatz kommen. Diese speziellen Angriffsprogramme nutzen Sicherheitslücken aus, die den Herstellern *unbekannt* sind (Pohl 2007: S. 685). Ein „Less-Than-Zero-Day"-Angriff ist für die betroffene Person weder erkennbar, noch existieren gegen diese Art von Exploits spezifische Schutzmaßnahmen – selbst Virenschutzprogramme sind wirkungslos, weil sie nur bereits bekannte Angriffe abwehren können (Pohl 2009: S. 115). Darum lassen sich mit „Less-Than-Zero-Day"-Exploits sogar hoch abgesicherte IT-Systeme erfolgreich angreifen (Pohl 2007: S. 687).

[4] Als „Zero Day" wird der Tag bezeichnet, an dem die Schwachstelle veröffentlicht wird (Pohl 2009: S. 115). Den Software-Herstellern bleiben dann genau null Tage (zero days) Zeit, um Gegenmaßnahmen zu ergreifen, mit denen die Ausnutzung der Schwachstelle durch ein Angriffsprogramm (Exploit) verhindert werden könnte.

Im „Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens“ existiert kein Verbot für die Verwendung solcher „Less-Than-Zero-Day“-Exploits (Buermeyer 2017: S. 22–23). Weiterhin verwendet der Bundesnachrichtendienst (BND) derartige Angriffsprogramme bereits seit Jahren für nachrichtendienstliche ODS (Pohl 2007: S. 687), sodass eine Verwendung durch die Strafverfolgungsbehörden zumindest naheliegt.

5.2.2 Wechselwirkungen beim Einsatz von „Less-Than-Zero-Day“-Exploits

Auf Basis dieser praktischen Erwägungen ist im Folgenden zu betrachten, welche Auswirkungen die Verwendung von „Less-Than-Zero-Day“-Exploits zur Infiltration von IT-Systemen mit dem Ziel, anschließend eine Software zur Quellen-TKÜ oder ODS zu installieren, auf die Innere Sicherheit hat.

Um den Bundestrojaner auf dem Endgerät einer tatverdächtigen Person zu installieren, kommen vermutlich sogenannte „Exploit Kits“ zum Einsatz. Dabei handelt es sich gewissermaßen um eine Art „Baukasten mit allen notwendigen Modulen für das automatische Ausnutzen von Schwachstellen“ (Pohlmann/Riedel 2018: S. 40). Für eine möglichst effektive Verteilung der Schadsoftware auf verschiedenen Endgeräten ist eine einzige Schwachstelle jedoch nicht ausreichend. Beliebte „Exploit Kits“ aus dem Bereich der Cyberkriminalität verwenden darum verschiedene Schwachstellen – im Jahr 2015 waren dies im Durchschnitt zwölf (ebd.: S. 41). Allerdings wurden bis 2015 überwiegend Desktop-Geräte mittels „Exploit Kits“ angegriffen. Um auch mobile Endgeräte abzudecken, dürfte also eine größere Anzahl an Schwachstellen benötigt werden. So ist die Anzahl an entdeckten Software-Schwachstellen auf eben diesen Endgeräten seit 2015 signifikant gestiegen, weil Cyberkriminelle ihre „Exploit Kits“ zunehmend für mobile Endgeräte optimieren (ebd.).

Der hohe Bedarf an Sicherheitslücken liegt auch in der hohen Fragmentierung hinsichtlich der verwendeten Software-Komponenten auf mobilen Endgeräten begründet (ebd.: S. 41). Werden die für den Desktop-Bereich benötigten Schwachstellen hochgerechnet, so kommt man auf 32 Schwachstellen pro Jahr alleine für den Bereich der mobilen Endgeräte. Zusammen mit den zwölf Schwachstellen aus dem Desktop-Bereich benötigten die Strafverfolgungsbehörden also insgesamt 44 Schwachstellen, um die Quellen-TKÜ und ODS auf allen erdenklichen Endgeräten zu ermöglichen (Pohlmann/Riedel 2018: S. 43).

Weiterhin muss davon ausgegangen werden, dass überwiegend kritische Schwachstellen zum Einsatz kommen, welche die Infiltration ohne jegliche Nutzerinteraktion ermöglichen (Neumann et. al 2017: S. 6–7). Diese Annahme wird bei der Betrachtung von populären

„Exploit Kits“ aus dem Zeitraum 2012–2015 bestätigt, denn hier wurden überwiegend Schwachstellen mit dem maximalen CVSS-Wert[5] von 10 verwendet (Pohlmann/Riedel 2018: S. 42).

Aus der Ausnutzung einer hohen Anzahl an kritischen „Less-than-Zero-Day“-Schwachstellen zur Quellen-TKÜ und ODS ergeben sich dabei hohe Risiken für die IT-Sicherheit der Allgemeinheit. Wer eine Schwachstelle entdeckt, der meldet diese in der Regel dem Hersteller der Software, sodass diese dann einen Patch entwickeln können (Pohl 2009: S. 114). Immer mehr Unternehmen bieten außerdem sogenannte „Bug Bounty“-Programme (BBP) an, welche das Finden von Vulnerabilitäten belohnen. Damit besteht ein finanzieller Anreiz für Hacker, Wissenschaftler oder andere Akteure, Schwachstellen zu finden und den Herstellern mitzuteilen (Pohlmann/Riedel 2018: S. 38). BPP bieten also gewissermaßen eine Art „Finderlohn“ für entdeckte Sicherheitslücken an.

Die Strafverfolgungsbehörden werden Schwachstellen, von denen sie Kenntnis erlangt haben, aber gerade nicht den jeweiligen Herstellern mitteilen. Vielmehr besteht ein Interesse, die gefundenen Sicherheitslücken „für sich“ zu behalten, um damit die Infiltration von IT-Systemen im Rahmen einer Quellen-TKÜ oder ODS zu gewährleisten (Buermeyer 2017: S. 21–22).

Die Notwendigkeit zur Geheimhaltung der Sicherheitslücken für eine fortwährende Ausnutzung durch einen Exploit sieht nicht nur *Buermeyer.* Vielmehr ergibt sich diese Notwendigkeit aus technischen Gegebenheiten. Sofern die Vulnerabilitäten den jeweiligen Herstellern mitgeteilt würden, ist nämlich, wie weiter oben unter 5.2.1 ausgeführt, mit einer zeitnahen Beseitigung zu rechnen (Neumann et. al 2017: S. 7). Sobald ein Patch veröffentlicht und auf dem Zielsystem installiert wurde, kann die Schwachstelle jedoch nicht mehr zum Abhören ausgenutzt werden (Bellovin et. al 2014: S. 49). Halten die Sicherheitsbehörden hingegen ihr Wissen zurück, lässt sich die Vulnerabilität immer wieder für eine Quellen-TKÜ oder ODS ausnutzen, bis die Schwachstelle irgendwann entdeckt wird (European Parliament 2017: S. 25).

Erlangen die Software-Hersteller selbst jedoch keine Kenntnis über kritische Schwachstellen in ihren Produkten, bleibt die Vulnerabilität gewissermaßen „offen“, und zwar auf allen IT-

[5] Das Common Vulnerability Scoring System (CVSS) ist ein Quasi-Industriestandard für die Bewertung des technischen Risikos von Software-Schwachstellen. Die Skala reicht von 0 (kein Risiko) bis 10 für kritische Schwachstellen (Neumann et. al 2017: S. 6–7).

Systemen, welche die betroffene Software verwenden. Selbst wenn die Strafverfolgungsbehörden verantwortungsbewusst mit ihrem Wissen über derartige Schwachstellen umgehen, ist nicht ausgeschlossen, dass andere Parteien die Schwachstelle ebenfalls entdecken und für ihre Zwecke ausnutzen (Neumann et al. 2017: S. 7). Eine solche simultane Verwendung von Schwachstellen (durch staatliche Akteure auf der einen und Kriminelle auf der anderen Seite) erscheint sogar recht wahrscheinlich, denn bei populären „Exploit Kits" aus dem Zeitraum 2012–2015 gibt es sehr viele Überschneidungen bei den eingesetzten Vulnerabilitäten (Pohlmann/Riedel 2018: S. 42).

Welche Folgen das Zurückhalten von Vulnerabilitäten haben kann, illustriert die massenhafte Infizierung von IT-Systemen mit dem Ransomware-Schadprogramm „WannaCry" im Mai 2017 (Neumann et al.: S. 7–8). So gelang es der Hackergruppe „The Shadow Brokers", den kritischen Exploit „EternalBlue" aus den Händen der NSA zu entwenden und zu veröffentlichen. Über fünf Jahre lang nutze die NSA mit dem Exploit eine Schwachstelle im Betriebssystem Windows aus, um in IT-Systeme einzudringen. Die Meldung von „EternalBlue" an den Hersteller Microsoft erfolgte allerdings erst, nachdem der Geheimdienst den Datendiebstahl bemerkte (Nakashima/Timberg 2017). Nicht nur Privatrechner wurden mit „WannaCry" infiziert, sondern auch IT-Systeme kritischer Infrastrukturen. So waren unter anderem der spanische Telekommunikationskonzern Telefónica, die Deutsche Bahn und sogar Krankenhäuser des britischen National Health Service (NHS) betroffen (Neumann et. al 2017: S. 7–8).

Darüber hinaus werden die staatlichen Behörden auch kaum in der Lage sein, die benötigte Anzahl an Schwachstellen selbst zu finden (Pohlmann/Riedel 2018: S. 41–42). Wenn die Überwachungssoftware wie im Falle von „FinSpy" über ein privates Unternehmen bezogen wird, stellt dies kein Problem dar. Allerdings entwickelt das BKA derzeit auch noch eine neue Version des Programmes RCIS, die auch auf Mobilgeräten funktionieren soll (Flade 2018). Dafür benötigt der Staat selbst Schwachstellen.

Um Techniken zu entwickeln, mit denen verschlüsselte Kommunikation mitgelesen werden kann, hat das BMI die „Zentrale Stelle für Informationstechnik im Sicherheitsbereich" (ZITiS) gegründet. Die Bundesbehörde ist auf dem Gelände der Universität der Bundeswehr in München angesiedelt und soll bis 2022 bis zu 400 Mitarbeiter beschäftigen (Pohlmann/Riedel 2018: S. 42). Unter der Voraussetzung, dass sich 300 der geplanten 400 Mitarbeiter mit der Suche nach Schwachstellen beschäftigen, wäre rein statistisch damit zu rechnen, dass ZITiS pro Jahr durchschnittlich 16 kritische Schwachstellen finden kann – 28 weniger also

als die benötigten 44 Schwachstellen (Pohlmann/Riedel 2018: S. 42–43). Dazu kommt, dass bei ZITiS im März 2018 gerade einmal 32 Personen arbeiteten (BT-Drucksache 19/1434: S. 12) – es scheint also Probleme zu geben, qualifiziertes Personal zu finden. Folglich wird es nötig sein, die fehlenden Schwachstellen einzukaufen, wie das bei Entwicklern von Schadsoftware bereits heute gängige Praxis ist (Pohlmann/Riedel 2018: S. 43). Der ehemalige Bundesinnenminister Thomas de Mazière schloss ein solches Vorgehen bei der Eröffnung von ZITiS auch nicht aus, obgleich der ZITiS-Direktor Wilfried Karl dem Kauf von Schwachstellen zuvor noch eine Absage erteilt hatte (Ermert 2017).

Wenn Sicherheitsbehörden kritische Schwachstellen bzw. die dazugehörigen Exploits auf dem „Grey Market“ [6] käuflich erwerben, befeuern sie diesen Markt zusätzlich (Neumann et. al 2017: S. 8–9), verhelfen indirekt dem Schwarzmarkt zu mehr Wachstum und schwächen gleichzeitig die „Bug Bounty“-Programme (Pohlmann/Riedel 2018: S. 43). Denn bei einer erhöhten Nachfrage von „Less-Than-Zero-Day“-Schwachstellen ist es für die „Entdecker“ der Vulnerabilitäten finanziell wesentlich attraktiver, ihr Wissen (ggf. mehrmals) auf dem „Grey Market“ oder sogar auf dem Schwarzmarkt zu verkaufen, anstatt die Sicherheitslücken im Rahmen eines „Bug Bounty“-Programmes an die jeweiligen Software-Hersteller zu melden (ebd.).

Zusätzlich erhöht sich auch die Wahrscheinlichkeit der bereits beschriebenen „simultanen Nutzung“ von Schwachstellen, weil ein Exploit auf dem „Grey Market“ oder dem Schwarzmarkt mehrmals an unterschiedliche Akteure verkauft werden kann (ebd.). Diese starken Wechselwirkungen lassen sich unmöglich von den Strafverfolgungsbehörden alleine kontrollieren (Pohlmann/Riedel 2018: S. 39).

Die Verwendung von kritischen Schwachstellen zur Quellen-TKÜ und ODS verringert also den Schutz von informationstechnischen Systemen vor externen Angriffen, die bestehende Schwachstellen mit dem Ziel ausnutzen, unautorisiert auf Daten zuzugreifen, unbemerkt und ohne Berechtigung Daten zu verändern oder die Verfügbarkeit von IT-Systemen ohne Autorisierung zu beeinträchtigen. Damit erhöhen Quellen-TKÜ und ODS das Risiko von Angriffen auf informationstechnische Systeme und weichen in gleichem Maße die IT-Sicherheit auf.

[6] Der „Grey Market“ ist eine Abstufung des Schwarzmarkts, auf dem Exploits für einen scheinbar „guten Zweck“ gehandelt werden, also z. B. für die Strafverfolgung durch Quellen-TKÜ und ODS (Pohlmann/Riedel 2018: S. 43).

Dabei ist auch die Innere Sicherheit betroffen, denn eine Schwächung der IT-Sicherheit bedeutet mehr Angriffsfläche für Cyberkriminalität und damit einen Anstieg des zu erwartenden Schadens durch Computerkriminalität (Pohlmann/Riedel 2018: S. 43). Dies verschlechtert den Schutz von Individuen, Staat und Gesellschaft vor Bedrohungen mit kriminellem, extremistischen oder terroristischen Hintergrund auf der lokalen bis hin zur nationalen Ebene – also die Innere Sicherheit.

Diese Ausführungen betreffen nun allesamt die objektive Sicherheitslage, es ist also noch auf das subjektive Sicherheitsgefühl einzugehen. Grundsätzlich erscheint es möglich, dass die Verwendung von kritischen „Less-Than-Zero-Day"-Schwachstellen zur Quellen-TKÜ und ODS bei den Bürgerinnen und Bürgern ein diffuses Gefühl der Unsicherheit bei der Nutzung von informationstechnischen Systemen hervorruft. Wie der Sicherheitsindex 2018 zeigt, nimmt die Verunsicherung im Internet im Vergleich zum Vorjahr leicht zu. Insbesondere Online-Banking-Anwendungen oder auch das Öffnen von E-Mail-Anhängen beunruhigen viele Nutzer (Herberg 2018). Das Wissen über die staatliche Verwendung von kritischen, den Herstellern nicht bekannten Schwachstellen zur Strafverfolgung und den damit verbundenen Risiken für die Innere Sicherheit könnten dieses Unsicherheitsgefühl noch weiter verstärken.

Der Einsatz von Quellen-TKÜ und ODS zur Strafverfolgung schafft also enorme, potenziell nicht kontrollierbare Risiken für die Innere Sicherheit, sofern „Less-Than-Zero-Day"-Exploits zum Einsatz kommen, um die IT-Systeme von tatverdächtigen Personen zu infiltrieren.

5.3 Das Sicherheitsparadox – ein neuer Zielkonflikt?

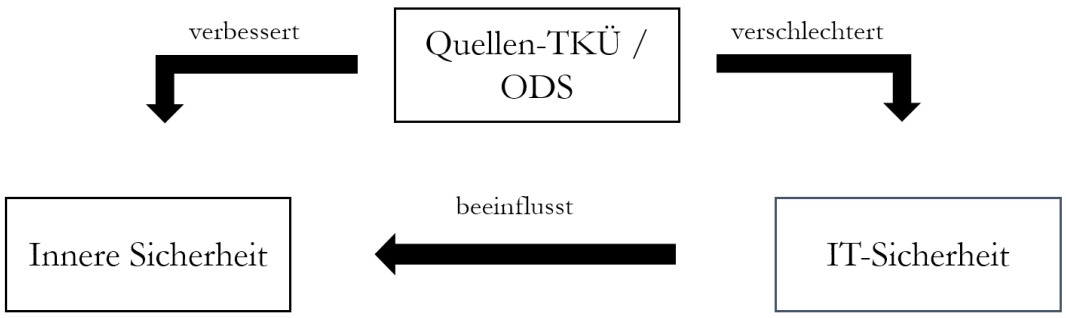
Aus den Betrachtungen dieses Kapitels ergibt sich eine geradezu paradoxe Situation: Ein vom Staat erlassenes Sicherheitsgesetz schafft eine Verbesserung und eine Verschlechterung der Innere Sicherheit zugleich. Es lässt sich hier also gewissermaßen von einem *Sicherheitsparadox* sprechen, weil die Einführung von Ermittlungsmaßnahmen, welche geeignet und zumindest in geringem Maße auch notwendig für eine Verbesserung der Inneren Sicherheit sind, durch verschiedenste Wechselwirkungen auch erhebliche Risiken für die Innere Sicherheit mit sich bringen.

Zunächst einmal schafft der Einsatz von „Less-Than-Zero-Day-Exploits" für die Infiltration von IT-Systemen zwar keine direkte Verschlechterung der Inneren Sicherheit. Allerdings

wirkt sich die beträchtliche Schwächung der IT-Sicherheit negativ auf die Innere Sicherheit aus, was mit Abbildung 6 grafisch verdeutlicht werden soll.

Vor diesem Hintergrund wird nun betrachtet, inwiefern sich das *Sicherheitsparadox* auch als Zielkonflikt beschreiben lässt.

Abbildung 6: Das Sicherheitsparadox als grafische Darstellung



Quelle: eigene Darstellung

Auf den ersten Blick stehen sich der Einsatz von Verschlüsselungstechnologien (IT-Sicherheit) und das Gebot einer effektiven Strafverfolgung (Innere Sicherheit), wie insbesondere aus 5.1 hervorgeht, tatsächlich gegenüber. Man könnte wie *Schulze* also durchaus zu dem Schluss kommen, dass die moderne Cyber-/IT-Sicherheit und die Innere Sicherheit zwei divergierenden Konzepte sind (Schulze 2017a: S. 28). Damit läge dann auch ein klassischer Zielkonflikt vor.

Diese Ansicht betrachtet die IT-Sicherheit und die Innere Sicherheit als zwei voneinander isolierte Konzepte, die nicht miteinander in Verbindung stehen. Dies ist jedoch, wie bereits in 3.3 aufgezeigt, nicht der Fall. Vielmehr wirkt sich eine mangelhafte IT-Sicherheit auch negativ auf die Innere Sicherheit aus, was insbesondere bei der Betrachtung der jeweiligen Fernziele deutlich wird. Schließlich dienen sowohl eine effektivere Strafverfolgung als auch der Einsatz von Verschlüsselungstechnologie zur Stärkung der IT-Sicherheit schlussendlich der Inneren Sicherheit. Es handelt sich hier also eher um konvergierende als um divergierende Konzepte.

Allerdings muss eingeschränkt werden, dass eine Stärkung der Inneren Sicherheit nicht auch gleichzeitig mit einer Stärkung der IT-Sicherheit einhergehen muss, wie in 5.2 aufgezeigt

wurde. Zudem könnten durch eine Stärkung der IT-Sicherheit durchaus die besagten „Überwachungslücken" entstehen. Sofern wirklich keine passenden Ermittlungsinstrumente als Ausgleichsmaßnahmen bereitstünden, was im vorliegenden Fall jedoch nicht zutreffend ist, läge hier sogar tatsächlich eine Schwächung der Inneren Sicherheit vor. Die Betrachtung von Innerer Sicherheit und IT-Sicherheit als zwei konvergierende Konzepte passt damit zwar noch am besten auf das vorliegende Phänomen, ist aber ebenfalls keine wirklich akkurate Beschreibung. Da es sich auch nicht um zwei antinomische oder indifferente Ziele handelt, erscheint die Bezeichnung *Sicherheitsparadox* für dieses Problem deshalb wesentlich treffender.

Angesichts der beträchtlichen Sicherheitsrisiken beim staatlichen Einsatz von Spionagesoftware zur Strafverfolgung wäre eigentlich mit einer breiten Debatte rund um das *Sicherheitsparadox* zu rechnen. Tatsächlich gab es bislang aber keine Diskussionen, die sich mit dieser Problematik auseinandergesetzt haben (European Parliament 2017: S. 67). Stattdessen entstehen die Diskussionen rund um staatliches Hacking, welche auf der internationalen und der EU-Ebene geführt werden, in erster Linie aus dem „Going Dark"-Phänomen (ebd.: S. 8) und setzen sich nicht mit der Frage auseinander, ob der Einsatz solcher Techniken überhaupt notwendig und verhältnismäßig ist (ebd.: S. 9). Wie sich im Verlauf dieser Arbeit gezeigt hat, treffen diese Erkenntnisse auch auf Deutschland zu.

Dabei gibt es auf internationaler Ebene durchaus vereinzelte Stimmen, die vor einer Schwächung von Verschlüsselungstechnologien warnen. So heißt es in einem Bericht der US-Geheimdienste, dass Verschlüsselung und Datenschutz die beste Verteidigung gegen Cyberangriffe sind (Schulze 2017a: S. 27). Jonathan Evans, der ehemalige Chef des britischen Inlandsgeheimdienstes MI5, hält einen „clampdown on use of encryption" (Grierson 2017) für äußerst gefährlich. Zwar erschwere der Einsatz von Verschlüsselungstechnologie den Zugriff auf die Kommunikation von Extremisten, gleichzeitig gebe es jedoch ein weiteres Problemfeld, und zwar Cybersicherheit im weiteren Sinne. Da die eigenen Fahrzeuge, der Lufttransport sowie kritische Infrastrukturen vom Internet abhängig sind, müsse sichergestellt sein, dass all dies vor Cyberangriffen geschützt ist (ebd.). Diese Ansicht teilt auch der ehemalige NSA-Direktor Michael Hayden. Die strategische IT-Sicherheit der US-Industrie müsse höher gewichtet werden als der Gewinn durch die Telekommunikationsüberwachung. Die USA seien mit mehr Verschlüsselung also insgesamt sicherer – auch wenn der Zugriff auf die Telekommunikation von Kriminellen dann nicht mehr so einfach möglich ist (Schulze 2017a: S. 27).

6 Ergebnisse und Ausblick

Wie diese Arbeit aufgezeigt hat, schafft der Staat mit den im „Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens“ eingeführten Ermittlungsmaßnahmen tatsächlich vermeidbare Risiken für die Innere Sicherheit. Der Einsatz von Quellen-TKÜ und ODS schafft erhebliche Risiken für die IT-Sicherheit, welche sich wiederum negativ auf die Innere Sicherheit auswirken. Gleichzeitig besteht für die neuen Befugnisse der Strafverfolgungsbehörden nur eine geringe Notwendigkeit, denn Überwachungslücken, welche durch die Nutzung von Verschlüsselungstechnologie entstehen, lassen sich auch mit anderen Ermittlungsmaßnahmen wie z. B. der Erhebung von Verkehrsdaten (§100i StPO) ausgleichen. Die positiven Auswirkungen von Quellen-TKÜ und ODS auf die Innere Sicherheit halten sich also in Grenzen, sodass die Sicherheitsrisiken als vermeidbar einzustufen sind.

Die Hypothese H1 hat sich damit nur in Teilen bestätigt. Tatsächlich sind für den Zugriff auf verschlüsselte Kommunikation und verschlüsselte Daten die Ermittlungsinstrumente Quellen-TKÜ und ODS nötig, da es an alternativen Methoden für den Zugriff mangelt. Um eine effektive Strafverfolgung ermöglichen zu können, benötigen die Ermittlungsbehörden allerdings nicht zwingend Zugriff auf verschlüsselte Kommunikation, da insbesondere die Analyse der unverschlüsselten Metadaten vielfältige Ermittlungsansätze liefern dürfte. Die Hypothese H2 hat sich vollumfänglich bestätigt, denn die Infiltration von IT-Systemen birgt in der Tat erhebliche Risiken für die IT-Sicherheit, sofern tatsächlich „Less-Than-Zero-Day“-Exploits für die Infiltration zum Einsatz kommen. Die Hypothese H3 trifft zwar zu, wird der Komplexität des Problems aber nicht gerecht. Deshalb erscheint es angebracht, nicht von einem Zielkonflikt zwischen effektiver Strafverfolgung und der IT-Sicherheit, sondern eher von einem *Sicherheitsparadox* zu sprechen.

Es lässt sich also resümieren, dass der Staat mit dem „Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens“ seiner „vornehmste Aufgabe“ (Glaeßner 2003: S. 10), nämlich der „Sicherung des inneren und äußeren Friedens, der Freiheit und der sozialen Wohlfahrt“ (ebd.), nicht mehr vollumfänglich nachkommt.

Diese Erkenntnisse ermöglichen eine gänzlich neue Perspektive auf die Debatte rund um den „Sicherheitsstaat“. Denn die Frage, wie weit der Staat bei der Gewährleistung von Sicherheit gehen darf und welche Maßnahmen staatliche Behörden ergreifen dürfen, wird kontrovers diskutiert (Glaeßner 2003: S. 174). Bei neuen Sicherheitsgesetzen wird dabei stets ein Zielkonflikt zwischen den beiden Polen „Sicherheit“ und „Freiheit“ angenommen (van

Ooyen 2012: S. 30), weil staatliche Maßnahmen in der Sicherheitspolitik oftmals die Grund- und Bürgerrechte einschränken (Glaeßner 2003: S. 275).

Im Hinblick auf das Sicherheitsparadox erscheint die ausschließliche Betrachtung dieses Zielkonflikts zwischen „Sicherheit" und „Freiheit" in der Debatte um den Sicherheitsstaat jedoch nicht mehr ausreichend, um die Problematik vollumfänglich zu erfassen. Im Zeitalter der globalen Vernetzung, die eine enorme Angriffsfläche für Cyberkriminalität bietet, wird die IT-Sicherheit zu einem immer wichtigeren Teil der Inneren Sicherheit. Daraus folgt, dass diesem Aspekt bei Diskussionen um neue Sicherheitsgesetze ein wesentlich höherer Stellenwert eingeräumt werden muss, als dies bislang der Fall ist.

Allerdings sollten die hier erarbeiteten Ergebnisse mit Vorsicht betrachtet werden – unter anderem, weil verlässliche Daten in vielerlei Hinsicht nicht verfügbar sind. So liegen tatsächliche Zahlen zum „Going-Dark"-Problem nicht vor. Es ist nicht bekannt, wie oft Verschlüsselungstechnologien tatsächlich Ermittlungen behindert haben, ohne dass es gangbare Alternativen zum Einsatz von Staatstrojanern gegeben hätte (Schulze 2017b: S. 4). Zusätzlich wird die Vorstellung, dass Sicherheitsbehörden gewissermaßen Sicherheit herstellen können, nicht den komplexen Bedrohungen und Risiken sowie den unterschiedlichen Ursachen von Kriminalität, Terrorismus und Extremismus gerecht (Frevel 2018: S. 166). Insofern ist die Annahme, dass eine effektivere Strafverfolgung auch mit einer verbesserten Inneren Sicherheit einhergeht, als stark vereinfacht einzustufen. Weiterhin ist die genaue technische Funktionsweise der verwendeten Software zur Quellen-TKÜ und ODS unbekannt, weil die Bundesregierung dies als Verschlusssache eingestuft hat (Tanriverdi 2018). Somit lässt sich das exakte Risiko für die IT-Sicherheit nur schwer einschätzen – es bleibt unklar, ob wirklich „Less-Than-Zero-Day"-Exploits zum Einsatz kommen. Nicht zuletzt haben die Ausführungen zur Verbesserung und Verschlechterung des subjektiven Sicherheitsgefühls der Bevölkerung eher hypothetischen Charakter. Es wäre eine breit angelegte Bevölkerungsumfrage zur staatlichen Nutzung von Spionagesoftware zur Strafverfolgung vonnöten, um diese Annahmen zu bestätigen.

Aus dem Einsatz von Quellen-TKÜ und ODS ergeben sich zusätzlich noch zahlreiche weitere Problemstellungen, die über den Horizont dieser Arbeit hinausgehen. Aus politikwissenschaftlicher Sicht stellt sich unter anderem die Frage, wie Staatstrojaner demokratisch kontrolliert werden können, wenn diese einer strikten Geheimhaltung unterliegen. Eine zusätzliche Hürde für eine effektive demokratische Kontrolle ist die technische Komplexität des Themas. Am Beispiel des britischen House of Lords zeigt sich, dass viele Mitglieder der

Legislative die Problemstellungen rund um das Thema Verschlüsselung gar nicht verstehen (European Parliament 2017: S. 20). Dazu kommt, dass selbst die Justiz unter Umständen nur unzureichendes Wissen über die „Hacking-Techniken" hat, deren Einsatz sie autorisiert (ebd.: S. 57).

Außerdem ist für die politikwissenschaftliche Teildisziplin der Internationalen Beziehungen von großen Interesse, welche Auswirkungen der Einsatz von Spionagesoftware zur Strafverfolgung auf die Äußere Sicherheit hat. Schließlich sind Innere und Äußere Sicherheit mittlerweile eng verflochten, wie in 3.2 und 3.3 aufgezeigt wurde.

Aus rechtswissenschaftlicher und technischer Sicht steht darüber hinaus die Frage nach der juristischen Verwertbarkeit der durch die Quellen-TKÜ und ODS erlangten Beweismittel im Raum, weil die Daten nicht wie in der IT-Forensik üblich im Ist-Zustand gesichert werden, sondern ein manipulativer Eingriff in das Beweismittel selbst erfolgt (Singlenstein 2018). Diese Herausforderung basiert auf dem sogenannten „Lying Endpoint Problem" (LEP). Das LEP besagt, dass sich der Zustand eines IT-Systems nicht auf dem IT-System selbst ermitteln lässt. Folglich kann eine revisionssichere Protokollierung durch den Staatstrojaner für die IT-Forensik möglicherweise gar nicht realisiert werden (Pohlmann/Riedel 2018: S. 43).

In Anbetracht dieser Problemstellungen erscheint der Vorschlag von *Schulze*, eine unabhängige wissenschaftliche Kommission zu Strafverfolgung im Verschlüsselungszeitalter einzurichten (Schulze 2017b: S. 4), als dringend geboten. Diese Kommission sollte sich jedoch nicht nur mit dem „Going-Dark"-Problem befassen und neue Ermittlungsstrategien entwickeln (ebd.), sondern auch die hier dargestellten Problemstellungen untersuchen. Dabei sollte der Fokus auf interdisziplinärem Arbeiten liegen, da beim Einsatz von Staatstrojanern viele wissenschaftliche Disziplinen (Politik- und Rechtswissenschaften sowie die Informatik) gleichermaßen betroffenen sind.

Um eine Schwächung der IT-Sicherheit zu verhindern ist es außerdem sinnvoll, den Empfehlungen von *Bellovin et. al* zu folgen und eine Meldepflicht für von Sicherheitsbehörden gefundene oder gekaufte Sicherheitslücken einzuführen. Damit könnte der Einsatz von Staatstrojanern die IT-Sicherheit schlussendlich sogar stärken (Bellovin et. al 2014: S. 63).

Das Thema Staatstrojaner wird in absehbarer Zeit nicht von der Bildfläche verschwinden, wie die Einführung von Quellen-TKÜ und ODS zur polizeilichen Gefahrenabwehr in Hessen zeigt (von Bebenburg 2018). Daher sind weitere Forschungen in diesem Problemfeld von hoher Relevanz, was an dieser Stelle nur mit Nachdruck unterstrichen werden kann.

Literaturverzeichnis

von Bebenburg, Pitt (2018): Die Polizei liest mit. In: *Frankfurter Rundschau*, Frankfurt am Main, 2018. Text abrufbar unter: http://www.fr.de/rhein-main/landespolitik/hessen-die-polizei-liest-mit-a-1530080 (Zugriff am 21.6.2018).

Bellovin, Steven M./Blaze, Matt/Clark, Sandy/Landau, Susan (2014): Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet. In: *Northwestern Journal of Technology and Intellectual Property*, 12 (1), 1–64.

Bewarder, Manuel/Jungholt, Thorsten (2013): Friedrich erklärt Sicherheit zum „Supergrundrecht". *WELT*, Text abrufbar unter: https://www.welt.de/politik/deutschland/article118110002/Friedrich-erklaert-Sicherheit-zum-Supergrundrecht.html (Zugriff am 29.4.2018).

Biselli, Anna (2018): Was die Regierung nicht über den Staatstrojaner verraten will – und was wir trotzdem wissen. *Motherboard*, Text abrufbar unter: https://motherboard.vice.com/de/article/d359y7/bka-staatstrojaner-was-regierung-nicht-verraten-will (Zugriff am 23.5.2018).

Bode, Thomas A. (2012): Verdeckte strafprozessuale Ermittlungsmaßnahmen. 1., 2013. Berlin [u.a.]: Springer Berlin.

Brühl, Jannis/Tanriverdi, Hakan (2018): Was Sie über den Hackerangriff auf das Regierungsnetz wissen müssen. In: *Süddeutsche Zeitung*, München, 2018. Text abrufbar unter: http://www.sueddeutsche.de/digital/hacker-regierungsnetz-fragen-1.3887668 (Zugriff am 9.5.2018).

Buermeyer, Ulf (2007): Die Online-Durchsuchung. Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme. In: *HRRS - Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht*, 8 (4), 154–166.

Buermeyer, Ulf (2017): Gutachterliche Stellungnahme zur Öffentlichen Anhörung zur „Formulierungshilfe" des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess. Berlin. Text abrufbar unter: https://www.bundestag.de/blob/508848/bdf7512e32578b699819a5aa33dde93c/buermeyer-data.pdf (Zugriff am 31.5.2018).

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2016): IT-Grundschutz-Kataloge. 15. Ergänzungslieferung. Text abrufbar unter: https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf (Zugriff am 8.5.2018).

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2017): Die Lage der IT-Sicherheit in Deutschland 2017. Text abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf;jsessionid=7FE38BCF99A3CFD6E3574A5C2DCF6307.2_cid351?__blob=publicationFile&v=4 (Zugriff am 9.5.2018).

Bundeskriminalamt (BKA) (2016): Standardisierende Leistungsbeschreibung Quellen-TKÜ. Text abrufbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Sonstiges/standardisierendeLeistungsbeschreibungQuellenTKUE.pdf?__blob=publicationFile&v=4 (Zugriff am 20.5.2018).

Bundesnetzagentur (BNetzA) (2018): Jahresbericht 2017 – Netze für die Zukunft. Bonn. Text abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Bundesnetzagentur/Publikationen/Berichte/2018/JB2017.pdf;jsessionid=954D10440CD00F6F815A1C280B974334?__blob=publicationFile&v=2 (Zugriff am 19.5.2018).

Bunzel, Maik (2015): Der strafprozessuale Zugriff auf IT-Systeme: eine Untersuchung aus technischer und verfassungsrechtlicher Perspektive. Berlin: Logos-Verl.

Comey, James B. (2014): Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? Washington, D.C.: Brookings Institution. Text abrufbar unter: https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course (Zugriff am 13.6.2018).

Daase, Christopher (2010): Der erweiterte Sicherheitsbegriff. Frankfurt am Main: Goethe-Universität. Text abrufbar unter: http://www.sicherheitskultur.org/fileadmin/files/WorkingPapers/01-Daase.pdf (Zugriff am 1.5.2018).

Deutscher Bundestag (2017): Bundestag gibt Strafermittlern neue Instrumente in die Hand. *bundestag.de*, Text abrufbar unter: https://www.bundestag.de/dokumente/textarchiv/2017/kw25-de-aenderung-stgb/511182 (Zugriff am 29.4.2018).

Eckert, Claudia (2008): IT-Sicherheit: Konzepte - Verfahren - Protokolle. 5., überarb. Aufl. München: Oldenbourg.

Ermert, Monika (2017): IT für Sicherheitsbehörden: Schwachstellen kann Zitis auch kaufen. *heise online*, Text abrufbar unter: https://www.heise.de/newsticker/meldung/IT-fuer-Sicherheitsbehoerden-Schwachstellen-kann-Zitis-auch-kaufen-3832667.html (Zugriff am 12.6.2018).

European Parliament (2017): Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices. European Union. Text abrufbar unter: http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf (Zugriff am 18.6.2018).

Fischer, Wulf/Zacharias, Christoph (Hrsg.) (2009): Forschungsspitzen und Spitzenforschung: Innovationen an der Fachhochschule Bonn-Rhein-Sieg: Festschrift für Wulf Fischer. Heidelberg: Physica-Verlag Heidelberg.

Flade, Florian (2018): Ministerium gibt neuen Bundestrojaner für den Einsatz frei. In: *WELT*, Berlin, 2018. Text abrufbar unter: https://www.welt.de/politik/deutschland/article173121473/Verdeckte-Ueberwachung-Ministerium-gibt-neuen-Bundestrojaner-fuer-den-Einsatz-frei.html (Zugriff am 23.5.2018).

Fox, Dirk (2007): Realisierung, Grenzen und Risiken der „Online-Durchsuchung". In: *Datenschutz und Datensicherheit DuD*, 31 (11), 82–834.

Freiling, Felix/Safferling, Christoph/Rückert, Christian (2017): Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung: Rechtliche und technische Herausforderungen. In: *Juristische Rundschau*, 2018 (1), 9–22.

Frevel, Bernhard (2018): Innere Sicherheit: Eine Einführung. 1. Auflage. Wiesbaden: Springer VS.

Generalbundesanwalt (2010): Rechtliche Zulässigkeit der sogenannten „Quellen-TKÜ". Karlsruhe: Generalbundesanwalt beim Bundesberichtshof. Text abrufbar unter: https://fragdenstaat.de/files/foi/7011/Gutachten_Quellen_TK.pdf (Zugriff am 23.5.2018).

Glaeßner, Gert-Joachim (2003): Sicherheit in Freiheit. Die Schutzfunktion des demokratischen Staates und die Freiheit der Bürger. Wiesbaden: VS Verlag für Sozialwissenschaften.

Greven, Michael (2017): Stellungnahme zum Gesetzesentwurf zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze. Karlsruhe. Text abrufbar unter: https://www.bundestag.de/blob/508850/76fc6296143a5eba18aff59fce987bb8/greven_drb-data.pdf (Zugriff am 26.5.2018).

Grierson, James (2017): Ex-MI5 chief warns against crackdown on encrypted messaging apps. In: *The Guardian*, 2017. Text abrufbar unter: https://www.theguardian.com/technology/2017/aug/11/ex-mi5-chief-warns-against-crackdown-encrypted-messaging-apps (Zugriff am 16.6.2018).

Grimm, Dieter (Hrsg.) (1996): Staatsaufgaben. 1. Aufl. Frankfurt am Main: Suhrkamp.

Gusy, Christoph (Hrsg.) (2015): Evaluation von Sicherheitsgesetzen. Wiesbaden: Springer VS.

Henzler, Peter (2017): Anhörung des Vizepräsidenten des Bundeskriminalamtes Peter Henzler im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages am 31. Mai 2017 zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze. Bundeskriminalamt. Text abrufbar unter: https://www.bundestag.de/blob/509190/ce315ac513c903afc986b8110078ddea/henzler-data.pdf (Zugriff am 18.3.2018).

Herberg, Ruth (2018): Skandale verunsichern Surfer. In: *Frankfurter Rundschau vom 13.06.2018*, Frankfurt am Main, 2018. Text abrufbar unter: http://www.fr.de/kultur/netz-tv-kritik-medien/netz/datenschutz-im-internet-skandale-verunsichern-surfer-a-1523629 (Zugriff am 13.6.2018).

Hoppenstedt, Max (2018): Das BKA spioniert seit Jahren Telegram-Nutzer aus. *Motherboard*, Text abrufbar unter: https://motherboard.vice.com/de/article/435gbd/telegram-ueberwachung-bka-chat-app-verschluesslung (Zugriff am 1.6.2018).

Horning, Jens Christian (2009): Sicherheit statt Freiheit? Text abrufbar unter: https://opus4.kobv.de/opus4-ku-eichstaett/files/41/dissjenshorniga.pdf (Zugriff am 2.5.2018).

International Association of Chiefs of Police (IACP) (2015): A Law Enforcement Perspective on the Challenges of Gathering Electronical Evidence. Alexandria, Virginia, USA: International Association of Chiefs of Police (IACP). Text abrufbar unter: http://www.theiacp.org/portals/0/documents/pdfs/IACPSummitReportGoingDark.pdf (Zugriff am 2.6.2018).

Kohlmann, Diana (2012): Online-Durchsuchungen und andere Maßnahmen mit Technikeinsatz: Bedeutung und Legitimation ihres Einsatzes im Ermittlungsverfahren. 1. Aufl. Baden-Baden: Nomos.

Könen, Andreas (2017): Gefahren für die innere Sicherheit aus dem Cyber-Raum – Wie kann Deutschland sich schützen? In: Sensburg, Patrick Ernst/Franosch, Rainer (Hrsg.), Sicherheit in einer digitalen Welt. 1. Aufl. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG, 45–60.

Krauß, Matthias (2017): Stellungnahme zum Gesetzentwurf zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze. Karlsruhe. Text abrufbar unter: https://www.bundestag.de/blob/509046/5aa0ea61c4f3df0429208b5fda260a0a/krauss-data.pdf (Zugriff am 17.3.2018).

Krüger, Kristin (2014): Zivile Cybersicherheit: Cybercrime zwischen Realität und Risiko. BIGS Essenz Nr. 14. Potsdam: Brandenburgisches Institut für Gesellschaft und Sicherheit. Text abrufbar unter: https://www.bigs-potsdam.org/images/Essenz/BIGS_Essenz_Nr.%2014%20zivile%20Cybersicherheit%20Bildschirmversion.pdf (Zugriff am 18.5.2018).

Kugelmann, Dieter (2012): Polizei- und Ordnungsrecht. 2., [überarb. und veränd.] Aufl. Berlin: Springer.

Lange, Hans-Jürgen (2006b): Innere Sicherheit. In: Lange, Hans-Jürgen/Gasch, Matthias (Hrsg.), Wörterbuch zur Inneren Sicherheit. 1. Aufl. Wiesbaden: VS, Verl. für Sozialwiss, 123–134.

Lange, Hans-Jürgen (2006a): Sicherheitsbegriff, erweiterter. In: Lange, Hans-Jürgen/Gasch, Matthias (Hrsg.), Wörterbuch zur Inneren Sicherheit. 1. Aufl. Wiesbaden: VS, Verl. für Sozialwiss, 287–292.

Lange, Hans-Jürgen/Gasch, Matthias (Hrsg.) (2006): Wörterbuch zur Inneren Sicherheit. 1. Aufl. Wiesbaden: VS, Verl. für Sozialwiss.

Ludwig, Kristiana (2016): Wenn Cyberkriminelle ein Krankenhaus lahmlegen. In: *Süddeutsche Zeitung vom 13.03.2016*, München, 2016. Text abrufbar unter: http://www.sueddeutsche.de/digital/angriff-auf-klinik-das-comeback-des-klemmbretts-1.2912255 (Zugriff am 30.5.2018).

Luhmann, Niklas (2005): Soziologische Aufklärung. [Bd.] 5: Konstruktivistische Perspektiven. Wiesbaden: VS Verl. für Sozialwiss.

Meister, Andre (2017): Staatstrojaner: Bundestag hat das krasseste Überwachungsgesetz der Legislaturperiode beschlossen (Updates). *Netzpolitik.org*, Text abrufbar unter: https://netzpolitik.org/2017/staatstrojaner-bundestag-beschliesst-diese-woche-das-krasseste-ueberwachungsgesetz-der-legislaturperiode/ (Zugriff am 15.3.2018).

Möllers, Martin H. W./Ooyen, Robert Christian van (Hrsg.) (2011): Neue Sicherheit. Frankfurt: Verlag für Polizeiwissenschaft.

Nakashima, Ellen/Timberg, Craig (2017): NSA officials worried about the day its potent hacking tool would get loose. Then it did. In: *Washington Post*, 2017. Text abrufbar unter: 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?utm_term=.ec235862412f (Zugriff am 11.6.2018).

National Intelligence Council (2017): Assessing Russian Activities and Intentions in Recent US Elections. Text abrufbar unter: https://www.dni.gov/files/documents/ICA_2017_01.pdf (Zugriff am 17.5.2018).

Neumann, Linus/Kurz, Constanze/Rieger, Frank (2017): Risiken für die innere Sicherheit beim Einsatz von Schadsoftware in der Strafverfolgung. Chaos Computer Club. Text abrufbar unter: https://www.bundestag.de/blob/509192/77ee7be3c9401ef4619fa0411758b045/neumann-data.pdf (Zugriff am 26.6.2018).

van Ooyen, Robert Christian (2012): Die neue Sicherheit des erweiterten Sicherheitsbegriffs. In: Möllers, Martin H. W./van Ooyen, Robert C. (Hrsg.), Theorie der Sicherheit, Bd. 1. 2. Auflage. Frankfurt am Main: Verlag für Polizeiwissenschaft, 29–33.

Pinkert, Reiko/Tanriverdi, Hakan (2018): Polizei spioniert Handynutzer mit Trojaner aus. In: *Süddeutsche Zeitung vom 27.01.2018*, München, 2018. Text abrufbar unter: http://www.sueddeutsche.de/digital/ueberwachung-polizei-spioniert-handynutzer-mit-trojaner-aus-1.3842439 (Zugriff am 23.5.2018).

Pohl, Hartmut (2007): Zur Technik der heimlichen Online-Durchsuchung. In: *Datenschutz und Datensicherheit DuD*, 31 (9), 684–688.

Pohl, Hartmut (2009): Zero-Day und Less-than-Zero-Day Vulnerabilities und Exploits. In: Fischer, Wulf/Zacharias, Christoph (Hrsg.), Forschungsspitzen und Spitzenforschung: Innovationen an der Fachhochschule Bonn-Rhein-Sieg: Festschrift für Wulf Fischer. Heidelberg: Physica-Verlag Heidelberg, 113–123.

Pohlmann, Norbert/Riedel, Rene (2018): Strafverfolgung darf die IT-Sicherheit im Internet nicht schwächen. In: *Datenschutz und Datensicherheit DuD*, 42 (1), 37–44.

Preuß, Torsten (2012): Terrorismus und Innere Sicherheit - Eine Untersuchung der politischen Reaktionen in Deutschland auf die Anschläge des 11. September 2001. Leipzig. Text abrufbar unter: http://www.qucosa.de/fileadmin/data/qucosa/documents/8861/20120602_Torsten_Preuß_Terrorismus_und_Innere_Sicherheit.pdf (Zugriff am 23.6.2018).

Preuß, Ulrich K. (1996): Risikovorsorge als Staatsaufgabe. In: Grimm, Dieter (Hrsg.), Staatsaufgaben. 1. Aufl. Frankfurt am Main: Suhrkamp, 523–551.

Rest, Jonas (2016): Kritik am IT-Sicherheitsgesetz. In: *Frankfurter Rundschau*, Frankfurt am Main, 2016. Text abrufbar unter: http://www.fr.de/wirtschaft/cyberkriminalitaet-kritik-am-it-sicherheitsgesetz-a-310966 (Zugriff am 18.5.2018).

Roggan, Frederik (2017): Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung: Elektronische Überwachungsmaßnahmen mit Risiken für Beschuldigte und die Allgemeinheit. In: *StV - Strafverteidiger*, 2017 (12), 821–829.

Rusbringer, Alan (2013): The Snowden Leaks and the Public. *The New York Review of Books*, Text abrufbar unter: http://www.nybooks.com/articles/2013/11/21/snowden-leaks-and-public/ (Zugriff am 5.6.2018).

safety, n. (2018): *OED Online*, Oxford University Press. Text abrufbar unter: www.oed.com/view/Entry/169687 (Zugriff am 1.5.2018).

Schewe, Christoph S. (2006): Subjektives Sicherheitsgefühl. In: Lange, Hans-Jürgen/Gasch, Matthias (Hrsg.), Wörterbuch zur Inneren Sicherheit. 1. Aufl. Wiesbaden: VS, Verl. für Sozialwiss, 322–325.

Schulze, Matthias (2017a): Going Dark? Dilemma zwischen sicherer, privater Kommunikation und den sicherheitsinteressen von Staaten. In: *Aus Politik und Zeitgeschichte (APuZ). Beilage zur Wochenzeitung Das Parlament*, 67 (46–47), 23–28.

Schulze, Matthias (2017b): Verschlüsselung in Gefahr. In: *SWP-Aktuell*, 2017 (A56).

security, n. (2018): *OED Online*, Oxford University Press. Text abrufbar unter: www.oed.com/view/Entry/174661 (Zugriff am 1.5.2018).

Sensburg, Patrick Ernst/Franosch, Rainer (Hrsg.) (2017): Sicherheit in einer digitalen Welt. 1. Auflage. Baden-Baden: Nomos.

Sicherheit (o. J.): *Duden Online*, Text abrufbar unter: https://www.duden.de/node/673347/revisions/1680756/view (Zugriff am 1.5.2018).

Singelnstein, Tobias (2017): Hacken zur Strafverfolgung? Gefahren und Grenzen der straf prozessualen Online-Durchsuchung. *verfassungsblog.de*, Text abrufbar unter: https://verfassungsblog.de/hacken-zur-strafverfolgung-gefahren-und-grenzen-der-strafprozessualen-online-durchsuchung/ (Zugriff am 18.3.2018).

Stoll, Peter-Tobias (2003): Sicherheit als Aufgabe von Staat und Gesellschaft: Verfassungsordnung, Umwelt- und Technikrecht im Umgang mit Unsicherheit und Risiko. Tübingen: Mohr-Siebeck.

Tanriverdi, Hakan (2018): BKA verpasst Staatstrojaner-Testern Maulkorb. In: *Süddeutsche Zeitung*, München, 2018. Text abrufbar unter: http://www.sueddeutsche.de/digital/it-sicherheit-bka-verpasst-staatstrojaner-testern-maulkorb-1.3942712 (Zugriff am 19.6.2018).

Tsagourias, Nicholas (2012): Cyber attacks, self-defence and the problem of attribution. In: *Journal of Conflict and Security Law*, 17 (2), 229–244.

Waldron, Jeremy (2006): Safety and Security. In: *Nebraska Law Review*, 85 (2), 454–506.

Weiß, André (2009): Online-Durchsuchungen im Strafverfahren. Hamburg: Kovač.

Wenzel, Frank-Thomas (2018): Digitales Misstrauen. In: *Frankfurter Rundschau vom 13.06.2018*, Frankfurt am Main, 2018. Text abrufbar unter: http://www.fr.de/kultur/netz-tv-kritik-medien/netz/cloud-computing-digitales-misstrauen-a-1523623 (Zugriff am 13.6.2018).

Wenzelburger, Georg (2015): Die Politik der Inneren Sicherheit. In: Wenzelburger, Georg/Zohlnhöfer, Reimut (Hrsg.), Handbuch Policy-Forschung. Wiesbaden: Springer VS, 663–698.

Wenzelburger, Georg/Zohlnhöfer, Reimut (Hrsg.) (2015): Handbuch Policy-Forschung. Wiesbaden: Springer VS.

Wessels, Johannes/Beulke, Werner/Satzger, Helmut (2016): Strafrecht, Allgemeiner Teil: die Straftat und ihr Aufbau: mit ebook: Lehrbuch, Entscheidungen, Gesetzestexte. 46., neu bearbeitete Auflage. Heidelberg: C.F. Müller.

Wolff, Heinrich Amadeus (2015): Gutachten zum Gesetz zur Änderung der gesetzlichen Befristung in § 29 des Gesetzes über den Verfassungsschutz in NRW, 2011. In: Gusy, Christoph (Hrsg.), Evaluation von Sicherheitsgesetzen. Wiesbaden: Springer VS, 39–58.

ZEIT Online (2016): BKA-Gesetz ist teilweise verfassungswidrig. *ZEIT Online*, Text abrufbar unter: http://www.zeit.de/digital/2016-04/bka-gesetz-zu-terrorbekaempfung-ist-teilweise-verfassungswidrig (Zugriff am 29.4.2018).

Zittrain, Jonathan L./Olsen, Matthew G./O'Brien, David/Schneier, Bruce (2016): Don't Panic: Making Progress on the „Going Dark" Debate. Cambridge: Berkman Klein Center for Internet & Society. Text abrufbar unter: https://dash.harvard.edu/handle/1/28552576 (Zugriff am 2.6.2018).

Erklärung zur Prüfungsleistung

Name,Vorname: Kuhn, Frank
Studiengang: BA Politikwissenschaften

Die am FB03 gültige Definition von Plagiaten ist mir vertraut und verständlich:

„Eine am FB03 eingereichte Arbeit wird als Plagiat identifiziert, wenn in ihr nachweislich fremdes geistiges Eigentum ohne Kennzeichnung verwendet wird und dadurch dessen Urheberschaft suggeriert oder behauptet wird. Das geistige Eigentum kann ganze Texte, Textteile, Formulierungen, Ideen, Argumente, Abbildungen, Tabellen oder Daten umfassen und muss als geistiges Eigentum der Urheberin/des Urhebers gekennzeichnet sein. Sofern eingereichte Arbeiten die Kennzeichnung vorsätzlich unterlassen, provozieren sie einen Irrtum bei denjenigen, welche die Arbeit bewerten und erfüllen somit den Tatbestand der Täuschung."

Ich versichere hiermit, dass ich die eingereichte Arbeit mit dem Titel

Gefährdet der staatliche Einsatz von Spionagesoftware die Innere Sicherheit? Eine Untersuchung anhand des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens

nach den Regeln guter wissenschaftlicher Praxis angefertigt habe. Alle Stellen, die wörtlich oder sinngemäß aus Veröffentlichungen oder aus anderen fremden Mitteilungen entnommen wurden, sind als solche kenntlich gemacht. Die vorliegende Arbeit ist von mir selbständig und ohne Benutzung anderer als der angegebenen Quellen und Hilfsmittel verfasst worden. Ebenfalls versichere ich, dass diese Arbeit noch in keinem anderen Modul oder Studiengang als Prüfungsleistung vorgelegt wurde.

Mir ist bekannt, dass Plagiate auf Grundlage der Studien- und Prüfungsordnung im Prüfungsamt dokumentiert und vom Prüfungsausschuss sanktioniert werden. Diese Sanktionen können neben dem Nichtbestehen der Prüfungsleistung weitreichende Folgen bis hin zum Ausschluss von der Erbringung weiterer Prüfungsleistungen für mich haben.

Frankfurt am Main, den 02.07.2018

Frank Kuhn