Chaos Computer Club Wien (C3W)
vorstand@c3w.at
ZVR-Zahl 656204875

in Zusammenarbeit mit
Chaos Computer Club e. V.

Stellungnahmen des Chaos Computer Club Wien (C3W) im Begutachtungsverfahren zum Entwurf eines Bundesgesetzes, mit dem die Strafprozessordnung 1975 und das Staatsanwaltschaftsgesetz geändert werden (192/ME)

(1) Vorbemerkung

Aus der Reaktion von Politik und Öffentlichkeit auf den Terrorismus ist der Zustand der Gesellschaft abzulesen – auch der Erfolg, den solche verbrecherischen Gewaltakte haben. Terrorismus ist eine Form der psychologischen Kriegsführung. Terrorakte zielen über das Leid der direkt Betroffenen hinaus, sie wollen die gesamte Gesellschaft treffen.

Der Sozialpsychiater Johannes Wancata warnt vor falschen Reaktionen auf die Terrorgefahr: "Wenn wir uns auseinanderdividieren lassen, hat der Terrorismus das erreicht, was er wollte. Wenn wir Reisefreiheit, Pressefreiheit und die Grundrechte eingeschränkt haben, haben die Terroristen Erfolg gehabt." Und die Linzer Gerichtsmedizinerin Adelheid Kastner spricht von einer "Radikalisierung der Mehrheitsbevölkerung" als Konsequenz überzogener Terror- und Migrationsängste [1]

[1] **derstandard**.at/2000035979573/Terrorismus-ist-keine-psychische-Erkrankung

Inhaltsverzeichnis

(2) Einleitung

In den Stellungnahmen zum Entwurf (192/ME) wurden zahlreiche verfassungsrechtliche Bedenken aufgeworfen.
Diese Stellungnahme widmet sich den Fragen des Einsatzes von Staatstrojanern und deren potentiellen Angriffszielen, damit einhergehenden Nebeneffekten für die IT-Sicherheit bei der Ausnutzung von Schwachstellen sowie den Eingriffen in den Kernbereich privater Lebensgestaltung.

(3) Qualität des Gesetzesvorhabens / Better Regulation

Seitens der Union gibt es in "Better Regulation / Guidelines on Impact Assessment (http://ec.europa.eu/smart-regulation/guidelines/ug_chap3_en.htm) Vorgaben, wie ordentliche Gesetzwerdungsprozesse ablaufen sollen, insbesondere die Wirkungsfolgenabschätzung daraus gibt dabei eine gute Hilfestellung.

Der Verfassungsdienst im Bundeskanzleramt hat die Notwendigkeit, den Gehalt und die Auswirkung einer Wirkungsorientierten Folgenabschätzung in https://www.oeffentlicherdienst.gv.at/wirkungsorientierte_verwaltung/folgenabschaetzung/index.html ausführlich beschrieben.

Gemäß diesen Vorgaben gilt:
"Die Folgenabschätzungen begleiten insbesondere den Gesetzesentwurf von der Vorbereitung bis zur parlamentarischen Beschlussfassung und über die Umsetzung hinaus."

Weiters gilt:
"Durchführung und Evaluierung der vollinhaltlichen wirkungsorientierten Folgenabschätzung
Die wirkungsorientierte Folgenabschätzung besteht aus den Schritten Problemanalyse, Zielformulierung, Maßnahmenformulierung sowie Abschätzung der Auswirkungen. Eine Evaluierung des zugrundeliegenden Vorhabens erfolgt nach spätestens fünf Jahren.

- **Problemanalyse:** In diesem Schritt wird aufgezeigt, warum staatliches Handeln notwendig ist.
- **Zielformulierung:** Bei der Zielformulierung wird angegeben, welche Wirkung in der Gesellschaft erreicht werden soll. Durch Indikatoren kann der tatsächliche Erfolg gemessen werden.
- **Maßnahmenformulierung:** Hier wird dargestellt, wie die jeweiligen Ziele verfolgt werden. Durch die hier ebenfalls verwendeten Indikatoren kann überprüft werden, ob die Maßnahmen wie geplant umgesetzt wurden.

- **Abschätzung der Auswirkungen:** Es wird in einem ersten Schritt geprüft, ob die Auswirkungen in den oben angeführten Politikbereichen eine bestimmte Intensität überschreiten. In jenen Wirkungsdimensionen, für welche dies zutrifft, wird anschließend eine vertiefende Abschätzung durchgeführt. Finanzielle Auswirkungen sind jedenfalls wesentlich und daher anzugeben. Seit dem 1. April 2015 besteht die Möglichkeit im Falle von Aufwendungen unter 1 Million Euro, eine vereinfachte Darstellung vorzunehmen. Ein IT-Tool unterstützt die Anwenderinnen und Anwender bei diesem Prozess und leitet sie an. Wo sinnvoll und möglich, werden dabei Quantifizierungen vorgenommen. Beispiele sind etwa die Anzahl der betroffenen Personen, die Menge an neu geschaffenen Arbeitsplätzen oder die für einen Verwaltungsweg anfallenden Stunden.
- **Evaluierung:** Spätestens nach fünf Jahren führt das jeweils zuständige Ressort eine interne Evaluierung der wirkungsorientierten Folgenabschätzung durch. Die tatsächlich eingetretenen Wirkungen werden dabei mit den damaligen Annahmen verglichen. Aus diesem Vergleich sollen wichtige Informationen über die angenommenen Wirkungszusammenhänge und mögliche Verbesserungspotentiale gewonnen werden."

Für das Gesetzesvorhaben 192/ME gibt es keine ernstzunehmende Problembeschreibung, das zu lösende Problem - in welchen Fällen war eine gerichtlich angeordnete Maßnahme nicht erfolgreich, wie oft, aus welchem Grund - wird nicht beschrieben. Im Gegenteil: In der Erläuterung wird eine Zeitungsente (Spielekonsole) angeführt, also eine Fiktion anstelle eines bestehenden Problems beschieben. Mangels klarer Problemstellung fehlt auch eine akzeptable Zielformulierung, die Voraussetzung wäre, die Sinnhaftigkeit der vorgeschlagenen Maßnahmen zu verifizieren. In weiterer Folge fehlen Evaluierungskriterien, um die beabsichtigte Wirksamkeit überprüfen zu können.

Das BMI hatte eine Abschätzung künftiger Ausgaben und diese Budgetvorschau als "Wirkungsfolgenabschätzung" betitelt. Dies könnte man schon als Verpackungsschwindel ansehen.
Dabei gilt: Wer Millionen Euro bereits für Software, Computer und Analysten ausgibt, muss bei klassischen Methoden wie Observation oder dem Aufbau von Quellen sparen.

(4) Rechtsfiktion?

Das BMI verweist in der Erläuterung auf die interdisziplinäre Arbeitsgruppe unter Leitung von o. Univ. Prof. Dr. Bernd-Christian Funk. Diese interdisziplinäre Arbeitsgruppe hat festgestellt, dass eine "Online-Durchsuchung" rechtlich nicht zulässig ist.
In der Erläuterung des BMI wird angeführt, die rechtliche Unterscheidung zwischen "Online-Durchsuchung" und "Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden" sei möglich und umsetzbar und ermögliche ein Vorgehen, das von der Beurteilung durch die interdisziplinäre Arbeitsgruppe nicht oder minder betroffen sei. Die technische Umsetzbarkeit dieser Überlegung wird nicht nachgewiesen. Geflissentlich übergangen wird auch, dass die Auswirkungen einer "rückwirkenden Überwachung" auf einem Computersystem gegenüber einem "großen Lauschangriff" viel weiter reichende Ermittlungen ermöglichen (Auslesen von Mailboxen, Chat-Protokollen, technischen Protokollen,

wie sie auf jedem Computersystem anfallen). Und für den Fall, dass eine Anordnung zu Überwachung vergangener Zeiträume (StPO § 137) angeordnet wird, ist das nichts anderes als unbemerkte Durchsuchung eines Computersystems. In der behaupteten Unterscheidung zwischen „Online-Durchsuchung" und den Überwachungsmöglichkeiten, die mit diesem Entwurf ermöglicht werden sollen, sehen wir eine Rechtsfiktion.

(5) Wie weitreichend ist die Durchsuchungsermächtigung?

Der § 134. Z4a soll lauten "... Computer ohne Kenntnis des Inhabers oder sonstiger Verfügungsberechtigter", also können davon unterschiedlichste Computersysteme und Firmennetzwerke betroffen sein und dann Zufallsfunde, auch von unbeteiligten Dritten, weiter genutzt werden, da kein Beweisverwertungsverbot besteht. Sind damit Computersysteme von Universitäten, Bibliotheken oder anderen Öffentlichen Einrichtungen umfasst, wenn die Vermutung aufgestellt wird, ein Beschuldigter könnte solch ein Computersystem zur Kommunikation nutzen?

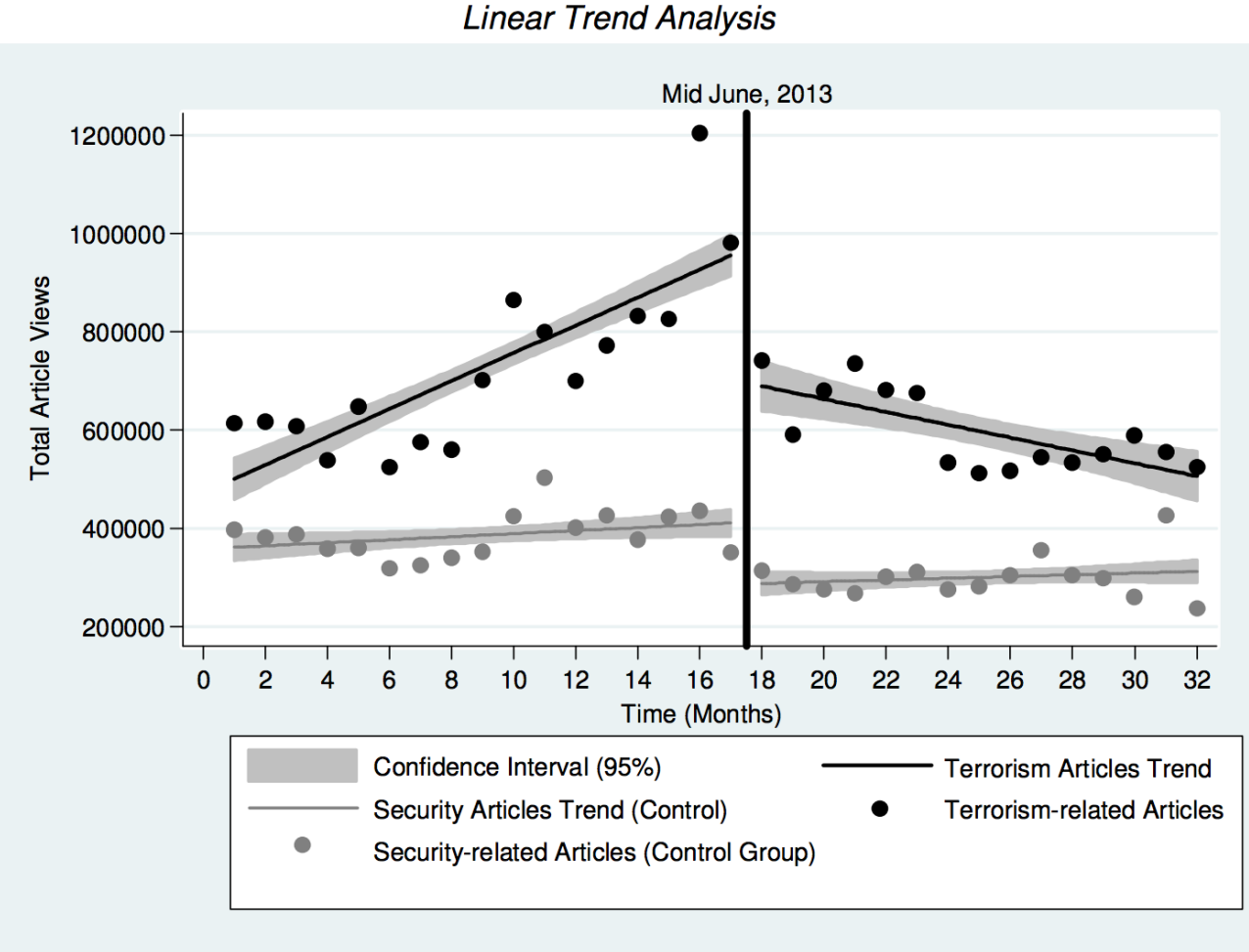
(6) Chilling Effects

Überwachung führt zu Effekten, die in der wissenschaftlichen Literatur als "Chilling Effects" beschrieben werden - wer sich überwacht fühlt, ändert sein Verhalten. Wie weit diese Verhaltensänderung und die damit einhergehende Einschränkung im persönlichen Kommunikationsverhalten reicht, zeigen Untersuchungen wie jene von Jonathon W. Penney im Berkley Technology Law Journal Vol. 31:1; ein zusammenfassender Bericht dazu findet sich in der Washington Post [2]. Diese Studie zeigt, in welchem Maß das Wissen um Überwachung die Meinungsfreiheit einschränkt, in Angst vor Überwachung oder aus „vorauseilendem Gehorsam".

[2] https://www.washingtonpost.com/news/wonk/wp/2016/04/27/new-study-snowdens-disclosures-about-nsa-spying-had-a-scary-effect-on-free-speech/

Figure E: Terrorism Articles vs. Control Group

The sudden drop and trend reversal for the terrorism-related articles is consistent with chilling effects. The security-related articles control group shows little impact.



Hier wird der Bruch in der Entwicklung von Abfragehäufigkeiten für Wikipedia-Artikel mit Terrorismus-Bezug und mit allgemeinem Sicherheitsbezug nach der Veröffentlichung der Snowdon-Papers über Überwachung dargestellt.

Diese Grafik zeigt deutlich die Bruchlinie ab dem Zeitpunkt der Veröffentlichung der Informationen zur Überwachung durch die USA. Die Befürchtung, dass unbescholtene Bürger anhand von Stichworten mit Bezug zu Terrorismus in die Überwachungsmaschinerie einbezogen würden, führt zu einer deutlichen Anpassung des Verhaltens und damit zum „freiwilligen" Verzicht auf Bürgerrechte (Freiheit der Meinungsäußerung, Freiheit des Zugangs zu Information). Selbst die Suche nach nur allgemein sicherheitsrelevanten Begriffen ist sprungartig zurückgegangen.

(7) Aufgaben von Justiz- und Sicherheitsbehörden

Grundsätzlich wird die Aufgabe der Justiz- und Sicherheitsbehörden darin gesehen, die Bevölkerung vor drohenden Gefahren zu schützen und insbesondere den Schutz unserer unteilbaren Grundrechte zu gewährleisten.[3]
Dementsprechend erwarten wir, dass Behörden angehalten sind, Gefährdungen und Risiken in der digitalen Welt aufzuzeigen und für die raschestmögliche Beseitigung der Gefahren zu sorgen. Das Aufzeigen von Sicheheitslücken und - wo möglich im Rahmen der übertragenen Aufgaben auch die Mitarbeit an der Beseitigung von Sicherheitslücken - gewinnt dabei zunehmend an Bedeutung. Mit dieser Zielsetzung arbeitet die Europäische Union an der „Richtlinie des europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union".

Österreich ist dem „Übereinkommen über Computerkriminalität" (Budapest, 23.XI.2001) beigetreten. Die daraus international geltenden Definitionen für Computersysteme, unberechtigten Zugang, rechtswidriges Abfangen, Eingriff in Daten, Missbrauch von Vorrichtungen führen wir im Anhang an ([i]).
Mit dem Beitritt zu diesem Übereinkommen hat sich Österreich verpflichtet, gesetzgeberische und andere Maßnahmen zu treffen, um diese Tatbestände als Straftat zu umschreiben.

Im österreichischen Strafgesetzbuch wird folgendes als strafbare Handlung definiert:

Widerrechtlicher Zugriff auf ein Computersystem

§ 118a. (1) Wer sich zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen durch Überwindung einer spezifischen Sicherheitsvorkehrung im Computersystem in der Absicht Zugang verschafft,

1. sich oder einem anderen Unbefugten Kenntnis von personenbezogenen Daten zu verschaffen, deren Kenntnis schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt, oder
2. einem anderen durch die Verwendung von im System gespeicherten und nicht für ihn

bestimmten Daten, deren Kenntnis er sich verschafft, oder durch die Verwendung des
Computersystems einen Nachteil zuzufügen, ...

Die Bestimmung
"StGB **§ 126c.** (1) Wer

1. ein Computerprogramm, das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung eines widerrechtlichen Zugriffs auf ein Computersystem (§ 118a), einer Verletzung des Telekommunikationsgeheimnisses (§ 119), eines missbräuchlichen Abfangens von Daten (§ 119a), einer Datenbeschädigung (§

[3] **Grundrecht**e sind niedergeschrieben in der Erklärung der Menschenrechte 1948, zusammen mit dem Internationalen Pakt über bürgerliche und politische Rechte und seinen beiden Fakultativprotokollen (über Beschwerdeverfahren und über die Todesstrafe) und dem Internationalen Pakt für wirtschaftliche, soziale und kulturelle Rechte und seinem Fakultativprotokoll), sowie in den weiteren Präzisierung der Grundrechte durch Bundesverfassung und die Charta der Grundrechte der Europäischen Union zu deren Einhaltung sich Österreich freiwillig verpflichtet hat).

126a), einer Störung der Funktionsfähigkeit eines Computersystems (§ 126b) oder eines betrügerischen Datenverarbeitungsmissbrauchs (§ 148a) geschaffen oder adaptiert worden ist, oder eine vergleichbare solche Vorrichtung oder

2. ein Computerpasswort, einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen,

mit dem Vorsatz herstellt, einführt, vertreibt, veräußert, sonst zugänglich macht, sich verschafft oder besitzt, dass sie zur Begehung einer der in Z 1 genannten strafbaren Handlungen gebraucht werden, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen." nicht automatisch aufgehoben, wenn ein solches Computerprogramm an eine Behörde verkauft wird.

Der vorliegende Gesetzesentwurf kehrt dies nunmehr um und geht davon aus, dass technische Mittel zu beschaffen und bereitzustellen sind, deren Anwendung normalerweise Straftatbestände darstellen (Schadsoftware, Spionagesoftware, „Bundestrojaner"). Zum Einsatz solcher Schadsoftware ist es nötig, kritische Sicherheitslücken („Exploits") von Computersystemen zu nutzen, bevor diese Sicherheitslücken von den Herstellern oder Betreibern geschlossen werden. Solche kritischen Sicherheitslücken werden auf internationalen Schwarzmärkten zu hohen Preisen gehandelt und zumeist für Computerschädlinge ("Trojaner" in allen erdenklichen Formen) genutzt. Es liegt im Interesse der Händler und verbrecherischer Anwender solcher „Exploits", dass diese kritischen Lücken nicht geschlossen werden und die Gefährdung möglichst vieler Computersysteme lange aufrechterhalten bleibt. Bei Umsetzung dieser Gesetzesänderung ergibt sich ein Behördeninteresse daran, kritische Sicherheitslücken nicht zu beheben. Behörden, die solche „Exploits" nutzen, tragen dadurch zur Aufrechterhaltung des genannten Schwarzmarktes aktiv bei.

(8) Welches Verständnis von "Computersystemen" legen wir einem neuen Gesetz zugrunde?

Die rasante Entwicklung der Informations- und Kommunikationstechnik verlangt, dass wir unser Verständnis von Computersystemen dem aktuellen Stand und den absehbaren technologischen Entwicklungen anpassen. Zu der Zeit, als die interdisziplinäre Arbeitsgruppe unter Leitung von o. Univ. Prof. Dr. Bernd-Christian Funk zusammentrat, war die Abgrenzung von Computersystemen zu anderen Gegenständen des täglichen Lebens noch relativ überschaubar, technische Grenzen per Augenschein ersichtlich. Inzwischen hat sich diese Situation dramatisch verändert. Dazu nur ein Beispiel: Das Auto ist inzwischen ein Konglomerat unterschiedlicher technischer Systeme. Wesentlich beteiligt daran ist ein Computersystem. Dabei kommunizieren in einem Auto die unterschiedlichsten Komponenten - Navigation, Bremsanlage und -assistent, Klimaanlage, Airbag-Steuerung und Notrufsystem untereinander, mit dem Mobiltelefon, mit dem Wartungs- und Sicherheitsportal des Herstellers, mit der öffentlichen Verkehrsleitstelle. Spätestens beim autonomen Fahren werden die Autos auch untereinander kommunizieren. In diesen komplexen, sicherheitsrelevanten Systemen soll Schadsoftware platziert werden können? Der vorliegende Gesetzesentwurf lässt dies zu und schließt die Installation von Schadsoftware aus der Ferne nicht explizit aus. Unbeabsichtigte Nebenwirkungen und Fehler in der Schadsoftware werden damit gesundheits- und lebensgefährdend. Eine ordentlich durchgeführte Abschätzung möglicher Auswirkungen würde noch viele weitere Risken aufzeigen.

(9) Telekommunikationsüberwachung - Trojaner - Spionagewerkzeug – Schadsoftware

Außer einer rein sprachlichen Trennung durch eine selbstauferlegte Funktionsbeschränkung gibt es technisch keinen Unterschied zwischen einer "Quellen-TKÜ" und einer sogenannten „Online-Durchsuchung“ in Computersystemen. Beide sind informationstechnisch als Schadprogramme klassifizierte Spionagewerkzeuge, die eine Kommunikation vor einer möglichen Verschlüsselung abgreifen. Technisch gesehen dürfte eine "Quellen-TKÜ" nur bei tatsächlicher Nachrichtenübermittlung eingesetzt werden, wenn die Übermittlung bereits eingeleitet ist. Logisch könnte dies frühestens beim Anstoßen des Übermittlungsvorganges durch den Bediener oder durch ein Programm erfolgen, erst dadurch wird Übermittlung von Nachrichten ausgelöst. Hingegen ist eine Verschlüsselung, die in der Folge einen verschlüsselten Datenbestand in einem Computersystem erzeugt, (noch) keine Übermittlung von Nachrichten. Bei der Verschlüsselung von Daten oder Dateien verbleibt der Datenbestand auf dem jeweiligen Computersystem. Wenn überhaupt, wird erst zu einem späteren, nicht zwangsläufig zusammenhängenden Zeitpunkt der Versand der Daten und damit die Kommunikation mit einem anderen Computersystem angestoßen. Daher sind die im Gesetzesvorschlag vorgesehenen Maßnahmen also nicht tauglich, den intendierten Zweck - Zugriff auf Nachrichteninhalte vor Verschlüsselung - zu erreichen. Wenn tatsächlich beabsichtigt sein sollte, auf Datenbestände zuzugreifen, deren Übermittlung nicht eingeleitet ist, hat das den Charakter einer Online-Durchsuchung und ist - dem Ergebnis der interdisziplinären Arbeitsgruppe unter Leitung von o. Univ. Prof. Dr. Bernd-Christian Funk folgend, eine Ermittlungsmaßnahme, die gesetzlich nicht zulässig ist.

Ob die Funktionsbeschränkung auf ausschließliche Überwachung von Kommunikation eingehalten wurde, ist in vielen Fällen nicht nachzuweisen, Überschreitungen der Befugnisse auch durch Programmierfehler ohne Absicht entstehen.

(10) Wie kann Schadsoftware in ein Computersystem eingebracht werden?

Im Gesetzesentwurf gibt es keine Beschränkung, wie die Schadsoftware in das "Zielsystem" eingebracht werden soll. In Pressemeldungen des zuständigen Ministers wird zwar davon gesprochen, dass "ausschließlich eine Installation durch physischen Zugriff auf das Computersystem, nicht jedoch eine remote-Installation der Überwachungssoftware zulässig sein soll." Die Einschränkung findet sich nicht im Gesetzesentwurf. Ob das nur übersehen wurde, kann nicht beurteilt werden.

(11) Schutz von Schadsoftware vor Entdeckung

Es ist davon auszugehen, dass Sicherungsmaßnahmen analog zur Informationsverordnung – InfoV § 9 Abs 2 (BGBl. II - Ausgegeben am 24. März 2015 - Nr. 58) – allgemein verfügbar sind und von jedem verwendet werden können. Daher gilt folgendes:
a) Versierte Benutzer von Verschlüsselung verfügen zumeist auch über notwendige Sach- und Fachkenntnis, die Kompromittierung ihres Computersystems zu erkennen. Dies insbesondere, falls sie über kriminelle Vereinigungen mit den nötigen Sachmitteln ausgestattet werden.
b) Qualifizierte Antivirensoftware ist zunehmend in der Lage, verdächtige Systemaufrufe und ungewöhnliche Kommunikationsvorgänge zu erkennen und dadurch Schadsoftware enttarnen zu können.
c) Es ist wahrscheinlich, dass über Antivirensoftware die Kenntnis über mögliche Kompromittierung weiterverbreitet wird.
d) Genauere Kenntnis kompromittierender Software kann auch zum Legen falscher Fährten und zur Beweismittelfälschung verwendet werden. Unter Umständen kann kompromittierende Software zum Angriff auf behördliche Infrastruktur oder Infrastruktur Dritter verwendet werden.

(12) Technische Restriktionen einer Schadsoftware

Computer sind komplexe elektronische Systeme (vereinfacht: eine spezifische Kombination von Hardwareelementen verschiedener Hersteller, darauf aufsetzendem Betriebssystem und unterschiedlichen darauf laufenden kommerziellen oder speziell geschaffenen Anwendungen mit benutzerspezifischen Anpassungen oder Spezialsoftware).
Diese komplexen Systeme sollen so verändert werden, dass – dem Gesetzesvorschlag folgend – Kommunikationsvorgänge unbemerkt ausgeleitet werden können.
Je nach konkreter Betriebsumgebung sind dazu Änderungen des bestehenden Systems nötig, ohne dass gewährleistet ist, dass die Laufzeitbedingungen vollständig bekannt sind und dadurch nicht vollständig auf gewünschte und

unerwünschte Wirkungen getestet werden können.
Die von den Behörden für die intendierten Zwecke benötigte Schadsoftware müsste darauf geprüft werden, dass sie ausschließlich beabsichtigte Zwecke erfüllt und keine Möglichkeit besteht, darüber hinausgehend Daten zu verändern oder zu sammeln.
Selbst wenn solche aus Sicherheitsgründen nötigen Tests der Schadsoftware erfolgreich verlaufen sollten, ist verschlüsselte Kommunikation möglich, wenn die Verschlüsselung nicht in der Zielumgebung vorgenommen wurde.

Die Verwaltungsstelle der Schadsoftware („Command and Control Server") und deren Schnittstelle zum Zielcomputer wird zu einem attraktiven Angriffsziel für organisierte Kriminalität und Geheimdienste und ermöglicht Dritten gleichermaßen wie den im Entwurf Genannten selbst zu agieren.

Ein Rechner mit offenen Sicherheitslücken und womöglich zusätzlich geöffnetem Rückkanal ist gegenüber einem Zugriff Dritter ungeschützt und damit als Angriffsziel eine allgemeine Gefahr. Sollten die von Behörden verwendeten Angriffsvektoren bekannt werden, ist zu erwarten, dass sie auch am Schwarzmarkt für „Exploits" weiter gehandelt werden.
Daten, die von einem solcherart ungeschützten System ausgehen, können von Dritten oder auch von übereifrigen Behörden ge- oder verfälscht sein, und sind dementsprechend von zweifelhafter Beweiswürdigkeit. Schon das Einbringen behördlicher Schadsoftware auf einen Rechner beweist, dass dieser Rechner ungenügend gegen Zugriffe Dritter geschützt war.

Mehrfachinfiltration kann zu Telekommunikationsvorgängen auf dem befallenen Rechner führen, die durch Dritte entstehen. Auffälliger Datenverkehr zur Ausleitung kann Dritte auf die Maßnahme einer staatlichen Infiltration aufmerksam machen. Dies kann gerade erst dazu führen, dass die Gelegenheit genutzt wird, einem so identifizierten informationstechnischen System zu schaden. Handwerklich schlecht implementierte Ausleitungsfunktionen, die offenkundig ohne einen sinnvollen Qualitätssicherungsprozess zur Anwendung kamen, exponierten zudem die Interna des infiltrierten Rechners gegenüber aktiv oder sogar passiv agierenden Dritten.

Aus den Snowden-Dokumenten ist bekannt, dass die NSA für die verdeckte Auswertung der von anderen Geheimdiensten und Polizeien vorgenommenen Abhör-Operationen und Infiltrationen einen eigenen Begrif hat: „Fourth Party Exploitation". Aus den Dokumenten geht eindeutig hervor, dass die Ausnutzung von Schwachstellen in den Trojanern anderer Angreifer eine Standard-Methode für die NSA ist, die gern und umfangreich verwendet wird. Es handelt sich also um ein nicht nur theoretisches Risiko.

Viele Plattformen wie Windows, OSX und iOS verlangen für die Ausführung von privilegiertem Code kryptographisch signierte Verfahren vom Hersteller (Code-Signing). Eine behördlich eingebrachte Schadsoftware würde unweigerlich zu einer Gefährdung der Integrität und Vertraulichkeit aller auf dem Gerät verarbeiteten Daten führen, da Schutzmechanismen wie das Code-Signing bei der Infiltration des Systems global deaktiviert oder durch nicht vertrauenswürdige Zertifikate ergänzt werden müssten. Diese Maßnahme erleichtert es Dritten maßgeblich, das Gerät zu kompromittieren und somit auch die Integrität der ausgeleiteten Überwachungsergebnisse zu gefährden.

(13) Abgrenzung von Kommunikation gegenüber anderen Dateninhalten

Nach heutigem Stand der Technik und auch in naher Zukunft findet der Großteil der Kommunikation auf informationstechnischen Systemen typischerweise mittels Webbrowser wie beispielsweise Internet Explorer, Safari, Firefox, Chrome etc. statt. Der Webbrowser stellt quasi ein universelles Kommunikationswerkzeug dar, mit dem typischerweise folgende Nutzungsarten verbunden werden:

- Empfang, Lesen, Entschlüsseln und Archivieren von E-Mails,
- Versand, Schreiben und Verschlüsseln von E-Mails,
- Chat, Instant Messaging, Social-Web-Dienste, Videotelefonie,
- Konferenzschaltungen, beispielsweise Webex,
- Abrufen von Webseiten über HTTP und HTTPS,
- Download von Dateien, Programmen etc.,
- Verwaltung von Foto-Alben, elektronischen Büchern und Musiksammlungen, Tagebüchern, Selbsthilfe-Foren etc.,
- Streaming-Plattformen und Games,
- Verwaltung von Medizingeräten und Auswertung derer Messwerte,
- Steuerung von Haustechnik und Videoüberwachungskameras,
- Remote-Zugrif auf Unternehmensdaten des Arbeitgebers oder Auftraggebers, beispielsweise über Citrix.

Die Definition, was davon in welchem Stadium der Nutzung eine Telekommunikation darstellt, ist nur schwer abgrenzbar. Dass es bei den vielfältigen Kommunikationsformen aber unvermeidlich sein wird, in den intimsten Kernbereich der zu überwachenden Person einzugreifen, liegt nahe.
Es ist nach der Infiltration des Systems zu keiner Zeit technisch möglich zu unterscheiden, welche Inhalte im Browser gerade aktiv dargestellt werden. Es ist ebenso nicht technisch möglich zu bestimmen, ob ein von der Zielperson verfasster Text, etwa E-Mail- oder Chat-Nachrichten, bereits abgeschickt und somit als Kommunikation zu klassifizieren ist.
Ein Entwurf einer E-Mail oder eines Beitrags in einem Web-Forum kann jederzeit vor dem Absenden abgelegt, verändert oder gelöscht werden, ohne dass eine Überwachungssoftware dies zuverlässig registrieren könnte. Ob diese festgehaltenen Gedanken jemals zu einer Kommunikation werden und das informationstechnische System verlassen, kann nicht vorab unterschieden werden. Daher ist es für jede Form der Kommunikations-Überwachung zwingend notwendig, dass für einen nachträglichen Rechtsschutz die Betroffenen Gelegenheit zur Prüfung von Quellcode, Binärcode und signierten Datenübertragungsprotokollen des in ihrem spezifischen Fall eingesetzten Trojaners erhalten. Eine zumindest nachgelagerte Quellcodeprüfung durchzuführen, muss möglich sein und liegt im unmittelbaren Interesse der Behörden, schon um Haftungsfragen eingrenzen zu können.

(14) Haftung beim Einsatz von Schadsoftware

Mobiltelefone, Autos, Navigationsgeräte, Hörgeräte, Fitnesstracker, Stromzähler (SmartMeter), e-Book-Lesegeräte, sogar Fernseher verfügen heute über autarke Kommunikationsfunktionen. In absehbarer Zeit wird es mehr Regel als Ausnahme sein, dass jedes Digitalgerät verschiedene Kommunikationsfunktionen aufweist

("Internet of Things"). Dies gilt auch für persönliche Medizingeräte, etwa Insulinpumpen, Dauer-EKG, Hörgeräte, verschiedene Implantate und digitale Sehhilfen, die durch Infektion mit Spionagesoftware zum Zielsystem werden können. Jedes dieser Geräte enthält, produziert und kommuniziert potentiell intime, kernbereichsrelevante Informationen.
Die Risiken bei einer Infiltration sind zudem gerade bei solchen Geräten erheblich, wenn an deren einwandfreier Funktionsfähigkeit Leben oder Gesundheit von Menschen hängen. Typische Beispiele dafür sind Fahrzeuge und Medizinsysteme.

Dass Änderungen an komplexen Computersystemen nicht immer zum beabsichtigten Ergebnis führen, selbst wenn die Vorbereitung mit großem Aufwand, zu einem vielfachen des im Ministerialentwurfs angeführten Kostenrahmens, führen, zeigen die Erfahrungen des täglichen Lebens, beispielsweise bei Änderungen an Computersystemen großer Banken, die manchmal zu mehrtägigen Computerausfällen führen.
Durch Manipulation an komplexen Computersystemen können leicht unbeabsichtigte Fehlfunktionen entstehen, die ursächlich dem behördlichen Eingriff zuzurechnen wären und wofür auch entsprechend zu Haften sein wird. Nach Angaben der Ermittlungsbehörden wird jeder Trojaner speziell für den jeweiligen Einsatz zusammengebaut. Damit ist das Risiko groß, dass durch Fehler oder Absicht Funktionsmodule integriert oder aktiviert werden, die über das zugelassene Maß hinausgehen oder Fehlfunktionen bewirken. In diesem Sinn ist die uneingeschränkte vermögensrechtliche Haftung des Bundes für Folgeschäden aus der Durchführung einer Überwachung von Personen, einer Überwachung von Nachrichten oder in Folge eines Datenabgleichs entstanden sind (§ 148), ein Schritt in die richtige Richtung. Diese Haftung müsste jedoch über vermögensrechtliche Haftung hinausgehend alle Folgeschäden, bis hin zu Reputationsschäden, umfassen.

(15) Besondere Aufgaben für den Rechtschutzbeauftragten

„Der Rechtsschutzbeauftragte hat insbesondere darauf zu achten, dass während der Durchführung Anordnung und gerichtliche Bewilligung nicht überschritten werden und die Ermittlungsmaßnahme nur solange durchgeführt wird, als die Verhältnismäßigkeit gewahrt ist."

In dieser Zuschreibung finden wir zwei anspruchsvolle Aufgaben, deren Wahrnehmung die bisherige Konzeption des Rechtsschutzbeauftragten in Frage stellt:

Der Rechtsschutzbeauftragte, beamteter Jurist im Bereich des Innenministeriums, soll – ohne dass für ihn technische Fachkenntnisse erforderlich sind oder von ihm nachgewiesen werden müssen – darauf achten, dass Anordnung und gerichtliche Bewilligung nicht überschritten werden.
Um dieser Aufgabe gerecht werden zu können, müsste er in der Lage sein, höchst qualifizierte Sicherheitsüberprüfungen vorzunehmen. Eine ordnungsmäßig korrekte Prüfung der Umsetzung von Anordnung und gerichtlicher Bewilligung ist für den Rechtschutzbeauftragten nur möglich, wenn in jedem einzelnen Fall Quellcode, Binärcode und die signierten Datenübertragungsprotokolle des in diesem spezifischen Fall eingesetzten Trojaners zur Verfügung gestellt und überprüft werden.

(16) Qualitätsanspruch bei der Gesetzwerdung

Die grundlegenden Ansprüche an ein qualitatives legistisches Verfahren – eine klare Problembeschreibung, eine klare Zieldefinition, Kriterien zur Erfolgsmessung und eine über die Kosten hinausgehende Folgenabschätzung, Plausibilität der Angaben zur Wesentlichkeit hinsichtlich der Abschätzung der Auswirkungen innerhalb der Wirkungsdimensionen – sind ebenso wenig erkennbar wie eine notwendige Eingrenzung auf informationstechnische Systeme, die nicht Leben oder Gesundheit gefährden können.

Elektronische Kommunikation ersetzt immer häufiger das intime Gespräch. Macht man die vom deutschen Bundesverfassungsgericht angeregte Gesamtüberwachungsrechnung auf, so ist auf die staatliche Trojanisierung nicht nur aufgrund der technischen Unwägbarkeiten und der unvermeidbaren Eingriffe in intimste Kernbereiche privater Lebensgestaltung der Betroffenen zu verzichten, sondern auch, weil neben den Telekommunikationsdaten auch der gesamte Datenbestand des Computers potentiell offen liegt. Zudem wird durch den Trojaner stets Einblick in Informationen des infiltrierten Systems genommen, die über einen gewissen, potentiell recht langen Zeitraum hinweg entstanden sind. Die Gefahr technischer Kollateralschäden ist hierbei nicht zu übersehen.[ii]

(17) Wie weiter mit diesem Gesetzesentwurf?

Wir sehen das beabsichtigte Gesetzesvorhaben im Widerspruch zu Grundrechten und internationalen Vereinbarungen Österreichs, für technisch unausgegoren und nicht den qualitativen Ansprüchen an eine bessere Rechtsetzung (Handbuch „Bessere Rechtsetzung" des BKA) entsprechend.

Daher empfehlen wir dem Gesetzgeber dringend, von der Umsetzung dieses Gesetzesvorhabens Abstand zu nehmen.

Unter Beachtung der Regeln für „Bessere Rechtssetzung" und einer „vollinhaltlichen wirkungsorientierten Folgenabschätzung" sollte ein grundlegend neuer Gesetzesvorschlag erarbeitet werden, der grundrechtskonform konkret bestehende Probleme der Sicherheitsbehörden lösbar macht.

i

Übereinkommen über Computerkriminalität, BGBl. III - Ausgegeben am 3. Oktober 2012 - Nr. 140, Ausschnitt

Im Sinne dieses Übereinkommens bedeutet

a „Computersystem" eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms automatische Datenverarbeitung durchführen; ...

Artikel 2 –Rechtswidriger Zugang

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um den unbefugten Zugang zu einem Computersystem als Ganzem oder zu einem Teil davon, wenn vorsätzlich begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben. Eine Vertragspartei kann als Voraussetzung vorsehen, dass die Straftat unter Verletzung von Sicherheitsmaßnahmen, in der Absicht, Computerdaten zu erlangen, in anderer unredlicher Absicht oder in Zusammenhang mit einem Computersystem, das mit einem anderen Computersystem verbunden ist, begangen worden sein muss.

Artikel 3 –Rechtswidriges Abfangen

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um das mit technischen Hilfsmitteln bewirkte unbefugte Abfangen nichtöffentlicher Computerdatenübermittlungen an ein Computersystem, aus einem Computersystem oder innerhalb eines Computersystems einschließlich elektromagnetischer Abstrahlungen aus einem Computersystem, das Träger solcher Computerdaten ist, wenn vorsätzlich begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben. Eine Vertragspartei kann als Voraussetzung vorsehen, dass die Straftat in unredlicher Absicht oder in Zusammenhang mit einem Computersystem, das mit einem anderen Computersystem verbunden ist, begangen worden sein muss.

Artikel 4 –Eingriff in Daten

1 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um das unbefugte Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten, wenn vorsätzlich begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben.

2 Eine Vertragspartei kann sich das Recht vorbehalten, als Voraussetzung vorzusehen, dass das in Absatz 1 beschriebene Verhalten zu einem schweren Schaden geführt haben muss.

Artikel 5 –Eingriff in ein System

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um die unbefugte schwere Behinderung des Betriebs eines Computersystems durch Eingeben, Übermitteln, Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten, wenn vorsätzlich begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben.

Artikel 6 –Missbrauch von Vorrichtungen

1 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um folgende Handlungen, wenn vorsätzlich und unbefugt begangen, nach ihrem innerstaatlichen Recht als Straftaten zu umschreiben:

a das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige

i Verfügbarmachen einer Vorrichtung einschließlich eines Computerprogramms, die in erster Linie dafür ausgelegt oder hergerichtet worden ist, eine nach den Artikeln 2 bis 5 umschriebene Straftat zu begehen;

ii eines Computerpassworts, eines Zugangscodes oder ähnlicher Daten, die den Zugang zu einem Computersystem als Ganzem oder zu einem Teil davon ermöglichen, mit dem Vorsatz, sie zur Begehung einer nach den Artikeln 2 bis 5 umschriebenen Straftat zu verwenden, und

b den Besitz eines unter Buchstabe a Ziffer i oder ii bezeichneten Mittels mit dem Vorsatz, es zur Begehung einer nach den Artikeln 2 bis 5 umschriebenen Straftat zu verwenden.

Eine Vertragspartei kann als gesetzliche Voraussetzung vorsehen, dass die strafrechtliche Verantwortlichkeit erst mit Besitz einer bestimmten Anzahl dieser Mittel eintritt.
2 Dieser Artikel darf nicht so ausgelegt werden, als begründe er die strafrechtliche Verantwortlichkeit in Fällen, in denen das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen oder der Besitz nach Absatz 1 nicht zum Zweck der Begehung einer nach den Artikeln 2 bis 5 umschriebenen Straftat, sondern beispielsweise zum genehmigten Testen oder zum Schutz eines Computersystems erfolgt.
3 Jede Vertragspartei kann sich das Recht vorbehalten, Absatz 1 nicht anzuwenden, sofern der Vorbehalt nicht das Verkaufen, Verbreiten oder anderweitige Verfügbarmachen der in Absatz 1 Buchstabe a Ziffer ii bezeichneten Mittel betrifft.

ii Wie auch andere Abschnitte dieses Textes stammt dieser Absatz als Ergebnis der Zusammenarbeit aus "CCC - Stellungnahme an das Bundesverfassungsgericht zum BKA-Gesetz und zum Einsatz von Staatstrojanern"
http://www.ccc.de/system/uploads/189/original/BKAG_Stellungnahme.pdf