universität wien

Institut für Strafrecht und Kriminologie
Univ.-Ass. Dr. Roland Pichler
Schenkenstraße 4
A-1010 Wien

T +43-1-4277-34656
F +43-1-4277-834656
roland.pichler@univie.ac.at

An das
Bundesministerium für Justiz
Museumsstraße 7
1070 Wien

Per E-Mail: team.s@bmj.gv.at
Cc: begutachtungsverfahren@parlament.gv.at

Wien, am 12.05.2016

Stellungnahme zum Entwurf eines Bundesgesetzes, mit dem die Strafprozessordnung 1975 und das Staatsanwaltschaftsgesetz geändert werden

Sehr geehrte Damen und Herren,

zum genannten Begutachtungsentwurf nehme ich wie folgt Stellung:

1 Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden

1.1 Inhaltliche Einführung und Stellungnahme zur Zielsetzung des Gesetzesentwurfs

„Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden“ ist ein Synonym für den in Deutschland schon länger Verwendung findenden und gebräuchlichen Begriff der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ). Dabei werden Telekommunikationsdaten (Sprache, Textnachricht, …) von Übertragungen abgegriffen, welche nicht über klassische Telefonverbindungen (Festnetz, Mobiltelefon), sondern über das Internet stattfinden (zB VoIP-Telefonie). Die Daten werden direkt am Zielsystem (Quelle) mittels Überwachungssoftware abgefangen, da diese nach Beginn des Übertragungsvorgangs nur noch in verschlüsselter Form vorliegen. Die übermittelten Daten könnten zwar über die Telekommunikationsinfrastruktur

mitgeschnitten werden, wären jedoch aufgrund der Verschlüsselung einer Verwertbarkeit nicht oder nur schwierig zugänglich.[1]

Ziel einer solchen Maßnahme sind also Kommunikationsdaten, die vom Zielsystem über das Internet empfangen oder versendet werden. Der vorliegende Entwurf geht aber noch ein Schritt weiter und umfasst generell alle Daten, die im Wege eines Computersystems übermittelt werden. Dadurch ist nicht nur die Überwachung von in der Cloud gespeicherten Daten möglich, sondern es kann generell der gesamte Internetverkehr überwacht werden, wie etwa auch das Surfverhalten der Zielperson. Darüber hinaus sollen dem Gesetzesentwurf zufolge auch Kontaktverzeichnisse und Adressbücher der neuen Ermittlungsmaßnahme zugänglich sein. Daher ist es irreführend, nur von einer Überwachung der internetbasierten Kommunikation zu sprechen. Vielmehr wäre auf Basis des Entwurfs eine umfassende Online-Überwachung bzw. –Durchsuchung möglich.[2] Abgesehen von den genannten Kontakt- und Adressdaten, sollen die übrigen am Zielsystem vorhandenen Daten nicht überwacht werden. Diese gesetzlich vorgesehene Einschränkung der Überwachung ist technisch allerdings nicht realisierbar.[3]

Von der Quellen-TKÜ zu unterscheiden ist der rechtlich nicht abschließend definierte[4] aber gebräuchliche Begriff der „Online-Durchsuchung".[5] Umfasst ist davon der verdeckt durchgeführte Zugriff auf IT-Systeme durch staatliche Ermittlungsorgane als Mittel der Beweisgewinnung. Dem Wesen dieser Methode als geheime Ermittlungsmethode eher entsprechen würde der Begriff der „Online-Überwachung". Die Beweisgewinnung erfolgt durch eine heimlich am Zielsystem installierte Software[6], welche das Zielsystem einmalig durchsucht (Online-Durchsicht) oder dauerhaft überwacht (Online-Überwachung). Die Untersuchung bzw. Überwachung erfolgt aufgrund vorher definierter Suchkriterien. Im Gegensatz zur Quellen-TKÜ sind Kommunikationsdaten also grundsätzlich nicht Ziel

[1] Zur Begriffsdefinition siehe u.a. *Rehak*, Angezapft. Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung[1.4] (Dipl.Arb. 2013) 16. (Druckfassung: Angezapft. Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung, Monsenstein und Vannerdat 2014); *Buermeyer/Bäcker*, Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des § 100a StPO, HRRS 2009, 433 (434); *Fox*, Realisierung, Grenzen und Risiken der „Online-Durchsuchung", DuD 2007, 827 (827).

[2] In diesem Sinne und mit ausführlicherer Problembeschreibung Salimi (24/SN-192/ME XXV GP).

[3] Im Detail dazu Kapitel 1.2.3.

[4] Dazu *Buermeyer*, Die „Online-Durchsuchung". Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, HRRS 2007, 154 (154).

[5] Siehe zB: *Feiler/Raschhofer*, Die Online-Durchsuchung, in Zankl (Hrsg), Auf dem Weg zum Überwachungsstaat? Neue Überwachungsmaßnahmen im Bereich der Informations- und Kommunikationstechnologie (2009) 171; BMJ/BMI-Interministerielle Arbeitsgruppe „Online-Durchsuchung", Erweiterung des Ermittlungsinstrumentariums zur Bekämpfung schwerer, organisierter und terroristischer Kriminalitätsformen („Online-Durchsuchung") (2008); *Bundesministerium für Inneres* (Hrsg), Online-Durchsuchung.

[6] Auf die hardwarebasierte Online-Durchsuchung soll hier nicht eingegangen werden, da sie vom Gesetzesentwurf jedenfalls nicht erfasst ist. Zu dieser Form der Online-Durchsuchung siehe u.a. *Rehak*, Angezapft[1.4], 14.

einer solchen Maßnahme. Die aufgrund der Suchkriterien ermittelten Daten werden später über das Internet an die überwachende Behörde übermittelt.[7]

Mitunter wird für die Überwachungssoftware selbst der Begriff „Remote Forensic Software" verwendet,[8] der jedoch irreführend ist, da eine Beweisgewinnung mittels Schadsoftware in der Regel nicht den Beweiswert einer forensischen Analyse besitzt.[9]

1.2 Technische Rahmenbedingungen

1.2.1 Möglichkeiten der Installation des Überwachungsprogramms

Technisch stehen mehrere Möglichkeiten offen, das staatliche Überwachungsprogramm auf dem Zielsystem zu installieren:[10]

a. **Entfernte manuelle Installation:** Durch die Ausnutzung einer unsicheren Konfiguration oder einer noch nicht öffentlich gemachten Sicherheitslücke im verwendeten Betriebssystem wird die Schadsoftware über das Internet auf das Zielsystem übertragen. Eine Mitwirkung der Benutzer/innen des Zielsystems ist nicht erforderlich.
b. **Installation über eine infizierte Website/E-Mail bzw. durch Manipulation der Netzwerkinfrastruktur:** Die Zielperson muss zumindest dazu gebracht werden eine infizierte Website aufzurufen, bzw. das Attachement einer infizierten E-Mail zu öffnen. Für eine erfolgreiche Installation muss das Zielsystem Sicherheitslücken aufweisen, welche eine Infizierung ermöglichen. Bei der Installation durch Manipulation der Netzwerkinfrastruktur wird dem Zielsystem zB ein modifiziertes Update aufgespielt. Damit dies unbemerkt erfolgen kann, ist die Mitwirkung des Internet Service Providers (ISP) nötig, bei welchem sozusagen das echte Update gegen das manipulierte ausgetauscht wird.
c. **Manuelle Installation durch die Zielperson:** Der Zielperson wird eine CD, ein USB-Stick bzw. andere Datenträger mit der Überwachungssoftware zugespielt. Beim Einlegen in das Zielsystem wird die Überwachungssoftware unbemerkt von der Zielperson installiert. Die Gefahr besteht darin, dass nicht nur das Zielsystem, sondern auch Computersysteme von unbeteiligten Dritten infiltriert werden.
d. **Manuelle Installation durch physikalischen Zugriff:** Diese ist nur möglich, sofern ein direkter physischer Zugriff auf das Zielsystem gegeben ist, etwa bei PCs durch das Eindringen in die

[7] Siehe zum ganzen *Rehak*, Angezapft[1.4], 13-15.
[8] Siehe etwa BMJ/BMI-Interministerielle Arbeitsgruppe „Online-Durchsuchung", Erweiterung, 10.
[9] Siehe dazu Kapitel 1.3.4 und *Fox*, DuD, 827 (827-828).
[10] Siehe dazu *Rehak*, Angezapft[1.4], 18-21; *Pfitzmann*, Contra Online-Durchsuchung, Informatik-Spektrum 2008, 65 (68f); *Buermeyer*, HRRS, 154 (155f, 163f); *Fox*, DuD, 827 (829); *Hansen/Pfitzmann*, Technische Grundlagen von Online-Durchsuchung und - beschlagnahme, DRiZ 2007, 225 (226); *Pohl*, Zur Technik der heimlichen Online-Durchsuchung, DuD 2007, 684 (685).

Wohnung. Bei Smartphones gestaltet sich dieses Vorhaben schon schwieriger, da diese meistens direkt von der Zielperson am Körper getragen werden oder sich in der unmittelbaren Nähe der Zielperson befinden. Auf technischer Seite ist diese Methode nur möglich, wenn das Zielsystem

i. im laufenden Betrieb mit Administratorenrechten vorgefunden wird oder zumindest in diesen Zustand versetzt werden kann (automatischer Login);
ii. unverschlüsselt ist und somit direkt auf den Datenträger zugegriffen werden kann. Die Überwachungssoftware muss in diesem Fall ohne gängige Installationsroutinen im Betriebssystem verankert werden;
iii. unverschlüsselt ist, die Benutzerverwaltung samt Passwortschutz umgangen wird, zB durch Ausnützen von Sicherheitslücken, und danach eine direkte Installation über die normale Installationsroutine des Betriebssystems erfolgt.

Ist das Zielsystem verschlüsselt, schließt das eine manuelle Installation durch physikalischen Zugriff praktisch aus, da die Verschlüsselung, wenn überhaupt, nur mit erheblichem Zeitaufwand überwunden werden könnte.

1.2.2 Architektur der Überwachungssoftware

Eine „eierlegende Wollmilchsau“ unter den Überwachungsprogrammen gibt es nicht. Das heißt, kein Programm kann ohne Anpassungen auf allen in Frage kommenden Computersystemen installiert werden.[11] Bevor überhaupt eine Installation der Überwachungssoftware vorgenommen werden kann, muss daher zuerst eine Analyse des Zielsystems erfolgen. Eine solche muss insb folgende Punkte umfassen:[12]

a. Betriebssystem inkl Version und aufgespielter Sicherheitsupdates
b. Art des Internetzugangs (zB Kabel, DSL, Mobilfunk)
c. Hard- bzw. softwareseitiger Schutz, dazu zählen ua Virenscanner, Firewall, Verschlüsselungs-software
d. Konfiguration der Zugangsberechtigungen
e. Verwendete Kommunikations- bzw. Clouddienste und Software (zB Skype, WhatsApp, Dropbox, …)

[11] *Fox*, DuD, 827 (829); *Pohl*, DuD, 684 (685f).
[12] Zu diesen siehe *Fox*, DuD, 827 (828). Rudimentär auch *Rehak*, Angezapft[1.4], 17.

1.2.3 Technische Grundlagen des eigentlichen Überwachungsvorgangs

Damit die Überwachungssoftware Zugriff auf die notwendigen Schnittstellen hat und um die eigene Existenz verschleiern zu können, ist es notwendig, dass die Überwachungssoftware mit erhöhten Rechten (Kernelmode) ausgestattet ist.[13]

Um die Kommunikationsdaten in unverschlüsselter Form ermitteln zu können, muss die Überwachungssoftware jene Datenquellen die für einen Kommunikationsvorgang in Frage kommen, überwachen. Wird ein Kommunikationsvorgang festgestellt, sind die Daten sofort auszulesen und an die Ermittlungsbehörden zu übermitteln. Ein unverzügliches Auslesen ist deshalb notwendig, da die Daten im Nachhinein gelöscht bzw. manipuliert werden könnten und sie dann keinen Beweiswert mehr hätten. Die Feststellung, ob gerade ein Kommunikationsvorgang stattfindet und welche Daten davon betroffen sind, kann jedoch nur anhand zusätzlicher Informationen und Daten des Zielsystem erfolgen. Die zwar rechtlich angestrebte Trennung der „Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden“ einerseits und einer kompletten „Online-Überwachung“ andererseits,[14] ist daher technisch nicht haltbar und zusätzlich im Nachhinein nicht belegbar.[15]

1.3 Stellungnahme zu einzelnen Passagen des Entwurfs

1.3.1 Installation des Überwachungsprogramms (Z 4 u Z 6)

Vom Justizminister[16] und anderen Vertretern des Ministeriums[17] wurde betont, dass eine Ferninstallation nicht vorgesehen sei. Im Gesetzesentwurf spiegeln sich diese Äußerungen nicht wider, denn § 134 Z 4a StPO nimmt nicht auf die Art der Installation Bezug. Es ist lediglich definiert, dass die Installation, wie es einer solchen Überwachungsmaßnahme immanent ist, geheim, also ohne Kenntnis der Zielperson bzw. der Verfügungsberechtigten erfolgen soll. Gem § 136a StPO ist es zulässig, zur Installation „in eine bestimmte Wohnung oder in andere durch das Hausrecht geschützte Räume einzudringen, Behältnisse zu durchsuchen und spezifische Sicherheitsvorkehrungen zu überwinden[, soweit dies zur Durchführung der Ermittlungsmaßnahme unumgänglich ist]“. Der vom Ministerium kommunizierte Regelfall der direkten physikalischen Installation, zB durch das Eindringen in geschützten Räumen, ist dem Gesetzeswortlaut nach also nur

[13] Einen Überblick über die komplexe Materie liefert *Rehak*, Angezapft[1.4], 21-26.
[14] Siehe dazu Kapitel 1.1.
[15] *Rehak*, Angezapft[1.4], 34f mit weiteren Ausführungen und Nachweisen.
[16] Aichinger, Justiz: Überwachungssoftware für Handy und Laptop, in: diepresse.com, http://diepresse.com/home/politik/innenpolitik/4955053/Justiz_Ueberwachungssoftware-fur-Handy-und-Laptop?_vl_backlink=/home/index.do (letzter Zugriff am 30.3.2016).
[17] Etwa Sektionschef Pilnacek, Kritik: Zeitungsente dient als Begründung für Bundestrojaner, in: derstandard.at, http://derstandard.at/2000034552505/Kritik-Zeitungsente-dient-als-Begruendung-fuer-Bundestrojaner (letzter Zugriff am 11.5.2016).

in Ausnahmefällen vorgesehen (arg unumgänglich). Realistisch betrachtet bleibt von den Installationsmöglichkeiten als Regelfall somit nur die entfernte manuelle Installation übrig, da alle übrigen in Kapitel 1.2.1 dargelegten Maßnahmen aufgrund der besonderen Gegebenheiten wohl ebenso nur in Ausnahmefällen greifen dürften.

Wenn also tatsächlich nur eine Installation per direktem physikalischem Zugriff intendiert ist, sollte dies explizit im Gesetz festgeschrieben werden und sich nicht mit Verweisen auf die eindeutige Absicht des Gesetzgebers[18] bzw. die Systematik des Gesetzes begnügt werden. Eine unklare gesetzliche Regelung bei einer solch eingriffsintensiven Maßnahme sollte tunlichst vermieden werden.

1.3.2 Deinstallation (Z 6, 13)

Nach Beendigung der Überwachungsmaßnahem soll die Überwachungssoftware funktionsunfähig gemacht oder entfernt werden. Eine hundertprozentige Deaktivierung der Überwachungssoftware ist allenfalls nur möglich, wenn der Quellcode bekannt ist. Ansonsten besteht die Gefahr, dass über unbekannte Schnittstellen (Backdoors) die Überwachungssoftware weiterhin benutzt werden kann. Zudem ist die Deaktivierung der Überwachungssoftware alleine nicht aussreichend, vielmehr muss sichergestellt werden, dass alle durch sie geöffneten Sicherheitslücken geschlossen werden.[19]

Laut den Erläuterungen ist vorgesehen, dass die Funktionsperiode der Überwachungssoftware von außen, das heißt ohne neuerlichen direkten physikalischen Zugriff, geändert werden kann.[20] Dies eröffnet eine neue Sicherheitslücke, da es Unbefugten die Möglichkeit einräumt, den Funktionszeitraum ohne Kenntnis der Ermittlungsbehörden zu verlängern bzw. ein deaktiviertes Überwachungsprogramm wieder zu reaktivieren.

1.3.3 Verständigung der Betroffenen (Z 10)

Nach Beendigung der Ermittlungsmaßnahme sind die beschuldigte Person und alle übrigen von der Überwachung Betroffenen zu informieren. Für einen umfassenden und wirksamen Rechtsschutz ist dies auch dringend erforderlich. Allerdings kann sich die in § 138 Abs 5 StPO vorgesehene Verständigung in der Praxis als schwierig erweisen, da bei der Online-Kommunikation oft nur Pseudonyme aber keine Klarnamen verwendet werden.[21] Ist eine Zustelladresse der betroffenen Personen nicht zu ermitteln, wäre anzudenken, diese über jenen Kommunikationsdienst zu verständigen, der überwacht worden ist.

[18] ErlME 5.
[19] Zu den weiteren damit zusammenhängenden technischen Problemen siehe Steinhammer (10/SN-192/ME XXV GP 13f).
[20] ErlME 6.
[21] Detailliert zu dieser Problematik Steinhammer (10/SN-192/ME XXV GP 15f).

1.3.4 Protokollierung (Z 13)

Bei der Beschlagnahme von Computersystemen bzw. Datenspeichern wird eine Kopie in Form eines identischen Abbildes (Image) angefertigt. Von diesem Image wird eine Prüfsumme („Hash“) berechnet, anhand derer sich einerseits die inhaltliche Identität mit dem Originaldatenträger beweisen lässt und andererseits Veränderungen auf der Image-Kopie nachvollzogen werden können. Erst nach dem Erstellen der Prüfsumme erfolgt die Untersuchung des angefertigten Images, wobei alle Untersuchungen zu protokollieren sind. Um die Revisionsfähigkeit, also die Nachvollziehbarkeit von Änderungen zu gewährleisten, erfolgen Untersuchungen niemals anhand des Originaldatenträgers. Andernfalls wäre der sichergestellte Datenträger als Beweismittel nicht mehr brauchbar, da dieser verändert und damit die Echtheit der gefundenen Daten in Zweifel gezogen werden könnte. [22]

In Anlehnung an dieses Konzept bestimmt § 145 Abs 4 StPO, dass „durch geeignete Protokollierung sicherzustellen ist, dass jeder Zugang zu dem Computersystem und jede nachträgliche Veränderung daran nachvollzogen werden können.“ Dabei sollen Prüfsummen gebildet werden, um zu gewährleisten, dass Datenpakete im Quell- und Zielsystem ident sind.[23] Solche Prüfsummen sind aber praktisch wertlos, denn sie bestätigten nur, dass eine fehlerlose Übertragung stattgefunden hat, sagen aber nichts über die Authentizität der Daten aus.[24]

Bereits durch die Installation der Überwachungssoftware wird eine Modifikation am Zielsystem vorgenommen und zudem dessen Funktionalität aufgrund des Ressourcenverbrauchs beeinträchtigt. Eine Revisionsfähigkeit ist bei der im Raum stehenden Überwachungsmethode nicht zu gewährleisten, da sich die Daten im Gegensatz zum sichergestellten Medium dynamisch verändern. [25] Da das Zielsystem weder von den Organen der Ermittlungsbehörde noch von der eigentlichen Zielperson alleine kontrolliert wird, ist somit eine Echtheitsbestätigung der übertragenen Daten nicht gegeben. Denn eine Prüfsumme kann verlässlich nur dann berechnet werden, wenn eine exklusive Kontrolle über das System gegeben ist. Zudem besteht die Gefahr, dass neben der Zielperson und den Organen der Ermittlungsbehörde auch dritte Personen unbemerkt Kontrolle über das Computersystem ausüben und auf diese Weise verfälschte Daten einschleusen.[26]

[22] *Hansen/Pfitzmann*, DRiZ, 225 (225).
[23] ErlME 6.
[24] So auch Verein Arbeitskreis Vorratsdaten Österreich (1/SN-192/ME XXV GP 23).
[25] *Buermeyer/Bäcker*, HRRS, 433 (437, 439); *Hansen/Pfitzmann*, DRiZ, 225 (225).
[26] *Buermeyer/Bäcker*, HRRS, 433 (437, 439); *Hansen/Pfitzmann*, DRiZ, 225 (227). Zur praktisch nicht durchführbaren Protokollierung auch *Rehak*, Angezapft[1.4], 38f.

Daher widerspricht die geplante Ermittlungsmaßnahme „allen Anforderungen, die aus technisch fundierten Gründen an einen sachverständigen Gutachter im Rahmen einer forensischen Analyse gestellt werden."[27]

1.3.5 Rechtsschutzbeauftragter (Z 16)

Die Kontrolle der geplanten Ermittlungsmaßnahme durch den Rechtsschutzbeauftragten ist zu begrüßen und aufgrund der Eingriffsintensität der Ermittlungsmaßnahme auch dringend geboten. Prinzipiell positiv hervorzuheben ist die Möglichkeit der Beiziehung von Sachverständigen durch den Rechtsschutzbeauftragten. Dass solche Sachverständigen allerdings gem der allgemeinen Vorschrift des § 126 Abs 3 StPO von der Staatsanwaltschaft zu bestellen sind, konterkariert die Aufgabe des Rechtsschutzbeauftragten. Diesem obliegt bekanntlich die Wahrung der Beschuldigtenrechte, indem er die Anordnung der jeweiligen Ermittlungsmethode prüft und die Durchführung begleitend kontrolliert.[28] Die Erfüllung dieser Aufgaben ist mit Sachverständigen, welche durch die Staatsanwaltschaft bestellt worden sind, jedenfalls nicht vereinbar.

Es ist im vorliegenden Fall auch kein Grund ersichtlich, warum dem Rechtsschutzbeauftragten beigegebene Sachverständige zwingend von der Staatsanwaltschaft zu bestellen wären. Es wäre daher anzudenken einen Sachverständigenpool einzurichten, welcher aus mehreren (juristischen) Personen besteht,[29] und auf welchen der Rechtsschutzbeauftragte bei Bedarf zurückgreifen kann.

1.4 Risiken der Online-Durchsuchung

1.4.1 Mangelnde Kontrollierbarkeit der eingesetzten Software

Aus dem Vorblatt und der WFA geht hervor, dass für die Überwachungssoftware Lizenzgebühren bezahlt werden sollen. Daraus ist zu schließen, dass die Überwachungssoftware nicht von staatlichen Stellen entwickelt wird, sondern von externen privaten Anbietern zugekauft werden soll. Da die Anbieterfirma profitorientiert arbeitet, wird sie den Quellcode der Überwachungssoftware nicht zur Verfügung stellen. Somit ist keine wirksame Überprüfung (audit) der Überwachungssoftware möglich. Es kann also nicht festgestellt werden, ob die Überwachungssoftware wirklich nur das kann, was gesetzlich vorgesehen ist. Selbst wenn der entsprechende Wille seitens der Ermittlungsbehörden vorhanden wäre, könnten diese also den Vorgaben des Gesetztes bzw. eines entsprechenden gerichtlichen Beschlusses nicht folgen, da sie schlicht nicht alle Funktionen der Überwachungssoftware kennen. Somit kann die Ermittlungsbehörde selbst nicht ausschließen, dass

[27] *Hansen/Pfitzmann*, DRiZ, 225 (228).
[28] U.a. R*eindl-Krauskopf* in *Fuchs/Ratz*, WK StPO § 47a (Stand 1.9.2012, rdb.at).
[29] So hat der Chaos Computer Club (CCC) in Deutschland bereits mehrmals Gutachten in Verfahren vor dem Bundesverfassungsgericht erstellt, zB über die Vorratsdatenspeicherung, https://www.ccc.de/de/vorratsdatenspeicherung (11.4.2016).

es zu überschießenden, nicht rechtmäßigen Datenerhebungen kommt.[30] Aufgrund der hohen grundrechtlichen Eingriffsintensivität darf sich der Staat aber nicht auf bloße Zusicherungen privater Dienstleister verlassen.[31] In Frage käme daher allenfalls eine Eigenentwicklung durch staatliche Behörden, welche aber die prognostizierten Kosten um ein Vielfaches übersteigen würde.[32]

1.4.2 Konterkarierung der Cybersicherheit

In allen Installation- bzw. Überwachungsmöglichkeiten werden Schwachstellen im Sicherheitssystem des Zielsystems ausgenützt bzw. durch die Überwachungssoftware weitere Sicherheitslücken (Einfallstore) für Kriminelle geöffnet. Da die Zielperson veröffentlichte Schwachstellen durch bereitgestellte Patches schließen kann, werden zur zweckentsprechenden Überwachung nur noch nicht öffentlich bekannte Schwachstellen eingesetzt werden können.

Idealerweise werden entdeckte Sicherheitslücken in Programmen an den Hersteller gemeldet, welcher darauf ein entsprechendes Update und Informationen liefert, durch welche die Sicherheitslücke geschlossen werden kann.

Zero-Day-Exploits sind Angriffsmethoden bzw. –programme, welche solche bekanntgewordenen Sicherheitslücken ausnutzen und noch am Tag der Veröffentlichung der Sicherheitslücke eingesetzt werden (daher Zero Day). Denn zu diesem Zeitpunkt ist die Wahrscheinlichkeit sehr hoch, noch Systeme vorzufinden, welche die Sicherheitslücke noch nicht durch das Aufspielen eines Updates geschlossen haben. Im Gegensatz dazu nützen Less-Than-Zero-Day-Exploits nicht veröffentlichte Sicherheitslücken aus. Es gibt Einzelpersonen und Firmen die im Auftrag für Unternehmen, Behörden und wohl auch kriminellen Organisationen nach Sicherheitslücken suchen. Für den Erwerb und zugehöriger Exploits solcher Sicherheitslücken werden zwischen 1.000 und 50.000 Dollar bezahlt. Diese Zahlen stammen aus 2007, daher ist anzunehmen, dass die Preise hierfür gestiegen sind. Selbst in Deutschland ist Zahl der Personen überschaubar, welche auf das Aufspüren solcher Less-Than-

[30] Die Analyse eines von deutschen Behörden eingesetzten Überwachungsprogramms lieferte neben eklatanten Sicherheitsmängeln auch Hinweise darauf, dass die Software mehr konnte als sie eigentlich durfte, Chaos Computer Club analysiert Staatstrojaner, https://ccc.de/de/updates/2011/staatstrojaner (letzter Zugriff am 11.5.2016); Chaos Computer Club analysiert aktuelle Version des Staatstrojaners, https://www.ccc.de/de/updates/2011/analysiert-aktueller-staatstrojaner (letzter Zugriff am 11.5.2016).

[31] *Buermeyer/Bäcker*, HRRS, 433 (439).

[32] Das BKA in Deutschland hat drei Jahre lang an einer eigenen Überwachungssoftware gearbeitet. Die Kosten hierfür beliefen sich auf ca. fünf Millionen Euro, Breithut, Staatstrojaner späht nur Windows-PCs aus, in: Suttgarter Nachrichten (11.4.2016), http://www.stuttgarter-nachrichten.de/inhalt.online-ueberwachung-staatstrojaner-spaeht-nur-windows-pcs-aus.1e318559-1bf6-45fd-9035-1a3e79deff16.html (letzter Zugriff am 12.5.2015).

Zero-Day-Exploits spezialisiert sind.[33] Für Österreich dürfte dies umso mehr gelten. Hingegen wird etwa für China Zahl derartiger Spezialist/innen im fünfstelligen Bereich geschätzt.[34]

Wird nun von staatlichen Behörden entgeltlich erworbene Überwachungssoftware eingesetzt, die auf solche Exploits zurückgreift, so werden dadurch kriminelle Kreise unterstützt, der zugrundeliegende Markt ausgeweitet und legitimiert. Es wird damit dazu beigetragen, dass Sicherheitslücken eher geheim gehalten denn veröffentlicht werden, da sich dadurch gutes Geld verdienen lässt.[35] Durch diese indirekte Förderung von Kriminellen, und der damit Verbundenen Verheimlichung von Less-Than-Zero-Day-Exploits, erhöht sich die Anfälligkeit von österreichischen Unternehmen und Bürger/innen für Cyberattacken.[36]. Schäden aufgrund von Wirtschaftsspionage, welche Less-Than-Zero-Day-Exploits ausnützen, sind extrem hoch.[37]. Die durch den Einsatz von staatlicher Überwachungssoftware geschaffenen Sicherheitslücken könnten auch für andere kriminelle Zwecke, wie etwa Botnetze,[38] missbraucht werden. Diese quasi staatliche Förderung von Sicherheitslücken steht im klaren Widerspruch zur „Österreichischen Strategie für Cyber Sicherheit". Werden Behörden Sicherheitslücken bekannt, sollten diese unverzüglich veröffentlicht werden, anstatt einen kriminellen Markt der Geheimhaltung zu bedienen.

1.4.3 Abwehr- und Täuschungsmaßnahmen

Die Überwachungssoftware ist nichts anderes als Schadsoftware von staatlicher Seite. Daher besteht die Gefahr, dass der Einsatz von der Zielperson erkannt wird, zB durch Virenscanner[39] oder erhöhtem Netzwerktraffic.[40] Vor allem bei mobilen Endgeräten mit begrenztem Datenvolumen ist die Wahrscheinlichkeit sehr hoch, dass der von der Überwachungssoftware generierte erhöhte Traffic und somit die Überwachungssoftware erkannt werden.[41]

Bemerkt die Zielperson die Überwachungssoftware, kann sie diese vom Zielsystem entfernen. Es besteht aber auch die Möglichkeit, dass die Ermittlungsbehörde getäuscht wird.[42] Entweder hinterlässt die Zielperson keine Beweise mehr und verhält sich unverdächtig, oder es findet sogar eine gezielte Desinformation der Ermittlungsbehörden statt. Ebenso ist nicht auszuschließen, dass Dritte die Überwachungssoftware auf dem Zielsystem entdecken und für ihre Zwecke nutzen, etwa

[33] *Pohl*, DuD, 684 (685).
[34] *Pohl*, DuD, 684 (685).
[35] *Rehak*, Angezapft[1.4], 59; *Pohl*, DuD, 684 (687).
[36] *Rehak*, Angezapft[1.4], 59.
[37] *Pohl*, DuD, 684 (687), ohne jedoch konkrete Zahlen zu nennen.
[38] *Pohl*, DuD, 684 (687).
[39] *Pohl*, DuD, 684 (684).
[40] Bei durchgeführten Online-Durchsuchen in Deutschland ist dies offenbar bereits aufgetreten, siehe dazu *Hansen/Pfitzmann*, DRiZ, 225 (227); *Pohl*, DuD, 684 (684, 686).
[41] *Buermeyer*, HRRS, 154 (164f).
[42] *Hansen/Pfitzmann*, DRiZ, 225 (227).

um falsche Beweise zu hinterlassen. Denn in allen Fällen, in denen eine erfolgreiche Infiltration des Systems durch die Behörden aufgrund der Ausnützung einer Sicherheitslücke erfolgte, ist dies ein Beleg dafür, dass der Zielrechner auch von dritten Personen in deren Kontrolle gebracht werden könnte.[43] Die Gefahr der Beeinflussung des Zielsystems durch dritte Personen würde dann auch bei beschlagnahmten Zielsystemen den Beweiswert schmälern, da nicht ausgeschlossen werden kann, dass dritte Personen falsche Beweise hinterlassen haben.

1.4.4 Infrastruktur

Der Server auf dem die Daten übermittelt werden, muss hochgradig geschützt werden. Einerseits um eine Rückverfolgung zu erschweren und anderseits um den Zugriff von unbefugten Personen zu unterbinden. Dabei ist es nicht abwegig, dass die eingesetzte Software selbst sicherheitsrelevante Fehler aufweist, vor allem wenn es sich dabei um ein zugekauftes Produkt handelt. Technisch ist es kaum möglich, solche Fehler gänzlich zu vermeiden und auszuschließen.[44] Die Ermittlungsmaßnahme ist jedenfalls mit erheblichen Aufwand und Kosten verbunden.[45] Die prognostizierten Kosten erscheinen jedenfalls als zu gering angesetzt.

1.5 Fazit

Zwar bietet die angedachte Überwachungsmaßnahme den Ermittlungsbehörden neue Möglichkeiten. Allerdings ist einerseits der Beweiswert der daraus gewonnen Ergebnisse anzuzweifeln und andererseits lässt sich die Überwachungsmaßnahme gerade durch intelligente und geschulte Täter/innen, wie es in der Szene der organisierten Kriminalität und bei Terrorist/innen großteils der Fall sein dürfte, leicht aushebeln. Auch wenn die intendierte Ermittlungsmaßnahme aufgrund des Zwecks zunächst legitim erscheinen mag, so muss doch konstatiert werden, „dass die Maßnahme regelmäßig nur gegen ‚virtuelle Eierdiebe' vom Schlage eines amateurhaft agierenden eBay-Betrügers wirksam anzuwenden sein wird".[46]

Mag zwar auf juristischer Ebene eine Unterscheidung zwischen einer umfassenden Online-Durchsuchung und einer „Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden" möglich sein, auf technischer Ebene ist sie es nicht. Während sich der Nutzen der geplanten Ermittlungsmaßnahme (noch) nicht abschätzen lässt, sind die Risiken jedenfalls als gravierend einzustufen. Daher sollte auf die Einführung der geplanten Ermittlungsmaßnahme gänzlich verzichtet werden.

[43] *Hansen/Pfitzmann*, DRiZ, 225 (227).
[44] *Pohl*, DuD, 684 (687).
[45] *Pohl*, DuD, 684 (687).
[46] *Buermeyer*, HRRS, 154 (166).

2 Funkzellenabfrage (Z 9)

Mit 12 Os 93/14i, 12 Os 94/14m erachtete der OGH eine sog Funkzellenabfrage für zulässig. Die Rechtmäßigkeit einer solchen auf § 135 Abs 2 Z 3 StPO gestützten Ermittlungsmaßnahme wurde zuvor überwiegend verneint.[47] Mit ein Argument gegen die „Funkzellenabfrage“ war, dass § 138 Abs 1 Z 3 StPO die Bezeichnung eines Endgerätes verlangte.

Die Entscheidung des OGH erscheint aus mehreren Gründen kritikwürdig, diese hier zu üben ist aber nicht Sinn des Begutachtungsverfahrens. Allerdings erscheint es zweifelhaft, im Gesetzentwurf zur Einführung der Online-Überwachung das Wort „Endgerät“ aus § 138 Abs 1 Z 3 StPO zu streichen, um dadurch die zweifelhafte gesetzliche Legitimierung einer „Funkzellenüberwachung“ abzusichern. Es wäre wünschenswert gewesen, entweder gesetzlich klarzustellen, dass eine Funkzellenabfrage nicht als Ermittlungsinstrumentarium in Frage kommt, oder aber, die Funkzellenabfrage als eigene nicht unter § 135 StPO fallende Ermittlungsmaßnahme zu normieren. Auf diese Weise könnte diese eingriffsintensive und viele unbeteiligte Dritte erfassende Ermittlungsmaßnahme in den Gesamtbericht über den Einsatz besonderer Ermittlungsmaßnahmen aufgenommen und deren Einsatz evaluiert sowie kontrolliert werden.

[47] Ablehnend *Reindl-Krauskopf*, Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit - Bemerkungen zum vorligenden Gutachten aus strafrechtlicher Sicht, in Österreichischer Juristentag (Hrsg), 18. ÖJT Band I/2 (2013) 146 (148-150); *Reindl-Krauskopf* in Fuchs/Ratz (Hrsg), Wiener Kommentar zur StPO § 138 Rz 32 (Stand 1.10.2009). Dieser folgend *Salimi*, Terrorbekämpfung durch Straf- und Sicherheitspolizeirecht. Überlegungen zur "erweierten Gefahrenforschung", "Online-Durchsuchung" und "Funkzellenabsaugung", JBl 2013, 698 (705-706) u. OLG Linz 26.4.2013, 9 Bs 108/13s. Dafür *Nimmervoll*, Das Strafverfahren. Systematische Darstellung für Ausbildung und Praxis(2015) 231, allerdings mit Verweis auf den fehlerhaften Rechtssatz RI0100007. Die Entscheidung OLG Innsbruck 14.6.2013, 11 Bs 150/13s Rz 1 = jusIT 2013/84, 175 (Thiele), aus welchem der Rechtssatz abgeleitet wurde, trifft die im Rechtssatz geäußerte Meinung in keiner Weise. In der genannten Entscheidung geht es vielmehr um die Auskunft aus – damals noch zulässig – Vorratsdaten auf Basis vorhandener Telefon- bzw. IMEI-Nummern. Die der Entscheidung zugrunde liegenden Anordnung der Staatsanwaltschaft bezeichnet eine solche Auskunft fälschlicherweise als „Funkzellenauswertung“. Gleichfalls fehlerhaft die dazu ergangene zitierte Entscheidungsbesprechung von Thiele. Ebensowenig enthält die von *Nimmervoll*, Strafverfahren, 231 Fn 264 zustimmend zitierte Entscheidung OGH 11.4.2013, 12 Os 26/13k eine Aussage über die Zulässigkeit einer „Funkzellenabfrage“. Ohne wertende Stellungnahme OGH 26.3.2014, 15 Os 32/14s = ÖJZ EvBl-LS 2014 116/, 689 (Ratz) = JBl 2014, 744 = JSt-LS OGH 2014/57, 173 = AnwBl 2014, 659 = RZ 2014/EÜ 168, 226; *Ohrnhofer* in Schmölzer Gabriele (Hrsg), StPO Strafprozessordnung § 138 Rz 32a (Onlineaktualisierung 1.02 Stand April 2015).