Chaos Computer Club

# Stellungnahme an das Bundesverfassungsgericht zum BKA-Gesetz und zum Einsatz von Staatstrojanern

1 BvR 966/09, 1 BvR 1140/09

Constanze Kurz,
Dirk Engling, Frank Rieger, Thorsten Schröder

7. Juli 2015

## Vorbemerkung

In den Verfassungsbeschwerden gegen das BKA-Gesetz 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.

## Technische Risiken

### Besondere Gefährlichkeit bei Infiltration eines informationstechnischen Systems

Generell unterminiert staatliche Infiltration das Vertrauen der Öffentlichkeit und der Nutzer in die Sicherheit, Vertraulichkeit und Integrität informationstechnischer Systeme. Beim Einsatz von Spionagesoftware werden nicht selten auch für Dritte Angriffswege eröffnet und somit Hintertüren geschaffen.

Die nach dem Inkrafttreten des BKA-Gesetzes offenbar gewordene mangelnde technische Kompetenz der Trojaner-Dienstleister von DigiTask[1] eröffnete Dritten die Möglichkeit der einfach durchführbaren Komplettübernahme des infiltrierten Systems mit genau den Rechten, die der staatliche Trojaner hatte.

Aus Unterlagen, die im Rahmen der Snowden-Enthüllungen öffentlich wurden, geht hervor, daß die Benutzbarkeit von staatlicher Spähsoftware bei bereits trojanisierten informationstechnischen Systemen von Überwacher-Seite aus in den letzten Jahren erheblich vereinfacht wurde.[2] Dabei wird vor allem daran gearbeitet, die Trojanisierung zu industrialisieren und die Auswertung auch über zehntausende Systeme hinweg zu ermöglichen. Die infiltrierten Systeme können über das XKeyScore-System genau so durchsucht werden wie Datenquellen, auf die man physisch Zugriff hat. Es besteht daher die Gefahr, daß mit der Einsickerung von Geheimdienst-

[1] Chaos Computer Club: Analyse einer Regierungsmalware, 8. Oktober 2011, http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf

[2] Vgl. https://s3.amazonaws.com/s3.documentcloud.org/documents/2116354/xks-for-counter-cne.pdf

Methoden in den Polizeibereich auch dieser Trend weg vom gezielten Einzeleinsatz von Trojanern hin zum massenweisen Infiltrieren und zentralisierten Auswerten bei den Strafverfolgungsbehörden ankommt.

Es stehen heute ohne Vorbildung verwendbare Interfaces für die Durchsuchung infiltrierter Systeme zur Verfügung. Dieser vereinfachte Zugriff auf Trojaner-Funktionen ist aber parallel auch für Dritte ebenso von Vorteil, die in trojanisierten System schon vorhandene Überwachungsfunktionen, etwa Keylogger, mitnutzen wollen, ohne sich große Mühe machen zu müssen.

Mehrfachinfiltration kann zu Telekommunikationsvorgängen auf dem befallenen Rechner führen, die durch Dritte entstehen. Der auffällige 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, wie beim Staatstrojaner von DigiTask, exponieren zudem die Interna des infiltrierten Rechners 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 Begriff 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 mitnichten um ein theoretisches Risiko.

Viele Plattformen wie Windows, OSX und iOS erlauben die Ausführung von privilegiertem Code nur dann, wenn er mittels kryptographischer Verfahren vom Hersteller signiert wurde, das sog. Code-Signing. Eine Quellen-TKÜ würde unweigerlich zu einer Gefährdung der Integrität und Vertraulichkeit aller auf dem Gerät verarbeiteten Daten führen, da etwaige Schutzmechanismen wie das Code-Signing bei der Infiltration des Systems global deaktiviert oder durch nicht vertrauenswürdige Zertifikate ergänzt werden müßten. Eine solche Maßnahme würde es Dritten maßgeblich erleichtern, das Gerät zu kompromittieren, und somit auch die Integrität der Quellen-TKÜ-Ergebnisse gefährden.

## Abwehrmethoden gegen Trojaner

Technisch versierten Zielpersonen oder deren Dienstleistern bleiben selbstverständlich weiterhin genügend Wege offen, um einen Angriff mit staatlicher Spionagesoftware regelmäßig abzuwehren.

Die Anbieter der großen Betriebssysteme haben – auch als Reaktion auf die Snowden-Enthüllungen – inzwischen Optionen für leicht benutzbare Endkunden-Festplattenverschlüsselung hinzugefügt, die eine Trojanisierung erschweren und Computerwanzen abwehren können. Prinzipiell können Abwehrmechanismen gegen Schadsoftware hohe oder sogar unüberwindbare Hürden für staatliche Spionagesoftware darstellen. Zuweilen können heute gar WLAN-Router automatisiert verdächtigen Traffic melden.

Je stärker der Druck auf die Hersteller wird, ihre Systeme grundlegend gegen Infiltration zu härten, desto schwerer wird die Trojanisierung auch für Ermittlungsbehörden, insbesondere auf Mobilgeräten. Die Forderung, bestimmte Härtungen informationstechnischer Systeme, etwa Verschlüsselung, zu untersagen, wird etwa in den USA und UK bereits diskutiert. Diese Entwicklung würde insgesamt eine absichtliche Verschlechterung der IT-Sicherheit bedeuten.

Eine Grundfunktion heutiger Trojaner ist es, Hintertür-Zugänge dauerhaft im angegriffenen System zu verankern, die auch ein Systemupdate überstehen. Dadurch wird eine dauerhafte Sicherheitslücke geschaffen, die auch dritten Angreifern offenstehen.

Bevor der Chaos Computer Club eine technisch ausgesprochen unzulängliche Variante eines Staatstrojaners öffentlich machte, scheiterten verbreitete Antivirus-Systeme an dessen Erkennung wegen des hemdsärmligen Aufbaus dieses DigiTask-Trojaners. Nachdem der in der Presse nicht zu Unrecht als „Schrottwanze“ bezeichnete DigiTask-Trojaner und seine technischen und rechtlichen Probleme öffentlich diskutiert worden waren, hat das BKA die Spähsoftware FinSpy gekauft. FinSpy ermöglicht es nicht nur, Daten von dem betroffenen System zu ziehen, sondern auch, Software zu installieren, weitere Lücken im System aufzumachen und damit den Rechner auf mehreren Ebenen zu mißbrauchen. Durch den erheblich größeren Funktionsumfang von FinSpy im Vergleich zum DigiTask-Trojaner ist ein Übertreten rechtlicher Grenzen dabei wahrscheinlich. Aufgrund öffentlich nicht konkret benannter Probleme verstößt offenbar auch dieses

Überwachungsprogramm gegen rechtliche Vorgaben und soll daher nicht zum Einsatz gekommen sein.[3]

## Schutz des Kernbereiches

Das Auslagern der Kommunikation und Interaktion in informationstechnische Systeme ist bei fast allen Formen sozialer Beziehungen zwischen Menschen heute schlicht Alltag. Das computergestützte Gespräch und zuweilen das tatsächliche Aufrechterhalten einer persönlichen oder intimen Beziehung wird durch die Systeme vereinfacht. Nicht nur Partnern oder Familienmitgliedern, die geographisch getrennt leben, bieten sich damit Wege, in engem Kontakt zu bleiben, Cybersex inklusive. Das Durchsuchen von Festplatten betrifft heute somit zwangsläufig kernbereichsrelevante Daten. Insbesondere der Zugriff auf die Audioeingänge der Mikrophone informationstechnischer Systeme können höchstpersönliche Gespräche offenbaren.

Technisch bedingt kann jede Information, auch aus allen vorhandenen Sensoren, auf die das IT-System Zugriff hat, bei einem Lauschangriff mit einem Trojaner ausgeleitet werden. Ein stärkerer Eingriff in den Kernbereich des Privatlebens ist kaum mehr vorstellbar.

### Technische Methoden, den Kernbereich zu eröffnen

Zieht man zum Vergleich heran, welche Informationen eine Wanze im Rahmen eines sog. Großen Lauschangriffes in Wohnräumen aufzeichnen kann, und stellt die ausleitbaren Daten eines informationstechnischen Systems dagegen, wird die Eingriffstiefe eines Trojaners deutlich. Anders als bei einem sog. Großen Lauschangriff kann ein Trojaner auch nicht geäußerte Gedanken erfassen in dem Sinne, dass sie vom dem ausgespähten informationstechnischen System aus nicht nach außen kommuniziert wurden. Beispiele sind Sätze, die der Nutzer in sein Chat- oder E-Mail-Programm tippt, später aber wieder löscht und nicht sendet. Typische weitere Beispiele für nicht nach außen kommunizierte Gedanken sind Text-Entwürfe aller Art oder nicht verschickte WhatsApp-Nachrichten oder Direct Messages auf Twitter etc.

Menschen vertrauen typischerweise ihren informationstechnischen Systemen heute viele Bereiche ihrer Privat- und Intimsphäre an, die sie

[3] Konrad Lischka: „Behörden-Trojaner: BKA testet Gamma-Schnüffelsoftware“, SPIEGEL-online,16.Januar 2013, http://www.spiegel.de/netzwelt/netzpolitik/gamma-group-bka-kauft-schnueffelsoftware-a-877969.html

als Texte, Bilder oder Filme gerade für sich bewahren und nicht an Dritte kommunizieren wollen. Der Rechner und das Mobiltelefon als zentrale Speicherinstanz für alle Lebensaspekte ist in den letzten Jahren zur Normalität geworden.

Ein Trojaner kann zudem medizinische Daten erfassen, etwa über ein HealthKit, wenn entsprechende Programme und Sensorik in dem informationstechnischen System vorhanden sind. Damit können Informationen zum Gemütszustand der ausspionierten Personen erlangt werden, die nicht nach außen kommuniziert werden, beispielsweise Aufregung oder Gelassenheit. Hinzu können medizinische Daten im engeren Sinne kommen, etwa der Herzschlag oder Blutdruckinformationen, die auf die körperliche Verfaßtheit oder Krankheiten schließen lassen. Viele informationstechnische Geräte und ihre Sensorik im Haushalt sind bereits an lokale Netzwerke angeschlossen und lassen sich ausschließlich über Webbrowser oder andere Software-Programme auf dem Computer steuern und auswerten. Hierzu zählen insbesondere Medizinal-Geräte, welche mittels Funkschnittstellen an den Computer oder das Netzwerk angebunden sind und darüber ausgewertet werden. In der Praxis sammeln solche Geräte zum Beispiel Blut- oder Kreislauf-Werte, welche Aufschluß über Krankheitsbilder oder Gewohnheiten (Sex, Erregung, Drogen, Alkoholkonsum, Depressionen etc.) geben können.

Ein Trojaner kann grundsätzlich auf alle Informationen zugreifen, die vor dem Zugriffszeitspunkt, also auch sehr weit vor der Installation des Spähprogramms, auf dem IT-System aggregiert wurden.

Mobile Endgeräte als informationstechnische Systeme fallen ebenfalls deutlich in die Problematik hinsichtlich der Verletzbarkeit des Kernbereiches. Sie werden, anders als bei normalen PCs dargestellt, sehr stark als Aggregator von Sensoren, Aktoren und weiteren Geräten aus der Klasse der „Internet of Things“ eingesetzt. Das bedeutet, daß hier neben den Geräten des täglichen Gebrauchs aus dem Haushalt ebenso moderne Kraftfahrzeuge und deren Steuerung, Konfiguration und Datenauswertung bei einer Infiltration von der Überwachung mitbetroffen sein kann. Zwar ist es in diesem Fall einfacher technisch umzusetzen, daß der Trojaner lediglich eine begrenzte Auswahl an mobilen Apps überwachen darf, jedoch ist absehbar, daß es aufgrund der Vielzahl verschiedener Kommunikations-Apps auf Mobiltelefonen jederzeit möglich sein wird, den Umfang der Überwachungsmaßnahme zu erweitern.

## Möglichkeiten, die Erfassung von Kernbereichsinformationen im Vorfeld zu vermeiden

Die Erfassung von Kernbereichsinformationen kann im Vorfeld nicht technisch vermieden werden. Informationstechnisch gesehen besteht bei der Funktionalität einer Spähsoftware keine Unterscheidung zwischen dem legalen und illegalen Ausspähen von Daten auf dem Zielsystem. Die Spähsoftware wird zwangsläufig mit den höchsten System-Rechten versehen werden, da ein verdeckter Betrieb auf dem Zielsystem andernfalls nicht möglich wäre. Einer technisch versierten Person wäre es zu jeder Zeit möglich, eine Spähsoftware durch illegale Komponenten zu ergänzen, ohne daß dies in einer Auditierung oder einem Audit-Trail ersichtlich wäre. Ein Audit-Trail darf daher nie auf Seite der Ermittler geführt werden, sondern immer an neutraler Stelle oder beim Verteidiger der Person, der die Überwachungsmaßnahme gewidmet war. Das bisher vorgesehene Dreier-Team aus dem BKA-Datenschutzbeauftragten und zwei weiteren BKA-Beamten ist nicht als neutrale oder unabhängige Stelle zu sehen.

Die eigentlich notwendigen Maßnahmen zur Sicherstellung der Verwertbarkeit der Daten sowie der Vermeidung einer Erhebung von Kernbereichsdaten stoßen an technische Grenzen. Die Erhebung von Daten auf dem Zielsystem müßte stets unter Berücksichtigung des jeweiligen Kontextes geschehen. Hierfür wären fortgeschrittene Methoden der Künstlichen Intelligenz notwendig, die Handlungen des Nutzers im semantischen Kontext verstehen könnten und nicht auf die nachträgliche Durchsicht der gesammelten Informationen angewiesen wären. Eine solche Form der Künstlichen Intelligenz ist in der heutigen Zeit nicht verfügbar.

## Quellen-TKÜ: Begrenzung auf Telekommunikation

Die technischen Anforderungen nach §20l BKAG Abs. 2 stoßen faktisch an technische Grenzen und sind nicht erfüllbar. Insbesondere die Anforderung an die Begrenzung der Überwachung und Aufzeichnung der Telekommunikation gemäß § 20l BKAG Abs. 2 Nummer 1 ist gar nicht durchführbar. Es kann durch technische Maßnahmen nicht sichergestellt werden, daß ausschließlich laufende Telekommunikation mit Dritten oder mit Informationsangeboten im Internet überwacht und aufgezeichnet werden. Der typische Umgehungsweg für die Überwachung der Browser-Nutzung sind Screenshots bzw. sog. „Application-Shots“, die in schneller Folge erstellt werden. Allein ein einfacher Tab-Wechsel im Browser, etwa zwischen einem webbasierten E-Mail-System, einem Google Hangout und beispielsweise der

Editiermaske eines privaten Tagebuchs im gleichen Browser-Fenster verdeutlicht, daß durch diese Technik mitnichten eine ausreichende technische Sicherstellung der ausschließlichen Aufzeichnung von Telekommunikation realisiert werden kann.

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 wird:

- 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 Musik-Sammlungen, Tagebüchern, Selbsthilfe-Foren etc.,
- Streaming-Plattformen und Games,
- Verwaltung von Medizinal-Geräten und Auswertung ihrer Meßwerte,
- Steuerung von Haustechnik und Videoüberwachungskameras,
- Remote-Zugriff 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 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.

Grundsätzlich ist das Abgreifen verschlüsselter E-Mails mittels Quellen-TKÜ aus technischen Gründen höchst fragwürdig, da das Verschlüsseln bei den üblichen Programmen gerade vor dem Absenden der E-Mail stattfindet. Entsprechend findet keine Kommunikation statt, wenn die Verschlüsselung durchgeführt wird. Erst nach dem Verschlüsseln entscheidet der Nutzer, ob die E-Mail seinen Computer verläßt oder nicht. Also muß das Abgreifen von E-Mails vor der Verschlüsselung immer als eine sog. „Online-Durchsuchung" klassifiziert werden, da eine Kommunikation unzweifelhaft erst nach der Verschlüsselung überhaupt eingeleitet wird.

Wenn mittels Quellen-TKÜ die sonst verschlüsselte Sprach- und E-Mail-Telekommunikation, etwa über Skype oder andere VoIP-Dienste sowie über Webmail überwacht werden soll, so werden zwangsläufig über den Browser all die oben genannten Kommunikationsdaten ebenso aufgezeichnet und an die Behörden übermittelt. Selbst bei einer auf einer Black-List beruhenden Beschränkung der eigenen Möglichkeiten seitens der Ermittlungsbehörden besteht zu keiner Zeit die Garantie, daß in der Überwachungssoftware unbemerkt selbstgesetzte Beschränkungen ausgehebelt werden.

Daß nach der Verschlüsselung eines VoIP-Gesprächs bei gängigen Programmen wie dem weitverbreiteten Skype eine Überwachung anders als durch einen Trojaner nicht möglich wäre, hat sich als lebensfremd erwiesen. Seit durch die Snowden-Veröffentlichungen bereits im Juni 2013 das „Prism"-Programm bekanntwurde, ist deutlich geworden, daß Skype ohne Trojanisierung in massenhafter Weise abgehört wird. Washington Post[4] und Guardian[5] beschrieben das Top-Secret-NSA-Programn „Prism", in dessen Rahmen Daten aus Skype, aber auch Kommunikationsdaten von Microsoft, Google, Facebook und Apple gesammelt werden.

---

[4] Barton Gellman, Laura Poitras: „U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program", Washington Post, 7. Juni 2013, http://wapo.st/1gIS8gu

[5] Glenn Greenwald, Ewen MacAskill: „NSA Prism program taps in to user data of Apple, Google and others", The Guardian, 6. Juni 2013, http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data

## Abgrenzung Quellen-TKÜ und sonstige TKÜ

Außer einer rein sprachlichen Trennung durch eine selbstauferlegte Funktionsbeschränkung gibt es keinen Unterschied technischer Natur zwischen einer Quellen-TKÜ und einer sog. „Online-Durchsuchung". Beides sind informationstechnisch als Schadprogramme klassifizierte Spionagewerkzeuge.

Die Funktionsbeschränkung ist im Nachhinein nur schwerlich zu beweisen und kann auch durch Programmierfehler unabsichtlich ausgehebelt und insbesondere für Dritte zugreifbar werden.

Bei der Quellen-TKÜ werden überwiegend Daten erfaßt, bei denen es sich (noch) um keine Kommunikation handelt. Die Unterscheidung, ob ein potentieller oder ein tatsächlicher Kommunikationsvorgang stattfindet, für den der Trojaner überwachungsbefugt wäre, muß in der Software nach automatisierter oder manueller Auswertung vor jeder Interaktion mit dem IT-System festgestellt werden. Dafür müssen aber viele Handlungen des Nutzers sowie Parameter und Daten des informationstechnischen Geräts bereits protokolliert werden. Die Quellen-TKÜ erfaßt daher grundsätzlich immer weit mehr als eine Momentaufnahme bezüglich der gesuchten Daten. Daher sind nach der Einnistung des Trojaners weitere Eingriffe in Grundrechte nicht vermeidbar, sowohl für die Zielperson als auch für weitere Kontaktpersonen.

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

Der grundlegende Ansatz der Quellen-TKÜ ist es, solche Systeme zu infiltrieren, die für die Kommunikation eingesetzt werden, um direkt an die Kommunikationsinhalte zu gelangen. Eine Regelwerk, das beim Kernbereichsschutz implizit davon ausgeht, daß es sich dabei nur um PCs handelt, greift viel zu kurz. Wir sind heute von einer Vielzahl von Geräten umgeben, die Kommunikationsfunktionen haben und damit potentielle Ziele für eine Quellen-TKÜ im Sinne des vorliegenden

Gesetzes sind. Durch den unterschiedlichen Charakter der Geräte entsteht gleichzeitig eine Vielzahl von Problemen bei der Abgrenzung des Kernbereichs, wenn heimlich und dauerhaft potentiell die gesamten Daten des Nutzers zugänglich sind.

Mobiltelefone, Autos, Navigationsgeräte, Hörgeräte, Fitnesstracker, Stromzähler, 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. 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 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.

## Überprüfbarkeit der Trojaner-Funktionen

Welche Funktionen ein Quellen-TKÜ-Trojaner hat, welche konkrete Zugriffe auf welche Daten einer bestimmten Festplatte er nimmt, welche Daten er dabei technisch tatsächlich erfasst und ausleitet, ist im Nachhinein nur durch umfangreiche forensische Analyse des konkret eingesetzten Trojaners zu ermitteln. Eine Art „Bauartprüfung“, bei der nur ein „Muster-Trojaner“ geprüft und danach darauf vertraut wird, daß das konkret eingesetzte Exemplar sich nicht signifikant von dem Muster-Trojaner unterscheidet, ist nicht ausreichend. Ein solches Vorgehen wäre auch technisch unsinnig, denn die Spionagesoftware wird regelmäßig den in der IT-Sicherheit üblichen Abwehrmechanismen für Schadsoftware entgegenwirken und kontinuierlich angepaßt werden müssen, dabei aber gleichzeitig seine Detektion durch den Nutzer vermeiden.

Da nach Angaben der Ermittlungsbehörden jeder Trojaner speziell für den jeweiligen Einsatz zusammengebaut wird, ist das Risiko groß, daß durch Fehler oder Absicht Funktionsmodule integriert oder aktiviert werden, die über das zugelassene Maß hinausgehen. Dabei ist nicht nur an Software für den Mitschnitt von Skype-Telefonaten zu denken, was häufig als Beispiel vorgebracht wird, sondern auch an Trojaner, die andere Formen der Kommunikation direkt auf informationstechnischen

Geräten abgreifen. Daher ist es für jede Form der Quellen-TKÜ 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 also möglich sein.

Die Beschreibung der Anforderungen an den Trojaner müßten zunächst sehr genau formuliert sein, um die Grundrechte der Spionageopfer über eine wasserdichte Präzisierung des Funktionsumfangs zu schützen und im Falle einer Quellen-TKÜ zu gewährleisten, daß nur die Daten der Kommunikation mitgeschnitten werden. Das gilt in gleicher Weise, wenn Konzeption, Gesamtarchitektur und Programmierung eine Eigenentwicklung des BKA sein sollte. Um aber eine richterliche Vorabprüfung sinnvoll durchführen zu können, ist das allein nicht ausreichend. Denn neben der Beschreibung, was der Trojaner können, vor allem aber nicht dürfen soll, muß der konkrete Plan des Einsatzes dokumentiert stattfinden. Daß die Spionagesoftware strukturell gegen die Sicherheit des Systems des Nutzers arbeitet, muß dabei einkalkuliert werden. Dabei ist sicherzustellen, daß nur die Bedarfsträger die ausgeleiteten Daten sehen können und daß sich nicht auch andere Programme auf dem infiltrierten System befinden, die dem installierten Trojaner Daten unterschieben könnten.

## Fazit

Der Einsatz staatlicher Trojaner wird neben den Folgen für den einzelnen Verdächtigen auch gesellschaftliche Auswirkungen haben, die sich aus der Schwarzmarkt-Problematik ergeben, die beim Kauf von Sicherheitslücken unvermeidbar ist.

Die Struktur der florierenden Schwarzmärkte, auf denen heute Sicherheitslücken für informationstechnische Systeme zum Kauf angeboten werden, wird durch das steigende Interesse staatlicher Behörden am Erwerb dieser ausnutzbaren Schwachstellen zum Nachteil aller Computerbenutzer verändert. Auch das BKA wird sich solcher Grau- und Schwarzmärkte und den hier agierenden fragwürdigen Dienstleistern bedienen müssen, da es selbst keine ausreichende Expertise hat, um stets aktuelle und funktionierende Sicherheitslücken in informationstechnischen Systemen zu entdecken und dafür sog. Exploits zu bauen, also funktionierende Angriffswege, die sich aus der Lücke ergeben. Damit stimuliert und finanziert das BKA einen Markt und setzt zugleich eine Incentivierung, diesen Schwarzmarkt noch zu

vergrößern. Dieser evidente Zielkonflikt ist nicht auflösbar und ganz praktischer Natur, da das BKA nach geltendem deutschen Recht gegen Anbieter solcher Exploits ermitteln müßte.

Unabhängig davon wird auch ein weiterer Zielkonflikt ersichtlich: Bekanntgewordene Sicherheitslücken sollten zum Schutze der eigenen Wirtschaft und Behördeninfrastruktur schnellstmöglich behoben werden, da die Wahrscheinlichkeit nicht sehr hoch ist, daß nur das BKA sie ausnutzen kann. Diese Einfallstore dürften regelmäßig auch weiteren Personenkreisen bekannt sein. Insgesamt steht das Bezahlen und Stimulieren der Schwarzmärkte für IT-Sicherheitslücken sowohl dem Gemeinwohlinteresse als auch den Interessen der Wirtschaft entgegen. Ganz besonders brisant wird dieser Interessenkonflikt im Lichte der Mitarbeit des Bundesamtes für Sicherheit in der Informationstechnik am öffentlich gewordenen Staatstrojaner.[6] Das BSI soll einerseits Bürger und Unternehmen als unabhängige Instanz in Sachen IT-Sicherheit zur Verfügung stehen, arbeitete aber heimlich unter dem Dach und im Sinne des Innenministeriums an der Ausnutzung von Sicherheitslücken für den Staatstrojaner mit.

## Gesamtüberwachungsrechnung

Das BKA-Gesetz erlaubt nicht nur den verdeckten Zugriff auf Computer und andere informationstechnische Systeme und die hier gespeicherten Daten, sondern enthält zahlreiche weitere Überwachungsmaßnahmen technischer und nicht-technischer Natur.

Elektronische Kommunikation ersetzt immer häufiger das intime Gespräch. Macht man die vom Bundesverfassungsgericht angeregte Gesamtüberwachungsrechnung auf, so ist auf die staatliche Trojanisierung nicht nur aufgrund der technischen Unwägbarkeiten und der unvermeidbaren Eingriffe in den Kernbereich privater Lebensgestaltung der Betroffenen zu verzichten, sondern auch, weil neben den Telekommunikationsdaten auch der gesamte Datenbestand des Computers potentiell offenliegt. 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 grundrechtliche Einhegung der Trojaner-Wanze wird außerdem erschwert, da sie nicht nur heimlich, sondern auch dauerhaft auf dem Computer hinterlassen wird und absichtlich Zugangssperren, Paßwörter und Detektoren überwindet. Die

---

[6] Andre Meister: „Geheime Kommunikation: BSI programmierte und arbeitete aktiv am Staatstrojaner, streitet aber Zusammenarbeit ab“, netzpolitik.org, 16. März 2015, https://netzpolitik.org/2015/geheime-kommunikation-bsi-programmierte-und-arbeitete-aktiv-am-staatstrojaner-streitet-aber-zusammenarbeit-ab/

Problematik der Kernbereichsrelevanz und des technischen Kollateralschaden-Risikos bei der Infiltration spezifischer informationstechnischer Systeme erfordert, daß auch für die Quellen-TKÜ eine dem sog. Großen Lauschangriff äquivalente Form der Abwägung und Kernbereichsprognose vor der Infiltration vorausgeht. Der staatlichen Trojanisierung sind jedoch prinzipiell grundrechtsschonende Alternativen vorzuziehen.

## Definition eines „informationstechnischen Systems“

Obgleich sich seit der Entscheidung zur sog. „Online-Durchsuchung“ der Begriff „informationstechnisches System“ etabliert hat und richtigerweise davon zeugt, daß sich die staatliche Trojanisierung keineswegs nur auf PCs im engeren Sinne bezieht, eröffnet das BKAG Ermittlern mit der Verwendung des Begriffs ein weites Feld zur Infiltration von höchst unterschiedlichen Systemen, auch solchen, deren Existenz wir derzeit noch nicht kennen können. Es erscheint daher angemessen, bestimmte informationstechnische Systeme von der Trojanisierung auszuschließen und die Begrifflichkeit im Gesetz deutlich enger zu fassen. Zu denken wäre etwa an Fahrzeuge, die heute und vor allem in Zukunft fahrende Kommunikationssysteme sind, oder an medizinische Systeme. Die Infiltration bei solchen Systemen kann konkret die Gesundheit von Personen und sogar Menschenleben bedrohen, da Funktionsstörungen nach einer Infiltration nicht ausgeschlossen werden können. Entsprechend darf dem BKA die Infiltration solcher Systeme prinzipiell nicht erlaubt sein, unabhängig davon, ob es sich um eine sog. „Online-Durchsuchung“ oder eine Quellen-TKÜ handelt.