Virtueller Einbruch – Update des Staatstrojaners

Verschriftlichung des Vortrags von Constanze Kurz

Das erste höchstrichterliche Urteil zum Staatstrojaner stammt schon aus dem Jahr 2008. Seither konnten keine Bundesregierung und kein Innenminister von dem Vorhaben lassen, zu versuchen, das staatliche Hacking in das Arsenal der Ermittlungswerkzeuge aufzunehmen.

In der letzten Legislaturperiode nun wurde der Staatstrojaner als normales Ermittlungsinstrument für Dutzende Straftaten erlaubt. Die technisch ziemlich komplexe Aufgabe, einen Staatstrojaner zur Anwendung zu bringen, bereitet den Behörden bis heute Probleme. Und viele ungelöste Fragen bestehen vor und beim Einsatz der Schadsoftware noch immer. Der Vortrag gibt einen Überblick über den Stand der Dinge bei deutschen Staatstrojanern und spart natürlich auch nicht mit Forderungen, was zu tun wäre.

Im Folgenden möchte ich tatsächlich ein Update geben. Dabei habe ich mir ein lustiges Wortspiel erlaubt, denn „Update des Staatstrojaners" kann man natürlich auch im technischen Sinne verstehen und der Kampf um diese Schadsoftware dauert inzwischen zehn Jahre. Ich will aber nicht die gesamte Geschichte abreißen, sondern mir geht es um folgende Fragen: Wo stehen wir zur Zeit in Bezug auf den Staatstrojaner und welche Entwicklungen haben sich in jüngster Zeit ergeben? Wie sind die politischen Entscheidungen und die des Gesetzgebers gefallen?

Vorgeschichte: Bundesverfassungsgerichtsurteil von 2008

Ich möchte nicht verhehlen, dass ich selbst Teil dieser Entwicklung war. Mehrmals war ich Sachverständige bei Staatstrojanern, bin erklärter Gegner von Staatstrojanern, habe aber auch gute Argumente, die ich im Rahmen dieses Updates darstellen werde. Der Begriff des „virtuellen Einbruchs" im Titel ist natürlich eine etwa so blöde Metapher wie der der „Online-Durchsuchung". Denn ein Einbruch zeichnet sich in der Regel nicht dadurch aus, dass man eine dauerhafte Schadsoftware auf einem System hinterlässt oder dass man die Tür für einen Dritten offen lässt. Ich bitte daher, den etwas unkorrekten Titel zu entschuldigen.

Über die folgenden Dinge werde ich nicht reden: Ich werde nicht nochmal zum 27. Februar 2008 zurückgehen, an dem das erste Urteil zum Staatstrojaner gefallen ist. Ein sehr wichtiges Urteil, das ich auf gar keinen Fall geringschätzen möchte. Denn in diesem über zehn Jahre alten Urteil haben wir ein neues Grundrecht geschenkt bekommen: das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Auf dieses Grundrecht werde ich mehrfach zu sprechen kommen.

Ausgangspunkt: Staatstrojaner-Hack von 2011

Mein Ausgangspunkt wird aber – damit ein paar Jahre der Entwicklung des Staatstrojaners gekürzt werden können – der Staatstrojaner-Hack vom Oktober 2011 sein. Auf den Hack selbst brauche ich nicht im Detail einzugehen. Wer das möchte, kann zwei technische Berichte von uns dazu lesen, die sehr genau sind. Wie sich herausstellte war die damals relativ weit verbreitete Software der hessischen Firma Digitask nicht nur handwerklich unterirdisch schlecht, sie eröffnete auch Dritten die Möglichkeit, die Schadsoftware mit zu nutzen. Ihr Hauptproblem aber war, dass die rechtlichen Grenzen, die damals gesetzt waren, mit dieser Software nicht eingehalten werden konnten. Dies hatte neben der politischen Diskussion – wir hatten ja die Binaries eines dieser Staatstrojaner veröffentlicht – auch einige konkrete Folgen, auf die ich kurz zu sprechen kommen möchte, um zu vergleichen, was tatsächlich in der Folge umgesetzt wurde.

Zum einen wurde eine standardisierende Leistungsbeschreibung erdacht. Eine interessante Sache, die es davor offenbar nicht gegeben hatte. Digitask war zwar bereits seit 2001 als technischer Dienstleister zertifiziert, man hatte aber offenbar keine Form von Pflichtenheft oder anderer standardisierender Leistungsbeschreibung erstellt. Nun wurde also versucht, technisch zu spezifizieren, was dieser Staatstrojaner eigentlich können soll und wie er technisch umzusetzen sei, damit die gesetzlichen Grenzen nicht überschritten werden.

Zum anderen entschied man sich für eine BKA-Eigenentwicklung. Anders als heute ging es damals immer nur um das BKA und um Fälle schwerer Verbrechen, insbesondere Terrorismus. Tatsächlich ist bis heute der internationale Terrorismus im BKA-Gesetz die Klammer für den Einsatz des Staatstrojaners. Das betrifft nicht einmal den NSU, sondern nur internationalen Terrorismus. Diese Beschränkung hat sich in der letzten Zeit, besonders in den letzten zwei Jahren, komplett aufgelöst. Tatsache ist etwa, dass der Einsatz des Staatstrojaners in einigen geplanten oder schon verabschiedeten Landespolizeigesetzen vorgesehen ist. Darauf komme ich später zurück.

Ich habe also diesen Ausgangspunkt gewählt, weil er ein politisch entscheidender Punkt war. Damals kamen relativ viele Informationen über den tatsächlichen praktischen Einsatz von

Staatstrojanern heraus. Dies auch, weil die Opposition in vielen Landtagen kritisch nachfragte und es in Bezug auf die politische Kommunikation noch eine andere Zeit war. Heute ist es wesentlich so, dass die Bundesregierung gar nichts mehr sagt. Alles ist nunmehr *national security* und die Herausgabe zu vieler Informationen an die Öffentlichkeit würde vorgeblich dem Projekt des Staatstrojaners zuwiderlaufen.

Kommerzielle Anbieter

Neben der BKA-Eigenentwicklung gab es aber auch noch einen anderen Strang, der besonders für die technische Weiterentwicklung des Staatstrojaners wichtig wird. Man hatte sich nämlich entschlossen, trotz der Eigenentwicklung auch bei kommerziellen Anbietern einzukaufen und über Firmen haben wir im Laufe der Zeit (immerhin von 2011 bis heute, also 2018) viel mehr Informationen sammeln können. Dies zum einen, da Gruppen – und hier ist insbesondere das Citizen Lab aus Kanada zu nennen – sehr detaillierte Berichte über staatliche Hacking-Software erstellt haben. Zum anderen hat die Presse mehr über die Überwachungsindustrie recherchiert.

Wir wissen also mehr über diese Anbieter und ihre Produkte. In Deutschland ist das insbesondere *FinSpy* der Firma FinFisher. Sehr schön passend zum zehnjährigen Jubiläum des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität kommunikationstechnischer Systeme wurde im Februar dieses Jahres dieser kommerzielle Trojaner freigegeben. Ob er tatsächlich eingesetzt wird, ist unbekannt. Wer also über ein Exemplar davon verfügt, wird um Übergabe gebeten. Seitdem ist es auf jeden Fall möglich, dass das BKA diesen Trojaner einsetzt. Offenbar erfüllt er die Anforderungen. Überprüfbar ist das nicht, von keiner Behörde, denn nach wie vor ist es auch nicht vorgesehen, dass diese kommerziellen Partner den Quellcode der Software herausrücken.

Auch den Aufsichtsbehörden – namentlich der für das BKA zuständigen Bundesbeauftragten für den Datenschutz – ist der Einblick verwehrt. Falls jemand Lust hat, sich etwas über die Firma FinFisher zu informieren: die haben ganz sicher Blut an ihren Händen. Die haben wenig Hemmungen mit den Diktaturen dieser Welt zusammenzuarbeiten und mittlerweile ist über die eine Menge bekannt. Die Bundesregierung hat dies bisher in keinster Weise dabei gestört, FinFisher als Geschäftspartner überhaupt in Erwägung zu ziehen und letzlich mit ihnen ins Geschäft zu kommen.

In den Landtagen verhält es sich etwas anders. Ich war auch in einigen Polizeigesetzgebungsprozessen Sachverständige und mein Eindruck war, dass in den Landtagen einige (auch regierende) Parteien sehr wohl Bedenken haben, mit solchen Firmen ins Geschäft zu kommen. Eine konkrete Regelung, die das untersagen würde, hat allerdings keines der bereits beschlossenen oder im Entwurf befindlichen Landespolizeigesetze enthalten.

Das bedeutet, dass dieser zweite Strang weiterhin existiert, der hinsichtlich der technischen Potenz in einer anderen Liga spielt. Das ist eine in vielen Beispielen getestete Software, die in Videos, wo sie beworben wird, wie in Verkaufsveranstaltungen lamadeckenartig vertickt wird. Ich glaube es gibt ein anderes Geschäftsfeld, wo man in diesen Hacking- und Überwachungsfirmenmarkt auch staatliche Gelder investiert.

Das Urteil zum BKA-Gesetz …

Ich möchte zum zweiten Urteil kommen. Die meisten werden wissen, dass es ein weiteres Urteil zum Staatstrojaner gab, allerdings in einer in verschiedener Hinsicht anderen Konstellation als zehn Jahre zuvor. Es gab auch hier eine lange Anhörung und man hat auch wieder technische Sachverständige angehört, was nicht selbstverständlich für ein Gerichtsverfahren ist, bei dem natürlich zuvörderst die juristische Perspektive interessiert. Die Anhörung dauerte sechseinhalb Stunden. Das BKA-Gesetz, das im Mittelpunkt des Rechtsstreits stand, war hochkomplex und wies neben dem Staatstrojaner sehr viele weitere Elemente auf, die enorm umstritten waren. Darunter auch andere technische Überwachungsmaßnahmen, die Übermittlung von Überwachungsdaten ins Ausland, aber auch die Frage des internationalen Terrorismus, der sich wie eine Klammer um dieses BKA-Gesetz herum befindet, und seine Definition.

Ich würde sagen, dass sich ungefähr ein Drittel der Anhörungen nur mit dem Staatstrojaner beschäftigt hat und zwar in beiden Varianten. Diese beiden Varianten, die Quellen-TKÜ (Quellen-Telekommunikationsüberwachung) und die Online-Durchsuchung, gibt es nach wie vor. Sie unterscheiden sich darin, dass die Onlinedurchsuchung uneingeschränkt das gesamte informationstechnische System durchleuchtet und daraus Daten ausleiten kann, während die Quellen-TKÜ ihre Grenze in der laufenden Kommunikation hat, zumindest annähernd. Das Urteil ist in Bezug auf den Staatstrojaner in beiden Varianten enttäuschend, weil es keine weiteren Sicherungen enthält, die an das Urteil von 2008 anschlössen und weil es letztlich die Festlegung manifestiert, dass es angeblich zwei verschiedene Arten von Staatstrojanern gäbe – nämlich einen für das Gesamtsystem und einen weiteren für die laufende Kommunikation.

Mir ist, generell gesagt, schon damals sehr aufgefallen, dass dieses Urteil einen gewissen Zeitgeist ausdrückt. Der Minister Thomas de Maizière ist, was nicht häufig vorkommt, selbst vor Gericht erschienen und hat eine sehr emotionale Rede für technische Überwachungsmaßnahmen im Fall des internationalen Terrorismus gehalten, die das Verfahren aus meiner Sicht stark beeinflusst hat. Dies nicht nur, weil er selbst Jurist ist, sondern auch weil er die Gefahren und den ganzen Zeitgeist, der sich mit der Terrorismusabwehr verbunden hat, sehr dezidiert vorgetragen hat. Man hat sehr deutlich gemerkt, dass der verhandelnde Senat nicht mehr derselbe war wie zehn Jahre zuvor unter Hans-Jürgen Papier und dem Berichterstatter Hoffmann-Riem. Das drückt sich auch im Urteil klar aus. Zwischen den Zeilen ist zu lesen, dass man im Falle von Terrorismus eigentlich Verständnis für Staatstrojaner habe. Das hat sich sehr gewandelt und war hier sehr greifbar. Der Wandel deutete sich vorher schon an. In der Verhandlung zum Anti-Terror-Gesetz, an der ich ebenfalls teilnahm, etwa zum Thema der Datenbank, die sich mit der Terror-Datei verbindet, hatte man das auch schon gemerkt, aber hier viel deutlicher.

Ein weiteres Problem war, dass es sich um ein fünf Jahre währendes, sehr komplexes Verfahren handelte. In der Verfassungsbeschwerde wurden sehr viele verschiedene Punkte angeführt und da eine neue Regierung an der Macht war, die das Gesetz gar nicht gemacht hatte, wurde die Politisierung sehr schwer. Die politische Diskussion war aus meiner Sicht auch schwieriger als beim Urteil zuvor.

Ein Vorteil war allerdings, dass die Öffentlichkeit viel besser als 2007/2008 darüber informiert war, was so ein Trojaner eigentlich bedeutet und was er kann. Damals hatten ich und die anderen Sachverständigen vor allem erklärbärt. Nun war die Öffentlichkeit schon aufgrund der Tatsache, dass man in jeder Zeitung über Schad- und Spionagesoftware lesen kann, viel besser informiert.

Das Verfahren bekam große Aufmerksamkeit, aber im Ergebnis ist zumindest für die Varianten des Staatstrojaners wenig gewonnen. Zwar sind Teile des BKA-Gesetzes verfassungswidrig und der Gesetzgeber musste Änderungen vornehmen, aber er hat sicherlich ein schwächeres Signal als 2008 erhalten.

… und seine politischen Folgen

Ich möchte damit zu den politischen Folgen kommen. Das ist mir sehr wichtig. Der damalige Innenminister de Maizière hat sich noch am selben Tag vor die Presse gestellt und mehrfach betont, dass er dieses Urteil vollumfänglich ausnutzen wolle, im Sinne einer Kopiervorlage. Er wolle die von Karlsruhe gesetzten Grenzen unmittelbar in ein neues Gesetz gießen, was dann an sich auch geschehen ist. Es ist heute noch umstritten, ob das dann erarbeitete BKA-Gesetz verfassungsgemäß ist. Vor allem aber umstritten ist die Übernahme dieser Grenzen in die Landespolizeigesetze und die Strafprozessordnung.

Ich möchte das noch einmal hervorheben: im BKA-Gesetz ging es um die Abwehr des internationalen Terrorismus, das ist die Klammer um dieses Gesetz. Was die Staatstrojanerregelung in der StPO aber auch in den Landespolizeigesetzen betrifft, haben wir uns von Terrorismus längst weit entfernt. Besonders hervorheben möchte ich das PAG in Bayern. Das ist bereits beschlossen und es hat eine gewisse Relevanz für uns alle, denn unser Heimatminister ist ja Bayer. Der mag als politische *Lame Duck* und als nicht mehr ernst zu nehmen gelten. Aber er plant mit seinen Kollegen zusammen dieses PAG als Mustervorlage für ein Musterpolizeigesetz aufzunehmen. So hat er dies gesagt.

Glücklicherweise äußert sich Seehofer derzeit nicht zu diesem Feld. Er ist ja eigentlich ein sehr monothematischer Minister. Dies kann durchaus von Vorteil sein, denn zum Südkreuz oder zu anderen Fragen, die technisierte Überwachung angehen, sagt er wenig. Mal sehen, wie dies nach der Bayernwahl aussehen wird.

Die Justizministerkonferenz hat über dieses Muster-PAG schon gesprochen, das dann natürlich auch bedeuten würde, dass alle Bundesländer eine vergleichbare Version bekommen würden, die jeweils beide Varianten des Staatstrojaners enthielte. Seehofer hat seine diesbezügliche Drohung wahr gemacht.

Was aus meiner Sicht auch ein Teil des Zeitgeistes ist: Die Grenzen, die Karlsruhe setzt, werden tatsächlich wortwörtlich als Kopiervorlagen für Gesetze genutzt. Man geht also genau bis an die Grenze, was ich gerade im Überwachungsgesetzgebungsumfeld als ausgesprochen beunruhigend empfinde.

Die Strafprozessordnung hebe ich besonders hervor, weil sie in einem in vielerlei Hinsicht interessanten Prozess zustande gekommen ist. Selten habe ich für eine so weitreichende und seit Jahren umstrittene Regelung so eine Art der beschleunigten Gesetzgebung gesehen. Die Regelung für den Staatstrojaner kam hinten herum und in einer ganz anderen Regelung, nämlich dem „Gesetz zur effektiveren und praxistauglichen Ausgestaltung des Strafverfahrens". Es gab heftige Kritik, aber die beiden Regierungsparteien haben sich in der Sache dazu kaum geäußert. Von der Bundesbeauftragten für den Datenschutz, die ja sonst kein Wort sagt, sich aber wenigstens hier dezidiert geäußert hat, gab es einen harschen Brief. In der Anhörung gab es keinen einzigen Sachverständigen, der nicht massive Kritik übte. Dennoch wurde diese enorme Erweiterung des Einsatzes des Staatstrojaners ohne viel Federlesen durchgewunken.

Die Erweiterung betrifft Dutzende Arten von Verbrechen bis hinunter zu Urkundenfälschung oder Verstößen gegen das Betäubungsmittelgesetz. Vergehen also, die sich weit unterhalb jener Schwelle befinden, über die wir eigentlich immer geredet hatten: schwerste Verbrechen, die die Bundesrepublik in ihrem Bestand gefährden, die Terrorismusbezug haben oder zumindest das Leben oder die Gesundheit der Menschen ernsthaft gefährden.

Ich habe ehrlich gesagt noch nie einen parlamentarischen Prozess erlebt, in dem mit solcher Rigorosität solche weitreichenden Befugnisse durchgesetzt wurden. Ich habe noch nie wie in diesem Prozess erlebt, wie die Stellungnahmen und Sachverständigen, die sich der Bundestag herbeigezogen hatte, mit Ignoranz behandelt wurden.

Im Detail und um den Kern herauszuheben lässt sich sagen: Das eine ist die Quellen-TKÜ. Sie wird im Wesentlichen wie eine allgemeine Telekommunikationsüberwachung behandelt. Ich will kurz den Unterschied klarmachen. Eine normale TKÜ, in der Regel eine Telefonüberwachung, wird mit Hilfe des Anbieters durchgeführt, durch standardisierte Abhörschnittstellen, die in Deutschland und Europa verbreitet sind. Man nimmt also sozusagen die Kommunikation beim Anbieter ab. Das ist natürlich ein großer Unterschied zu der Situation, in der ich das Gerät, auf dem die Kommunikation stattfindet, hacke. Diese Gleichstellung ist in vielerlei Hinsicht kritisiert worden und auch technisch dämlich.

Risiken

Über die Jahre hat sich eine Risikodiskussion entfaltet. Da geht es um ganz verschiedene Bereiche und Fragen wie: sollte der Staat mit unseren Steuergeldern überhaupt für so eine Form von Sicherheitslücken bezahlen? Für kommerzielle Trojanerpartner? Oder generell für die Unterstützung einer ganzen Industrie, die darauf basiert, Sicherheitslücken möglichst lang geheim zu halten, um daraus ein Geschäft zu machen? Sollten wir das unterstützen? Ist das, in einer etwas weiteren Perspektive betrachtet, nicht eigentlich ein Nachteil für die Innere Sicherheit? Kann man in einer Zeit, in der viel über Milliardenschäden durch Trojaner, namentlich NotPetya und WannaCry, bekannt wird und man in Betracht zieht, welche Risiken man in Kauf nimmt, wenn man in diesen Markt investiert, diesen politischen Weg überhaupt noch weitergehen?

Wieso glauben Polizeien, seien es Landespolizeien oder BKA, dass sie besser seien als die NSA und die CIA, deren kompletter Trojanerschrank abhanden gekommen und ins Netz gewandert ist? Wieso glauben die eigentlich, sie könnten das besser? Wer kann eigentlich überprüfen, welche Versprechungen die kommerziellen Partner machen?

Vom Kernbereich der privaten Lebensgestaltung zur IT-Sicherheitsdiskussion

An diesen Risiken hängen eine Menge verschiedener Probleme, die sich aus meiner Sicht über die Jahre verändert haben. Die Diskussion hat sich mehr auf die Risiken fokussiert, was aus meiner Sicht ein Nachteil ist. Natürlich bin ich ein Hacker und sehe das alles stärker aus der Angreifer-Perspektive, aber die ursprüngliche Diskussion drehte sich um etwas anderes, nämlich um den Kernbereich der privaten Lebensgestaltung, unsere Intimsphäre. Ich möchte betonen, dass es einen Unterschied zwischen Privatsphäre und dem Konzept des Kernbereichs der privaten Lebensgestaltung, also dem innersten hochpersönlichen Kern einer Persönlichkeit, in die hier eingegriffen wird, gibt. Darum drehte sich die Diskussion eigentlich einmal. Da redete man über das ausgelagerte Gehirn und darüber, wie der Alltag und auch die Geschichte der Menschen in technische Artefakte eingehen und wer unter welchen Umständen darauf zugreifen darf.

Die IT-Sicherheitsdiskussion, die aus meiner Sicht sehr wichtig ist, hat das auf gewisse Art und Weise überlagert. Ebenso die Frage, wie weit eigentlich diese Geräte Extension unserer Körper sind und wie viel wir denen eigentlich anvertrauen. Was sagt eigentlich das Grundrecht, wenn es über eine Gewährleistung der Integrität und Vertraulichkeit redet, wenn wir immer nur darüber reden, auf welchem Wege sie hintenrum reinkommen? Und wie totalitär ist diese Ansicht, dass es keine Form der Kommunikation geben darf, die geschützt ist?

Letztere Ansicht stammt aus der Debatte um das „Going Dark", die ja noch parallel dazu lief und die ursprünglich im US-amerikanischen Raum debattiert wurde, sich aber auch bei uns sehr verbreitet hat.

Ich finde, das ist eine schwierige Diskussion, die man unbedingt hätte führen müssen, als die StPO im Gesetzgebungsprozess war, die aber einfach abgewürgt wurde. Das heißt nicht, dass es nicht auch einen gewissen juristischen und akademischen Streit gibt und eine Menge Papiere und Techniker, die darüber geschrieben haben. Aus meiner Sicht ist das aber im politischen Prozess in keiner Weise so reflektiert besprochen worden, wie es nötig gewesen wäre.

Ich möchte eine kleine Ausnahme machen, die auf das BKA-Gesetzurteil zurückgeht. Bei der Online-Durchsuchung, also jenem Trojaner, der alle Aspekte der Festplatte betrachten darf und auch ausleiten dürfte, hat man als Hürde den Verdacht auf eine besonders schwere Straftat und wesentlich die Schranken des großen Lauschangriffs gesetzt. Das bedeutet ganz praktisch, dass es zu diesen Online-Durchsuchungen in der StPO nur im äußersten Ausnahmefall kommen kann. Zur Erinnerung: der Streit um den großen Lauschangriff, war der um die Wanze im Schlafzimmer. Da ging es also auch um den Kernbereich der privaten Lebensgestaltung. Man hat hier sehr hohe juristische Grenzen gesetzt und die werden auch tatsächlich beachtet. Das kann man in Statistiken gut nachvollziehen, die dokumentieren, wie selten große Lauschangriffe durchgeführt oder Wanzen in Wohnungen angebracht werden. Man darf also zumindest im Rahmen der StPO die Hoffnung haben, dass die Online-Durchsuchung nicht sehr häufig sein wird, was sich aber letztendlich erst mit der Zeit zeigen wird.

Verfassungsbeschwerden

Mittlerweile weiß man von vier anhängigen Verfassungsbeschwerden. Es könnte natürlich noch weitere geben, aber die vier sind die, die relativ viel Aufmerksamkeit erreicht haben. Sie fokussieren sich sehr stark auf die Quellen-TKÜ, die Online-Durchsuchung und ein paar nebensächliche Themen. Ein Teil davon ist im Netz nachlesbar und auch für Nicht-Juristen durchaus interessant.

Wir werden vor allem warten müssen, wie lange das Gericht braucht, um die Verfassungsbeschwerden zu behandeln. Ich habe aber eigentlich keine Zweifel, dass sie zumindest diese Fragen wieder aufrollen, weil im Gesetz einige Dinge erlaubt wurden, die sich mit früheren Urteilen nicht vertragen und gegen die Juristen eine sehr gute Argumentation vorgebracht haben. Ich glaube, die technischen Argumente sind nicht unwichtig. Sie finden sich auch in allen vier Verfassungsbeschwerden. Erfahrungsgemäß werden wir aber noch eine Weile warten müssen bis wir Ergebnisse bekommen. Zumindest ein Zurückstutzen würde mich allerdings nicht überraschen.

Technisches Wettrüsten

Für den allgemeinen Zeitgeist heißt das aber nicht viel. Es gibt noch eine andere Form der Entwicklung, die ich von der juristischen trennen will. Ich habe sie mal „Technisches Wettrüsten" genannt, wegen der Entscheidungen, die parallel dazu in Bezug auf Behörden oder Institutionen fielen, welche gegründet wurden, um eine Form der technischen Unterstützung zu leisten.

Hier ist insbesondere ZITIS zu nennen. Das ist eine Behörde, die ziemlich nah an der Bundeswehr-Uni angesiedelt ist und sozusagen als technischer Dienstleister fungiert. Sie soll nicht nur im Bereich „Angriff auf Verschlüsselungssysteme" oder „offensive Angriffsmethoden", sondern auch in anderen Bereichen wie etwa Forensik liefern. Man hat da tatsächlich – die haben da gar keine Scham – einen BND-Mann an die Spitze gesetzt, als sei das normal. ZITIS ist bisher faktisch noch im Aufbau. Sie haben mit dem Strukturaufbau begonnen und bisher wenig Inhalte geliefert, aber da wird sicherlich viel kommen, das dann natürlich geheim sein wird. Es wird wenig gesagt, obwohl sich der Chef von ZITIS einigen Diskussionen gestellt hat.

Eine andere Sache ist die Agentur für disruptive Innovation in der Cybersicherheit (AdIC). Mittlerweile nutzen Innen- und Verteidigungsministerium das Wort „disruptiv" nicht mehr. Diese Agentur ist sozusagen noch einen Zacken dreister, da eine Kooperation zwischen dem Verteidigungs- und dem Innenministerium in Deutschland nicht der Normalfall ist. Da geht es in diese Richtung „Hack-Back", die auch politisch etwas debattiert wird: in wieweit darf man gegen wen und unter welchen Bedingungen zurück hacken? Inwieweit betrifft dies Völkerrecht? Dazu gibt es auch eine interessante Studie der wissenschaftlichen Dienste des Bundestages: welche Entitäten in Deutschland dürfen das? Armee? Geheimdienste? Polizei? Das ist noch etwas im Fluss. Gesetzgebung gibt es bisher noch nicht. Die Agentur steht aber natürlich in diesem Zusammenhang. Die Darstellung, die von der Leyen und Seehofer dazu machten, war natürlich eine andere. In jedem zweiten Satz dieser Pressekonferenz haben die DARPA erwähnt, um eine Anleihe an die amerikanische

Agentur zu machen. Aber ehrlich gesagt konnte bei dieser Pressekonferenz eigentlich gar nicht so viel zu dem Thema rausgeholt werden, weil das direkt nach Chemnitz war. Wenn man sich allerdings ansieht, wie sich die Bundeswehr in der letztens Zeit zu CNO (ComputerNetworkOperation) positioniert, wenn man die Frage von Hack-Back und wer das eigentlich machen kann überlegt und dass die Agentur von beiden, vom Innen- und vom Verteidigungsministerium gegründet wurde, dann ist das schon ein relativ klares Zeichen der strukturellen Positionierung.

Die Rolle der Geheimdienste

Nun zu einem anderen Bereich: Wir haben da auch noch ein Geheimdienstproblem. Natürlich haben wir verschiedene Geheimdienstprobleme, aber wir haben auch eines, das mit dem Staatstrojaner verbunden ist. Aus meiner Sicht war diesbezüglich die Diskussion in Hessen am deutlichsten: In Hessen gab es das erste Landespolizeigesetz und gleichzeitig auch ein Update des Landesamts für Verfassungsschutz, in dem geheimdienstliche Trojaner enthalten waren.

Auch in Hessen gab es einen interessanten Streit. Sie hatten hier mehr als 20, sehr verschiedene Sachverständige geladen, die auch alle Stellungnahmen abgegeben hatten. Auch im hessischen Gesetzentwurf war sehr viel mehr als nur der Trojaner enthalten, aber es war der erste, in dem sie einen Staatstrojaner für Geheimdienste wollten. In Hessen haben sie ein ziemlich kleines Landesamt für Verfassungsschutz – und plötzlich sollten die hacken dürfen. Die fanden das völlig normal.

Zu meiner Überraschung hat sich der hessische Landtag im Ergebnis dagegen entschieden. Zwar darf die hessische Polizei jetzt hacken, aber für das Landesamt für Verfassungsschutz haben sie es nicht zugelassen. Da waren wir doch überrascht. Wahrscheinlich ist man als Sachverständiger schon gewohnt, dass die eigenen Stellungnahmen geschreddert werden, so dass man gar nicht mehr erwartet, dass sie dem tatsächlich folgen. Aber es gab auch eine relativ breite Kritik, die auch in die Zeitungen getragen wurde und eine Demo im Februar.

Im hessischen Gesetzentwurf ist aber darüberhinaus eine interessante Sache drin, die ich so noch nicht gesehen hatte: sie wollten in Hessen auch noch die Computer Dritter hacken. Man hat also eine Fortsetzungsregel für den Staatstrojaner drinnen gehabt, dergestalt, dass wenn die überwachte Person auch informationstechnische Systeme Dritter verwendet, die Online-Durchsuchungen auch auf diesen Computern Dritter durchgeführt werden können. Das war neu. Es gab natürlich auch eine Menge Kritik juristischer Art, aber tatsächlich ist diese Regelung drinnen geblieben, zwar nicht für die Geheimdienste, aber für die hessische Polizei.

Die Diskussion war insgesamt in Hessen etwas anders, denn Landtag ist nicht Bundestag. Das kann ich für alle Anhörungen sagen, bei denen ich bei Landespolizeigesetzen dabei war. Die Landtagsdiskussionen sind aus meiner Sicht sehr viel sachlicher als im Bundestag. Man merkt, dass die Abgeordneten der Regierungs- und Oppositionsseite oft wirkliches technisches Erkenntnisinteresse haben. Das kann ich im Bundestag selten feststellen. Dennoch bleiben diese Regierungs-/Oppositionsgräben, die man auch in Hessen gesehen hat.

Ich will aber beim Geheimdienst etwas anderes nicht verschweigen. Unser Heimatministerium, genauer ein Staatssekretär, tingelt jetzt durch die Lande. Durchs Informationsfreiheitsgesetz habe ich mal eine seiner Reden frei bekommen und darin wird auch Hacken für den Verfassungsschutz gefordert. Nun muss ich sagen, dass diese Rede von Staatssekretär Wittwer noch vor der Maaßen-Anomalie stattgefunden hatte. Möglicherweise würde man heute nicht mehr ganz so offensiv an das Bundesamt für Verfassungsschutz gehen, aber die Argumentation läuft etwa so: Die dürfen das doch jetzt alle, warum sollen wir das nicht auch dürfen? Es ist ja jetzt sozusagen breit in der Strafprozessordnung und in mehrere Landespolizeigesetze übergegangen, warum soll da der Verfassungsschutz jetzt nicht auch hacken?

So entsteht natürlich ein großes Problem. Schon bei der Polizei teilt die Regierung in der Regel nichts mit und es gibt nur wenige Möglichkeiten der Kontrolle. Wenn der Geheimdienst hacken wird, werden wir genau gar nichts darüber erfahren. Weder ob es eine Eigenentwicklung ist, noch ob es ein kommerzieller Partner ist oder wie oft gehackt wurde. Wir werden gar nichts erfahren. Das sind alles Bereichsausnahmen, wo wir davon ausgehen können, dass es überhaupt keine Form von öffentlicher Kontrolle gibt. Daher müssen wir sehr, sehr wachsam sein, ob sie diese Idee tatsächlich umsetzen. Wie sich das weiter entwickelt, das werden wir dann vielleicht nach der Bayernwahl sehen, wenn wir einen ernsthaften Innenminister haben. Die Selbstverständlichkeit, mit welcher die Geheimdienste in die Trojaner integriert werden, finde ich sehr beunruhigend.

Gesamtüberwachungsrechnung

Ich will natürlich die Gesamtüberwachungsrechnung aufmachen und habe schon angesprochen, dass sich die Diskussion verändert hat. Trojaner werden mittlerweile selbstverständlich für ganz andere Geräte entwickelt, mit einem sehr starken Fokus auf Mobilgeräte. Während sich die Diskussion am Anfang zum Beispiel um Skype auf Desktop-Computern gedreht hat, geht es heute längst um Tablet und Mobiltelefone. Sie haben auch schon angekündigt, dass sie Staatstrojaner auch für mobile Geräte haben. Das hat sich sehr verändert. Aber ich glaube, die gesamte Gesamtüberwachungsrechnung müssen wir neu aufmachen und auch stärker fordern. Das wird wenig getan. Das ist mir auch in den Landespolizeigesetzen sehr aufgefallen, dass man, wenn jemand – vielleicht auch zurecht – überwacht wird, nicht mehr die Gesamtheit der Überwachungsmöglichkeiten und verschiedenen Datensätze betrachtet, sondern alles nur noch einzeln. Und dieser Zeitgeist, dass es keine Art von Kommunikation geben dürfe, in die man nicht hineinschauen kann, ist aus meiner Sicht stärker geworden. Wir müssen das noch stärker betonen, dass wir technisierte Überwachung in ihrer Gesamtheit betrachten müssen und nicht immer nur vereinzelt.

Dazu möchte ich einen zweiten Punkt nehmen, der vielen bewusst ist, die sich damit beschäftigen, dass diese Überwachungsausweitung-Hackingindustrie ein richtig signifikanter Industriezweig geworden ist. Insbesondere durch die enormen Gelder, die aus dem Geheimdienstbereich dort hineinfließen und wo sich Deutschland anschickt, selber zu investieren. Das ist eine große Änderung, weil dadurch natürlich auch dieser Markt professionalisiert wird und letztlich die Schwachstellen in Software,

mit denen wir jeden Tag zu kämpfen haben, auf eine Weise ausgebaut werden, wie wir das vor ein paar Jahren noch nicht gesehen haben. Seit der Zeit des ersten Urteils zum Staatstrojaner, wo es diesen Markt noch gar nicht gab, hat er sich zu einem großen Gebilde ausdifferenziert.

Ich kann nur empfehlen, die Studie zu lesen, die Privacy International einmal im Jahr herausgibt, um sich klarzumachen, wie groß dieser Markt ist.

Ein Punkt, zu dem ich nicht allzuviel sagen möchte: Transaktionen werden Kommunikation. Dinge, die wir automatisieren in all den Geräten, die eher Handlungen sind, die kommen in eine solche Auswertung mit rein. Und die betreffen natürlich auch den Staatstrojaner. Niemand von euch würde mir sein Mobiltelefon geben. Und ich kann das verstehen. Aber dazu brauche ich nicht so viel sagen.

Gefährdung von Menschenleben

Ich möchte noch einen letzten Punkt machen, den ich vor allem in den Landtagen immer mit in die Sachverständigen-Gutachten hineingeschrieben habe. Es geht um den Punkt, dass sie dort keine Grenzen setzen. Der Begriff des informationstechnischen Geräts ist sehr breit und sie nehmen keine Rücksicht darauf, ob es sich dabei vielleicht um ein Gerät handelt, das die Gesundheit oder das Leben von Menschen gefährden kann. Das ist nicht erst ein Problem, seit wir diese Hacks wie z. B. beim Jeep gesehen haben, sondern ich glaube das muss man noch holistischer betrachten, wenn man die Art der informationstechnischen Geräte, die gehackt werden dürfen, staatlicherseits beschränkt.

Ich möchte dazu eine kurze Geschichte aus dem Landtag in Niedersachsen, also in Hannover, erzählen, wo es auch um diesen Trojaner ging. Ich hatte dort den Punkt angesprochen, als es um das Gutachten, das der CCC abgegeben hatte, ging. Und da entstand eine interessante Diskussion mit Doris Schröder-Köpf, die für die SPD dort drin sitzt. Ich hatte also erläutert, dass ich es für eine gute Idee hielte, wenn der Gesetzgeber hier eine Beschränkung einbauen würde und sozusagen sowas wie Medizinalgeräte oder Fahrzeuge, in denen Menschen sitzen, ausnimmt. Da sagte Doris Schröder-Köpf zu mir: „Ja, Frau Kurz, aber wenn wir das machen, dann steht es ja so im Gesetz und dann wissen ja die Verbrecher, dass sie darüber kommunizieren können." Ich musste erst kurz parsen, was sie eigentlich sagt und sagte dann: „Ahhhh, ich muss ihnen da was sagen: Falls sie angenommen haben, das staatliche Hacken ist so wie in US-Vorabendserien; das ist nicht der Fall. Es gibt ganz viele Geräte und Betriebssysteme, die sie nicht hacken können. Wenn sie also eine Ausnahme für Medizinalgeräte oder vielleicht für Fahrzeuge reinschreiben, heißt das noch lange nicht, dass es die einzige Ausnahme wäre, die irgendwelche Verbrecher ausnutzen können." Der Einwurf sagte mir etwas über diese Denke, die dahinter steckt. Er machte klar, dass sie nach wie vor nicht wissen, wovon sie reden, wenn sie von Staatstrojanern reden, sondern so eine Vorstellung haben wie im Fernsehen. Jedes Gerät sei zack-zack-zack zu hacken. Sie können sich auch nicht vorstellen, dass es sehr viele Betriebssysteme oder Geräte gibt, wo man nicht schnell reinhacken kann. Sie wollen keinen Bereich, und sei er sogar verbunden mit dem Leben und der Gesundheit von Menschen, auch nur potenziell ausschließen. Ich musste mich erstmal wieder fangen, als mir klar wurde, was sie da eigentlich fragte. Und das ist nur ein Beispiel. Mir geht es hier nicht um diese Person; mir geht es um die Denke. Das fand ich sehr gruselig.

Wir müssen wieder die richtige Debatte führen

Aber weil ich nicht so negativ enden will, habe ich ein kleines Zitat aus dem allerersten Urteil, das zehn Jahre alt ist. Ich möchte an etwas erinnern. Nämlich daran, dass schon vor zehn Jahren jene Verfassungsrichter, die uns das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme geschenkt haben, etwas anderes im Blick hatten:

Ich möchte endlich zu der Situation zurück, in der wir wieder über die beträchtliche Ausforschung reden und nicht nur über die Sicherheit und die Probleme, die sie damit haben. Ich möchte, dass wir auch darüber reden, was bereits in diesem Urteil in Bezug auf Beschlagnahmen steht, über die schon gar nicht mehr gesprochen wird. Und in Bezug auf die Mächtigkeit dieser Tools wünsche ich mir generell, dass wieder mehr die Perspektive der Potenz so einer staatlichen Hacking-Software in den Fokus rückt und auch die Tatsachen, die in den Urteilen stehen. Zum Beispiel jene Tatsachen, dass es nicht nur darum geht,

Constanze Kurz

Constanze Kurz ist promovierte Informatikerin, Autorin und Herausgeberin mehrerer Bücher, aktuell zum Cyberwar. Ihre Kolumne *Aus dem Maschinenraum* erscheint im Feuilleton der FAZ. Sie ist Aktivistin und ehrenamtlich Sprecherin des Chaos Computer Clubs. Sie forschte an der Humboldt-Universität zu Berlin am Lehrstuhl *Informatik in Bildung und Gesellschaft* und war Sachverständige der Enquête-Kommission *Internet und digitale Gesellschaft* des Bundestags und im Beirat des FIfF.

Dinge zu hacken, sondern dass durchaus auch dann der Kernbereich betroffen sein kann, wenn man einfach nur unsere Smartphones oder Festplatten beschlagnahmt. Ich wünsche mir, dass wir darüber wieder stärker reden, um eine Agenda zu haben, etwas, um dagegen zu halten und nicht immer nur zu reagieren, wenn sie schon wieder irgendeinen Gesetzentwurf in Landespolizeigesetzen oder im Bundestag haben.

Dies war ein wirklich ziemlich krampfhafter Versuch, aus der Entwicklung des Staatstrojanerproblems etwas Positives heraus zu extrahieren. Im Gesamtbild ist sicher klar geworden, dass wir beim Staatstrojaner einen relativ schlechten Stand haben. Aber falls jemand einen hat, nehmen wir den immer noch mit Freuden entgegen und werden die Binaries auch veröffentlichen. Ich bedanke mich für die Aufmerksamkeit.

Benjamin Kees, Rainer Rehak, Stefan Hügel

Jahresrückblick des FIfF

Eine freudige Panoramafahrt durch das FIfF-Jahr

In unserem Jahresrückblick stellten wir die wichtigsten Aktivitäten des FIfF seit der FIfF-Konferenz 2017 im Oktober 2017 in Jena dar. Mit Auszügen aus unseren Stellungnahmen, Pressemitteilungen und Beiträgen zur FIfF-Kommunikation illustrieren wir die Aktivitäten.

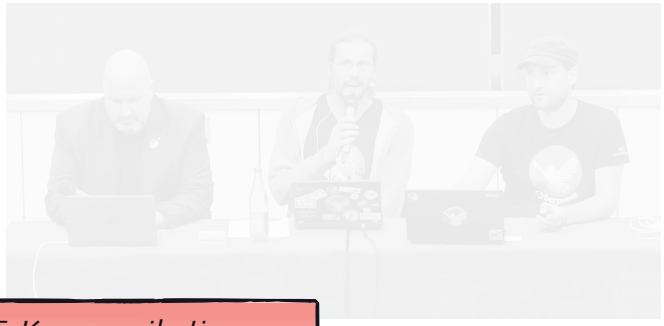
Oktober 2017

Startpunkt des FIfF-Jahres, über das hier berichtet werden soll, ist die **FIfF-Konferenz 2017**[1], die von Eberhard Zehendner und seinem Team organisiert wurde und am 20.-22. Oktober 2017 an der Universität Jena stattfand: *TRUST – wem kann ich trauen im Netz und warum?* In der Eröffnungsrede hieß es:

> *„TRUST – Vertrauen – ist die Basis, auf der unsere Gesellschaft aufgebaut ist. Wenn w[illegible] trauen können, funktioniert [illegible] – das gilt selbstverständlich a[illegible] Vertrauen wird heute im Netz [illegible] legal als auch legal. Wir müssen uns vor kriminellen Menschen schützen, die unser Vertrauen missbrauchen. Seit den Veröffentlichungen des Whistleblowers Edward Snowden wissen wir aber auch, dass Behörden unsere Kommunikation umfassend ausspähen. […] Dazu kommt der Datenhunger der Diensteanbieter, die ihre Geschäftsmodelle auf der Nutzung der Daten aufbauen und dies zum Beispiel durch für den Laien unverständliche Nutzungsbedingungen formaljuristisch legalisieren. Dem soll mit dem neuen europäischen Datenschutzrecht gegengesteuert werden – doch inzwischen wissen wir, dass gerade die deutsche Bundesregierung massiv versucht, dieses Recht aufzuweichen und zu bremsen. Auch damit wird Vertrauen zerstört."*

Im Rahmen der FIfFKon17 wurde der **FIfF-Studienpreis 2017** an Tobias Krafft verliehen: *Qualitätsmaße binärer Klassifikatoren im Bereich kriminalprognostischer Instrumente der vierten Generation*, so der Titel seiner Arbeit.

Bekanntlich fanden im September 2017 Wahlen zum Deutschen Bundestag statt. Die daran anschließenden Koalitionsverhandlungen zogen sich hin; lange sah es so aus, dass es zu einer christlich-ökologisch-liberalen Koalition kommen könnte (*Jamaika*-Koalition, so die etwas alberne Bezeichnung, die auf den Landesfarben Jamaikas basiert). Aus der Erwartung heraus, dass sich vor allem Bündnis90/Die Grünen und die FDP wieder stärker für Bürgerrechte einsetzen würden, wandten sich 23 Nichtregierungsorganisationen – unter ihnen das FIfF – mit einem **Offenen Brief zur**



Ben Kees beim Jahresrückblick

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Vorratsdatenspeicherung an deren Vorsitzende. Wir forderten sie darin auf, sich für eine Abschaffung der Vorratsdatenspeicherung von Telekommunikationsdaten einzusetzen. Heute wissen wir, dass es nicht zu einer solchen Koalition kam. Doch auch die Hoffnung auf eine bürgerrechtsfreundliche Politik von Bündnis90/Die Grünen und der FDP hat seither so manchen Dämpfer erhalten.

November 2017

Im Jahr 2016 hatten wir uns ausführlich mit dem Thema Transhumanismus beschäftigt – unter anderem mit zwei Schwerpunktausgaben der FIfF-Kommunikation. Der Beziehung des Transhumanismus zum Miltär widmeten wir uns in einem **Dossier für die Zeitschrift Wissenschaft & Frieden 4/2017**: *Transhumanismus und Militär*[2], das von Hans-Jörg Kreowski herausgegeben wurde.

Unsere Kontakte zur Tübinger Informationsstelle Militarisierung (IMI) konnte ebenfalls Hans-Jörg Kreowski durch einen eingeladenen **Vortrag beim IMI-Kongress**[3] *Der Informationsraum aus militärischer Sicht* vertiefen. Dem folgte eine Veröffentlichung in der IMI-Studie 2018/04 *Krieg im Informationsraum*[4].

Dezember 2017

Beim Friedensratschlag in Kassel waren wir 2017 leider nicht vertreten. Doch in der **Konferenzdokumentation zum Friedens-**