Gutachterliche Stellungnahme

zur Öffentlichen Anhörung zu den Entwürfen eines Zwölften Gesetzes zur Änderung des Brandenburgischen Polizeigesetzes – Gesetzentwürfe der Landesregierung sowie der Fraktion der CDU

Ausschuss-Drucksachen 6/9821 sowie 6/9828

im Ausschuss für Inneres und Kommunales des Landtages von Brandenburg

am 9. Januar2019

von

Dr. iur. Ulf Buermeyer, LL.M. (Columbia)

Richter am Landgericht Berlin
Vorsitzender der Gesellschaft für Freiheitsrechte e.V. (GFF)

ulf@buermeyer.de

Berlin, den 7. Januar 2019

We live in dangerous times, but we are not the first generation
of Americans to face threats to our security. Like those before us,
we will be judged by future generations on how we react to this crisis.
And by that I mean not just whether we win … but also
whether, as we fight that war, we safeguard for our citizens the
very liberties for which we are fighting.[1]

Robert Swan Mueller III
Director, Federal Bureau of Investigation

Vorbemerkung

Angesichts des erheblichen Umfangs des Gesetzgebungsvorhabens und der kurzen Bearbeitungszeit war es unerlässlich, für diese Stellungnahme Schwerpunkte zu setzen. Der Verfasser hat sich daher entschieden, sich auf die geplanten Rechtsgrundlagen zur Abwehr terroristischer Gefahren durch sogenannte „Staatstrojaner“ zu konzentrieren.

Wesentliche Ergebnisse

1. Die geplante Rechtsgrundlage zur Abwehr terroristischer Gefahren durch „Staatstrojaner“ ist gerade auch unter dem Aspekt der wirksamen Gefahrenabwehr verfehlt. Denn die intendierte Zuständigkeit der Polizei des Landes Brandenburg würde die bereits heute bestehende gefährliche Zersplitterung der Kompetenzen auf diesem Gebiet vertiefen. Sie droht daher die effektive Abwehr terroristischer Gefahren nicht zu befördern, sondern eher zu behindern.

---

1 Wir leben in gefährlichen Zeiten, aber wir sind nicht die erste Generation von Amerikanern, die sich mit Gefahren für ihre Sicherheit konfrontiert sieht. Wie die Menschen früher, werden auch wir von späteren Generationen danach beurteilt werden, wie wir auf diese Krise reagieren. Und damit meine ich nicht die Frage, ob wir gewinnen, sondern ob wir – während wir diesen Krieg führen – unseren Bürgern ebenjene Freiheiten bewahren, für die wir Krieg führen. – Zitiert nach https://archives.fbi.gov/archives/news/speeches/protecting-americans-against-terrorism (letzter Abruf: 6. Januar 2019), Übersetzung des Verfassers.

2. „Staatstrojaner“ sind ein außerordentlich eingriffsintensives Instrument. Gravierende Bedenken bestehen vor diesem Hintergrund insbesondere gegen die verfahrensrechtliche Ausgestaltung des Einsatzes von Staatstrojanern: § 28e des Entwurfs stellt in keiner Weise sicher, dass die von den Ermittlungsbehörden einzusetzende Überwachungs-Software Mindestanforderungen an die Datensicherheit und Resistenz gegen Manipulationsversuche erfüllen. Hier **fehlen Regelungen** sowohl **über die** an Staatstrojaner zu stellenden **technischen Anforderungen**, die wenigstens im Verordnungswege erlassen werden müssen, als auch über eine **obligatorische unabhängige Prüfung**, dass ein Staatstrojaner diese Anforderungen tatsächlich erfüllt.

3. Zudem schafft die beabsichtigte Norm ein massives Interesse für Sicherheitsbehörden, die Cyber-Sicherheit weltweit zu schwächen (!), um Systeme von Zielpersonen gegebenenfalls gem. § 28e des Entwurfs „hacken“ zu können. Die gesellschaftlichen Folgen einer solchen **Kultur der kalkulierten IT-Unsicherheit** können erheblich sein, wie etwa der Ausbruch des „wannacry“-Trojaners deutlich gemacht hat. Diese Fehlanreize sollten durch ein bisher **fehlendes Verbot der Ausnutzung von Sicherheitslücken** verhindert werden, die auch den Herstellern noch unbekannt sind. Hierzu wird unten ein Formulierungsvorschlag gemacht.

Einzelaspekte

Eine erschöpfende Stellungnahme zu einem 64 Seiten umfassenden und inhaltlich sehr komplexen Gesetzentwurf würde deutlich mehr Zeit erfordern, als zur Vorbereitung zur Verfügung stand. Hingewiesen werden kann daher nur auf ausgewählte rechtlich besonders bedenkliche Vorschläge oder sonst änderungsbedürftige Aspekte des Entwurfs der Regierungsfraktionen, während der Entwurf der CDU-Fraktion keine Berücksichtigung finden konnte. Zudem war es unabdingbar, Schwerpunkte setzen, wobei sich der Verfasser für den geplanten Einsatz von „Staatstrojanern" entschieden hat.

Ist eine Regelung in dieser Stellungnahme nicht ausdrücklich erwähnt, so ist dies daher keineswegs dahingehend zu verstehen, dass sie als unbedenklich anzusehen wäre.

I. Abwehr terroristischer Gefahren durch präventiven Einsatz von Staatstrojanern auf Landesebene im föderalen Kompetenzgefüge

Der Gesetzentwurf der Landesregierung verweist eingangs auf eine „angespannte Terror- und Gefährdungslage" sowie auf „die festgestellten Sicherheitslücken", die es zu schließen gelte, indem der Landespolizei besondere Vollmachten zur „Bekämpfung der Gefahren des Terrorismus" eingeräumt werden. Die Diagnose der Landesregierung soll an dieser Stelle nicht in Zweifel gezogen werden, obwohl auch insoweit die Kriminalstatistiken des Bundeskriminalamts, die eine beständig sinkende Kriminalität ausweisen, eher in eine andere Richtung deuten. Denn fraglich ist jedenfalls, ob – eine außergewöhnliche Bedrohungslage unterstellt – zusätzliche Kompetenzen gerade für die Landespolizei tatsächlich geeignet sind, eine solche Lage abzumildern.

Die Bekämpfung des Terrorismus ist beileibe keine neue staatliche Aufgabe, die sich in einem normativen Vakuum vollzöge. Im Gegenteil ist bereits die heutige Rechtslage von einer Vielzahl sich überlappender Kompetenzen gekennzeichnet:

- Im Vorfeld einer Gefahr sind sowohl das sogenannte Bundesamt für Verfassungsschutz als auch der Bundesnachrichtendienst für die Sammlung von Erkenntnissen über mögliche (zukünftige) terroristische Bedrohungen zuständig, vgl. § 1 Abs. 2 und § 6 Abs. 1 Nr. 1 BNDG, § 5 BVerfSchG.

- Für die Abwehr terroristischer Gefahren ist außerdem das Bundeskriminalamt umfassend zuständig, § 5 Abs. 1 BKAG, sofern eine Gefahr länderübergreifend ist – was angesichts der örtlichen Flexibilität terroristischer Gefährder und der Insellage des Landes Berlin inmitten des Landes Brandenburg jedenfalls in der Praxis der Brandenburger Polizei nahezu ausnahmslos der Fall sein wird. Außerdem liegt es in der Hand der obersten Landesbehörden, selbst im Falle einer nur auf ein Land beschränkten Gefahr das BKA um Übernahme zu ersuchen (§ 5 Abs. 1 Nr. 3 BKAG). Das BKA wiederum verfügt zur Abwehr der Gefahren des internationalen Terrorismus über einen umfassenden Katalog von Ermächtigungsgrundlagen (vgl. §§ 38 ff. BKAG), die spätestens nach der Umsetzung der Entscheidung des BVerfG durch die BKAG-Novelle des Jahres 2017 den verfassungsrechtlichen Rahmen lückenlos ausschöpfen dürften.

- Sobald der Anfangsverdacht einer Straftat vorliegt, ist die Zuständigkeit der Staatsanwaltschaften sowie – als deren Ermittlungspersonen – wiederum der Polizei eröffnet. Angesichts der inzwischen sehr weitgehenden Kriminalisierung bereits des Vorfelds terroristischer Gewalttaten ermöglichen auch die formal repressiven Ermächtigungsgrundlagen der Strafprozessordnung der Sache nach präventives Handeln weit im Vorfeld einer tatsächlichen Gefährdung von Rechtsgütern. Neben dem „Klassiker“ § 129a StGB (Terroristische Vereinigung) ist inzwischen insbesondere § 89a StGB (Vorbereitung einer schweren staatsgefährdenden Gewalttat) getreten, der vielfältige Vorbereitungshandlungen des Terrorismus erfasst. Zur Verfolgung dieser Vorfeldstraftaten bereits im Stadium eines einfachen, also möglicherweise noch sehr vagen Tatverdachts können Polizei und Staatsanwaltschaften auf die vielfältigen Eingriffsmöglichkeiten der Strafprozessordnung zurückgreifen, bis hin zum Einsatz von sogenannten Staatstrojanern (§§ 100a, 100b StPO) und der

akustischen Wohnraumüberwachung (§ 100c StPO). Damit können sie *de facto* auch zur Verhinderung von terroristischen Gewalttaten einschreiten, wenngleich ihr Handeln *de jure* der Durchführung und Sicherung eines Strafverfahrens gegen die Beschuldigten dient.

Hält man sich diese bereits bestehenden Kompetenzen vor Augen, so ist kaum ein Fall denkbar, in dem eine der Polizei des Landes Brandenburg zur Kenntnis gelangende terroristische Gefahr nicht bereits durch bestehende Kompetenzen abgewehrt werden könnte – sei es durch die Polizei unter Rückgriff auf repressive Ermächtigungsgrundlagen, sei es durch Behörden des Bundes, nachdem die Erkenntnisse der Polizei dem BKA mitgeteilt wurden. Vor diesem Hintergrund erscheint die vom Gesetzentwurf letztlich begründungslos postulierte „Sicherheitslücke" als weitgehend fiktiv, zumindest soweit sie zur Begründung des Einsatzes von „Staatstrojanern" herangezogen werden soll. Die Kompetenzen des geplanten § 28e werden vielmehr zu neuen Mehrfachzuständigkeiten führen.

Das bereits heute bestehende und durch die geplante Ermächtigungsgrundlage absehbar noch vertiefte Kompetenzwirrwarr bei der Abwehr terroristischer Gefahren ist dabei nicht nur eine Frage legislativer Ästhetik. Im Gegenteil *verringern* unklar abgegrenzte und mehrfach sich überlagernde Kompetenzen die Effektivität der Abwehr terroristischer Gefahren:

- Sie verringern zum einen den Anreiz, die weitere Bearbeitung einer möglichen Gefährdungslage an eine andere Behörde (insbesondere des Bundes) abzugeben, und führen damit zu einer Zersplitterung der Abwehr terroristischer Gefahren, bei der letztlich keine Stelle mehr über alle relevanten Informationen verfügt.

- Zum anderen erschweren sie auch die klare Zuordnung der Verantwortlichkeit im Falle behördlichen Versagens: Wenn viele Stellen irgendwie zuständig sind, ist in der Regel niemand mehr verantwortlich zu machen, wenn tatsächlich etwas „anbrennt". Der Fall Anis Amri zeigt mustergültig, wie die unklare Abgrenzung und Doppelung von Kompetenzen zwischen Bund und Ländern sowie zwischen Polizei,

Justiz und Diensten eine Aufarbeitung des – wenigstens vom Ergebnis her betrachtet – doch offensichtlichen Behördenversagens erschwert.

Vor diesem Hintergrund droht der Entwurf, entgegen seiner ausdrücklichen Zielsetzung die Abwehr terroristischer Gefahren im Gefüge der Bund-Länder-Kompetenzen eher zu erschweren. Statt die Polizei des Landes Brandenburg (halbherzig) mit einigen an §§ 38 ff. BKAG angelehnten Ermächtigungsgrundlagen auszustatten, sollte der Schwerpunkt auf die konsequente Übermittlung aller Terrorismus-bezogenen Erkenntnisse an das BKA sowie auf die Verfolgung möglicher terroristischer Straftaten auf der Grundlage strafprozessualer Ermächtigungsgrundlagen gelegt werden.

II. Einzelaspekte des Einsatzes von Staatstrojanern

1. Einführung

Der Entwurf der Landesregierung sieht mit Ermächtigungen für den Einsatz von sogenannten Staatstrojanern die weitgehendsten Eingriffe in Grundrechte vor, die zur Informationsgewinnung unter dem Grundgesetz zulässig sind. Denn durch Infektion der informationstechnischen Systeme von Beschuldigten soll die heimliche Auswertung der gesamten laufenden Kommunikation ermöglicht werden.

Dem Gesetzentwurf liegt die Überlegung zugrunde, dass sich der Einsatz eines Staatstrojaners auf bestimmte Inhalte beschränken ließe. Dies ist jedoch aus technischer Perspektive eine Fiktion: Wird ein informationstechnisches System mit einer Späh-Software infiziert, so ist die Integrität und Vertraulichkeit des Systems *insgesamt* aufgehoben. Die Begrenzung auf „laufende Kommunikation“ ist technisch als künstliche Beschränkung einer technisch zunächst allumfassenden Zugriffsmöglichkeit auf das System zu betrachten: Wer ein Zielsystem „hackt“, erlangt die Möglichkeit, alle Daten dieses Systems auszulesen. Es ist dann letztlich eine Frage des Vertrauens in die Zuverlässigkeit des eingesetzten Staatstrojaners sowie der ihn einsetzenden Personen, ob die Beschränkung des Zugriffs auf erlaubte Inhalte technisch funktioniert und auch tatsächlich eingehalten wird.

Die Bedeutung der geplanten Regelung wird deutlich, wenn man sich vor Augen führt, dass Computer und Smartphones heute oft eine unermessliche Fülle an Informationen[2] enthalten: alltägliche bis intimste Emails und Nachrichten wie SMS oder WhatsApp, Terminkalender, Kontakte, Kontoumsätze, Tagebücher und Social-Media-Daten. Mit Speicherkapazitäten im Giga- bis Terabyte-Bereich enthalten sie ein weitgehendes digitales Abbild unseres Lebens. Moderne informationstechnische Systeme gleichen so einem ausgelagerten Teil des Gehirns. Erhalten Ermittlungsbehörden Zugriff auf diese Datenmengen, können sie die Besitzer der Systeme so vollständig ausspähen, dass sie sie nicht selten besser kennen als die Besitzer sich selbst. Hinzu kommt die Möglichkeit des Live-Zugriffs – Ermittler können den Betroffenen also virtuell heimlich über die Schulter blicken und ihnen so beim Denken und Kommunizieren zuschauen. Ein staatlicher Zugriff auf einen derart umfassenden Datenbestand ist mit dem naheliegenden Risiko verbunden, dass die erhobenen Daten in einer Gesamtschau weitreichende Rückschlüsse auf die Persönlichkeit des Betroffenen bis hin zu einer Bildung von Verhaltens- und Kommunikationsprofilen ermöglichen[3].

Dieser unvergleichlich tiefe Einblick in das Wissen und Fühlen eines Menschen macht den Einsatz von Trojanern in einem Rechtsstaat unvergleichlich heikel. Wie keine andere Ermittlungsmethode erlaubt es diese Maßnahme, Menschen zum Objekt der Ausspähung zu machen. Gegen keine andere Methode sind Verdächtige so wehrlos, denn der direkte Zugriff auf das System dient gerade dem Zweck, Verschlüsselungsverfahren zu umgehen, also den informationellen Selbstschutz ins Leere laufen zu lassen. Keine andere Ermittlungsmethode bietet insgesamt ein vergleichbares totalitäres Potential.

Neben einer ganz gravierenden Eingriffstiefe weisen die vorgesehene Regelungen zum Einsatz von Staatstrojanern auch verfahrensrechtliche Defizite auf, die miteinander verzahnt sind: Die vorgesehenen Regelungen in der Fassung des Entwurfs überlassen es den Ermittlungsbehörden und dem Gericht, die technischen Anforderungen an Software zu definieren, die in informationstechnische Systeme eingreift, obwohl von ihnen –

[2] Vgl. bereits BVerfGE 120, 274, 303 ff. (2008).
[3] BVerfGE 120, 274, 323.

ebenso wie von den verfahrensrechtlichen Vorkehrungen, um ihre Einhaltung sicherzustellen – das Gewicht des Grundrechtseingriffs maßgeblich bestimmt wird. Insbesondere hängt es von der Ausgestaltung der Software ab, ob der Zugriff tatsächlich auf „laufende Kommunikation“ beschränkt ist oder ob technisch eine vollumfängliche Ausspähung des Systems (sogenannte Online-Durchsuchung) möglich ist. Diese „carte blanche“ für die Polizei ist mit dem Gebot des Grundrechtsschutzes durch Verfahrensgestaltung ebenso wie mit dem Wesentlichkeitsgrundsatz unvereinbar.

Außerdem lässt § 28e des Entwurfs der Polizei und dem Gericht Raum für den Missbrauch von Sicherheitslücken in informationstechnischen Systemen (sog. *Zero Day Exploits* oder kurz *0days*[4]) zum Zwecke der Infiltration. Dies schafft fatale Fehlanreize, weil die Behörden des Landes Brandenburg damit ein erhebliches Interesse haben, Sicherheitslücken in informationstechnischen Systemen nicht an die Hersteller zu melden, sodass sie geschlossen werden können, sondern sie vielmehr zu horten. Dies ist der Mechanismus, der dem 2017 unter dem Stichwort „wannacry“ bekannt gewordenen Trojaner-Ausbruch zugrunde lag: Der US-amerikanische Geheimdienst National Security Agency (NSA) hatte seit Jahren Kenntnis von der Lücke in verschiedenen Versionen des Betriebssystems Windows, meldete sie aber dem Hersteller Microsoft nicht, sodass dieser seine Systeme nicht nachbessern konnte. Erst nachdem die NSA ihrerseits Opfer eines Cyber-Angriffs wurde, im Zuge dessen Unbekannte Informationen über die Lücke gestohlen und sie im Internet veröffentlicht hatten, gab Microsoft für einige (nicht alle) betroffenen Systeme Updates heraus. Diese konnten in der kurzen Zeit bis zum Ausbruch von „wannacry“ aber nicht mehr flächendeckend eingespielt werden. In der Folge legte der Trojaner u.a. weite Teile des britisches Gesundheitswesens „National Health Service“ lahm, was in zahlreichen Fällen lebensgefährliche Folgen hatte. Dies ist nur ein Beispiel für die real bestehende Missbrauchsgefahr aus jüngster Vergangenheit.

Die vorgeschlagenen Regelungen sind vor diesem Hintergrund insgesamt verfassungsrechtlich wie rechtspolitisch deutlich misslungen.

---

[4] Gesprochen: Oh-Days.

1.) Vorgaben des Bundesverfassungsgerichts

Der unvergleichlichen Gefahren staatlicher Überwachungssoftware war sich auch das Bundesverfassungsgericht bewusst, als es im Jahre 2008 über eine Rechtsgrundlage für Staatstrojaner im Verfassungsschutzgesetz des Landes Nordrhein-Westfalen zu entscheiden hatte. Der Erste Senat leitete aus der Menschenwürdegarantie des Art. 1 Abs. 1 GG sowie dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 GG) das „Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme“ ab (BVerfGE 120, 274). Wie alle Grundrechte mit Ausnahme der Menschenwürdegarantie gilt es zwar nicht schrankenlos. Doch geht das BVerfG von einem außerordentlichen Gewicht aller Eingriffe in dieses „Computer-Grundrecht“ aus. Denn eine heimliche technische Infiltration ermöglicht die längerfristige Überwachung der Nutzung des Systems und die laufende Erfassung der entsprechenden Daten[5]. Weiter vertieft wird der Eingriff durch seine unvermeidliche Streubreite[6]. Angesichts dieser Intensität entspricht ein Grundrechtseingriff, der in dem heimlichen Zugriff auf ein informationstechnisches System liegt, selbst im Rahmen einer präventiven Zielsetzung

> *„nur dann dem Gebot der Angemessenheit, wenn bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen, selbst wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt. Zudem muss das Gesetz, das zu einem derartigen Eingriff ermächtigt, den Grundrechtsschutz für den Betroffenen auch durch geeignete Verfahrensvorkehrungen sichern.“*[7]

Zudem muss die Gefahr ganz bestimmten besonders wichtigen Rechtsgütern drohen:

---

[5] BVerfGE 120, 274, 323.
[6] BVerfG a.a.O.
[7] BVerfGE 120, 274, 326.

> *„Ein derartiger Eingriff darf nur vorgesehen werden, wenn die Eingriffsermächtigung ihn davon abhängig macht, dass tatsächliche Anhaltspunkte einer konkreten Gefahr für ein **überragend wichtiges Rechtsgut** vorliegen. Überragend wichtig sind zunächst Leib, Leben und Freiheit der Person. Ferner sind überragend wichtig solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Hierzu zählt etwa auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen.“*[8]

Das bedeutet im Umkehrschluss:

> *„Zum Schutz sonstiger Rechtsgüter Einzelner oder der Allgemeinheit in Situationen, in denen eine **existentielle Bedrohungslage** nicht besteht, ist eine staatliche Maßnahme grundsätzlich nicht angemessen, durch die ... die Persönlichkeit des Betroffenen einer weitgehenden Ausspähung durch die Ermittlungsbehörde preisgegeben wird. Zum Schutz solcher Rechtsgüter hat sich der Staat auf andere Ermittlungsbefugnisse zu beschränken, die ihm das jeweils anwendbare Fachrecht im präventiven Bereich einräumt.“*[9]

Selbst präventiv ist der Einsatz von Staatstrojanern mithin nur dann zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr vorliegen, die für Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt, besteht. Andere Rechtsgüter wie etwa Eigentum oder Vermögen können einen Eingriff in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme hingegen per se nicht rechtfertigen.

---

[8] BVerfGE 120, 274, 328 – Hervorhebung nicht im Original.
[9] BVerfGE 120, 274, 328 – Hervorhebung nicht im Original.

Eingriffe mittels Staatstrojanern sind hingegen nicht am „Computer-Grundrecht“, sondern lediglich am Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG zu messen, wenn ausschließlich „laufende Kommunikation“ mitgeschnitten wird. Im Falle einer solchen Online-Durchsuchung „light“ – genannt Quellen-Telekommunikationsüberwachung oder auch Quellen-TKÜ – muss jedoch durch „technische Vorkehrungen und rechtliche Vorgaben“[10] sichergestellt werden, dass sich die Datenerhebung wirklich auf die laufende Kommunikation beschränkt.

Dies ist insbesondere deswegen bedeutsam, weil eine Quellen-TKÜ technisch von einer vollumfänglichen Online-Durchsuchung nicht zu unterscheiden ist: In beiden Fällen muss das Zielsystem mittels eines Staatstrojaners infiziert werden, was die Integrität und Vertraulichkeit des Systems insgesamt aufhebt. Dieser Eingriff muss sodann jedoch durch „technische Vorkehrungen und rechtliche Vorgaben“ gleichsam kastriert werden, damit ausschließlich laufende Kommunikation erhoben werden kann.

Daraus ergibt sich sogleich die besondere Gefährlichkeit von Quellen-TKÜ-Maßnahmen: Sie laufen stets Gefahr, bei einer Fehlfunktion des eingesetzten Trojaners oder bewusst pflichtwidrigem oder gar nur fahrlässigem Handeln des bedienenden Personals in eine vollumfängliche Online-Durchsuchung abzugleiten, die wesentlich höheren verfassungsrechtlichen Anforderungen unterliegt[11]. Neutrale IT-Sicherheits-Experten außerhalb der Ermittlungsbehörden vertreten daher praktisch einhellig die Ansicht, dass die Anforderungen an eine Quellen-TKÜ technisch nicht zu erfüllen sind[12]. Das BVerfG hat eindeutig verlangt, dass eine solche Maßnahme zu unterbleiben hat, solange dies technisch nicht möglich ist[13].

[10] BVerfGE 120, 274, 309.
[11] BVerfGE 120, 274, 309.
[12] Vgl. die Wiedergabe in BVerfGE 120, 274, 309, die sich der Senat zu eigen macht.
[13] BVerfG a.a.O.

2.) Die Regelung zur Quellen-TKÜ (§ 28e des Entwurfs)

Vor dem Hintergrund ist der Gesetzentwurf verfassungsrechtlich schon im Ansatz problematisch, weil er eine Rechtsgrundlage für eine Maßnahme schafft, die aus tatsächlichen Gründen nicht legal durchzuführen sein dürfte. Dies wiederum schafft erhebliche Anreize, die verfassungsrechtlichen Vorgaben „im Eifer des Gefechts" bei der vermeintlichen Abwehr terroristischer Gefahren hintanzustellen.

Darüber hinaus enthält die Eingriffsbefugnis in § 28e des Entwurfs der Landesregierung zwar bestimmte an der Rechtsprechung des BVerfG orientierte Begrenzungen des „Eingreifens", etwa eine Beschränkung von Veränderungen auf das Notwendige (§ 28e Abs. 3 Satz 1 Nr. 1 des Entwurfs) oder einen Schutz vor unberechtigten Zugriffen durch Dritte (§ 28e Abs. 3 Satz 2 des Entwurfs). Diese als solche begrüßenswerten Regelungen finden indes im Gesetz keinerlei verfahrensrechtliche Absicherung. Gemessen an den Anforderungen an die Anordnung und ihre Begründung (§ 28e Abs. 7 des Entwurfs) muss das „technische Mittel", dessen Einsatz beabsichtigt ist – also immerhin der einzusetzende Staatstrojaner (!) – nicht einmal benannt, geschweige denn in seinen technischen Spezifikationen näher bezeichnet werden. Dies ermöglicht nach dem Wortlaut des Entwurfs den Einsatz beliebiger Staatstrojaner nach Gutdünken der Ermittlungsbehörden, sofern ein Beschluss über eine Maßnahme einmal erlangt werden kann. Das ist angesichts der großen Gefahr einer schleichenden Ausweitung einer Quellen-TKÜ hin zu einer Online-Durchsuchung, der nur durch die Gestaltung des Trojaners entgegengewirkt werden kann, in jeder Hinsicht unangemessen. Jedenfalls nach den Vorstellungen des Entwurfs soll offenbar jede Steckdose [14] strengeren Anforderungen an die technisch sichere Gestaltung unterliegen als eine Software, die zur Ausspähung von Bürgerinnen und Bürgern eingesetzt werden soll. Das erscheint in einem Rechtsstaat schwer vorstellbar.

Die Verantwortung für die Prüfung der technischen Beschaffenheit des einzusetzenden Staatstrojaners kann auch nicht auf die Richter abgewälzt werden, die die Maßnahme anordnen sollen. Zum einen müssten sie gezielt Rückfragen stellen, um überhaupt zu

[14] Vgl. nur https://de.wikipedia.org/wiki/IEC_60309.

erfahren, welches technische Mittel eingesetzt werden soll und wie dieses im Einzelnen beschaffen ist. Zum anderen kann von dem zuständigen Gericht nicht ernsthaft verlangt werden, eine EDV-technische Überprüfung des beabsichtigten Staatstrojaners selbst vorzunehmen. Eine externe Prüfung wiederum dürfte angesichts der hierfür notwendigen Zeit – wenigstens Tage, wohl eher Wochen – in vielen Fällen den Zweck der Maßnahme gefährden. Die Verantwortung hierfür wird kaum ein Gericht auf sich nehmen wollen, sodass man sich im Zweifel auf Beteuerungen der antragstellenden Behörde verlassen wird, mit dem Staatstrojaner habe schon alles seine rechte Ordnung. Im Ergebnis ist daher zu besorgen, dass die Einhaltung der § 28e des Entwurfs genannten, aber auch weiterer aus der Perspektive der Informationssicherheit gebotener technischer Anforderungen an Staatstrojaner allenfalls von den Ermittlungsbehörden wohlwollend geprüft werden wird – soweit sie ihrerseits hierzu in der Lage sind. In der Praxis dürfte es daher weitgehend mit Beteuerungen der Software-Hersteller sein Bewenden haben.

Aus der Perspektive des Schutzes der Integrität und Vertraulichkeit informationstechnischer Systeme (Art. 1 Abs. 1, Art. 2 Abs. 1 GG) ist ein derart blindes Vertrauen in die von den Ermittlungsbehörden einzusetzenden Staatstrojaner ohne einen rechtsstaatlich ausreichenden Überprüfungsmechanismus nicht hinnehmbar. Dies gilt insbesondere angesichts des Umstands, dass die Software nach dem Wortlaut des Gesetzes durchaus von einem externen Anbieter stammen kann, sodass die Ermittlungsbehörden mitunter selbst nicht mit Sicherheit einzuschätzen vermöchten, welche Funktionen die einzusetzende Software ausführt.

Ausdrücklich zu begrüßen ist in diesem Kontext allerdings, dass sich das Bundeskriminalamt nach Presseberichten um die Eigenprogrammierung einer Überwachungssoftware bemüht; für den Bereich der sogenannten Quellen-TKÜ soll diese einsatzbereit sein[15]. Der vorliegende Gesetzentwurf schließt aber gerade nicht aus, dass auch – oder gar ausschließlich – Staatstrojaner zum Einsatz kommen, die weder vom BKA selbst programmiert noch extern und unabhängig geprüft sind.

---

[15] https://www.heise.de/newsticker/meldung/Quellen-Telekommunikationsueberwachung-Neuer-Bundestrojaner-steht-kurz-vor-Einsatzgenehmigung-3113444.html

Zwar mögen die technischen Details eines Staatstrojaners nicht unbedingt durch formelles Gesetz zu regeln sein. Zumindest aber muss das Gesetz im Lichte des Wesentlichkeitsgrundsatzes eine unabhängige technische Überprüfung der einzusetzenden Staatstrojaner vorschreiben. Dementsprechend sollte ausschließlich der Einsatz erfolgreich geprüfter Staatstrojaner zulässig sein. Eine entsprechende Darlegung dessen sollte in den Katalog der obligatorischen Inhalte einer Anordnung (§ 28e Abs. 7 des Entwurfs) aufgenommen werden.

3.) Fehlanreize, die die Datensicherheit insgesamt schwächen

Zumindest ebenso schwer wie die geschilderten rechtlichen Bedenken gegen die fehlende Prüfung der Staatstrojaner wiegen indes die fatalen Fehlanreize, die die Norm für die Arbeit der Behörden – namentlich die im Aufbau befindliche „ZITIS“ (Zentrale Stelle für Informationstechnik im Sicherheitsbereich) – mit sich bringt. Nach dem Entwurf sollen Polizeibehörden in informationstechnische Systeme „eingreifen“ dürfen, um aus ihnen Daten zu erheben. Hierzu ist denklogisch ein „Fuß in der Tür“ erforderlich, also das Aufbringen eines Staatstrojaners. Der Entwurf definiert indes nicht weiter, wie der Staatstrojaner auf das Zielsystem aufgebracht werden darf. Denkbar sind insbesondere folgende Wege[16]:

- Aufspielen durch Hoheitsträger, etwa bei einer polizeilichen Kontrolle

- Aufspielen durch Hoheitsträger durch heimliches Betreten der Räumlichkeiten, in denen sich das System befindet

- Ausnutzen der Unaufmerksamkeit des berechtigten Nutzers, etwa indem man ihm einen EMail-Anhang mit einem (getarnten) Infektions-Programm in der Hoffnung zuspielt, dass er ihn ausführen werde

- Aufspielen durch Ausnutzen von Sicherheitslücken des genutzten Systems, etwa indem der berechtigte Nutzer zum Aufruf einer speziell präparierten WWW-Seite

[16] Vertiefend zu den technischen Grundlagen *Buermeyer* HRRS 2007, S. 154 ff.

animiert wird, deren bloße Ansicht aufgrund von Sicherheitslücken zur Infektion des Zielsystems führt (sogenannte *drive by downloads*)

Es erschließt sich leicht, dass die rechtliche Bewertung der Zugriffe völlig unterschiedlich ausfällt: Das Betreten von Räumlichkeiten zur Infektion von Systemen ist im Lichte von Art. 13 Abs. 1 GG ohne eine (bisher fehlende) spezifische Ermächtigungsgrundlage hierzu schlechthin rechtswidrig. Das Aufspielen etwa bei einer Polizeikontrolle ist hingegen als solches unbedenklich, ebenso das Zusenden eine E-Mail mit einem getarnten Staatstrojaner (kriminalistische List), soweit dieser E-Mail-Anhang keine Sicherheitslücken ausnutzt.

Die Infektion des Zielsystems durch Ausnutzen von Sicherheitslücken – wiewohl vom Wortlaut des § 28e des Entwurfs gedeckt – führt hingegen zu gravierenden Fehlanreizen: Wenn Behörden solche Lücken ausnutzen dürfen, so haben sie ein durchaus nachvollziehbares Interesse daran, ein „Arsenal“ von Sicherheitslücken aufzubauen, um im Falle des Falles eine Zielperson angreifen zu können. Dieses Interesse wird sie jedoch davon abhalten, gefundene oder gar auf dem Schwarzmarkt angekaufte Sicherheitslücke den jeweiligen Herstellern der IT-Systeme mitzuteilen, damit die Lücken geschlossen werden können. So entstehen Anreize für Behörden, ihnen bekannte Sicherheitslücken gerade nicht schließen zu lassen, sondern sie lieber zu horten.

Solange aber die Lücken nicht von den Herstellern der Systeme geschlossen werden können, weil sie von ihnen keine Kenntnis erlangen, können natürlich nicht nur Behörden diese Lücken für den Einsatz von Staatstrojanern ausnutzen. Vielmehr kann jeder, der sie findet oder seinerseits auf dem Schwarzmarkt für *0days* kauft, die Lücken zur Infiltration informationstechnischer Systeme missbrauchen – insbesondere auch Cyber-Kriminelle, die es beispielsweise darauf anlegen könnten, die betroffenen Systeme zum Teil eines Botnetzes zu machen oder Zahlungsdaten für Online-Überweisungen abzugreifen.

Im Ergebnis würden Behörden mitunter viele Millionen Nutzerinnen und Nutzer von IT-Systeme weltweit, die von der jeweiligen Lücke betroffen sind, einem fortbestehenden Risiko von Cyber-Angriffen aussetzen, um Sicherheitslücken im Einzelfall selbst für

Maßnahmen nach § 28e des Entwurfs ausnutzen zu können. Das weltweite Missbrauchsrisiko, das hier durch ein Horten von Sicherheitslücken eingegangen wird, steht in keinem ausgewogenen Verhältnis zu dem verfolgten Zweck (bessere Gefahrenabwehr im Einzelfall).

Eine solche aus der Sicht einer Behörde möglicherweise noch nachvollziehbare Güterabwägung verbietet sich aus der Perspektive des Gesetzgebers, der das Wohl der Allgemeinheit in den Blick zu nehmen hat. Damit sind Anreize für Behörden, die Cyber-Sicherheit in Deutschland und weltweit im Interesse einer möglicherweise einmal erforderlichen Gefahrenabwehr zu schwächen, schlechthin unvereinbar.

§ 28e des Entwurfs sollte daher zumindest um ein explizites Verbot des Einsatzes von dem Hersteller eines informationstechnischen Systems bisher unbekannten Sicherheitslücken (sog. *0days*) ergänzt werden, um sicherzustellen, dass sich alle Behörden darum bemühen, ihnen bekannte Sicherheitslücken durch die Hersteller der Systeme so schnell wie möglich schließen zu lassen. Eine Sicherheitslücke, die dem Hersteller bereits bekannt ist, aber beispielsweise wegen Nachlässigkeit des Systembetreibers noch nicht geschlossen wurde, kann hingegen auch aus der Perspektive der IT-Sicherheit ausgenutzt werden. Gleiches gilt für Sicherheitslücken, die nicht auf Fehlern der Hersteller beruhen, sondern auf einer individuellen fehlerhaften Einrichtung des informationstechnischen Systems.

Formulierungsvorschlag

Nach § 28e Abs. 3 Satz 2 des Entwurfs wird der folgende Satz eingefügt:

Für den Einsatz des technischen Mittels dürfen Sicherheitslücken des informationstechnischen Systems, die auf die fehlerhafte Gestaltung von Systemkomponenten durch ihre Hersteller zurückgehen, nur ausgenutzt werden, wenn die Sicherheitslücken den jeweiligen Herstellern bereits bekannt sind.

Berlin, den 7. Januar 2019

Dr. Ulf Buermeyer, LL.M. (Columbia)