Michael Greven
Oberstaatsanwalt
beim Bundesgerichtshof

Karlsruhe, den 29. Mai 2017

Stellungnahme zum Gesetzentwurf zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze

Hier:

Gesetzentwurf der Bundesregierung vom 22. Februar 2017, Drucksache 18/11272

Formulierungshilfe der Bundesregierung für einen Änderungsantrag der Fraktionen CDU/CSU und SPD vom 15. Mai 2017, Ausschussdrucksache 18(6)334

A. Tenor der Stellungnahme

Der Gesetzentwurf zur Schaffung einer Rechtsgrundlage für die Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung in der Strafprozessordnung wird ausdrücklich begrüßt, da die staatsanwaltschaftliche Praxis dringend klare gesetzliche Vorgaben benötigt.

Seit Beginn des 21. Jahrhunderts hat die Technik der Internettelefonie und sogenannte Voice-over-IP-Dienste - wie etwa das Programm „Skype" oder der Instant Messenger „WhatsApp" - eine immer größere Bedeutung gewonnen. Eine grundlegende Anpassung der wichtigen Eingriffsrechte der Strafverfolgungsbehörden gemäß §§ 100a ff. StPO an den rasanten Fortschrift moderner Kommunikationstechnologien ist jedoch bislang unterblieben.

B. Forderungen der Praxis

1. Bereits im September 2012 hat die Abteilung Strafrecht des 69. Deutschen Juristentags in München mehrheitlich die Schaffung einer Rechtsgrundlage für die Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung in der Strafprozess-

ordnung gefordert (vgl. 69. Deutscher Juristentag München 2012 - Beschlüsse, Seite 10 f.; http://www.djt-net.de/beschluesse/beschluesse.pdf).

2. Im Oktober 2015 ist die „Expertenkommission zur effektiveren und praxistauglicheren Ausgestaltung des allgemeinen Strafverfahrens und des jugendgerichtlichen Verfahrens" zur Empfehlung gelangt, zum Zwecke des Grundrechtsschutzes der Betroffenen die Voraussetzungen der Quellen-Telekommunikationsüberwachung gesetzlich zu regeln und insoweit eine eigene Ermächtigungsgrundlage zu schaffen, die sowohl dem Eingriff in das Telekommunikationsgeheimnis als auch dem für diese Maßnahme typischen zusätzlichen Eingriff in das Grundrecht auf Vertraulichkeit und die Integrität informationstechnischer Systeme Rechnung trägt. Technisch müsse sichergestellt werden, dass mit der für die Quellen-TKÜ eingesetzten Software nur Zugriff auf Inhalt und Umstände der laufenden Telekommunikation genommen werden kann, nicht aber auf die auf dem überwachten Endgerät gespeicherten Daten (vgl. Bericht der „Expertenkommission zur effektiveren und praxistauglicheren Ausgestaltung des allgemeinen Strafverfahrens und des jugendgerichtlichen Verfahrens", Oktober 2015, Seite 73 ff.; https://www.bmjv.de/SharedDocs/Downloads/DE/PDF/Abschlussbericht_Reform_StPO Kommission.pdf?blob=publicationFile&v=2; insbesondere auch Anlagenband II - Protokolle Siebte Sitzung der Expertenkommission am 13./14. Juli 2015, Seite 247 ff.; https://www.bmjv.de/SharedDocs/Downloads/DE/PDF/Anlage_2_StPO_Kommission .pdf? blob=publicationFile&v=2).

3. Mit Beschluss vom 9. November 2016 wurde auf der Arbeitstagung des Generalbundesanwalts mit den Generalstaatsanwältinnen und Generalstaatsanwälten gefordert:

„Die Generalstaatsanwältinnen und Generalstaatsanwälte der Länder sowie der Generalbundesanwalt halten es für dringend erforderlich, die Strafverfolgungsbehörden durch eine Anpassung der bestehenden gesetzlichen Regelungen wieder in die Lage zu versetzen, bei schweren Straftaten aufgrund richterlicher Anordnung die Telekommunikation von Beschuldigten (und deren Nachrichtenmittlern) effektiv zu überwachen. Notwendig ist hierfür die technikoffene Fortschreibung der strafprozessualen Rechtsgrundlagen, die den verdeckten Zugriff auf laufende Telekommunikation möglich macht und den technisch bedingten, zwingend mit der Überwachung einhergehenden Eingriff in die informationstechnischen Systeme im Wege einer Installationsbefugnis gestattet."

Zur Begründung wurde ausgeführt:

„Die Telekommunikationsüberwachung stellte lange Zeit im Bereich der Verfolgung schwerer und organisierter Kriminalität einen Eckpfeiler erfolgreicher Ermittlungen dar. Dies galt in besonderer Weise für die Bekämpfung des Terrorismus und anderer schwerster Straftaten. Die technische Entwicklung hat jedoch dazu geführt, dass der für die Sicherheitsbehörden auswertbare Anteil an der Kommunikation rapide abgesunken ist und weiter rasant abnimmt. Die Telekommunikationsüberwachung nach geltendem Recht fällt deshalb als Ermittlungsinstrument weitgehend aus.

Die fortschreitende Umstellung der Festnetztelefonie auf VoIP, die Ende-zu-Ende-Verschlüsselung weit verbreiteter Kommunikationsapplikationen und der technische Fortschritt im Hardware-Bereich haben einen Zustand entstehen lassen, der die Erfüllung des grundgesetzlichen Auftrages des Schutzes der Bevölkerung vor Straftaten durch deren nachdrückliche Verfolgung in Frage stellt.

Aktuell ist festzustellen, dass nur noch in weniger als 15 % aller Fälle vollständig unverschlüsselte Kommunikation auf Seiten der Beschuldigten durchgeführt wird und damit von den Strafverfolgungsbehörden überwacht werden kann. Gleichzeitig ist ausweislich von Stichproben des BKA erkennbar geworden, dass in zwei Drittel der Fälle seitens der Täter bewusst verschlüsselte Kommunikation zur Verschleierung eingesetzt wird, während in den restlichen Fällen der Anstieg des verschlüsselten Anteils dem mittlerweile üblichen Verbraucherverhalten und den Entwicklungen der Anbieter geschuldet sein dürfte, standardmäßig verschlüsselte Applikationen anzubieten oder zu nutzen.

Im Ergebnis führt dies zu einem massiven Defizit bei der Gewinnung von Beweismitteln durch Telekommunikationsüberwachung, die gerade durch die wachsende Relevanz elektronischer Kommunikation von zentraler Bedeutung bei der Aufklärung schwerer und organisierter Kriminalität ist. Zugleich belegen die verschlüsselungsbedingten Ausfälle, dass es nicht um eine Ausweitung staatlicher Grundrechtseingriffe, sondern ausschließlich um die Wiederherstellung des Zustandes geht, der bei der klassischen Telefonie bestand, bevor die Strafverfolgungsbehörden durch die technische Weiterentwicklung von dieser Beweiserhebungsmöglichkeit weitgehend abgeschnitten wurden. Die rechtliche Möglichkeit einer Ausleitung von zum Zeitpunkt der Überwachung

erzeugten (laufenden) Kommunikationsinhalten noch vor ihrer Verschlüsselung ist daher dringend erforderlich.

Bereits im Koalitionsvertrag des Bundes ist deshalb eine Neufassung der gesetzlichen Regelung zur sog. Quellen-TKÜ festgeschrieben worden. Auch die Justizministerkonferenz hat am 1./2. Juni 2016 einstimmig eine Entschließung zum Erfordernis einer gesetzlichen Regelung der „Quellen-TKÜ" gefasst (TOP 11.21). Die Entscheidungen des Bundesverfassungsgerichts, insbesondere diejenigen zum Verfassungsschutzgesetz Nordrhein-Westfalen und zum BKAG (1 BvR 370/07 vom 27.02.2008; 1 BvR 966/09 vom 20.04.2016), haben einen gangbaren Weg für eine gesetzliche Regelung aufgezeigt.

Aus Sicht der Generalstaatsanwältinnen und Generalstaatsanwälte sowie des Generalbundesanwalts wird die erforderliche Neuregelung zu bedenken haben, dass es - jedenfalls solange eine Verpflichtung (auch ausländischer) Kommunikationsanbieter im Inland zur Entschlüsselung nicht existiert - eines verdeckten Zugriffs der Strafverfolgungsbehörden auf die Endgeräte der Betroffenen bedarf und dass zur Sicherstellung der Überwachung laufender Kommunikation zunächst ein technisch bedingter Eingriff in das informationstechnische System notwendig ist. Soweit davon unvermeidlich sonstige Daten des Systems betroffen sind, kann dem mit den bewährten Instrumentarien von Richtervorbehalt, gerichtlicher Überprüfung, Verwertungsverboten und Löschungspflichten begegnet werden.

Da eine Lösung unter Berufung auf lediglich ungeschriebene Annexkompetenzen auf rechtliche Bedenken stößt, wird in der Gesamtschau angeregt, dass der Gesetzgeber die gebotenen engen rechtlichen Grenzen für eine Installationsbefugnis technikoffen beschreibt, indem er sicherstellt, dass der Eingriff in das informationstechnische System im Ergebnis lediglich die Überwachung der laufenden Kommunikation bezwecken darf, mithin der Ermöglichung hergebrachter Telekommunikationsüberwachung dient."

C. Eigene Erfahrungen

Als Praktiker, der - mit kürzeren Unterbrechungen - seit rund fünfzehn Jahren als Staatsanwalt bei der Bundesanwaltschaft, weit überwiegend in der Abteilung für Straftaten gegen die äußere Sicherheit der Bundesrepublik Deutschland, tätig ist, teile ich diese Sicht.

Bei meiner arbeitstäglichen Befassung mit Ermittlungsverfahren, zumeist im Bereich der Spionage (§§ 94 ff. Strafgesetzbuch) und der Proliferation (§§ 17, 18 Außenwirtschaftsgesetz und §§ 19 ff. Kriegswaffenkontrollgesetz), ist festzustellen, dass die herkömmliche Telekommunikationsüberwachung, die noch vor zehn Jahren zumeist verlässliche Erkenntnisse zu strafbaren Handlungen von Beschuldigten erbracht hat, im Laufe der vergangenen Jahre in immer weniger Fällen einen erfolgversprechenden Ermittlungsansatz darstellt. Die technische Entwicklung hat dazu geführt, dass der für die Polizeibehörden auswertbare Anteil an der Kommunikation nur noch marginal ist und weiter rasant abnimmt. Die herkömmliche, sich nach geltendem Recht richtende Telekommunikationsüberwachung erbrachte in der weit überwiegenden Anzahl der von mir in den vergangenen Jahren geführten Ermittlungsverfahren nur noch geringe oder überhaupt keine Erkenntnisse mehr. Es hat sich ein Dunkelfeld gebildet, das immer größer wird, weil sich in der kriminellen Szene mittlerweile herumgesprochen hat, dass die Polizei „WhatsApp nicht (überwachen) kann", und an diesem Zustand wird sich auch nichts mehr ändern. Die klassische Telekommunikationsüberwachung fällt deshalb als Ermittlungsinstrument weitgehend aus.

Diese Feststellungen decken sich durchweg mit den Erfahrungen von Kolleginnen und Kollegen der Bundesanwaltschaft und der Staatsanwaltschaften der Länder, mit denen ich mich im Laufe der vergangenen Jahre über ihre Erfahrungen im Bereich der Telekommunikationsüberwachung nach geltendem Recht ausgetauscht habe.

„Klassisches" Einsatzgebiet der Telekommunikationsüberwachung war und ist die schwere und organisierte Kriminalität sowie die Bekämpfung von Staatsschutzstraftaten wie Terrorismus, Spionage, Straftaten gegen das Völkerstrafgesetzbuch und das Außenwirtschaftsgesetz. Dies ergibt sich auch aus der jährlichen Statistik des Bundesamtes für Justiz über Telekommunikationsüberwachungsmaßnahmen. Noch vor einigen Jahren haben die Beschuldigten versucht, durch den häufigen Wechsel von Prepaid-Mobiltelefonen der Überwachung ihrer Anschlüsse zu entgehen. Heute ist dies nicht mehr notwendig, da die Ende-zu-Ende-Verschlüsselung weit verbreiteter Kommunikationsapplikationen nahezu allen Beschuldigten bekannt ist und genutzt

wird. So ist bereits verschiedentlich in Protokollen herkömmlicher Telekommunikationsüberwachungsmaßnahmen zu lesen, dass die Beschuldigten vereinbaren, im Anschluss an das gerade geführte Telefongespräch „sensible Inhalte" über einen Instant Messenger auszutauschen, da dieser „von der Polizei ja nicht abgehört werden könne." Sollten dann noch Personen beteiligt sein, die, wie beispielsweise die Quellen und Führungsoffiziere fremder Nachrichtendienste oder die Mitglieder terroristischer Vereinigungen im Hinblick auf ihr Kommunikationsverhalten in besonderer Weise in konspirativem Verhalten geschult wurden, fallen auf diesem Wege keinerlei nutzbringende Erkenntnisse mehr an. Auch im Bereich der organisierten Kriminalität gehen die Täter immer professioneller vor, was eine abgetarnte, auf Verschleierung ausgerichtete Kommunikation einschließt. Nicht zuletzt durch die technische Weiterentwicklung von Kryptierungsmöglichkeiten werden die Strafverfolgungsbehörden von der Möglichkeit, über den Austausch von Information mittels technischer Kommunikation Beweise zu erheben, abgeschnitten.

Die aktuell geäußerte Befürchtung, dass die neu geschaffenen Rechtsgrundlagen für die Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung zum massenhaften und unkontrollierbaren Abhören von zehntausenden Mobiltelefonen von Beschuldigten aus dem Bereich der mittleren oder sogar leichten Kriminalität führen, teile ich nicht. Im Jahr 2015 wurden von den deutschen Staatsanwaltschaften rund fünf Millionen Ermittlungsverfahren eingeleitet. In 5.945 Ermittlungsverfahren kam es zu Telekommunikationsüberwachungsmaßnahmen und in sieben Verfahren zu Maßnahmen der akustischen Wohnraumüberwachung. Durch die neuen Vorschriften wird sich an diesem Zahlenverhältnis wenig ändern. Fälle der Online-Durchsuchung werden genauso selten vorkommen wie die akustische Wohnraumüberwachung. Angesichts des bei jedem staatsanwaltschaftlichem Antrag zu beachtenden Grundsatzes der Verhältnismäßigkeit, des zu betreibenden erheblichen technischen Aufwandes bei den Polizeibehörden, der hohen Regelungs- und Dokumentationsdichte der neuen Vorschriften, der fein ziselierten Benachrichtigungspflichten und nicht zuletzt der - in den letzten Jahren immer stärkeren - Arbeitsbelastung der Kolleginnen und Kollegen der Bundesanwaltschaft und der Staatsanwaltschaften der Länder, wird sich jede Staatsanwältin und jeder Staatsanwalt genau überlegen, ob er einen entsprechenden Antrag beim zuständigen Ermittlungsrichter (§ 100a StPO-E) oder der zuständigen Kammer des Landgerichts (§ 100b StPO-E) stellen wird. Auch versteht es sich von selbst, dass jede Richterin und jeder Richter ihren Prüfpflichten zum Vorliegen der gesetzlichen Voraussetzungen für den Erlass einer entsprechenden Anordnung mit der gebotenen Sorgfalt und Verantwortung nachkommen wird.

D. Bewertung im Einzelnen mit besonderem Blick auf das Staatsschutzstrafrecht

1. Zu § 100b StPO-E:

a) Etliche der in dem Katalog des § 100b StPO-E genannten Tatbestände erfordern die Feststellung, dass es sich um einen besonders schweren Fall handelt. Das setzt voraus, dass das benannte oder unbenannte Regelbeispiel bereits in einem sehr frühen Stadium, in dem - neben anderen verdeckten Maßnahmen - die Überwachung der Telekommunikation ein zentrales Instrument der Beweisführung ist, mit einem den gesetzlichen Anforderungen entsprechenden verdichteten Tatverdacht bejaht werden kann. Dies wird in den seltensten Fällen möglich sein. Die Frage, ob ein besonders schwerer Fall vorliegt, kann in aller Regel erst nach erfolgter Durchsuchung, nach Auswertung aller Beweismittel, bejaht oder verneint werden.

Ich will dieses Problem am Beispiel der geheimdienstlichen Agententätigkeit verdeutlichen. Nach § 100b Abs. 1 Nr. 1, Abs. 2 Nr. 1 a) StPO-E soll die Online-Durchsuchung in Fällen der geheimdienstlichen Agententätigkeit gemäß § 99 Abs. 1 StGB auf solche Taten beschränkt sein, in denen ein besonders schwerer Fall im Sinne von § 99 Abs. 2 StGB vorliegt. Diese Regelung überzeugt bereits auf Grund ihrer Unbestimmtheit nicht. Bei § 99 Abs. 2 StGB handelt es sich um eine bloße Strafzumessungsregel mit Regelbeispielen. Das Verwirklichen eines Regelbeispiels führt nicht dazu, dass zwingend ein „besonders schwerer Fall" der geheimdienstlichen Agententätigkeit vorliegt. Zudem ist ein „besonders schwerer Fall" selbst dann nicht ausgeschlossen, wenn keines der zugehörigen Regelbeispiele verwirklicht ist. Hieraus können sich im Einzelfall erhebliche Unsicherheiten ergeben, ob ein Fall des § 99 Abs. 2 StGB vorliegt und damit die Voraussetzungen einer Online-Durchsuchung gemäß § 100b Abs. 1 Nr. 1, Abs. 2 Nr. 1 a) StPO-E erfüllt sind.

Zudem kann die Frage, ob ein besonders schwerer Fall i. S. von § 99 Abs. 2 StGB vorliegt, selbst bei Außerachtlassung der vorgenannten Unsicherheiten in aller Regel erst nach Auswertung der im Rahmen von Durchsuchungsmaßnahmen etc. gewonnenen Beweismittel - mithin zu einem Zeitpunkt, zu dem der Beschuldigte über den Tatverdacht bereits unterrichtet ist - zuverlässig beantwortet

werden. Dann wird kein Beschuldigter mehr einschlägige Daten speichern oder anderweitig auf seinem Computer verarbeiten. Durch die Beschränkung auf Fälle des § 99 Abs. 2 StGB läuft die Maßnahme in Bezug auf Straftaten nach § 99 StGB mithin praktisch ins Leere. Dies gilt im Übrigen in gleicher Weise für weitere Staatsschutztatbestände wie der landesverräterischen Ausspähung, aber auch beispielsweise für den schweren sexuellen Missbrauch von Kindern nach § 176a Abs. 1 StGB oder der sexuellen Nötigung und Vergewaltigung, wenn die Tat nicht von mehreren gemeinschaftlich begangen wird.

So konnte bei den von mir in den vergangenen rund fünfzehn Jahren bearbeitenden Ermittlungsverfahren wegen geheimdienstlicher Agententätigkeit in keinem einzigen Verfahren (!) die Frage, ob ein besonders schwerer Fall i. S. von § 99 Abs. 2 StGB vorliegt, bereits zum Zeitpunkt der Beantragung von Telekommunikationsüberwachungsmaßnahmen beantwortet werden. Ein aktuelles Beispiel für einen solchen Fall ist die - von der Presse ausführlich berichtete - Ausspähung des ehemaligen Bundestagsabgeordneten, Wehrbeauftragten und seinerzeitigen Präsidenten der Deutsch-Israelischen Gesellschaft, Reinhold Robbe, in Berlin durch eine der Islamischen Republik Iran zuzuordnende geheimdienstliche Einheit, die Qods-Kräfte des Korps der Revolutionsgarden. Mit (noch nicht rechtskräftigem) Urteil des Kammergerichts vom 27. März 2017 wurde der Angeklagte wegen geheimdienstlicher Agententätigkeit gemäß § 99 Abs. 1 StGB zu einer Freiheitsstrafe von vier Jahren und drei Monaten verurteilt.

Die Online-Durchsuchung würde demzufolge auch im Bereich der Cyber-Spionage, die von zunehmender Bedeutung und beachtlichem Gewicht (vgl. nur den von den Medien ebenfalls ausführlich berichteten Angriff auf den Deutschen Bundestag) ist, als Ermittlungsmaßnahme ausscheiden. Auch und gerade vor diesem Hintergrund erscheint es deshalb notwendig, im Katalog des § 100b Abs. 2 StPO-E den „Grundtatbestand" des § 99 Abs. 1 StGB aufzunehmen und die Beschränkung auf besonders schwere Fälle im Sinne von § 99 Abs. 2 StGB zu streichen. Angesichts der Tatsache, dass diese Straftaten unter Nutzung kompletter Serverstrukturen und einer Vielzahl „informationstechnischer Systeme" begangen werden und diese Ermittlungsmaßnahme hier deshalb in besonderer Weise erforderlich und geeignet ist, erscheint auch die geringfügige

Abweichung vom Katalog des § 100c Abs. 2 StPO (akustische Wohnraumüberwachung) sachgerecht.

Im Übrigen ist für den Bereich der Cyber-Spionage anzumerken, dass - bei der vorgesehenen Gesetzesfassung - damit ein Bereich von der Online-Durchsuchung ausgenommen wäre, bei dem diese Ermittlungsmaßnahme in besonderer Weise in Betracht kommt. Insofern ist darauf hinzuweisen, dass das Gesetz an anderer Stelle - § 100g Abs. 1 StPO - durchaus berücksichtigt, dass geringere Voraussetzungen für die Anwendung der Vorschrift genügen, wenn eine Straftat mittels Telekommunikation begangen worden ist. In diesen Fällen dürfen Verkehrsdaten auch erhoben werden, wenn keine Katalogtat nach § 100g Abs. 1 Nr. 1 i.V.m. § 100a Abs. 2 StPO vorliegt (§ 100g Abs. 1 Nr. 2 StPO). Sollte also § 99 StGB - was vorzugswürdig ist - nicht unabhängig vom Vorliegen eines „besonders schweren Falles" in den Katalog des § 100b Abs. 2 StPO-E aufgenommen werden, halte ich es für sachgerecht, dem § 100b Abs. 1 Nr. 1 StPO-E eine Alternative anzufügen, die den Anwendungsbereich für Fälle eröffnet, in den die Straftat „mittels Telekommunikation oder unter Nutzung eines informationstechnischen Systems begangen worden ist" (vgl. § 100g Abs. 1 Nr. 2 StPO). Die weitere Voraussetzung (Tat muss auch im Einzelfall besonders schwer wiegen) stellt dennoch sicher, dass die Online-Durchsuchung nicht in Fällen nur mittlerer oder leichter Kriminalität zum Einsatz kommt.

Die vorgenannte Problematik beschränkt sich schließlich nicht allein auf Strafgesetzverletzungen nach § 99 StGB. In gleicher Weise sind auch Taten nach §§ 95, 98, und 100a StGB betroffen, die ebenfalls nur bei Vorliegen eines „besonders schweren Falles" als Grundlage für eine Online-Durchsuchung in Betracht kommen sollen.

b) Im Entwurf [§ 100b Abs. 2 Nr. 1 lit. b) StPO-E] sind die Strafvorschriften des § 129a Abs. 3 und des § 129a Abs. 5 Satz 1 Alt. 2 und 3 und Satz 2 StGB bislang nicht enthalten. Eine Online-Durchsuchung wäre demnach bei der Unterstützung einer Vereinigung nicht möglich, deren Zwecke auf die Androhung der Straftaten nach § 129a Abs. 1 und Abs. 2 StGB gerichtet ist. Gleiches gilt für den Tatvorwurf der Unterstützung einer Vereinigung nach § 129a Abs. 2 und Abs. 3

StGB. Ebenso wenig in den Fällen des Werbens um Mitglieder oder Unterstützer für eine terroristische Vereinigung.

Ich rege an, den Straftatbestand der Unterstützung einer Vereinigung nach § 129a Abs. 2 StGB [§ 129a Abs. 5 Satz 1 Alt. 2 StGB] in den Gesetzesentwurf als mögliche Anlasstat für eine Online-Durchsuchung mit aufzunehmen. § 129a Abs. 2 StGB umfasst insbesondere Vereinigungen, deren Zwecke und Tätigkeit auf die Begehung von Brandstiftungs- und Sprengstoffdelikten gerichtet sind und denen ebenfalls ein hohes Gefährdungspotential innenwohnen kann. Gerade im Bereich der politisch motivierten Kriminalität rechts könnten Zusammenschlüsse zum Zwecke der Begehung solcher Straftaten relevant werden (zum Beispiel eine Vereinigung, die Anschläge auf noch unbewohnte Asylbewohnerwohnheime plant und durchführt).

Weiter empfehle ich die Aufnahme des § 129a Abs. 5 Satz 2 StGB („Werben um Mitglieder oder Unterstützer") in den Straftatenkatalog des § 100b Abs. 2 Nr. 1 lit. b) StPO-E, da diese Vorschrift im Bereich der Propagandadelikte für die Bundesanwaltschaft eine erhebliche tatsächliche Bedeutung hat: Jihadistisch motivierte Propaganda ist der wesentliche Grund für Radikalisierungen, für Ausreisen in jihadistische Kampfgebiete und für Anschlagsplanungen radikalisierter Einzelpersonen oder Gruppierungen. Aktuell existieren im Internet unzählige jihadistische Foren, Webseiten oder Plattformen auf sozialen Medien mit Deutschlandbezug, auf denen Propaganda des IS veröffentlicht und so zum „Globalen Jihad" gegen „Ungläubige" und „Abtrünnige" aufgerufen wird. Identifizierung und Verfolgung von Personen, die für diese Veröffentlichungen verantwortlich sind, quasi die „geistigen Brandstifter", sind aber wegen der regelmäßig getroffenen Schutzmaßnahmen mit erheblichen Schwierigkeiten verbunden oder gar erfolglos. Bei Propagandadelikten liegen zudem oftmals gerade keine zureichenden tatsächlichen Anhaltspunkte für eine vollendete Unterstützungshandlung im Sinne des § 129a Abs. 5 Satz 1 Alt. 1 StGB oder gar für eine mitgliedschaftliche Betätigungshandlung vor, was eine Online-Durchsuchung unmöglich machen würde und Strafbarkeitslücken befürchten ließe. Die praktische Relevanz der Propagandadelikte zeigt sich exemplarisch bei den von der Bundesanwaltschaft geführten und von den Medien ausführlich berichteten Ermittlungsverfahren gegen die „Globale Islamische Medienfront" (GIMF), deren Zielsetzung es war, jihadisti-

sche Texte, Bilder, Tondokumente und Filme durch die Veröffentlichung in ihren Foren weltweit im Internet zugänglich zu machen, gegen den Betreiber des GIMF-Nachfolgeforums „Al-Ansar-Medienbataillon" sowie jüngst im Ermittlungsverfahren gegen den „Prediger" „Abu Walaa" und andere.

2. Zu § 100e StPO-E:

Hinsichtlich des Verfahrens ist darauf hinzuweisen, dass die in § 100e Abs. 2 Satz 4 StPO-E enthaltene Monatsfrist bei der Umsetzung einer Online-Durchsuchung schon im Hinblick auf die zu schaffenden technischen Voraussetzungen für die tatsächliche Durchführung der Maßnahme unzureichend sein dürfte. Hier sollte eine Frist von zumindest zwei Monaten bei der Erstanordnung möglich sein. Dabei wird nicht verkannt, dass dann der „Gleichlauf" der Fristen mit einer Anordnung einer akustischen Wohnraumüberwachung nicht mehr gewährleistet wäre. Die tatsächliche Umsetzung einer akustischen Wohnraumüberwachung ist aber typischerweise nicht mit den technischen Hürden verbunden, die bei einer geplanten Online-Durchsuchung zu überwinden sind.

3. Hinweis zur Begründung in der Formulierungshilfe zum Gesetzentwurf (B., zu Buchstabe c, Absatz 5):

Die Aussage, eine nicht zur Verfügung stehende Software mache eine Maßnahme zur Quellen-TKÜ „unzulässig", dürfte jedenfalls für den Fall einer bereits laufenden Maßnahme zu weit gehen, wenn die Software lediglich aufgrund von äußeren Umständen (zum Beispiel Updates einer Software eines Messengerprogramms) funktionsunfähig wird. Sollte die Maßnahme nach einer Veränderung des Zielsystems durch den Betroffenen nicht mehr vollzogen werden können, müsste bei dieser strikten Auslegung nach Anpassung der Überwachungssoftware ein erneuter Beschluss zur Überwachung beantragt werden, weil die Maßnahme selbst (vorübergehend) nicht mehr durchgeführt werden konnte und demnach beendet wäre. Dies scheint zur Wahrung der Verhältnismäßigkeit des Eingriffs aber nicht erforderlich, weil sich an der Überwachungssituation sonst nicht geändert hat. Eine solch strenge Auslegung findet im geplanten Wortlaut des Entwurfs aus meiner Sicht auch keine ausreichende Stütze.

4. Weiterer Hinweis zur Begründung in der Formulierungshilfe zum Gesetzentwurf (B., zu Buchstabe c, Absatz 6):

Grundsätzlich ist die Dokumentation und Protokollierung der Funktionsweise, der Änderungen im Zielsystem und der übermittelten Daten verfassungsrechtlich erforderlich, um den Eingriff so nachvollziehbar wie möglich zu dokumentieren und ihn richterlich überprüfbar zu machen. Soweit hierfür allerdings die Dokumentation des Quellcodes einer Überwachungssoftware für erforderlich gehalten wird, gebe ich zu bedenken, dass dieser Quellcode mit der Dokumentation der konkreten Funktionsweisen des Programms auch in den Akten nachvollziehbar dargelegt werden müsste. Dies würde - angesichts der Erfahrungen mit der tatsächlichen Geheimhaltung von sicherheitsrelevanten Sachverhalten - mit an Sicherheit grenzender Wahrscheinlichkeit regelmäßig dazu führen, dass die Überwachungssoftware lediglich einmalig einsetzbar wäre, weil Quellcode und konkrete Arbeitsweise des Überwachungsprogramms über die Akteneinsicht an die Beschuldigten heraus an die Öffentlichkeit gelangen und gegebenenfalls in öffentlicher Hauptverhandlung umfassend erörtert würden. Angesichts der tatsächlichen Umstände würden entsprechende Gegenmaßnahmen innerhalb kürzester Zeit zu erwarten sein, die die Überwachungssoftware funktionsunfähig machen und eine komplette Neukonstruktion derselben erfordern würde. Diese Neukonstruktion müsste wiederum umfassend in den Akten dokumentiert werden („Hase-und-Igel-Spiel"). Ausreichend muss daher aus meiner Sicht die nachvollziehbare Dokumentation der Funktionsweise und der durchgeführten Eingriffe sein, ferner, dass es über die dokumentierten Zugriffe und Änderungen hinaus keine weiteren gegeben hat. Hierzu bedarf es einer Darlegung des Quellcodes in den Akten nicht.