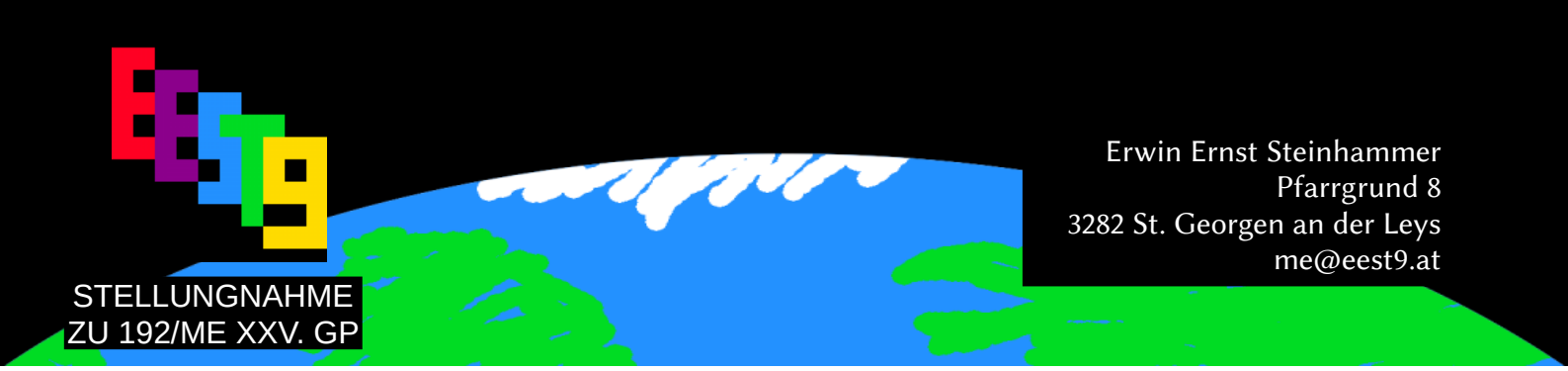

Erwin Ernst Steinhammer
Pfarrgrund 8
3282 St. Georgen an der Leys
me@eest9.at

Bundesministerium für Justiz
Museumstraße 7
1070 Wien
team.s@bmj.gv.at / begutachtungsverfahren@parlament.gv.at

01.05.2016

Betreff: Stellungnahme zum Ministerialentwurf 192/ME XXV. GP, mit dem die Strafprozessordnung 1975 und das Staatsanwaltschaftsgesetz geändert werden

Sehr geehrte Damen und Herren,

bezugnehmend auf das Begutachtungsverfahren zum Ministerialentwurf 192/ME XXV. GP, nehme ich als Techniker wie folgt Stellung:

Inhaltsverzeichnis

Erwin Ernst Steinhammer
Pfarrgrund 8
3282 St. Georgen an der Leys
me@eest9.at

Allgemeine Kritik

Grundsätzlich ist an diesem Gesetz zu kritisieren, dass die Erläuterungen vom Gesetzestext stark abweichen. Deshalb ist nicht klar in welcher Art und Weise dieses Gesetz in der Praxis angewendet werden wird, weswegen in dieser Stellungnahme versucht wurde ein breites Feld an Anwendungsmöglichkeiten abzudecken. Bei der Analyse dieses Gesetzes wurden folgende Hauptkritikpunkte festgemacht:

- Dieses Gesetz ist in sich nicht konsistent und weist zahlreiche Widersprüche zu den Erläuterungen auf.
- Die Folgenabschätzung ist unzureichend und lässt sowohl Grundrechtsbedenken aus noch beinhaltet sie eine Abschätzung der Wirksamkeit dieses Gesetzes.
    - Die Notwendigkeit des Gesetzes bleibt offen.
    - Grundrechtsbedenken wurden nicht behandelt.
    - Die Abschätzung der finanziellen Folgen ist unvollständig.
- Dieses Gesetz bleibt grundrechtlich bedenklich.

Widersprüchlichkeiten

Widersprüchlichkeiten ergeben sich beispielsweise, da in Teilen der Erläuterungen davon ausgegangen wird, dass dieses Gesetz nur eine physische Installation bzw. „direkter Zugriff“ erlaubt. Das Gesetz verbietet aber nirgends eine „Remote Installation“, sondern geht in mehreren Paragraphen sogar davon aus, dass ein physischer Zugriff nur erfolgen darf, wenn dieser unumgänglich ist.

Erwin Ernst Steinhammer
Pfarrgrund 8
3282 St. Georgen an der Leys
me@eest9.at

In folgender Tabelle findet sich eine Auflistung aller Stellen in den Erläuterungen und im Gesetzestext, die direkt oder indirekt mit der Frage des Zugriffs zu tun haben:

Remote Installation	Direkte Installation
Erl. zu Z 4 und 5 Abs. 3	Erl. zu Z 4 und 5 Abs. 1
Erl. zu Z 6 Abs. 1	Erl. zu Z 4 und 5 Abs. 2
Erl. zu Z 7 bis 10 Abs. 1	Erl. zu Z 6 Abs. 1
Erl. zu Z 7 bis 10 Abs. 3	Erl. zu Z 6 Abs. 2
Art. 1 Z 4: § 134 Z 4a	
Art. 1 Z 6: § 136 Z 2	
Art. 1 Z 7: § 137 Abs. 1	
Art. 1 Z 9: § 138 Abs. 1 Z 2	

Tabelle 1: "Remote Installation" vs. "Direkter Installation"

Weiters widerspricht sich das Gesetz in der Frage welche Daten überwacht bzw. erhoben werden dürfen. An einigen Stellen wird nur von Nachrichten an sich gesprochen, während andere Stellen auch Kontaktdaten, die Protokollierung aller Änderungen oder gesamte Back-ups verlangen.

In folgender Tabelle findet sich eine Auflistung aller Stellen, die in den Erläuterungen und im Gesetzestext direkt oder indirekt mit der Frage der zu erhebenden Daten zu tun haben:

Reine Nachrichtenüberwachung	Erweiterte Onlineüberwachung
Erl. Allg. Abs. 6	Erl. Allg. Abs. 9 vorletzter Satz
Erl. Allg. Abs. 9 letzter Satz	Erl. Allg. Abs. 12 letzter Satz
Erl. Allg. Abs. 12 2. Satz	Erl. zu Z 4 und 5 Abs. 1
Erl. zu Z 6 Abs. 3 Beginn	Erl. zu Z 6 Abs. 3 Mitte
Erl. zu Z 6 Abs. 3 Ende	Erl. zu Z 11
Art. 1 Z 6: § 136a Abs. 1	Erl. zu Z 12 bis 16 Abs. 1
Art. 1 Z 6: § 136a Abs. 3 Z 1 Beginn	Art. 1 Z 5: § 134 Z 5
	Art. 1 Z 6: § 136a Abs. 3 Z 1 Ende
	Art. 1 Z 13: § 145 Abs. 4

Tabelle 2: "Nachrichtenüberwachung" vs. "Erweiterte Onlineüberwachung"

Beide Bereiche befassen sich mit grundlegenden Befugnissen in diesem Gesetz und benötigen daher eine Eindeutigkeit.

Erwin Ernst Steinhammer
Pfarrgrund 8
3282 St. Georgen an der Leys
me@eest9.at

Notwendigkeit

In den Erläuterungen wurde auf Seite 3 einerseits unter Hinzunahme der terroristischen Straftaten (§§ 278b bis 278f StGB) die Notwendigkeit begründet, andererseits aber mit dem kleinen und großen Späh- und Lauschangriff (§ 136 Abs. 1 Z 2 und 3 StPO) ein maßvoller Einsatz konstruiert.

	an Verfahren wegen § 278b StGB	an Anklagen wegen § 278b StGB	Überwachte nach § 136 Abs. 1 Z 3 StPO	Überwachte nach § 136 Abs. 1 Z 2 StPO	§ 136 Abs. 1 Z 3 StPO & § 136 Abs. 1 Z 2 StPO
2012	75		2	3	5
2013	62		3	1	4
2014	115			6	6
2015	200	49			
2016	30	8			

Tabelle 3: Auflistung der Werte aus Seite 3 der Erläuterungen

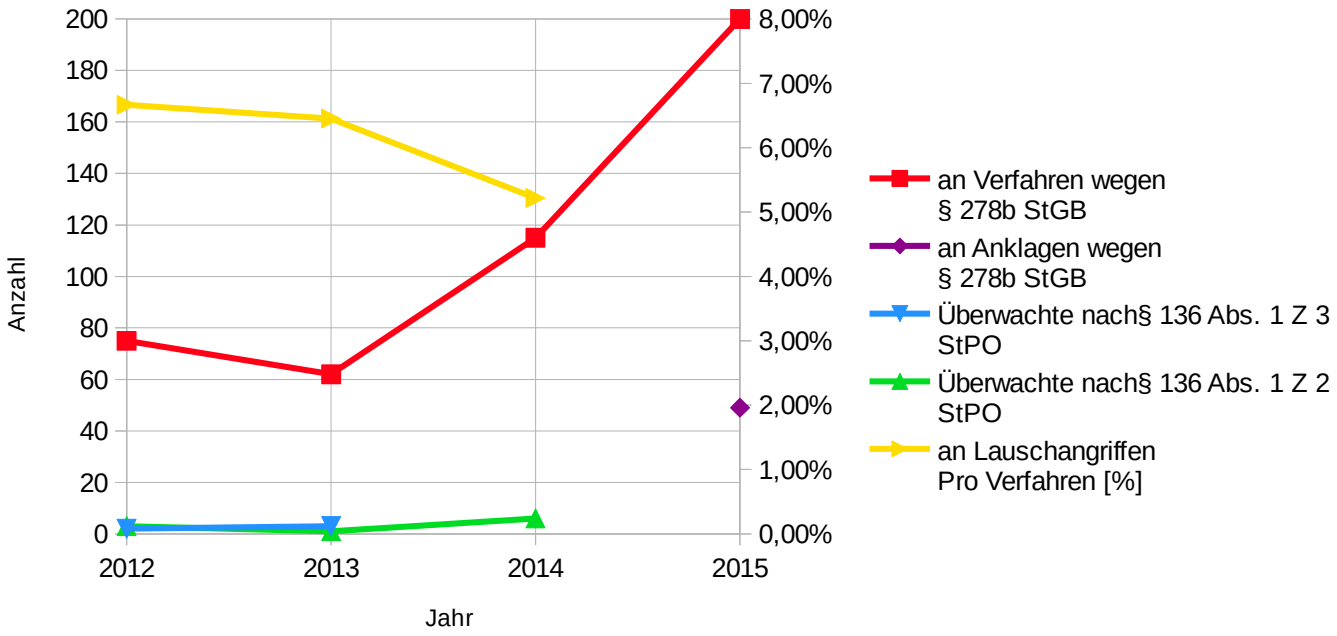

Abbildung 1: Diagramm mit den Werten aus Tabelle 3

Erwin Ernst Steinhammer
Pfarrgrund 8
3282 St. Georgen an der Leys
me@eest9.at

Anzeigen und Anklagen terroristischer Straftaten

Wie in Abbildung 1 ersichtlich, reichen diese Zahlen nicht aus, um einen Trend zu erkennen. Die Werte aus dem Jahr 2016 wurde absichtlich ausgelassen, da für diese im Vergleichszeitraum der vergangenen Jahre keine Werte angegeben waren.

Da der § 278b nicht in der jährlichen Kriminalitätsstatistik[i] aufscheint, konnten für eine Trendanalyse nur §§ 278 und 278a herangezogen werden.

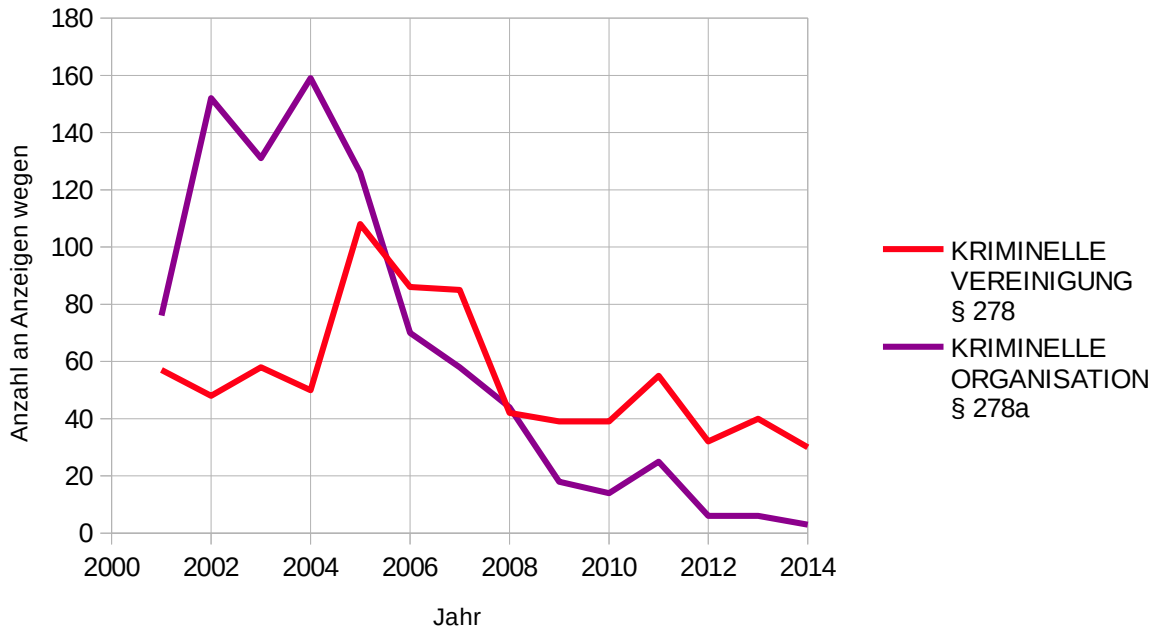

Abbildung 2: Anzeigen nach §§ 278 und 278a pro Jahr

Wie deutlich zu erkennen ist, gehen die Anzeigen für beide Paragraphen zurück. In den Jahren 2004 bis 2009 sogar deutlich, daher ist aufgrund der beiden §§ 278 und 278a keine Notwendigkeit erkennbar. Im Gegenteil, der starke Rückgang in den letzten 15 Jahren sollte sogar als Argument gegen eine derartige Notwendigkeit angesehen werden.

Erwin Ernst Steinhammer
Pfarrgrund 8
3282 St. Georgen an der Leys
me@eest9.at

Da in den Erläuterungen für 2015 ebenfalls Anklagen angeführt waren, diese aber als ein Einzelwert nicht ausreichen, habe ich diese ebenfalls mit öffentlich einsehbaren Zahlen verglichen. In der Gerichtlichen Kriminalstatistik[ii] werden die terroristischen Straftaten (§§ 278b bis 278f StGB) nicht einzeln aufgelistet, weshalb für das Diagramm die §§ 274-287 herangezogen wurden, welche die §§ 278b bis 278f StGB beinhalten.

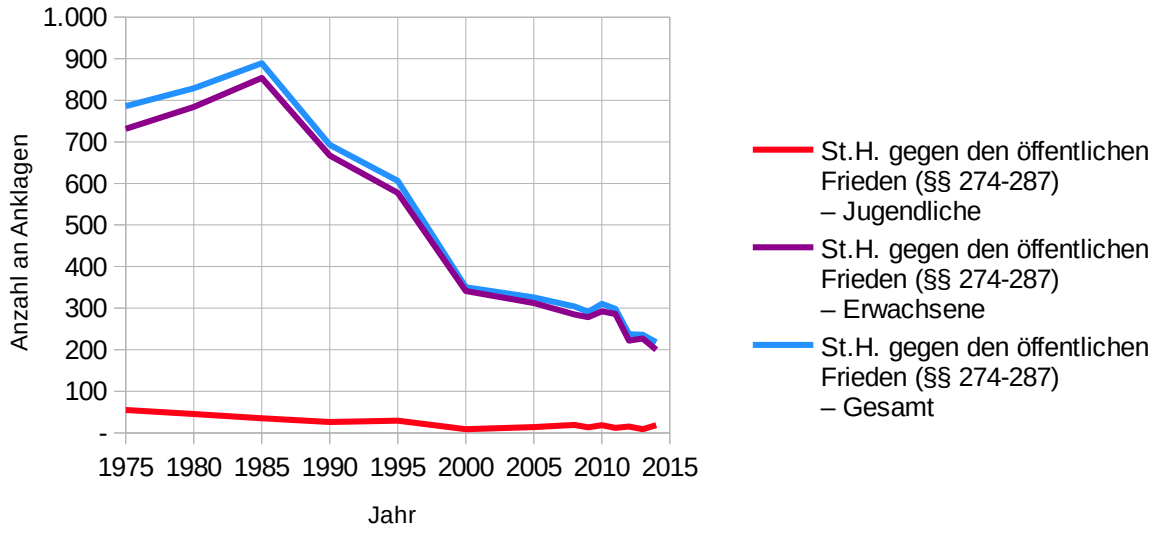

Abbildung 3: Anklagen nach §§ 274-287 pro Jahr

Wie zu erkennen ist, existiert auch hier ein rückläufiger Trend, der sich in den letzten Jahren sogar verstärkt hat.

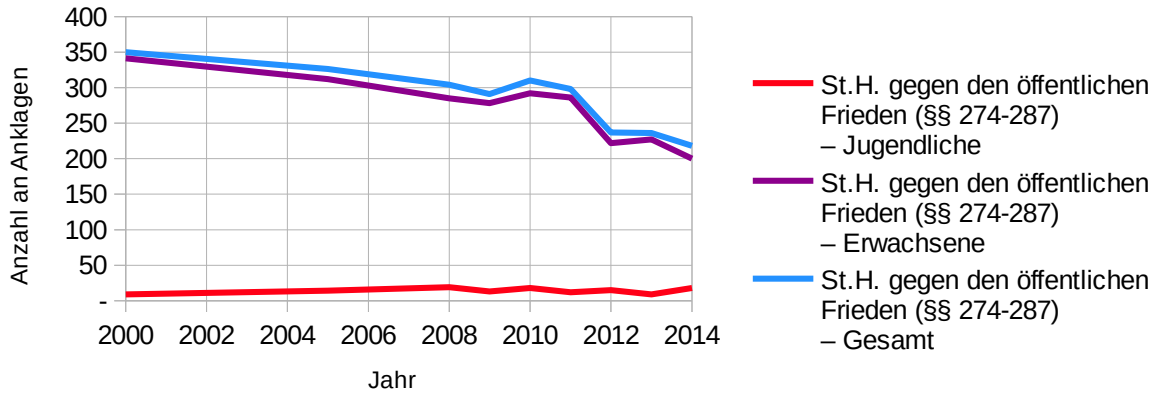

Abbildung 4: Anklagen nach §§ 274-287 seit 2000 pro Jahr

Erwin Ernst Steinhammer
Pfarrgrund 8
3282 St. Georgen an der Leys
me@eest9.at

Diese beiden Werte stützen also nicht die in den Erläuterungen geltend gemachte Notwendigkeit dieses Überwachungsparagraphen. Weder die „Deutlichkeit“, noch die Existenz einer Zunahme von terroristischen Straftaten konnten dort oder hier belegt werden.

Nachtrag: Auf meine Anfrage vom 11.04.2016 an das BMJ über die terroristischen Straftaten (§§ 278b bis 278f StGB) erhielt ich eine Antwort[iii] mit folgenden Tabellen:

	278b StGB	278c StGB	278d StGB	278e StGB	278f StGB
2012	36	4	30	3	4
2013	31	4	22	5	
2014	72	2	38	8	3
2015	142	5	23	7	2
Gesamt	281	15	113	23	9

Tabelle 4: Verfahren bei der Staatsanwaltschaft

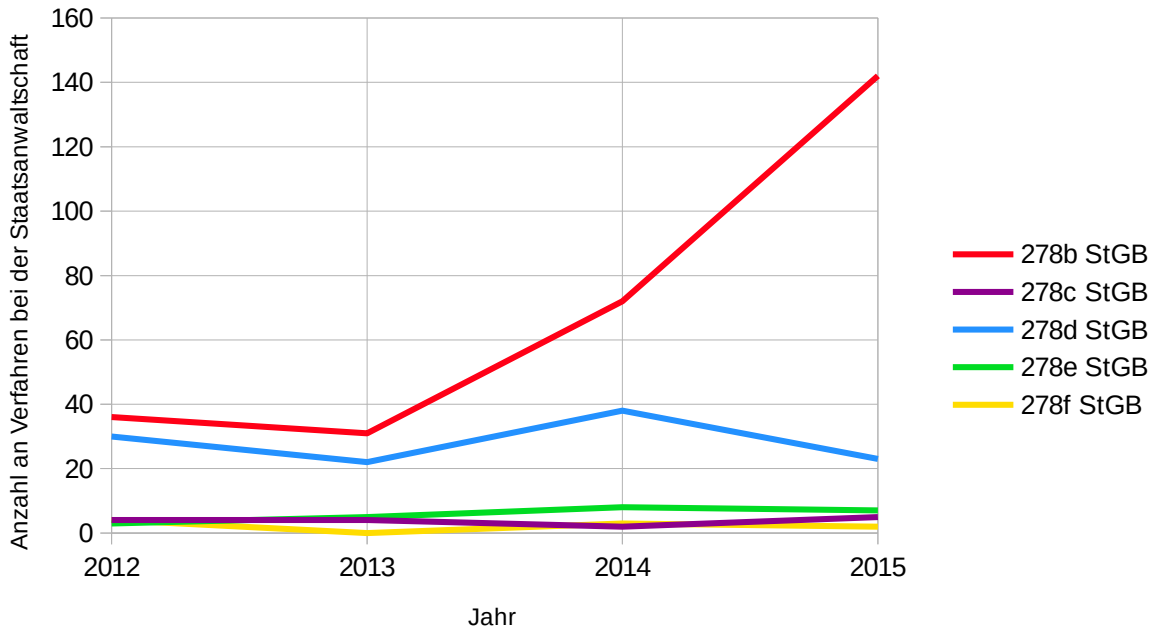

Abbildung 5: Verfahren zu terroristischen Straftaten bei der Staatsanwaltschaft

Erwin Ernst Steinhammer
Pfarrgrund 8
3282 St. Georgen an der Leys
me@eest9.at

	278b StGB	278c StGB	278d StGB	278e StGB	278f StGB
2012	6	2	1		
2013	1		2		1
2014	9			1	
2015	43	2	2	2	1
Gesamt	59	4	5	3	2

Tabelle 5: Anklagen

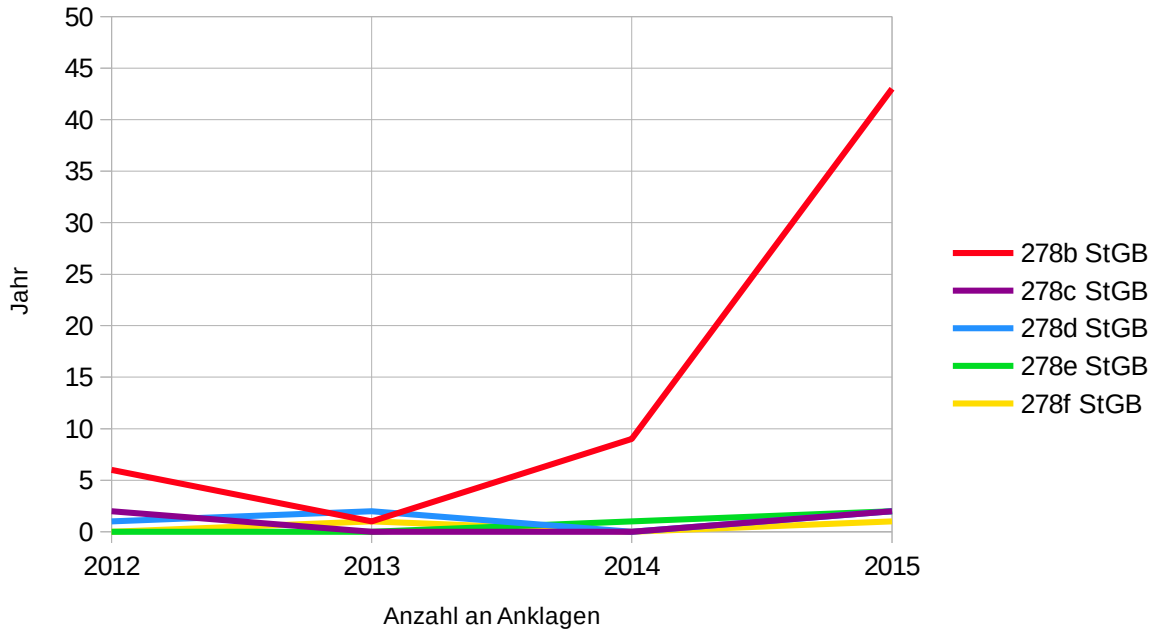

Abbildung 6: Anklagen nach terroristischen Straftaten

Die bereitgestellten Daten zeigen, dass nur bei den Anzeigen und Anklagen nach § 278b StGB (Terroristische Vereinigung) ein steigender Trend zu erkennen ist. Dieser Paragraph behandelt weder die Ausübung von terroristische Straftaten, Terrorismusfinanzierung, die Ausbildung für terroristische Zwecke oder die Anleitung zur Begehung einer terroristischen Straftat. Es hat also den Anschein, dass die derzeitigen Ermittlungsmaßnahmen ausreichen um schwerere terroristische Straftaten zu verhindern.

Es ist auch zu beachten, dass diese Daten nicht zeigen ob wirklich die Anzahl der Straftaten zugenommen hat, die Ermittlungsbehörden die Qualität der Aufklärung verbessert haben oder diese Straftaten häufiger zur Anzeige gebracht werden.

Erwin Ernst Steinhammer
Pfarrgrund 8
3282 St. Georgen an der Leys
me@eest9.at

Aus den herausgegeben Daten lässt sich durch den kurzen Betrachtungszeitraum auch nicht schließen, ob solche Spitzenwerte öfter auftreten oder den Beginn eines Trends kennzeichnen könnten.

Kleiner und großer Späh- und Lauschangriff

Ob mit den bisherigen Paragraphen des kleinen und großen Späh- und Lauschangriffs maßvoll umgegangen wurden, lässt, ohne Hintergrundinformationen über die einzelnen Einsätze, keine objektive Bewertung zu. Es konnten jedenfalls von 1999 bis 2014 nach den Kriminalberichten[iv] keine Trends ausgemacht werden:

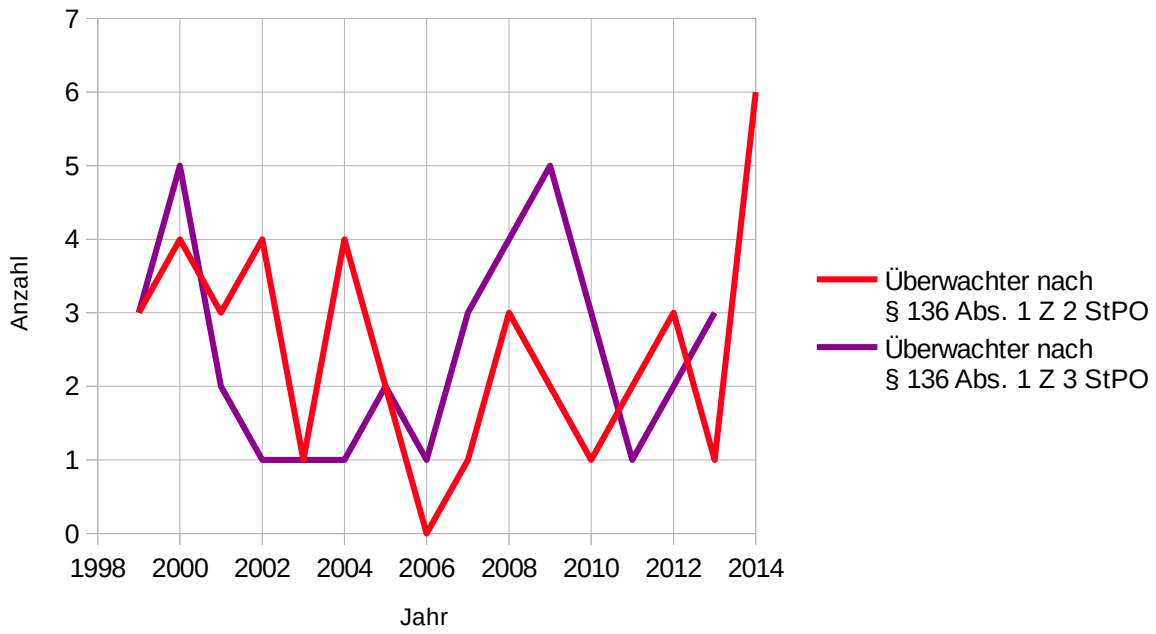

Abbildung 7: Häufigkeit der Anwendungen des kleinen und großen Späh- und Lauschangriffes

Alternativen

Im Vorblatt Seite 2, im Bereich „Nullszenario und allfällige Alternativen“ wird davon ausgegangen, dass die bisherigen Ermittlungsmethoden nicht ausreichen, um terroristischer Straftaten verdächtigte Personen, zu überführen. Es gibt jedoch keine Evaluierung dazu, ob das vorgeschlagene Gesetz dazu in der Lage ist.

Erwin Ernst Steinhammer
Pfarrgrund 8
3282 St. Georgen an der Leys
me@eest9.at

Folgenabschätzung

Zu kritisieren ist die im Vorblatt fehlende Folgenabschätzung bzw. die Begrenzung dieser auf die Lizenzgebühren. Dies deckt weder alle durch das Gesetz anfallenden Kosten ab, noch beinhaltet es Analysen über die Auswirkungen auf Grundrechte, Softwaresicherheit und anderer Aspekte die von diesem Gesetz berührt werden.

Detaillierte Darstellung der finanziellen Auswirkungen

Die behandelten Kosten beinhalten nur die Anschaffungskosten und Lizenzgebühren. Weitere Kostenpunkte, die durch dieses Gesetz entstehen, werden davon nicht behandelt, insbesondere jene nicht, die die angeführten Lizenzgebühren weit überschreiten werden.

- Fehlende Aufstellung der Kosten, die durch die manuelle Auswertung der Daten entstehen.
- Fehlende Kosten, die durch Weiterentwicklung und Updates der Software entstehen.
- Fehlende Kosten für das Beschaffen der Informationen über Sicherheitslücken.
- Fehlende Kosten durch das Schaffen und Offenhalten von Sicherheitslücken.
- Fehlende Kosten für die zu Artikel 1 Z 10 nötige Durchsicht aller Daten. Diese dürften die Lizenzgebühren bei weitem überschreiten.
- Weitere Kosten im Zusammenhang mit Artikel 1 Z 10.
- Fehlende Auflistung der Haftungen aus Artikel 1 Z 17.

Die Kostenabschätzung gibt auch nicht an, woher sie die Anschaffungskosten und Lizenzkosten kommen und können daher nicht nachvollzogen werden.

Weitere Auswirkungen

Wie bereits oben erwähnt, wird in der Folgenabschätzung nicht auf nicht finanzielle Folgen eingegangen. Dies beinhaltet vor allem:

- Grundrechtliche Folgen.
- Folgen auf die Entwicklung der Kriminalstatistik.

Erwin Ernst Steinhammer
Pfarrgrund 8
3282 St. Georgen an der Leys
me@eest9.at

Außerdem entwickelt der Staat Österreich durch ein solches Gesetz ein Interesse daran, dass Softwarebugs/-fehler, die von der Überwachungssoftware genutzt werden, nicht geschlossen werden. Dies bedeutet, dass er aktiv Sicherheitslücken ausnutzt und nicht mehr an ihrer Schließung mitwirken wird. Da durch die selben Sicherheitslücken auch andere in Computersysteme eindringen könnten, beeinträchtigt dies die Softwaresicherheit aller Computersysteme der Österreicherinnen und Österreicher. Würde eine weitere Ziffer eingefügt, dass sich der Staat trotzdem an der Schließung der ausgenutzten Softwarebugs beteiligt, würde dies eine aktive Selbstbehinderung bei der Überwachung bedeuten.

Beschwerdemöglichkeit

Im Vorblatt wird auf Seite 4 die Schaffung einer umfangreichen Beschwerdemöglichkeit beschrieben. Diese existiert jedoch nicht im Gesetz.

Wortwahl

Die Erläuterungen sprechen davon, dass dieses Gesetz keinen Staatstrojaner darstellt, weil er nicht remote installiert wird. Dies ist 1. falsch, weil das Gesetz eine remote Installation nicht verbietet, sondern sogar bevorzugt[1]. Andererseits hat die Begrifflichkeit „Trojaner“ nichts mit der Art der Installation zu tun. Ein Trojaner beschreibt eine Software, die ohne Wissen der Benutzerin/des Benutzers Daten vom Rechner an Dritte weiterleitet.

Installationen über das Internet unterscheiden sich nur insofern von lokalen Installationen, dass diese auch als „Würmer“ bezeichnet werden, während lokal vorgenommene Installationen als „Viren“ gelten. Aber auch diese Begrifflichkeiten haben keinerlei Auswirkungen auf die Folgen einer solchen Software, sondern stellen nur Definitionen für den vereinfachten Sprachgebrauch dar.

Im folgendem wird deshalb die Art der installierten Software als „Staatstrojaner“ bezeichnet.

1 Siehe Absatz Widersprüchlichkeiten.

Erwin Ernst Steinhammer
Pfarrgrund 8
3282 St. Georgen an der Leys
me@eest9.at

Spezifische Kritik

Bezieht sich in allen Punkten auf Artikel 1

Zu Ziffer 4

> *„4a. „Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden“ das Ermitteln von Nachrichten und sonstigen Daten (§ 74 Abs. 2 StGB), die im Wege eines Computersystems (§ 74 Abs. 1 Z 8 StGB) übermittelt und empfangen werden, durch Installation eines Überwachungsprogramms im Computersystem ohne Kenntnis des Inhabers eines solchen Systems oder sonstiger Verfügungsbefugter,“*

Im Gegensatz zum gelb hinterlegten Teil wird in den Erläuterungen eindeutig von einer „direkten Installation“ gesprochen.

Dieses Gesetz spricht von einer Installation ohne Kenntnisnahme des Inhabers. Technisch versierte Nutzer sind jedoch sehr wohl in der Lage zu überprüfen, welche Daten von einem System aus- und eingehen. Bei einer remote Installation des Staatstrojaners, die im Gesetz nicht verboten wird, würde dies bedeuten, dass der Inhaber des Computersystems unmittelbar während der Installation über verdächtige Datenübertragungen informiert werden würde. Eine unmittelbare Kenntnisnahme würde auch bedeuten, dass die Viren-/Wurmsoftware nicht in der Lage ist die Installation zu verschleiern, da diese zum Installationszeitpunkt noch gar nicht aktiv ist. Bei einer Installation direkt vor Ort könnten ebenfalls Logdaten von allen direkten Zugriffen auf das Computersystem Auffälligkeiten aufzeigen und somit einen Hinweis auf die Installation geben. Es kann also weder bei einer direkten, noch bei einer remote Installation des Staatstrojaners gewährleistet werden, dass ein Zugriff unbemerkt bleibt. Da sich Smartphones und -watches meistens am Körper oder in der Nähe des Inhabers befinden, kann hier eine direkte Installation ausgeschlossen werden, da eine solche Installation jederzeit entdeckt werden würde.

Zu Ziffer 5

In den Erläuterungen heißt es, dass auch Passwörter und PINs überwacht werden dürfen. Dies widerspricht aber dem Gesetzestext da viele Passwörter und PINs lokal verarbeitet werden und gar nicht erst übertragen werden. Siehe z.B. auch den Messanger „Signal“.

Erwin Ernst Steinhammer
Pfarrgrund 8
3282 St. Georgen an der Leys
me@eest9.at

Zu Ziffer 6

In Absatz 2 dieses Paragraphen wird davon gesprochen, dass das Eindringen in vom Hausrecht geschützte Räume nur erlaubt ist, sofern es unumgänglich ist. Da ein Eindringen in vom Hausrecht geschützte Räume für eine **direkte** Installation meistens nötig sein wird, nicht jedoch für eine remote Installation, bedeutet dies, dass per Default eine remote Installation zu wählen ist und nur im äußersten Ausnahmefall eine direkte Installation in Frage kommt. Den Erläuterungen, die hierzu von einer Notwendigkeit sprechen, dass das Überwachungsprogramm direkt auf den Computer installiert werden muss, kann nicht gefolgt werden. Damit stehen diese im Widerspruch zu diesem Gesetz.

In Absatz 3 Z 1 wird auch das Ermitteln von Kontaktdaten erlaubt, dies geht über die im Titel angedeutete Überwachung von Nachrichten weit hinaus. Im 3. Absatz der Erläuterungen, zu dieser Ziffer, wird ein solcher Zugriff sogar ausgeschlossen.

> *Unter einem solchen Zugriff ist allerdings keinesfalls eine Durchsuchung des Computersystems nach weiteren Daten zur Identifizierung einer Person oder sonstiger im Computersystem gespeicherter oder verarbeiteter Daten im Sinne einer „Online-Durchsuchung“ zu verstehen.*

In Absatz 3 Z 2 wird verlangt, dass der Staatstrojaner nach Beendigung der Ermittlungsmaßnahmen funktionsunfähig gemacht werden muss. Dies kann jedoch aus technischer Sicht nicht sichergestellt werden.

1. Ein entferntes Abschalten kann nicht sichergestellt werden da das Computersystem von Netz getrennt werden könnte.
2. Ein Timer kann den Zeitraum nicht zweifelsfrei feststellen, da ein Manipulieren der Computerzeit diesen umgehen könnte.
3. Falls die Biosbatterie bereits erschöpft ist würde sich die Computerzeit nach jedem Neustart auf 0 setzen und im abgeschalteten Zustand nicht weiterlaufen, damit kann das Einhalten des Ermittlungszeitraumes nicht mehr festgestellt werden.
4. Eine automatische Löschung bei leerer Biosbatterie könnte ausgenutzt werden um den Trojaner Aufwandslos zu deaktivieren/entfernen.

Erwin Ernst Steinhammer
Pfarrgrund 8
3282 St. Georgen an der Leys
me@eest9.at

5. Ein Programm kann seine eigene Entfernung nicht sicherstellen, überwachen, protokollieren und/oder festhalten.
6. Eine physische Deinstallation kann nicht sichergestellt werden, da das Computersystem, besonders auch bei mobilen Geräten, um die es laut den Erläuterungen auch geht, jederzeit den Ort wechseln könnte.
7. Eine Deinstallation kann auch nicht beim Wechsel des Besitzers sichergestellt werden, da ein solcher Wechsel nicht einwandfrei festgestellt werden kann. Eine Neuinstallation kann auch ohne Besitzerwechsel stattfinden und ein Besitzerwechsel kann auch ohne Neuinstallation stattfinden. Besonders der 2. Fall wird bei Laien oft vorkommen.
8. Der Staatstrojaner würde sich auch in Backups befinden. Diese sind meistens verschlüsselt wodurch es ohne den Schlüssel unmöglich wird, sie aus dem Back-up zu entfernen. Das Gesetz lässt aber nicht das Überwachen dieses Schlüssels zu. Da sich der Schlüssel auch ändern kann, was alle 6 Monate empfohlen wird, reichen Informationen über den Schlüssel zum Installationszeitpunkt nicht aus, um ein restloses Entfernen sicherzustellen.

Als Techniker gehe ich im Moment davon aus, dass für das Sicherstellen, nicht jedoch für die Deinstallation selbst, einer restlosen Deinstallation, ein gesamtes Back-up des Systems vor der Installation notwendig ist. Ein solches Back-up widerspricht jedoch dem im Gesetz festgeschriebenen Prinzip, dass nur übertragene Daten überwacht werden dürfen und kommt einer Gesamtüberwachung des Systems gleich.

Zu Ziffer 7

Ich erachte es als unbedingt notwendig, dass dieser Paragraph erhalten bleibt. Es sei aber darauf hingewiesen, dass hier wieder der Eindruck entsteht, dass eine remote Installation der Standardfall ist.

Zu Ziffer 8

Die Erläuterungen stellen klar, dass das Anordnen für einen vergangenen Zeitraum keine Bewilligung für eine unrechtmäßige Überwachung sein kann. Was ansonsten mit vergangenem Zeitraum gemeint ist bleibt unklar, daher sollte dieser Teil gestrichen oder präzisiert werden.

Erwin Ernst Steinhammer
Pfarrgrund 8
3282 St. Georgen an der Leys
me@eest9.at

Zu Ziffer 9

§ 138 Abs. 1 lautet:

„(1) Anordnung und gerichtliche Bewilligung einer Beschlagnahme von Briefen nach § 135 Abs. 1 haben die Bezeichnung des Verfahrens, den Namen des Beschuldigten, die Tat, deren der Beschuldigte verdächtig ist, und ihre gesetzliche Bezeichnung sowie die Tatsachen, aus denen sich ergibt, dass die Anordnung oder Genehmigung zur Aufklärung der Tat erforderlich und verhältnismäßig ist, anzuführen; Anordnung und Bewilligung nach den §§ 135 Abs. 2 und 3, 136 und 136a haben überdies zu enthalten:

…

2. die für die Durchführung der Ermittlungsmaßnahme in Aussicht genommenen Örtlichkeiten sowie das Computersystem, das überwacht werden soll,

…

Dieser Paragraph spricht von einer „in Aussicht genommenen Örtlichkeit“. In den Erläuterungen wird klar, dass diese Formulierung gewählt wurde, da man von einem Unbekannten oder nicht fixierten Örtlichkeit ausgeht. Damit wird wiederum eindeutig ein remote Zugriff beschreibt, da man ansonsten die Örtlichkeit kennen müsste. Bei einer direkten Installation könnte man zumindest ersatzweise den Installationsort als „Örtlichkeit“ annehmen.

Zu Ziffer 10

Die nach einer durchgeführten Überwachungsmaßnahme obligatorische Information aller von der Maßnahme betroffenen Personen ist unbedingt notwendig für einen angemessenen Rechtsschutz. Trotz der Notwendigkeit ist aber darauf hinzuweisen, dass dieser Paragraph in der Praxis kaum durchführbar ist. Wie den Erläuterungen schon an früheren Stellen zu entnehmen ist, soll dieses Gesetz auch dazu dienen Onlinekommunikation und Datenübertragungen auf Smartphones, im Speziellen auch Whats App, zu überwachen. Besonders beim Dienst Whats App haben sich aber so genannte „Gruppenchats“ eingebürgert bei denen oft auch über 30 Personen zeitgleich beteiligt sind. Es kann weder bei echten Terroristen noch bei fälschlich Verdächtigten ausgeschlossen werden, dass solche Gruppenchats verwendet werden wodurch die Anzahl der Betroffenen ein hohes Maß aufweist und damit eine hohe Anzahl an Personen zu informieren sind. Ferner noch beschreibt dieses Gesetz alle Datenübertragungen im Internet als Nachrichten im Sinne des Gesetzes, dies bedeutet auch, dass alle in der Facebook Timeline erschienen Personen betroffen wären. Im Moment beträgt der Median an Facebook-Freunden 342[v]. Theoretisch sind sogar alle

Erwin Ernst Steinhammer
Pfarrgrund 8
3282 St. Georgen an der Leys
me@eest9.at

Personen betroffen, die auf einer vom Überwachten angesurften Seite[vi] Inhalte verbreitet haben. Wie zum Beispiel Journalisten von Onlinezeitungen und Blogger. Weiters sind beteiligte an Onlinespielen oder in Onlineforen betroffen, die Erläuterungen sprechen sogar explizit von der Playstation 4, was die Anzahl an zu informierenden weiter erhöht. Das informieren all dieser Personen stellt einen unglaublichen Verwaltungsaufwand und damit einen im Vorblatt fehlenden Kostenpunkt, dar.

Der Paragraph lässt auch offen wie damit umgegangen wird, wenn die an der Kommunikation Beteiligten nicht zweifelsfrei festgestellt werden können. Dies benötigt unbedingt eine Klärung, da solche Fälle mit Sicherheit vorkommen werden:

- In Internetforen wird oft mit Pseudonymen agiert, damit können die Personen nicht zweifelsfrei identifiziert werden.
    - In Onlinespielen wird fast ausschließlich Pseudonym kommuniziert.
- Es ist oft unklar woher die Inhalte von in der Cloud gespeicherten Dateien stammen wodurch deren Urheber und damit von der Überwachung betroffene nicht informiert/identifiziert werden können.
    - Dateien geben zwar oft den ursprünglichen Urheber und den letzten Bearbeiter an, aber alle dazwischen beteiligten Personen gehen meistens verloren.
- Wer wird bei, an der Kommunikation beteiligten Fake-Profilen informiert?

10. *§ 138 Abs. 5 lautet:*
„(5) Nach Beendigung einer Ermittlungsmaßnahme nach den §§ 135 Abs. 2 und 3, 136 und 136a hat die Staatsanwaltschaft ihre Anordnung und deren gerichtliche Bewilligung dem Beschuldigten und den von der Durchführung der Ermittlungsmaßnahme Betroffenen unverzüglich zuzustellen. Die Zustellung kann jedoch aufgeschoben werden, solange durch sie der Zweck dieses oder eines anderen Verfahrens gefährdet wäre. Wenn die Ermittlungsmaßnahme später begonnen oder früher beendet wurde als zu den in Abs. 1 Z 4 genannten Zeitpunkten, ist auch der Zeitraum der tatsächlichen Durchführung mitzuteilen.“

Dieser Paragraph sollte entsprechend angepasst werden, damit Betroffene auch bei einer, durch eine Verlängerung der Maßnahme zustande gekommenen, späteren Beendigung der Überwachungsmaßnahme über den tatsächlichen Durchführungszeitraum zu informieren ist.

Erwin Ernst Steinhammer
Pfarrgrund 8
3282 St. Georgen an der Leys
me@eest9.at

Der Paragraph lässt weiters unklar wie mit Betroffen aus dem Ausland umgegangen wird um nicht in diplomatische Schwierigkeiten mit anderen Ländern zu kommen. Eine solche Überwachung fremder Staatsbürger, zu der es in unserer vernetzten Welt zwingend kommen wird und die auch in den Erläuterungen explizit erwähnt wird, könnte von vielen Ländern als Spionageakt, gegen eben diese Länder, gewertet werden. Besonders problematisch wird es wenn fremde Würdenträger, Diplomaten oder andere Vertreter fremder Staaten betroffen sind. Da sich im Vorhinein nicht voraussagen lässt, mit welchen Personen online kommuniziert wird, kommt auch eine vorhergehende Koordination mit den Ausländischen Behörden nicht in Frage.

Zu Ziffer 13

Die in diesem Paragraph verlangte Protokollierung umfasst alle Veränderungen am Computersystem und geht damit weit über die, im Gesetz beschriebene, Überwachung von Nachrichtenübermittlungen hinaus. Daher sollte dieser Teil ersatzlos gestrichen werden.

Weiters fehlt eine Speicherfrist für diese umfassenden Daten über das gesamte Computersystem. Ein Staat hat nicht nur die Aufgabe seine Bürgerinnen und Bürger von terroristischen Straftaten zu beschützen, sondern auch, wie am Beispiel der „Rosa Liste“ gut zu sehen war, alle Bürgerinnen und Bürger vor einem späteren Missbrauch der gesammelten Daten zu bewahren. Dafür ist eine Speicherfrist unumgänglich.

Zu den Problemen bei der Deinstallation des Staatstrojaners siehe auch die dementsprechende Kritik zu Ziffer 6.

Zu Ziffer 17

Die hier aufgeführten Haftungen fehlen in der Folgenabschätzung.

In diesem Paragraphen soll die, in vielen Ländern ungeklärte, Frage der Haftungen bei durch den Trojaner verursachten Schäden klären und wird daher begrüßt. Dabei geht dieser Paragraph jedoch nicht weit genug und behandelt nur finanzielle Folgen. Wie wird bei anderen Folgen, zum Beispiel, wenn der Überwachte nach Bekanntwerden der Maßnahme sozial Isoliert wird oder wenn sich nach Beendigung der Maßnahme ein psychisches Trauma, zum Beispiel ein Verfolgungswahn, manifestiert, umgegangen? Diese Fragen bedürfen einer Klärung im Gesetz.

Erwin Ernst Steinhammer
Pfarrgrund 8
3282 St. Georgen an der Leys
me@eest9.at

Conclusio

Anlassgesetzgebung

Wie oben Erläutert gibt es keine feststellbare Notwendigkeit für dieses Gesetz. Es wurde kurz nach den Anschlägen in Brüssel, in einer seit Monaten unveränderter Form, aus der Schublade[vii] gezogen um eine Reaktion auf diese vorweisen zu können. Es gibt nicht einmal einen Beleg für die Wirksamkeit dieses Gesetzes. Außerdem fehlt eine Abschätzung darüber, ob es überhaupt in der Lage ist die im Vorblatt gewünschten Auswirkungen zu zeigen.

Grundrechte

Da ich kein Jurist bin verweise ich hierfür auf die Stellungnahme vom „Verein Arbeitskreis Vorratsdaten Österreich“, der ich mich vollinhaltlich anschließe.[viii]

Empfehlung

Es wird empfohlen den Gesetzesvorschlag aufgrund mangelnder Notwendigkeit, fehlender Folgenabschätzung und Grundrechtlicher Bedenken zurückzuziehen.
Falls dieser Empfehlung nicht nachgekommen wird, wird zumindest eine Generalüberarbeitung des Gesetzes und ein erneutes Begutachtungsverfahren oder eine Ausschussbegutachtung empfohlen.

Mit freundlichen Grüßen
Erwin Ernst Steinhammer

Erwin Ernst Steinahmmer
Pfarrgrund 8
3282 St. Georgen an der Leys
me@eest9.at

i Quellen:
- http://www.bmi.gv.at/cms/BMI_Service/SIB_2014/Kriminalitaetsbericht_2014_BK.pdf
- https://www.parlament.gv.at/PAKT/VHG/XXIII/III/III_00114/imfname_100252.pdf
- https://www.parlament.gv.at/PAKT/VHG/XXIV/III/III_00186/imfname_200623.pdf

ii Quelle: www.statistik.at/wcm/idc/idcplg?IdcService=GET_PDF_FILE&dDocName=103629
iii Quelle: https://fragdenstaat.at/anfrage/bedrohung-durch-terroristische-straftaten-278b-bis-278f-stgb/#nachricht-1580
iv Quellen:
- Erläuterungen
- https://www.parlament.gv.at/PAKT/VHG/XXII/III/III_00105/imfname_417578.pdf
- https://www.parlament.gv.at/PAKT/VHG/XXIII/III/III_00004/imfname_070588.pdf
- https://www.parlament.gv.at/PAKT/VHG/XXIII/III/III_00115/imfname_101124.pdf
- https://www.parlament.gv.at/PAKT/VHG/XXIV/III/III_00110/imfname_178075.pdf
- https://www.parlament.gv.at/PAKT/VHG/XXIV/III/III_00373/imfname_283705.pdf
- https://www.parlament.gv.at/PAKT/VHG/XXV/III/III_00079/imfname_353270.pdf
- https://www.parlament.gv.at/PAKT/VHG/XXV/III/III_00170/imfname_407406.pdf

v Quelle: http://blog.stephenwolfram.com/2013/04/data-science-of-the-facebook-world/
vi Quelle: http://de.statista.com/statistik/daten/studie/185092/umfrage/anzahl-der-webseitenbesuche-pro-nutzer-in-europa/
vii Quelle: http://fm4.orf.at/stories/1764335/
viii https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06426/index.shtml