Deutscher Bundestag
Enquete-Kommission
Internet und digitale Gesellschaft

Mitglieder der Projektgruppe

Zugang, Struktur und Sicherheit im Netz

Termine

26. März 2012 Sitzung

Weitere Termine folgen.

Berlin, 20. März 2012
Geschäftszeichen: PA 24/3
Bezug: -
Anlagen: -

Ergebnisprotokoll der 8. Sitzung der Projektgruppe Zugang, Struktur und Sicherheit im Netz am 5. März 2012

Vor Eintritt in die Tagesordnung
Die Protokolle der Sitzungen vom 16. Januar, 23. Januar und 6. Februar 2012 werden einstimmig genehmigt.

Änderungen der Tagesordnung werden nicht beantragt.

TOP 1
Diskussion des zweiten Teils des Textbeitrages zu den Themenfeldern „Kriminalität im Internet – Spionage – Sabotage“

Die Mitglieder beraten absatzweise das vorliegende Dokument zu den Themenfeldern „Kriminalität im Internet – Spionage – Sabotage“ (*Hinweis: Die Zeilennummern im Protokoll beziehen sich auf die am 1. März 2012 versandte PDF-Datei*).

Ein Mitglied bittet um Einfügung einer Fußnote (Zeile 45 ff.) mit Verweis auf die Erklärungen des Bundesverfassungsgerichtes bezüglich der Ablehnung der Verfassungsbeschwerde gegen § 202c Abs. 1 Nr. 2 StGB. Die Fußnote wird aufgenommen.

Ein Mitglied weist darauf hin, dass Spionage eine Vorstufe von Sabotage sei. Es bittet daher um Korrektur der Zeilen 56 bis 57.
Ein Mitglied führt aus, dass dies auch umgekehrt der Fall sei. Beide Varianten werden in den Text aufgenommen.

Ein Mitglied wirft ein, dass die Darstellung in Zeile 66 ff., dass Hacking-Kenntnisse generell nicht erforderlich seien, falsch sei. Es erfolgt eine Umformulierung in „nicht immer“.

Ein Mitglied bittet um Streichung des Wortes „frei“ in Zeile 66. Den Absatz ab Zeile 77 schlägt er vor, wie folgt umzuformulieren: „Die Anonymität führt dazu, dass Spionage von Ermittlungsbehörden und den dazugehörigen Nachrichtendiensten, oft nicht als feindliche Akte ausländischer Staaten oder Organisati-

onen erkannt werden können, so dass Spionage über das Internet für die Späher politisch-militärisch wesentlich geringere Risiken bieten.“ **Ein Mitglied** regt in diesem Zusammenhang an, das Wort „Anonymität“ gegen „die Möglichkeit der Verschleierung der eigenen Identität“ zu ersetzen. Nicht die Anonymität, sondern die Möglichkeit sich mittels der Nutzung einer ausländischen IP-Adresse verschleiert im Netz zu bewegen, stehe im Vordergrund. Beiden Änderung wird zugestimmt. Zudem wird die Aussage in Zeile 74 f., dass im Ausland sitzende Spione keine Strafverfolgung zu befürchten hätten, durch die Ersetzung des Wortes „aber“ durch „häufig“ relativiert.

Ein Mitglied informiert die Mitglieder über das Gespräch mit Oberstaatsanwalt Rainer Franosch von der Generalstaatsanwaltschaft Frankfurt am Main, Zentralstelle zur Bekämpfung der Internetkriminalität. Dieses habe am Vormittag stattgefunden und sei sehr informativ gewesen.

Ein Mitglied erklärt, dass der Absatz zur Organisierten Kriminalität ab Zeile 102 noch einmal überarbeitet werde. Die am Vormittag gewonnenen Erkenntnisse sollten integriert werden. **Ein Mitglied** plädiert dafür, dass der Absatz gekürzt und auf die ausführliche Darstellung im Kapitel „Kriminalität im Internet“ verwiesen werde. Dem Änderungswunsch wird entsprochen.

Ein Mitglied bittet – wie auch in den vorherigen Texten – um Ersetzung des Wortes „Diebstahl“ in Zeile 125 durch das Wort „Ausspähen“.

Ein Mitglied trägt vor, dass das *Kapitel 2.1.3.3 Staaten* (Zeile 119 ff.) eine Überbetonung der VR China enthalte und damit den typischen Medienberichten entspreche. Auch andere Staaten seien hier zu nennen. Vor allem die USA sei zu erwähnen, die ein solches Vorgehen auch eingeräumt habe. Insgesamt sei die Darstellung sehr oberflächlich und entspreche nicht der gebotenen Qualität. Die zitierten Quellen seien zum Teil fragwürdig. **Ein Mitglied** stimmt diesem Einwand zu. Eine objektivere Formulierung sei geboten. **Ein Mitglied** kündigt einen überarbeiteten Textvorschlag an. Diesem, so führt es aus, werde ein Satz vorangestellt, dass davon auszugehen sei, dass das Internet bei der Aufklärung aller Staaten eine Rolle spiele. Zudem solle darauf hingewiesen werden, dass es sich bei den angebrachten Beispielen um nicht bestätigte Presseberichte handle.

Ein Mitglied erläutert, dass Patente, wie in Zeile 148 dargestellt, nicht ausgespäht werden müssten. Diese seien veröffentlicht. **Ein Mitglied** erklärt, dass hier das Ausspähen vor Patentanmeldung gemeint sei. Der Text wird entsprechend korrigiert.

Auf Anregung **eines Mitglieds** werden in Zeile 145 neben „staatlichen Stellen“ auch „andere Wirtschaftunternehmen“ erwähnt.

Ein Mitglied erläutert, dass es in vielen Fällen – anders als im Text ab Zeile 153 dargestellt – feststellbar sei, ob hinter einem Angriff eine staatliche Stelle oder ein Unternehmen stehe. Der Text wird entsprechend korrigiert („nicht immer“).

Ein Mitglied spricht sich dafür aus, das *Kapitel 2.1.3.5 Weitere Akteure* (Zeile 163 ff.) zu streichen. Die genannten Akteure könnten in die zuvor genannten Gruppen eingegliedert werden. Nach kurzer Diskussion verständigen sich die Mitglieder darauf, den Abschnitt nicht zu streichen.

Ein Mitglied stellt fest, dass die Darstellung der Rechtsdurchsetzung in *Kapitel 2.2.2.1.2* (Zeile 208 ff.) sehr kurz sei. Es gehe zwar um „enforcement“, aber es müsse auch auf die Ausstattung und Ausbildung der Strafverfolger eingegangen werden. Auch die Defizite in der Strafprozessordnung müssten aufgezeigt werden. Es weist darauf hin, dass im Expertengespräch auch die Problematik der Vergütung und der daraus resultierende Personalmangel angesprochen worden sei. Andere Staaten setzen auch finanzielle Anreiz zur Gewinnung qualifizierter Hacker ein.

Ein Mitglied fasst den genannten Abschnitt als Rekurs auf das *Kapitel Kriminalität im Internet* auf. Ihm fehle jedoch die Überlegung, ob sich besondere Herausforderungen in Bezug auf Spionagefragen bei der Rechtsdurchsetzung stellten. Die Durchsetzung von Strafrechten sei bei unabhängig handelnden privaten Akteuren noch möglich. Gegenüber ausländischen Staaten, die sich des Instruments der Spionage bemächtigten, strafrechtlich vorzugehen, sei jedoch sehr schwierig. Schließlich werde man wahrscheinlich auch nicht gegen den eigenen Geheimdienst vorgehen. Dies sei im Text zu erwähnen.

Ein Mitglied stimmt der Erwähnung dieses Aspektes zu. Zudem solle der Text um die Erkenntnisse aus dem Gespräch mit OStA Rainer Franosch ergänzt werden.

Ein Mitglied weist darauf hin, dass mit OStA Rainer Franosch die Frage der personalen Ausstattung bei Polizei und Staatsanwaltsschaft ganz ausführlich diskutiert worden sei. Vor allem bei der Polizei gebe es einen strukturelle Bedarf hochqualifizierter Mitarbeiter. Des Weiteren sei über die Einbindung in die Laufbahnstrukturen gesprochen worden. Es schlägt vor, diese Aspekte bei der Kriminalitätsbekämpfung zu verorten. Auch für die Handlungsempfehlungen sei dies von Interesse.

Hinsichtlich des Kapitels Rechtsdurchsetzung im Kapitel Spionage teilt es mit, dass es aufgrund der Überschneidungen viele Querverweise geben müsse. Es sei jedoch bei der Frage der Rechtsdurchsetzung zwischen strafrechtlicher und strafprozessualer Rechtsdurchsetzung zu unterscheiden. Rechtsdurchsetzung könne sich nur gegen Menschen richten und Spione seien im Internetbereich noch schlechter zu fassen, als in der analogen Welt. **Dem Mitglied** fehle ein Absatz, in dem darauf hingewiesen werde, dass daher verstärkt auf Schutzmaßnahmen gegen solche Spionageaktivitäten gesetzt werden müsse.

Ein Mitglied bittet um Zusendung eines entsprechenden Absatzes.

Ein Mitglied stimmt den Ausführungen zu. Es habe hinsichtlich der Rechtsdurchsetzung noch eine Anmerkung. Diese beziehe sich nicht nur auf Spionage, sondern gelte auch für andere Bereiche. Es bittet um Erstellung eines Absatzes hinsichtlich der Probleme mit den Souveränitätsrechten der Staaten bei der Rechtsdurchsetzung.

Ein Mitglied antwortet, dass OStA Rainer Franosch genau diesen Aspekt sehr ausführlich dargelegt habe. Dies solle im Kapitel *Kriminalität im Internet* eingearbeitet werden.

Ein Mitglied greift den Vorschlag auf. Die Texte werden vor dem Hintergrund der Stellungnahme des Oberstaatsanwaltes noch einmal überarbeitet.

Ein Mitglied regt an, in *Kapitel 3.1.1.2 Begründung* (Zeile 282 ff.) neben politischen, militärischen und wirtschaftlichen auch gesellschaftliche Einrichtungen zu nennen, die der Sabotage ausgesetzt sein könnten. **Ein Mitglied** befürwortet diesen Vorschlag. Der Text wird entsprechend ergänzt.

Ein Mitglied sichert einen ergänzenden Absatz zu *Kapitel 3.1.2 Bedeutung des Internets für Sabotage* (Zeile 318 ff.) zu, in dem der Fall „Conficker“ beleuchtet werde.

Ein Mitglied kritisiert die in *Kapitel 3.1.4.1 Angriff mit hochentwickelter Malware (z.B. Stuxnet)* (Zeile 368 ff.) angeführte Quelle *Cyberwar* von Dr. Sandro Gaycken. Der Fall Stuxnet werde dort in vielen Details nicht korrekt wiedergegeben. Die Quelle sei daher nicht angemessen. **Ein Mitglied** fügt hinzu, dass die Darstellung sehr technisch und damit schwer verständlich sei. Der Abschnitt wird überarbeitet.

Ein Mitglied bezieht sich auf Zeile 448. Es führt aus, dass die Täter nicht eine entsprechende Sanktion ins Kalkül zögen, sondern die Tatsache, dass die Verfolgung schwierig sei. Sie setzten darauf, nicht gefasst zu werden. Der Text wird entsprechend angepasst.

Ein Mitglied wertet den Abschnitt *3.2.2.3 Initiativen* (Zeile 495 ff.) als sehr kurz. Hier seien auch Initiativen im Bereich der Aus- und Fortbildung zu erwähnen. **Ein Mitglied** merkt an, dass der Faktor Mensch auch bereits im Kapitel Schutz Kritischer Infrastrukturen erwähnt worden sei. Es erfolgt eine Prüfung und ggf. Anpassung des Textes.

Ein Mitglied teilt mit, dass in Kapitel *3.2.3 Defizitanalyse* (Zeile 504 ff.) ein Aspekt fehle. Es müsse erwähnt werden, dass Monokulturen im Softwarebereich Sabotage und Spionage vereinfachten. In Behörden und in der Wirtschaft sei gewisse Software sehr verbreitet. **Ein Mitglied** pflichtet der Ausführung bei. **Ein Mitglied** sichert einen entsprechenden Absatz zu. An welcher Stelle dieser verortet wird, ist noch offen.

Auf Anregung **eines Mitglieds** soll der Begriff Cyberterrorismus im Text vermieden werden. Die Mitglieder diskutieren über die Verwendung der Begriffe Cyberterrorismus und Terrorismus sowie die Frage, ob der Fall Stuxnet als terroristischer Akt anzusehen sei. **Ein Mitglied** sichert eine Überarbeitung des Textes zu.

TOP 2
Verschiedenes

Der **Vorsitzende** weist darauf hin, dass nur noch ein Sitzungstermin anberaumt sei. Er bittet das Sekretariat weitere mögliche Sitzungstermine zu benennen.

Der nächste Sitzungstermin ist Montag, der 26. März 2012.