Deutscher Bundestag **Drucksache 18/2505**

18. Wahlperiode 09.09.2014

Kleine Anfrage

der Abgeordneten Andrej Hunko, Annette Groth, Dr. André Hahn, Inge Höger, Ulla Jelpke, Kerstin Kassner, Niema Movassat, Harald Petzold (Havelland), Kathrin Vogler und der Fraktion DIE LINKE.

Die neue „Joint Cybercrime Action Taskforce“ bei Europol

Das Europäische Polizeiamt (Europol) hat am 1. September 2014 seine „Joint Cybercrime Action Taskforce“ (J-CAT) in Betrieb genommen (Pressemitteilung Europol vom 1. September 2014). Die Einheit ist in Den Haag angesiedelt. Dort hatte Europol bereits vor zwei Jahren das European Cybercrime Center (EC3) eingerichtet. Laut einer Mitteilung des Bundeskriminalamtes (BKA) vom 1. September 2014 haben Behörden aus Deutschland, Frankreich, Italien, Spanien, Großbritannien, den Niederlanden und Österreich „Cybercrime-Experten“ entsandt. Demnach seien auch „Cybercrimedienststellen“ aus den USA, Kanada, Australien und Kolumbien an der Initiative beteiligt. Auch die Privatwirtschaft sei eingebunden.

Die Einrichtung der „Joint Cybercrime Action Taskforce“ wird mit „gestiegenen Herausforderungen bei der Bekämpfung der Computer- und Internetkriminalität“ begründet. Das BKA hatte hierzu im September 2014 ein „Bundeslagebild Cybercrime 2013“ veröffentlicht. Es ist aus Sicht der Fragesteller fraglich, wozu die neue „Joint Cybercrime Action Taskforce“ überhaupt notwendig ist: Europol kann bei Bedarf sogenannte Gemeinsame Ermittlungsteams einrichten. Hiervon wird auch im Bereich der Internetkriminalität rege Gebrauch gemacht. Mehrere Mitgliedstaaten der Europäischen Union (EU), darunter auch Deutschland, beteiligten sich unter Mitarbeit von Europol an Razzien gegen vermeintliche Mitglieder des Anonymous-Netzwerks. Die weltweite Aktion wurde zusammen mit der Internationalen kriminalpolizeilichen Organisation (Interpol) ausgeführt (Pressemitteilung Europol vom 28. Februar 2012). Europol richtete damals ein internationales Treffen zu „Hacktivismus“ aus, um Ermittlungsverfahren zu koordinieren und das weitere Vorgehen zu planen.

Wir fragen die Bundesregierung:

1. Inwiefern hat sich die Bundesregierung am Zustandekommen der „Joint Cybercrime Action Taskforce“ beteiligt?
2. Wie hat sich die deutsche Delegation hierzu in den zuständigen Ratsarbeitsgruppen positioniert, und welche Fragen waren diesbezüglich strittig?
3. Worin liegt aus Sicht der Bundesregierung der Mehrwert gegenüber bereits existierenden Zusammenarbeitsformen mit Europol?
4. Welche privaten Firmen oder Institute sind nach Kenntnis der Bundesregierung an der „Joint Cybercrime Action Taskforce“ beteiligt, und worin besteht deren Mitarbeit?

5. Welche Behörden sind nach Kenntnis der Bundesregierung aus Frankreich, Italien, Spanien, Großbritannien, den Niederlanden und Österreich an der „Joint Cybercrime Action Taskforce“ beteiligt?
6. Welche „Cybercrimedienststellen“ sind nach Kenntnis der Bundesregierung aus den USA, Kanada, Australien und Kolumbien an „Joint Cybercrime Action Taskforce“ beteiligt?
7. Worin besteht aus Sicht der Bundesregierung der Mehrwert ihrer Teilnahme?
8. Welche Aufgaben sollen diese „Cybercrimedienststellen“ aus den USA, Kanada, Australien und Kolumbien nach Kenntnis der Bundesregierung in der „Joint Cybercrime Action Taskforce“ übernehmen?
9. Wie sollen diese „Cybercrimedienststellen“ aus den USA, Kanada, Australien und Kolumbien in der „Joint Cybercrime Action Taskforce“ nach Kenntnis der Bundesregierung administrativ und organisatorisch eingebunden werden, und an welchen Treffen werden diese teilnehmen?
10. Welche Kriminalitätsphänomene sollen nach Kenntnis der Bundesregierung von der „Joint Cybercrime Action Taskforce“ konkret verfolgt werden?
11. Auf welche Weise wird sich die „Joint Cybercrime Action Taskforce“ nach Kenntnis der Bundesregierung mit Hackerangriffen und dem Netzwerk TOR befassen?
12. Inwiefern hält die Bundesregierung TOR für ein brauchbares Werkzeug zur Aufrechterhaltung der digitalen Privatsphäre?
13. Auf welche Weise wird das BKA mit der „Joint Cybercrime Action Taskforce“ kooperieren?
14. In welcher Dienststelle ist der entsandte „Cybercrime-Experte“ angesiedelt?
15. Inwiefern und auf welche Weise soll die „Joint Cybercrime Action Taskforce“ nach Kenntnis der Bundesregierung Bedrohungen bereits im Vorfeld analysieren?
16. Auf welche Weise werden hierzu nach Kenntnis der Bundesregierung Informationen aus „offenen Quellen“ gespeichert und verarbeitet?
17. Auf welche Weise und in welchen Fällen werden hierzu nach Kenntnis der Bundesregierung Informationen aus polizeilichen Informationssystemen gespeichert und verarbeitet?
18. Welche Datensammlungen wurden nach Kenntnis der Bundesregierung für die Arbeit der „Joint Cybercrime Action Taskforce“ eingerichtet?
19. Auf welche „Focal Points“ kann die „Joint Cybercrime Action Taskforce“ nach Kenntnis der Bundesregierung zugreifen?
20. Was ist der Bundesregierung über Hintergründe einer Forderung der Innenminister der Länder zur Schaffung einer „Zentralstelle für die Verfolgung von Internetkriminalität“ bei den Staatsanwaltschaften bekannt, und wie wird sie sich hierzu positionieren (Pressemitteilung des Ministeriums für Inneres und Sport des Landes Mecklenburg-Vorpommern vom 5. September 2014)?
21. Auf welche Weise befassen sich das BKA und Europol nach Kenntnis der Bundesregierung derzeit mit dem Phänomen „Hacktivismus“ und der Repression vermeintlicher Mitglieder des Anonymous-Netzwerks?

22. Welche Mitteilungen haben Bundesbehörden im Rahmen von Ermittlungen bzw. der Anklageerhebung gegen den Gründer der Filesharing-Website Pirate Bay, Gottfrid Svartholm Warg, gegenüber dänischen Behörden gemacht, der für das Eindringen in das Schengen-Informationssystem verantwortlich gemacht wird, dies aber vehement bestreitet (www.heise.de vom 2. September 2014)?
23. Welche neueren Erkenntnisse hat die Bundesregierung darüber, ob bzw. wo es bis heute einen versuchten oder erfolgreich ausgeführten „cyberterroristischen Anschlag“ gegeben hat (Bundestagsdrucksachen 17/7578 und 18/164)?
24. Welche Angriffe auf digitale Infrastrukturen der Bundesregierung hat es im Jahr 2013 gegeben, die nachweislich bzw. mit großer Wahrscheinlichkeit von ausländischen Nachrichtendiensten begangen wurden, um welche Angriffe bzw. Urheber handelt es sich dabei, und in wie vielen Fällen wurde Schadsoftware mittels mobiler Datenträger in die IT-Netze eingebracht?
25. Welche Angriffe auf digitale Infrastrukturen der Bundesregierung hat es im Jahr 2013 gegeben, die vermutlich von ausländischen Nachrichtendiensten begangen wurden, um welche Angriffe bzw. Urheber handelt es sich dabei, und in wie vielen Fällen wurde Schadsoftware mittels mobiler Datenträger in die IT-Netze eingebracht?
26. Welche Treffen der „Friends of the Presidency Group on Cyber Issues“ haben nach Kenntnis der Bundesregierung auf EU-Ebene im Jahr 2014 stattgefunden, wer nahm daran jeweils teil, und welche Tagesordnung wurde behandelt?
27. Auf welche Weise ist der Komplex „Cybersicherheit“ nach Kenntnis der Bundesregierung im Rahmen der „Integrated Political Crisis Response“ (IPCR) der Europäischen Union berücksichtigt?
28. Welche IPCR-Übungen sollen nach Kenntnis der Bundesregierung in den Jahren 2014 und 2015 stattfinden, wo werden diese abgehalten, und wer wird jeweils teilnehmen?
29. Welche Auslöser von Krisen werden nach Kenntnis der Bundesregierung jeweils angenommen, und welche Szenarien werden jeweils durchgespielt?
30. Auf welche Weise bringen sich Bundesbehörden in die Vorbereitung der Übungen ein?

Berlin, den 9. September 2014

Dr. Gregor Gysi und Fraktion

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333