



POSTANSCHRIFT Bundesministerium des Innern, 11014 Berlin

Präsident des Deutschen Bundestages
– Parlamentssekretariat –
Reichstagsgebäude
11011 Berlin

HAUSANSCHRIFT Alt-Moabit 101 D, 10559 Berlin

POSTANSCHRIFT 11014 Berlin

TEL +49 (0)30 18 681-1117

FAX +49 (0)30 18 681-1019

INTERNET www.bmi.bund.de

DATUM 7. April 2015

BETREFF **Kleine Anfrage des Abgeordneten Andrej Hunko u. a. und der Fraktion DIE LINKE.**

Maßnahmen im operativen Europol-Aktionsplan für das Jahr 2015 zu Cyberangriffen mit deutscher Beteiligung

BT-Drucksache 18/4382

Auf die Kleine Anfrage übersende ich namens der Bundesregierung die beigelegte Antwort in 4-facher Ausfertigung.

Mit freundlichen Grüßen
in Vertretung

Cornelia Rogall-Grothe

Kleine Anfrage des Abgeordneten Andrej Hunko u. a. und der Fraktion DIE LINKE.

Maßnahmen im operativen Europol-Aktionsplan für das Jahr 2015 zu Cyberangriffen mit deutscher Beteiligung

BT-Drucksache 18/4382

Vorbemerkung der Fragesteller:

Im operativen Aktionsplan (OAP) zur Priorität „Cyberangriffe“ sind für das Jahr 2015 zahlreiche Maßnahmen mit deutscher Beteiligung enthalten (Bundestagsdrucksache 18/4074). Zu den deutschen Teilnehmenden gehören das Bundeskriminalamt (BKA), aber auch das Landeskriminalamt Bayern (BLKA). Behörden aus Deutschland würden laut der Bundesregierung „als Aktionsleiter, Co-Aktionsleiter oder Teilnehmer fungieren“. Zwar werden die einzelnen Maßnahmen in der Antwort auf die Kleine Anfrage vom Bundesinnenministerium aufgelistet, eine Beschreibung der Inhalte fehlt allerdings genauso wie eine Präzisierung der vom BKA oder dem BLKA übernommenen Tätigkeiten. Lediglich die deutsche Teilnahme in den Arbeitsgruppen „Joint Cyber Action Task Force“ (J-CAT) „Cybercrime Expertengruppe“ wurde auf Nachfrage beaufkündet (Bundestagsdrucksachen 18/2674, 18/4193). Letztere wird demnach vom BKA, dem BLKA „sowie Frankreich“ geleitet.

Laut der Antwort auf eine frühere Kleine Anfrage sind Aktionsleiter „insbesondere für die Koordination der Aktivitäten der Teilnehmer an der Maßnahme verantwortlich“ (Bundestagsdrucksache 18/4193). Sie sollten sich des Weiteren „mit den Co-Aktionsleitern zur weiteren Gestaltung der Maßnahme abstimmen und weitere Teilnehmer einbinden“. Arbeiten der Maßnahmen könnten demnach auch in „Arbeitsgruppen“ erfolgen (Bundestagsdrucksache 18/4193). Allerdings ist auch deren Zusammensetzung und Aufgabenstellung unbekannt.

Vorbemerkung:

Die Antworten auf die Fragen 1 und 7 beinhalten zum Teil Einzelheiten zu den technischen Fähigkeiten und ermittlungstaktischen Verfahrensweisen der Ermittlungsbehörden. Aus ihrem Bekanntwerden könnten Rückschlüsse auf den Modus Operandi, die Fähigkeiten und Methoden der Behörden gezogen werden. Deshalb sind einzelne Informationen gemäß der Verschlussanweisung (VSA) mit dem Geheimhaltungsgrad „VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestuft und werden als nicht zur Veröffentlichung in einer Bundestagsdrucksache bestimmte Anlage übermittelt.

1. Welche weiteren Details kann die Bundesregierung zu den folgenden, der Bundestagsdrucksache 18/4074 entnommenen Maßnahmen des OAP „Cyberangriffe“ mitteilen (bitte Kurzbeschreibung, Zielsetzung, voraussichtlicher Beginn/ voraussichtliches Ende, Rolle der „Leader“ und „Co-Leader“ ausführlich darstellen)

- a) Konsolidierung einer Internetauswertungskoordinierungsgruppe, Aktionsleiter ist das BKA, Co-Aktionsleiter ist Spanien, Unterstützer sind die EU-Mitgliedstaaten, Norwegen, Schweiz, Europol und Eurojust,
- b) Maßnahmen gegen inkriminierte Kommunikationsplattformen, Aktionsleitung durch das BKA, Unterstützer sind Griechenland und Spanien,
- c) Erhebung von Informationen zur Notwendigkeit eines „Compromised Data Clearing House“, Aktionsleitung durch das BKA, Co-Aktionsleitung durch die Niederlande, Unterstützer sind EU-Mitgliedstaaten, Europol, Interpol, CERTs,
- d) Entwicklung/Implementierung eines Anonymisierungsverfahrens für die Datenauswertung, Aktionsleitung durch Europol, Unterstützung durch Deutschland (BKA), Kroatien, J-CAT, Eurojust,
- e) Entwicklung/Implementierung einer Online-Ausbildungsplattform, Aktionsleitung durch Europol, Unterstützung durch Deutschland (BKA), CEPOL, EC-TEG,
- f) Erstellung des Internet Organised Crime Threat Assessment-I-OCTA, Aktionsleiter ist Europol, Unterstützer sind die EU-Mitgliedstaaten (für Deutschland das BKA), Norwegen, Eurojust und Interpol,
- g) Identifizierung von Cyberbedrohungen mit Auswirkung auf zwei oder mehr Mitgliedstaaten, Aktionsleiter ist Großbritannien, Co-Aktionsleiter ist Europol, Unterstützer sind die EU-Mitgliedstaaten (für Deutschland das BKA), Norwegen,
- h) Entwicklung gemeinsamer Methoden zur Cybercrimebekämpfung, Aktionsleiter ist Großbritannien, Co-Aktionsleiter ist Europol, Unterstützer sind die EU-Mitgliedstaaten (für Deutschland das BKA), Norwegen, Interpol,
- i) Identifizierung von wertigen Tätergruppen für gemeinsame Ermittlungen, Aktionsleiter ist Großbritannien, Co-Aktionsleiter ist Europol, Unterstützer sind die EU-Mitgliedstaaten (für Deutschland das BKA), J-CAT,
- j) Sammlung und Auswertung von Schadsoftware, die gegen Banken eingesetzt werden, Aktionsleiter ist Großbritannien, Co-Aktionsleiter ist Europol, Unterstützer sind die EU-Mitgliedstaaten (für Deutschland das BKA), J-CAT, Interpol,
- k) Maßnahmen gegen wertige Cybercrime-Gruppierungen, Aktionsleiter ist Großbritannien, Co-Aktionsleiter ist Rumänien, Unterstützer sind die EU-Mitgliedstaaten (für Deutschland das BKA), EUCTF, Europol, Eurojust,

- l) Identifizierung von und Ermittlungen gegen Cybercrime-Gruppierungen, die den Service von OK-Gruppierungen nutzen, Aktionsleiter ist Frankreich, Co-Aktionsleiter ist Rumänien, Unterstützer sind die EU-Mitgliedstaaten (für Deutschland das BKA), Norwegen, Europol, Eurojust,*
- m) Unterstützung der EU-Mitgliedstaaten und operativen Partner in der Integration von Finanzermittlungen in Ermittlungen im Rahmen des OAP, Aktionsleiter ist Europol, Unterstützer sind die EU-Mitgliedstaaten (für Deutschland das BKA), Norwegen, Eurojust,*
- n) Implementierung eines Koordinierungsmechanismus zur Bekämpfung von Botnetzen, Aktionsleiter ist Europol, Unterstützer sind Frankreich, Großbritannien und die EUCTF,*
- o) Erstellung von Richtlinien gemäß Art. 13 der Richtlinie 2013/40/EU zu Cyberangriffen gegen Informationssysteme, Aktionsleitung durch Kroatien, Co-Aktionsleitung durch Slowenien, Unterstützer sind Deutschland (BKA), Portugal, Europol, Eurojust, EUCTF, DG Home,*
- p) Entwicklung von Kursen und Kursmaterialien zur Aus- und Fortbildung von Cybercrime-Ermittlern, Aktionsleiter ist CEPOL, Co-Aktionsleiter sind Europol, Eurojust, ECTEG, Unterstützung durch die EU-Mitgliedstaaten (für Deutschland durch das BKA), DG Home,*
- q) Unterstützung einer operativen ITOM-Maßnahme zu Trainingszwecken, Aktionsleitung durch Niederlande, Co-Aktionsleitung durch Europol, Eurojust, Unterstützer sind die EU-Mitgliedstaaten (für Deutschland das BKA)?*

Zu 1.

Die Antwort zu Frage 1 ist als Verschlussache gemäß der VSA mit dem Geheimhaltungsgrad „VS - NUR FÜR DEN DIENSTGEBRAUCH“ eingestuft. Hierzu wird auf die Vorbemerkung verwiesen.

2. Welche Treffen haben bereits im Rahmen jener Maßnahmen stattgefunden, bei denen das BKA oder andere deutsche Behörden als Aktionsleiter oder Co-Aktionsleiter geführt sind (bitte Datum und Ort benennen)?

Zu 2.

Bisher hat eine Auftaktveranstaltung der Teilnehmer im Rahmen des Operativen Aktionsplans (OAP) Cyber-Attacks 2015 am 4./5. Februar 2015 in Den Haag stattgefunden.

3. Für welche der gesamten Maßnahmen im operativen Europol-Aktionsplan für das Jahr 2015 zu Cyberangriffen wurde nach Kenntnis der Bundesregierung für die Umsetzung die Form von Arbeitsgruppen gewählt, worum handelt es sich dabei und wer gehört diesen an?

Zu 3.

Für die Etablierung der Joint Cybercrime Action Taskforce (J-CAT) wurde die Form einer Arbeitsgruppe gewählt. Zu J-CAT wird auf die Antwort der Bundesregierung vom 26. September 2014 zur Kleinen Anfrage der Fraktion DIE LINKE. „Die neue ‚Joint Cybercrime Action Taskforce‘ bei Europol“ auf Bundestagsdrucksache 18/2674 verwiesen.

4. Welche der gesamten Maßnahmen im operativen Europol-Aktionsplan für das Jahr 2015 zu Cyberangriffen soll nach Kenntnis der Bundesregierung direkt oder indirekt mit dem eigentlich zur Internetbeobachtung gestarteten BKA-Projekt „Check the Web“ zusammenarbeiten und auf welche Weise wird dies umgesetzt?

Zu 4.

Eine Zusammenarbeit zwischen den Maßnahmen des OAP Cyber-Attacks aus dem EMPACT-Rahmen (Zielrichtung Schwere und Organisierte Kriminalität) und dem Focal Point „Check the Web“, der im AWF CT (Analysis Work File Counter Terrorism) bei Europol angesiedelt ist, ist nach Kenntnis der Bundesregierung nicht vorgesehen.

5. Welche französischen Behörden sind mit dem BKA und dem BLKA als „Leader“ in der „Cybercrime Expertengruppe“ organisiert?

Zu 5.

Die französische Gendarmerie.

6. Für welche der gesamten Maßnahmen im operativen Europol-Aktionsplan für das Jahr 2015 zu Cyberangriffen hat das BKA wie viele „Experten“ entsandt und aus welchen Abteilungen stammen diese jeweils (bitte auflisten, wenn ein „Experte“ mehrere Maßnahmen bzw. Arbeitsgruppen betreut oder begleitet)?

Zu 6.

Das Bundeskriminalamt (BKA) hat einen Mitarbeiter in das J-CAT entsandt, der aus der Abteilung Schwere und Organisierte Kriminalität stammt. Zu J-CAT wird auf die Antwort der Bundesregierung vom 26. September 2014 zur Kleinen Anfrage der Fraktion DIE LINKE. „Die neue ‚Joint Cybercrime Action Taskforce‘ bei Europol“ auf Bundestagsdrucksache 18/2674 verwiesen.

7. Inwiefern könnte die OAP-Maßnahme „Identifizierung von Cyberbedrohungen mit Auswirkung auf zwei oder mehr Mitgliedstaaten“ aus Sicht der Bundesregierung auch die Zusammenarbeit zur Abwehr und/oder Aufklärung von Cyberangriffen verbessern, wie sie beispielsweise auf den belgischen Provider Belgacom oder die EU-Kommission verübt wurden und mutmaßlich auf das Abhören auch deutscher EU-Abgeordneter zielte (www.heise.de vom 4. Oktober 2013, Der Spiegel vom 28. Dezember 2014)?

- a) Über welche neueren Erkenntnisse verfügt die Bundesregierung zur Urhebererschaft der im Jahr 2013 bekannt gewordenen Cyberangriffe auf Belgacom oder Einrichtungen der Europäischen Union?*
- b) Welche eigenen Ermittlungen bzw. Erkundigungen hat die Bundesregierung hierzu angestellt bzw. eingeholt?*
- c) Welche weiteren Möglichkeiten sieht die Bundesregierung zur Verbesserung der Aufklärung zur Urhebererschaft zukünftiger ähnlicher Cyberangriffe bzw. welche Anstrengungen hat sie hierzu bereits unternommen?*

Zu 7.

Die Antwort zu Frage 7 ist als Verschlussache gemäß der VSA mit dem Geheimhaltungsgrad „VS - NUR FÜR DEN DIENSTGEBRAUCH“ eingestuft. Hierzu wird auf die Vorbemerkung verwiesen.

8. Welche weitere „bekannte internationale staatliche Ansprechpartner“ [...] die sich mit der Thematik Gesichtserkennung befassen“ hat das BKA gegenüber Europol auf Nachfrage benannt (Bundestagsdrucksache 18/4193)?

Zu 8.

Das BKA hat nachfolgende internationale staatliche Ansprechpartner gegenüber Europol benannt:

- „International Facial Recognition Working Group“ (Interpol Lyon),
- „Facial Identification Scientific Working Group (FISWIG)“ (USA),
- „European Network of Forensic Science Institutes (ENFSI)“ (Sitz in den Niederlanden),
- „Netherlands Forensic Institute“ (Niederlande),
- „Swedish National Laboratory of Forensic Science“ (Schweden),
- „Centre for Applied Science and Technology, Home Office“ (Großbritannien),
- „Israel National Police“ (Israel).

9. Inwiefern ist nach Kenntnis der Bundesregierung mittlerweile bekannt, auf welche Weise das Projekt „Interpol project on interoperability – A practical development for enhanced police cooperation within EU Member States“ inzwischen weiterbetrieben oder umgesetzt wird (Ratsdokument 10094/14, Bundestagsdrucksache 18/4193)?

Zu 9.

Es wird auf die Antwort der Bundesregierung zu Frage 29 in der Bundestagsdrucksache 18/4193 vom 4. März 2015 verwiesen. Weitere Erkenntnisse liegen hierzu nicht vor.