Deutscher Bundestag **Drucksache 20/1040**

20. Wahlperiode 15.03.2022

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Ali Al-Dailami, Dr. Petra Sitte und der Fraktion DIE LINKE.
– Drucksache 20/902 –

Beteiligung des Bundeskriminalamtes an der „Joint Cybercrime Action Taskforce“ bei Europol

Vorbemerkung der Fragesteller

Am 1. September 2014 hat Europol ihre „Joint Cybercrime Action Taskforce“ (J-CAT) in Betrieb genommen (Pressemitteilung Europol vom 1. September 2014). Die Einheit mit Behörden aus Deutschland, Frankreich, Italien, Spanien, Großbritannien, den Niederlanden und Österreich ist in Den Haag angesiedelt. Dem Bundesministerium des Innern und für Heimat zufolge war das Bundeskriminalamt (BKA) mindestens „im Rahmen von drei Workshops“ bei Europol in die Vorbereitung der J-CAT eingebunden (Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 18/2674). Laut einer Mitteilung des Bundeskriminalamtes vom 1. September 2014 sei auch die Privatwirtschaft eingebunden.

Die J-CAT soll die gemeinsame, grenzüberschreitende Zusammenarbeit „in relevanten und in der Regel mehrere Staaten betreffenden Cybercrime-Sachverhalten bzw. Ermittlungsverfahren“ beschleunigen und intensivieren (Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 18/2674). Die J-CAT soll sich „bedarfs- und anlassbezogen mit als relevant eingeschätzten Bedrohungslagen und Sachverhalten aus dem Bereich der Cybercrime befassen“. In der genannten Bundestagsdrucksache ist auch die Rede von einem „Zusammenführen der Vertreter von Sicherheits- bzw. Strafverfolgungsbehörden“ der teilnehmenden Länder bei Europol. Mit „Sicherheitsbehörden“ werden in EU-Dokumenten gemeinhin Geheimdienste bezeichnet. Ein „Mehrwert“ sei außerdem durch die in der J-CAT organisierte „Einbindung der Nicht-EU-Mitgliedstaaten zu erwarten“. Genannt werden das US-amerikanische FBI (Federal Bureau of Investigation) und der US-amerikanische Secret Service sowie Behörden aus Kanada, Australien und Kolumbien. Die J-CAT und demnach womöglich auch die beteiligten Drittstaaten greifen laut dem Bundesministerium des Innern und für Heimat „auf die bei Europol vorliegenden Informations- und Auswertemöglichkeiten zurück“. „Bedarfs- bzw. anlassbezogen“ arbeite die Abteilung auch mit „Vertretern“ der Focal Points „Cyborg“, „Terminal“ und „Twins“ zusammen.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern und für Heimat vom 15. März 2022 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

1. Welche EU-Mitgliedstaaten nehmen nach Kenntnis der Bundesregierung derzeit an der „Joint Cybercrime Action Taskforce“ (J-CAT) bei Europol teil, und mit welchen Abteilungen ist die Bundesregierung dort vertreten?

Folgende EU-Mitgliedstaaten (MS) nehmen aktuell an der Joint Cybercrime Action Taskforce (J-CAT) teil:

Österreich, Belgien, Spanien, Rumänien, Niederlande, Italien, Schweden, Frankreich, Polen, Deutschland.

Das BKA hat einen Verbindungsbeamten in die Taskforce entsandt.

2. Welche Kriminalitätsphänomene werden nach Kenntnis der Bundesregierung in der J-CAT konkret verfolgt?

Die Mitglieder des J-CAT unterstützen sich gegenseitig in Fällen von Cybercrime im engeren Sinne, Zahlungskartenkriminalität, Bekämpfung der sexuellen Gewalt gegen Kinder und Jugendliche im Internet sowie Organisierter Kriminalität in Verbindung mit dem Darknet.

3. Worin liegt aus Sicht der Bundesregierung der Mehrwert der J-CAT gegenüber bereits existierenden Zusammenarbeitsformen im Bereich der Cyberkriminalität mit Europol?

Der Mehrwert des J-CAT liegt insbesondere in der gezielten, adressatengerechten und beschleunigten Suche nach internationalen Partnern im Sinne einer operativen Zusammenarbeit im Bereich Cybercrime.

4. Welche privaten Firmen oder Institute sind nach Kenntnis der Bundesregierung an der J-CAT mittelbar oder unmittelbar beteiligt, und worin besteht deren Mitarbeit?

Durch die Mitglieder des J-CAT erfolgt keine unmittelbare Zusammenarbeit mit privaten Anbietern. Im Rahmen von Ermittlungsverfahren kann durch die Verbindungsbeamten in der J-CAT eine Vermittlung von privaten Partnern erfolgen, die entweder durch eine bereits bestehende Kooperation eines Mitgliedstaats oder durch ein Kooperationsformat von EUROPOL selbst eingeleitet worden ist.

5. Welche Nicht-EU-Staaten sind nach Kenntnis der Bundesregierung mit welchen Behörden an der J-CAT beteiligt, und welche Aufgaben übernehmen diese dort?

Nachstehende Nicht-EU-Staaten sind ebenfalls am J-CAT beteiligt:

Vereinigte Staaten (FBI, US Secret Service, Internal Revenue Service), Norwegen, Schweiz, Australien, Kolumbien, Kanada, Vereinigtes Königreich.

Die Nicht-EU-Mitglieder des J-CAT sind mit mindestens einem Verbindungsbeamten vertreten, die ihrerseits dem jeweiligen Verbindungsbüro als erfahrene Kollegen im Bereich Cybercrime zugeordnet sind.

a) An welchen Treffen der J-CAT nehmen diese Behörden aus Nicht-EU-Staaten gewöhnlich teil?

Alle Mitglieder der J-CAT treffen sich wöchentlich mit dem European Cybercrime Centre (EC3) zur Abstimmung über Cybercrime-Fälle, an denen international mehrere Behörden beteiligt sind.

b) Mit welchen dieser Behörden arbeitete das Bundeskriminalamt bislang im Rahmen des J-CAT in einzelnen Ermittlungen zusammen?

Mit dem größten Teil dieser Behörden hat das BKA bereits in einzelnen Ermittlungen im Rahmen des J-CAT zusammengearbeitet.

6. Mit welchen Ermittlungskomplexen (etwa Encrochat, SkyECC, ANOM etc.) hat sich die J-CAT nach Kenntnis der Bundesregierung bislang „bedarfs- und anlassbezogen“ befasst (Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 18/2674)?

7. Welche Behörden aus welchen Nicht-EU-Staaten waren bei diesen Ermittlungen jeweils beteiligt (bitte für jeden Komplex einzeln darstellen)?

Die Fragen 6 und 7 werden gemeinsam beantwortet.

Die genannten Verfahrenskomplexe waren und sind nicht Teil der Befassung der J-CAT. Bezüglich des Befassungsgegenstands wird auf die Antwort zu Frage 2 verwiesen.

8. Mit welchen anderen EU-Strukturen bzw. Abteilungen hat die J-CAT nach Kenntnis der Bundesregierung bislang anlassbezogen zusammengearbeitet?

Die J-CAT hat anlassbezogen mit CEPOL, ENISA und CERT-EU zusammengearbeitet.

9. Mit welchen weiteren „Bedrohungslagen“ hat sich die J-CAT außerhalb der oben bereits erfragten Maßnahmen zur Strafverfolgung befasst (Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 18/2674)?

Es wird auf die Antwort zu Frage 2 verwiesen. Die Kooperation findet nur in den dort aufgeführten Deliktsfeldern statt.

10. Welche Datensammlungen wurden nach Kenntnis der Bundesregierung für die Arbeit der J-CAT eingerichtet?

Es wurden keine Datensammlungen für die Arbeit der J-CAT eingerichtet.

11. Auf welche „Focal Points“ kann die J-CAT nach Kenntnis der Bundesregierung bei Europol zugreifen?

Die Mitglieder der J-CAT vermitteln zwischen Strafverfolgungsbehörden des repräsentierten Staates und den Analysis Projects (ehemals „Focal Points“) des EC3 (APs Cyborg, Twins, Terminal und Dark Web).

12. Im Rahmen welcher Beschaffungs- oder Forschungsprojekte haben das Bundesministerium des Innern und für Heimat, das Bundesministerium der Verteidigung oder das Bundeskanzleramt mit der Firma „Go Root“ zusammengearbeitet (Schriftliche Frage 18 des Abgeordneten Manuel Höferlin auf Bundestagsdrucksache 19/31996), und welche „verschiedene[n] Produkte“ hat die Firma dabei „vorgestellt“?

Es wird auf die Antwort der Bundesregierung auf die Schriftliche Frage 18 des Abgeordneten Manuel Höferlin auf Bundestagsdrucksache 19/31996 verwiesen. In Bezug auf den Kontakt zwischen Kommando Cyber- und Informationsraum (KdoCIR) einerseits sowie der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) andererseits und der Firma „Go Root“ hat sich der Sachstand nicht verändert.

Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine darüberhinausgehende Beantwortung auch der Frage 12 dieser Kleinen Anfrage nicht, auch nicht in eingestufter Form, erfolgen kann. Das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung wird insoweit durch das gleichfalls Verfassungsrang genießende schutzwürdige Interesse des Staatswohls begrenzt.

Die Beantwortung der Frage betrifft solche Informationen, die in besonders hohem Maße das Staatswohl berühren und daher selbst in eingestufter Form nicht beantwortet werden können. Eine Offenlegung der angefragten Informationen bezüglich möglicher Kontakte zur Firma „Go Root“ bzw. dessen Produkte oder in Aussicht gestellter Aufträge birgt die Gefahr, dass Einzelheiten zur konkreten Methodik und zu in hohem Maße schutzwürdigen spezifischen Fähigkeiten der Sicherheitsbehörden bekannt würden. Infolgedessen könnten sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf spezifische Vorgehensweisen, Arbeitsmethoden und Fähigkeiten der Sicherheitsbehörden ziehen.

Dies könnte folgenschwere Einschränkungen der Informationsgewinnung und Analysefähigkeit zur Folge haben, womit letztlich die gesetzliche Aufgabenwahrnehmung der Sicherheitsbehörden nicht mehr sachgerecht erfüllt werden könnte.

Selbst eine Verschlusssachen-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde ihrer erheblichen Bedeutung für die Aufgabenerfüllung der Sicherheitsbehörden nicht ausreichend Rechnung tragen. Die angefragten Inhalte bezüglich möglicher Kontakte, aber insbesondere hinsichtlich der in Aussicht gestellten Aufträge, die unmittelbar mit Produkten des Software-Unternehmens Go Root einhergehen, beschreiben die Fähigkeiten und Arbeitsweisen der Sicherheitsbehörden so detailliert, dass eine Bekanntgabe auch gegenüber einem begrenzten Kreis von Empfängern ihrem Schutzbedürfnis nicht Rechnung tragen kann. Hierunter fällt insbesondere auch die Frage, ob etwaiger Kontakt zu einer Firma oder sonstigen Entität mit spezifischen Fähigkeiten stattgefunden hat oder stattfindet. Dies gilt umso mehr für die Nutzung relevanter Techniken oder Fähigkeiten für die Aufgabenerfüllung der Sicherheitsbehörden und für die Aufrechterhaltung der Effektivität nachrichtendienstlicher und polizeilicher Informationsbeschaffung durch den Einsatz spezifischer technischer Fähigkeiten. Bei einem Bekanntwerden der schutzbedürftigen Information wäre kein Ersatz durch andere Instrumente der Informationsgewinnung möglich.

Hieraus ergibt sich, dass die erbetenen Informationen in ihrer Detailtiefe derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht in diesem besonderen Einzelfall wesentlich überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber dem Geheimhaltungsinteresse der Bundesregierung zurückstehen.

13. Welche neueren Erkenntnisse hat die Bundesregierung darüber, ob bzw. wo es bis heute einen versuchten oder erfolgreich ausgeführten „cyberterroristischen Anschlag“ gegeben hat (Antworten der Bundesregierung auf die Kleinen Anfragen auf den Bundestagsdrucksachen 17/7578, 18/164 und 18/2674)?

Der Bundesregierung liegen hierzu keine Erkenntnisse vor.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, 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