Auswärtiges Amt

An den
Präsidenten des Deutschen Bundestages
Herrn Dr. Wolfgang Schäuble, MdB
Platz der Republik 1
11011 Berlin

Andreas Michaelis
Staatssekretär

Berlin, den 14. Mai 2019

Kleine Anfrage der Abgeordneten Andrej Hunko, Heike Hänsel, Anke Domscheit-Berg, Dr. André Hahn, Ulla Jelpke, Thomas Nord, Petra Pau, Tobias Pflüger, Alexander Ulrich und der Fraktion DIE LINKE.

Bundestagsdrucksache Nr. 19-9086 vom 05.04.2019

Titel - Attribuierung von „böswilligen Cyberaktivitäten“ durch das geheimdienstliche EU-Lagezentrum INTCEN

Sehr geehrter Herr Präsident,

als Anlage übersende ich die Antwort der Bundesregierung auf die oben genannte Kleine Anfrage.

Mit freundlichen Grüßen

Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Heike Hänsel, Anke Domscheit-Berg, Dr. André Hahn, Ulla Jelpke, Thomas Nord, Petra Pau, Tobias Pflüger, Alexander Ulrich und der Fraktion DIE LINKE.

- Bundestagsdrucksache Nr.: 19-9086 vom 05.04.2019 -

Attribuierung von „böswilligen Cyberaktivitäten" durch das geheimdienstliche EU-Lagezentrum INTCEN

Vorbemerkung der Fragesteller

Der Rat der Europäischen Union hat beschlossen, eine „Cyber Diplomacy Toolbox" für eine gemeinsame Reaktion der EU auf „böswillige Cyberaktivitäten" zu entwickeln (Ratsdokument 9916/17). Der Cyberraum bringe Herausforderungen auch für die Gemeinsame Außen- und Sicherheitspolitik mit sich. So sei es „mehr und mehr notwendig", die Integrität und Sicherheit der EU, ihrer Mitgliedstaaten sowie ihrer Bürgerinnen und Bürger „vor Bedrohungen aus dem Cyberraum und böswilligen Cyberaktivitäten zu schützen".

Ein gemeinsamer umfassender Ansatz der EU für die Cyberdiplomatie soll auch die „Eindämmung von Cyberbedrohungen" besorgen. Dabei geht es auch um die Attribuierung von Störungen oder Angriffen im Cyberraum. Hierzu soll unter anderem das geheimdienstliche EU-Lagezentrum INTCEN Erkenntnisse beisteuern, sammeln und bewerten (Ratsdokument 6852/19). Das EU-INTCEN soll außerdem bei der Entscheidungsfindung für eine mögliche Reaktion auf „böswillige Cyberaktivitäten" mitarbeiten. Dies ist jedoch aus Sicht der Fragestellerinnen und Fragesteller mit den EU-Verträgen unvereinbar, denn diese sehen keine Kompetenz für die Koordination der Geheimdienste vor. Auch eine nicht-bindende Einschätzung des EU-INTCEN zu möglichen Reaktionen wäre kritisch, da Mitgliedstaaten dadurch im Sinne anderer Geheimdienste, die über mehr Aufklärungsfähigkeiten verfügen und Erkenntnisse bewusst an das INTCEN steuern, beeinflusst werden könnten.

Wir fragen die Bundesregierung:

1. *Wie definiert die Bundesregierung „böswillige Cyberaktivitäten" und inwiefern wird dabei auch zwischen staatlichen und nicht-staatlichen Akteuren unterschieden (vgl. Ratsdokument 7298/19)?*

Der in den „Schlussfolgerungen des Rates über einen Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten" („Cyberdiplomatischer Reaktionsrahmen"; Ratsdokument 9916/17; data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/de/pdf) verwendete Begriff der böswilligen Cyberaktivitäten beschreibt Cyberoperationen, die geeignet sind,

die Integrität und Sicherheit der EU, ihrer Mitgliedstaaten sowie ihrer Bürgerinnen und Bürger zu beeinträchtigen. Diese Definition wird von der Bundesregierung geteilt. Der Cyberdiplomatische Reaktionsrahmen ist eindeutig in seiner Festlegung, dass böswillige Cyberaktivitäten sowohl durch staatliche als auch durch nicht-staatliche Akteure durchgeführt werden können.

2. ***Hat die Bundesregierung jemals einen terroristischen Cyberangriff zweifelsfrei oder mit einer hohen Wahrscheinlichkeit attribuiert?***

Die Bundesregierung hat bislang keinen terroristischen Cyberangriff attribuiert.

3. ***Welche Akteure und Einrichtungen der Europäischen Union sollten aus Sicht der Bundesregierung bei der Attribuierung „böswilliger Cyberaktivitäten" Erkenntnisse beisteuern und mit welchen Einschränkungen soll dies auch für das geheimdienstliche EU-Lagezentrum INTCEN gelten?***

Die Bundesregierung entscheidet nach Lage des Einzelfalls über die Quellenauswertung bei der Attribuierung böswilliger Cyberaktivitäten.

4. ***Sollte das EU-INTCEN aus Sicht der Bundesregierung auch dann aktiv werden, wenn nur ein einzelner EU-Mitgliedstaat von „böswilligen Cyberaktivitäten" betroffen ist?***

Die unmittelbare Betroffenheit eines oder mehrerer EU-Mitgliedstaaten ist für die Arbeit des EU-INTCEN nicht ausschlaggebend.

5. ***Welche Akteure und Einrichtungen der Europäischen Union sollten aus Sicht der Bundesregierung Vorschläge für eine Reaktion auf „böswillige Cyberaktivitäten" machen und mit welchen Einschränkungen soll dies auch für das EU-INTCEN gelten?***

Die Attribuierung böswilliger Cyberaktivitäten ist grundsätzlich eine souveräne politische Entscheidung der Mitgliedstaaten. Darüber hinaus sind alle Akteure und Einrichtungen der Europäischen Union, die für die Durchführung der Gemeinsamen Außen- und Sicherheitspolitik zuständig sind, berechtigt, Vorschläge für eine Reaktion auf böswillige Cyberaktivitäten zu machen. Ergänzend wird auf die Antworten zu den Fragen 18 und 18 a) bis c) verwiesen.

6. ***Welche einzelnen Aspekte „böswilliger Cyberaktivitäten" sollte das EU-INTCEN aus Sicht der Bundesregierung vorrangig bewerten (etwa Tragweite, Größenordnung, Dauer, Intensität, Komplexität, Raffiniertheit und Wirkung; vgl. Ratsdokument 9916/17)?***

Aus Sicht der Bundesregierung sind bei der Bewertung einer Cyberoperation die Maßstäbe Tragweite, Größenordnung, Dauer, Intensität, Komplexität und Wirkung maßgeblich.

7. ***Welche technischen Mittel könnte die Europäische Union aus Sicht der Bundesregierung zur Attribuierung „böswilliger Cyberaktivitäten" beisteuern (bitte auch die verantwortlichen Agenturen nennen)?***

Über die Frage, inwieweit die Institutionen der Europäischen Union über technische Mittel verfügen, die zur Attribuierung eingesetzt werden können, liegen der Bundesregierung keine Erkenntnisse vor.

8. ***Nach welchem Verfahren könnte das EU-INTCEN aus Sicht der Bundesregierung bewerten, mit welcher Wahrscheinlichkeit „böswillige Cyberaktivitäten" tatsächlich einem bestimmten Akteur zugeordnet werden können (etwa das im Ratsdokument 7298/19 aufgeführte Verfahren, das von weniger als 5% bis hin zu mehr als 95% reicht)?***

Die Beratungen der Mitgliedstaaten zur Frage eines Verfahrens zur Abstimmung von Attribuierungen dauern an.

9. ***Welche eigenen, nicht von Geheimdiensten der EU-Mitgliedstaaten gelieferten Erkenntnisse sollte das EU-INTCEN aus Sicht der Bundesregierung für die Attribuierung „böswilliger Cyberaktivitäten" nutzen?***

EU-INTCEN betreibt keine eigene Aufklärung. Das Zentrum arbeitet auf der Basis von eingestuften Informationen und von durch die nationalen Nachrichtendienste bereits aufbereitetem Material, die seitens der Mitgliedstaaten zur Verfügung gestellt werden, sowie auf Basis von Erkenntnissen von EU-Institutionen. Des Weiteren nutzt EU-INTCEN offene Quellen.

10. ***In welchem Umfang haben die Geheimdienste des Bundes in den letzten zwei Jahren im Rahmen ihrer jeweiligen gesetzlichen Vorschriften für die EU-Ebene relevante Erkenntnisse zu „böswilligen Cyberaktivitäten" an das EU-INTCEN bzw. die dort angesiedelte EU-Analyseeinheit für hybride Bedrohungen („Hybrid Fusion Cell") geliefert (Bundestagsdrucksache 19/7881, Frage 18)?***

Die Antwort auf diese Frage kann nicht offen erfolgen. Nach § 3 Nummer 4 der Allgemeinen Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlusssachen (Verschlusssachenanweisung, VSA) sind Informationen, deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein können, entsprechend einzustufen. Eine zur Veröffentlichung bestimmte Antwort der Bundesregierung auf diese Fragen würde Informationen zur Arbeitsweise der Nachrichtendienste der Bundesregierung einem nicht eingrenzbaren Personenkreis nicht nur im Inland, sondern auch im Ausland zugänglich machen. Dies kann für die wirksame Erfüllung der gesetzlichen Aufgaben der Nachrichtendienste und damit für die Interessen der Bundesrepublik Deutschland nachteilig sein. Diese Informationen werden daher gemäß § 3 Nummer 4 VSA als „VS-Nur für den Dienstgebrauch" eingestuft und dem Deutschen Bundestag gesondert übermittelt.

11. Inwiefern arbeitet das EU-INTCEN nach Kenntnis der Bundesregierung auch mit Geheimdiensten aus Drittstaaten zusammen und um welche handelt es sich dabei?

Das EU-INTCEN betreibt Konsultationen mit Drittstaaten nach Maßgabe des Bedarfs und der relevanten EU Vorschriften. Über die Herkunft der von EU-INTCEN verwendeten Informationen im Einzelnen liegen der Bundesregierung keine Erkenntnisse vor.

12. Inwiefern sollten Mitgliedstaaten der Europäischen Union aus Sicht der Bundesregierung angehalten oder gedrängt werden, Erkenntnisse zur Attribuierung „böswilliger Cyberaktivitäten" auf EU-Ebene oder gegenüber dem EU-INTCEN offenzulegen?

Die Weitergabe solcher Informationen an EU-Institutionen, also auch an das EU-INTCEN, liegt in der nationalen Entscheidung der Mitgliedstaaten.

13. Inwiefern soll das INTCEN nach Kenntnis der Bundesregierung auch mit dem „internen Netz zur Abwehr von Desinformation" der Generaldirektion Kommunikation (DG-COMM) der Europäischen Kommission zusammenarbeiten bzw. zuarbeiten, in dem Vertreterinnen und Vertreter aller Generaldirektionen sowie der Mitgliedstaaten organisiert sind (Bundestagsdrucksache 19/7881, Frage 12)?

Das EU-INTCEN unterstützt alle Institutionen der Europäischen Union und die Mitgliedstaaten durch Analysen zu außen- und sicherheitspolitischen Themen.

14. Welche deutschen Einrichtungen sollen nach Kenntnis der Bundesregierung nach gegenwärtigem Stand mit dem EU-INTCEN zur Attribuierung „böswilliger Cyberaktivitäten" kooperieren?

Die Einstufung der Antwort auf die Frage als Verschlusssache (VS) mit dem Geheimhaltungsgrad „VS-Nur für den Dienstgebrauch" ist im vorliegenden Fall im Hinblick auf das Staatswohl erforderlich. Nach § 3 Nummer 4 der Allgemeinen Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlusssachen (Verschlusssachenanweisung, VSA) sind Informationen, deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein können, entsprechend einzustufen. Eine zur Veröffentlichung bestimmte Antwort der Bundesregierung auf diese Fragen würde Informationen zur Arbeitsweise des BND einem nicht eingrenzbaren Personenkreis nicht nur im Inland, sondern auch im Ausland zugänglich machen. Dies kann für die wirksame Erfüllung der gesetzlichen Aufgaben der Nachrichtendienste und damit für die Interessen der Bundesrepublik Deutschland nachteilig sein. Zudem können sich in diesem Fall Nachteile für die zukünftige Zusammenarbeit mit ausländischen Nachrichtendiensten ergeben. Diese Informationen werden daher gemäß § 3 Nummer 4 VSA als „VS-Nur für den Dienstgebrauch" eingestuft und dem Deutschen Bundestag gesondert übermittelt.

15. ***Mit wie vielen Mitarbeiterinnen und Mitarbeitern welcher Behörden ist die Bundesregierung am INTCEN und dem EUMS INT Directorate beteiligt (Bundestagsdrucksache 18/146, Frage 12)?***

Die Bundeswehr ist derzeit mit zwei Mitarbeitern im EUMS Intelligence Directorate vertreten.

Darüber hinaus kann die Beantwortung der Frage nicht offen erfolgen. Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung aus Gründen des Staatswohls nicht in offener Form erfolgen kann. Die erbetenen Auskünfte sind geheimhaltungsbedürftig, weil sie Informationen enthalten, die im Zusammenhang mit der Arbeitsweise des Bundesnachrichtendienstes stehen. Arbeitsmethoden und Vorgehensweisen der Nachrichtendienste des Bundes sind im Hinblick auf die künftige Erfüllung des gesetzlichen Auftrags aus § 1 Abs. 2 BNDG besonders schutzwürdig. Ebenso schutzbedürftig sind Einzelheiten zu der nachrichtendienstlichen Erkenntnislage. Hierzu zählen auch Informationen über die personelle Ausstattung einzelner Arbeitsbereiche des BND. Eine zur Veröffentlichung bestimmte Antwort der Bundesregierung auf die Frage würde Informationen zur personellen Ausstattung und damit einhergehend mittelbar zu Aufklärungspotentialen und Arbeitsweisen des BND einem nicht eingrenzbaren Personenkreis nicht nur im Inland, sondern auch im Ausland zugänglich machen. Insbesondere könnten interessierte Stellen im Ausland (vor allem ausländische Nachrichtendienste) einen über die allgemein zugänglichen Informationen zum BND hinausgehenden Einblick in die personelle Ausstattung und die Arbeitsweise des BND gewinnen. Derartige Informationen zu Interna des BND sind schutzwürdig, um nicht als Einstieg für Ausforschungsmaßnahmen zum Nachteil des BND verwandt werden zu können. Eine solche Verwendung könnte die wirksame Erfüllung der gesetzlichen Aufgaben des BND beeinträchtigen und damit die Sicherheit der Bundesrepublik Deutschland gefährden oder ihren Interessen schweren Schaden zufügen. Deshalb sind die entsprechenden Informationen als Verschlusssache gemäß der VSA mit dem VS-Grad „VS – Geheim" eingestuft.

16. ***Welche Technik nutzen das INTCEN und das EUMS INT nach Kenntnis der Bundesregierung zur „Krisenfrüherkennung" (vgl. Bundestagsdrucksache 19/7604)?***

Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

17. ***Wann soll das „Frühwarnsystem" der Steuerungsgruppe Strategische Kommunikation im Auswärtigen Amt fertiggestellt bzw. betriebsbereit sein (Bundestagsdrucksache 19/7881, Frage 19)?***

Das Rapid Alert System (Frühwarnsystem) der EU wurde im Aktionsplan gegen Desinformation der EU angekündigt und wird entsprechend vom Europäischem Auswärtigen Dienst und der Europäischen Kommission geleitet. Die Steuerungsgruppe Strategische Kommunikation im Auswärtigen Amt nimmt

für Deutschland die Funktion der nationalen Kontaktstelle wahr. Das Rapid Alert System ist seit dem 18. März 2019 in Betrieb.

18. ***Welche Akteure und Einrichtungen der Europäischen Union könnten aus Sicht der Bundesregierung eine gemeinsame Attribuierung „böswilliger Cyberaktivitäten" koordinieren?***

    a) ***Wo sollte analysiert und bewertet werden, welche Konsequenzen eine gemeinsame EU-Antwort auf „böswillige Cyberaktivitäten" für die EU-Außenbeziehungen hat?***

    b) ***Wo sollte analysiert und bewertet werden, inwiefern eine gemeinsame EU-Antwort auf „böswillige Cyberaktivitäten" die Arbeit der einbezogenen Agenturen und Einrichtungen der Europäischen Union behindert oder gefährdet?***

    c) ***Wo sollte analysiert und bewertet werden, ob eine gemeinsame EU-Antwort auf „böswillige Cyberaktivitäten" mögliche Gegenmaßnahmen provozieren und einen Konflikt damit eskalieren könnte?***

Die Fragen 18 und 18 a) bis c) werden gemeinsam beantwortet. Die Frage der Attribuierung, die grundsätzlich in souveräner nationaler Zuständigkeit liegt, ist ein Teilaspekt bei der Beratung in der zuständigen Ratsarbeitsgruppe (Horizontale Ratsarbeitsgruppe „Fragen des Cyberraums") von Maßnahmen zur Reaktion auf oder Abschreckung von Cyberaktivitäten, die die sicherheits- oder außenpolitischen Interessen der Union oder ihrer Mitgliedstaaten bedrohen. Des Weiteren wird auf die Antwort zu Frage 8 verwiesen.

19. ***Welche Aufgaben sollte ein „Europäisches Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung" oder ein „Netz nationaler Koordinierungszentren" aus Sicht der Bundesregierung bei der Attribuierung „böswilliger Cyberaktivitäten" und einer gemeinsamen EU-Antwort übernehmen (Kommissionsdokument COM(2018) 630 final)?***

Das Aufgabenspektrum des Zentrums ist noch nicht festgelegt. Es besteht von Seiten der Bundesregierung nicht die Absicht, dem Zentrum Aufgaben bei der Attribuierung böswilliger Cyberaktivitäten zuzuweisen.

20. ***Welche Haltung vertritt die Bundesregierung zur Frage, das „Rapid-Alert-System" gegen „Desinformationskampagnen" und „ausländische Beeinflussung" von Wahlen für andere Organisationen (etwa NATO, G7) und Drittstaaten zu öffnen (http://gleft.de/2JYw), und auf welche Weise sollen auch Firmen (etwa Facebook, Google) eingebunden werden?***

Zum aktuellen Zeitpunkt ist eine Öffnung für andere Organisationen wie NATO, Gruppen wie den G7 oder eine Anbindung von Unternehmen nicht vorgesehen.