Deutscher Bundestag **Drucksache 19/20082**

19. Wahlperiode 17.06.2020

Kleine Anfrage

der Abgeordneten Andrej Hunko, Heike Hänsel, Ulla Jelpke, Niema Movassat, Dr. Alexander S. Neu, Tobias Pflüger, Alexander Ulrich und der Fraktion DIE LINKE.

Deutsche Aktivierung einer EU-Reaktion auf „böswillige Cyberaktivitäten“

Die im Juni 2017 verabschiedeten Schlussfolgerungen des Rates der Europäischen Union über einen Rahmen für eine gemeinsame diplomatische Reaktion auf „böswillige Cyberaktivitäten“ (Ratsdokument 9916/17) beschreiben „Cyberoperationen, die geeignet sind, die Integrität und Sicherheit der EU, ihrer Mitgliedstaaten sowie ihrer Bürgerinnen und Bürger zu beeinträchtigen“ (Bundestagsdrucksache 19/10273, Antwort zu Frage 1). Sie sollen die „Cybersicherheitsstrategie“ der EU ergänzen und einen „offenen, freien, stabilen und sicheren Cyberraum“ bewahren helfen. Im Mittelpunkt steht die Reaktion auf Cyberangriffe, die EU soll sich aber auch um „Cyberdialoge“ mit anderen Staaten bemühen. Die Schlussfolgerungen enthalten auch eine sogenannte Cyber Diplomacy Toolbox, die auf einer gemeinsamen Initiative der EU-Kommission und des Auswärtigen Dienstes beruht. Entsprechende Maßnahmen „zur Konfliktverhütung, zur Eindämmung von Cyberbedrohungen und zu größerer Stabilität in den internationalen Beziehungen“ werden in der horizontalen Ratsarbeitsgruppe „Fragen des Cyberraums“ (HWPCI) weiterverfolgt.

Wenige Monate später hatte die EU entsprechende Umsetzungsrichtlinien mit fünf Kategorien für eine etwaige diplomatischen Reaktion (Ratsdokument 13007/17) erlassen. Darin geht es unter der Frage der Aktivierung einer gemeinsamen Reaktion auch um die Frage der Attribuierung eines Cyberangriffs. Die Zuschreibung zu einem staatlichen oder nichtstaatlichen Akteur soll eine souveräne politische Entscheidung der EU-Mitgliedstaaten bleiben. Sie werden dabei von „Akteuren und Einrichtungen“ der Europäischen Union, die für die Durchführung der Gemeinsamen Außen- und Sicherheitspolitik zuständig sind, unterstützt. Hierzu gehört auch das geheimdienstliche Lagezentrum INTCEN in Brüssel (Bundestagsdrucksache 19/10273).

Im April 2018 schrieb die Bundesregierung, dass die EU den „Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten“ endlich zur Anwendung bringen sollte (Bundestagsdrucksache 19/1900, Antwort zu Frage 16). Sechs Monate später berichtete die Bundesregierung von bislang einem Fall, in dem eine Maßnahme nach den Kategorien eins bis fünf der Umsetzungsrichtlinien erfolgte (Bundestagsdrucksache 19/4946, Antwort zu Frage 33).

Zu den möglichen gemeinsamen EU-Reaktionen gehören auch Listungen für Sanktionen. Die Bundesregierung hat sich, im Rahmen der Verordnung (EU) 2019/796 zu restriktiven Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen, dafür eingesetzt, dass diese mit qualifizierter

Mehrheit beschlossen werden können. Damit wollte sie den „zeitlichen Zusammenhang zwischen dem Handeln böswilliger Akteure und eventueller Sanktionsverhängung […] verkürzen“ (Bundestagsdrucksache 19/11920, Antwort zu Frage 25).

Nach fünf Jahre dauernden Ermittlungen hat die Generalbundesanwaltschaft im Mai 2020 einen Haftbefehl gegen einen des Cyberangriffs auf den Deutschen Bundestag Tatverdächtigen erwirkt. Dieser wird russischen Gruppen zugeordnet, bislang ohne Belege werden auch russische Geheimdienste als Urheber genannt. Es ist nach Ansicht der Fragesteller möglich, dass die Bundesregierung den Vorfall jetzt zum Anlass nimmt, eine gemeinsame diplomatische EU-Reaktion auf „böswillige Cyberaktivitäten“ in Deutschland zu aktivieren. Einen „terroristischen Cyberangriff“, der ebenfalls als Grundlage für eine solche Aktivierung dienen könnte, hat die Bundesregierung soweit bekannt noch nicht attribuiert (Bundestagsdrucksache 19/10273, Antwort zu Frage 2).

Wir fragen die Bundesregierung:

1. Wie wurden der „Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten“ bzw. die „Cyber Diplomacy Toolbox“ der Europäischen Union nach Kenntnis der Bundesregierung bislang eingesetzt, und inwiefern bewertet sie dies als erfolgreich oder nutzlos?

   a) Inwiefern wurde der Rahmen bereits zur Unterstützung bei der Attribuierung eines Cyberangriffs genutzt, und um welche Vorfälle handelt es sich dabei?

   b) Welche Ratsarbeitsgruppen sind hiermit jeweils befasst gewesen?

   c) Konnten die Urheber zweifelsfrei attribuiert werden, und falls ja, mit welchen Mitteln?

   d) Inwiefern hat das geheimdienstliche Lagezentrum INTCEN in Brüssel hierzu Informationen oder Bewertungen beigesteuert?

   e) Kennt die Bundesregierung Möglichkeiten, anhand offener Quellen die Verantwortlichkeit für einen Cyberangriff zu belegen, und inwiefern sind das INTCEN oder der Auswärtige Dienst mit derartigen Verfahren befasst?

2. Nach welchem Verfahren bewertet das EU-INTCEN nach Kenntnis der Bundesregierung, mit welcher Wahrscheinlichkeit „böswillige Cyberaktivitäten“ tatsächlich einem bestimmten Akteur zugeordnet werden können (Bundestagsdrucksache 19/10273, Antwort zu Frage 8)?

3. Welche deutschen Einrichtungen kooperieren mit dem EU-INTCEN zur Attribuierung „böswilliger Cyberaktivitäten“, bzw. was ist hierzu geplant?

4. In welchem Umfang haben die Geheimdienste des Bundes seit der Antwort auf Bundestagsdrucksache 19/10273 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?

5. Zu welchen Vorfällen wurden nach Kenntnis der Bundesregierung von welchen Mitgliedstaaten welche Maßnahmen in welchen Kategorien der Umsetzungsrichtlinien des „Rahmens für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten“ bzw. der „Cyber Diplomacy Toolbox“ angeregt bzw. gefordert?

   a) Wann erfolgte die Vorstellung der jeweiligen Vorfälle in den zuständigen Ratsarbeitsgruppen?

b) Zu welchen Vorfällen sind welche Maßnahmen tatsächlich erfolgt?

c) Welche staatlichen oder nichtstaatlichen Akteure wurden bei der Attribuierung ausgemacht, und gegen welche Akteure richtete sich dann die gemeinsame Reaktion?

6. In welchen dieser „gemeinsamen Reaktionen“ erfolgten nach Kenntnis der Bundesregierung anschließend Listungen für Sanktionen gegen welche Personen oder Einrichtungen?

a) Hat sich das von der Bundesregierung durchgesetzte Verfahren bewährt, den „zeitlichen Zusammenhang zwischen dem Handeln böswilliger Akteure und eventueller Sanktionsverhängung zu verkürzen“, indem Abstimmungen zukünftig mit qualifizierter Mehrheit erfolgen können (Bundestagsdrucksache 19/11920, Antwort zu Frage 25)?

b) Wie viel Zeit verging in den in Rede stehenden Fällen zwischen der Vorstellung der Cyberangriffe in den zuständigen Ratsarbeitsgruppen bis zur Listung?

7. Auf welchen Ebenen und in welchen Formationen tauschen sich die Bundesregierung und die russische sowie die chinesische Regierung regelmäßig darüber aus, wie „böswillige Cyberaktivitäten“ verhindert werden können (vgl. dazu Bundestagsdrucksache 19/10137), und wann haben diese Cyberkonsultationsmechanismen zuletzt stattgefunden, und welche weiteren sind geplant?

8. Hat die Bundesregierung auch den Cyberangriff auf den Deutschen Bundestag von 2015 („Haftbefehl gegen russischen Hacker“; www.tagesschau.de vom 5. Mai 2020) bei der Europäischen Union als „böswillige Cyberaktivitäten“ vorgestellt und/oder Maßnahmen aus der „Cyber Diplomacy Toolbox“ gefordert?

a) Wann, und wo erfolgte diese Vorstellung, und welche Maßnahmen wurden dazu wann beschlossen?

b) Wie wurde der Vorfall zuvor zweifelsfrei attribuiert, und welche Beweise haben Bundesbehörden vorgelegt?

c) Wie haben Einrichtungen der Europäischen Union bei der Attribuierung unterstützt?

d) Sofern von deutscher Seite in den zuständigen Ratsarbeitsgruppen noch keine Beweise vorgelegt wurden, welche Gründe kann die Bundesregierung dazu mitteilen?

e) Inwiefern beurteilt die Bundesregierung den mutmaßlichen Urheber des Cyberangriffs auf den Deutschen Bundestag als weiterhin gefährlich, oder ist dies für die Beantragung einer „gemeinsamen Reaktion“ der Europäischen Union aus ihrer Sicht unerheblich?

f) Inwiefern wurde der Vorfall auch im Rahmen der Cyberkonsultationsmechanismen mit China oder Russland behandelt?

g) Mit welchen Medien haben welche Bundesbehörden Gespräche „Unter Drei“ oder andere Hintergrundgespräche zu den Ermittlungen geführt, bevor der Haftbefehl gegen einen Verdächtigen von der Bundesregierung selbst öffentlich gemacht wurde?

h) Wie soll ein etwaiger Sanktionsbeschluss des Cyberangriffs auf den Deutschen Bundestag im Rahmen der Reaktion auf „böswillige Cyberaktivitäten“ bekannt gemacht werden, und inwiefern will die Bundesregierung hierzu vorher wieder Hintergrundgespräche mit einzelnen Medien führen?

9. Welche Fortschritte kann die Bundesregierung zur Entwicklung eines „Protokoll[s] für die Notfallreaktion“ auf Cybersicherheitsvorfälle („Emergency Response Protocol“) europäischer Strafverfolgungsbehörden mitteilen (Bundestagsdrucksache 19/1900, Antwort zu Frage 21)?
10. Welches Ausmaß müssten IT-Störungen annehmen, um das Protokoll zu aktivieren, bzw. wie würde die Aktivierung bestimmt?
    a) Welche zivilen und militärischen EU-Lagezentren sollten daraufhin aktiviert werden?
    b) Welche Einrichtungen sollten mit der Überwachung offener Quellen („Open Source Monitoring“) und taktischer Koordination beauftragt werden?
11. Über wie viel Personal verfügt nach Kenntnis der Bundesregierung die Abteilung für Strategische Kommunikation und Informationsanalyse des Auswärtigen Dienstes der Europäischen Union (StratCom), und wie viele davon gehören zum StratCom East?
    a) Welcher Aufwuchs ist für das StratCom geplant?
    b) Mit welchen neuen Initiativen will die Europäische Union unabhängige Medien und „Faktenprüfer“ (auch in Drittstaaten) unterstützen?
12. Welche Initiativen zur Bekämpfung von Cyberbedrohungen und Desinformation will die Bundesregierung im Rahmen ihrer Ratspräsidentschaft in der Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats (ERCHT) vorschlagen, und welche bereits bestehenden Initiativen werden dort derzeit behandelt?
13. Welche Anstrengungen sind der Bundesregierung auf EU-Ratsebene bekannt, aus der Corona-Krise Schlussfolgerungen für eine verbesserte Kommunikation unter den EU-Mitgliedstaaten im Falle von Krisen sowie eine verbesserte Krisenkommunikation nach außen zu ziehen?
14. Ist der Bundesregierung mittlerweile ein „terroristischer Cyberangriff“ in Deutschland oder der Europäischen Union bekannt geworden, und falls ja, wie wurde dieser attribuiert (Bundestagsdrucksache 19/10273, Antwort zu Frage 2)?

Berlin, den 15. Juni 2020

Amira Mohamed Ali, Dr. Dietmar Bartsch und Fraktion

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