Auswärtiges Amt

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

Antje Leendertse
Staatssekretärin

Berlin, den 7. Juli 2020

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

Bundestagsdrucksache Nr. 19-20082 vom 17.06.2020

Titel - Deutsche Aktivierung einer EU-Reaktion auf böswillige Cyberaktivitäten

Sehr geehrter Herr Präsident,

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

Mit freundlichen Grüßen

Antje Leendertse

Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Heike Hänsel, Ulla Jelpke, Niema Movasat, Dr. Alexander S. Neu, Tobias Pflüger, Alexander Ulrich und der Fraktion DIE LINKE.

- Bundestagsdrucksache Nr.: 19-20082 vom 17.06.2020 -

Deutsche Aktivierung einer EU-Reaktion auf böswillige Cyberaktivitäten

---

Vorbemerkung der Fragesteller

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 auf ␣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 gemein-samen 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 Durch-führung der Gemeinsamen Außen- und Sicherheitspolitik zuständig sind, unter-stützt. 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 auf ␣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 auf ␣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 auf ␣Frage 25).

Nach fünf Jahre dauernden Ermittlungen hat die Generalbundesanwaltschaft im Mai 2020 einen Haftbefehl gegen einen Tatverdächtigen des Cyberangriffs auf den Deutschen Bundestag 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 Vor-fall 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 auf Frage 2).

Vorbemerkung der Bundesregierung:

Die Beantwortung der Fragen 1.d), 2, 4 und 14 kann aus Gründen des Staatswohls nicht offen erfolgen. Arbeitsmethoden und Vorgehensweisen der Nachrichtendienste des Bundes sowie Einzelheiten zur nachrichtendienstlichen Erkenntnislage sind im Hinblick auf die künftige Erfüllung des gesetzlichen Auftrages aus § 1 Abs. 2 BNDG und § 3 Abs. 1 Nr. 2 BVerfSchG besonders schutzwürdig. Eine Veröffentlichung von Einzelheiten betreffend solche Erkenntnisse würde zu einer Schwächung der den Nachrichtendiensten des Bundes zur Verfügung stehenden Möglichkeiten zur Informationsgewinnung führen. Insofern könnte die Offenlegung entsprechender Informationen für die Sicherheit und die Interessen der Bundesrepublik Deutschland nachteilig sein. Deshalb sind die Informationen als Verschlusssache gemäß der VSA mit dem VS-Grad „VS-Nur für den Dienstgebrauch“ eingestuft und werden dem Deutschen Bundestag gesondert übermittelt.

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?***

Der Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten („Cyber Diplomacy Toolbox“) wurde bisher in Form von Demarchen, Dialogformaten und Erklärungen des Hohen Vertreters der Europäischen Union für Außen- und Sicherheitspolitik angewendet, so zuletzt durch die Erklärung des Hohen Vertreters im Namen der EU vom 21. Februar 2020 im Zusammenhang mit einem Cyberangriff auf Medienunternehmen und öffentliche Einrichtungen in Georgien und durch die Erklärung des Hohen Vertreters vom 30. April 2020 zu

böswilligen Cyberaktivitäten unter Ausnutzung der Corona-Pandemie. Die Toolbox trägt nach Ansicht der Bundesregierung zur Stärkung eines regelbasierten, sicheren und stabilen Cyberraums bei.

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?

Die Fragen 1 a) bis c) werden gemeinsam beantwortet. Die Nutzung der Toolbox dient nicht der Attribuierung. Attribuierung im Sinne einer politischen Zurechnung bösartiger Cyberaktivitäten zu staatlichen Akteuren bleibt eine souveräne, politische Entscheidung der Mitgliedstaaten und ist keine Voraussetzung für die Anwendung der Toolbox. Die Toolbox dient der EU-gemeinsamen Reaktion auf Cybervorfälle und zielt auf Individuen oder Gruppen ab, nicht auf Staaten. Die Horizontale Ratsarbeitsgruppe zu Cyberfragen („Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats“ / HWP ERCHT) ist das für Cyberfragen fachlich zuständige Gremium innerhalb der EU, das auch das gemeinsame Vorgehen der EU Mitgliedstaaten koordiniert.

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

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

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?

Für das EU Cyber-Sanktionsregime auf Grundlage des Beschlusses und der Verordnung des Rates vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen,gibt es die Möglichkeit, die Sanktionslistung von Personen oder Entitäten anhand offener Quellen zu begründen. Die Begründung kann sich auf die Recherche von Medien, Behörden, Cyber-Sicherheitsunternehmen oder –netzwerken oder Nichtregierungsorganisationen stützen. Sowohl INTCEN als auch das Auswärtige Amt machen von dieser Möglichkeit Gebrauch.

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 auf ␣Frage 8)?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

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

Es wird auf die Antwort zu Frage 2 verwiesen.

4. ***In welchem Umfang haben die Geheimdienste des Bundes seit Beantwortung der Drucksache 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?***

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

5. ***Zu welchen Vorfällen wurde 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?***

Die Fragen 5 und 5 a) bis d) werden gemeinsam beantwortet. Zu vertraulichen Inhalten äußert sich die Bundesregierung grundsätzlich nicht. Im Übrigen wird auf die Antwort zu den Fragen 1 a) bis d) verwiesen.

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 auf Frage 25)?***
   b) ***Wieviel Zeit verging in den in Rede stehenden Fällen zwischen der Vorstellung der Cyberangriffe in den zuständigen Ratsarbeitsgruppen bis zur Listung?***

Die Fragen 6, 6 a) und b) werden gemeinsam behandelt. Das EU-Cybersanktionsregime wurde bisher noch nicht angewendet. Darüber hinaus wird auf die Antwort zu Frage 8 a) verwiesen.

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?***

Die bilateralen Cyber-Konsultationen mit der Russischen Föderation wurden im Frühjahr 2018 in Zusammenhang mit dem Hackerangriff auf den Bundestag suspendiert. Ein Austausch zu bösartigen Cyberaktivitäten fand danach vor allem im Rahmen der Untergruppe Nichtverbreitung von Massenvernichtungswaffen und Rüstungskontrolle der Hochrangigen Arbeitsgruppe für Sicherheitspolitik im März 2019 statt. Auf den deutschen Vorschlag zur Schaffung einer Unterarbeitsgruppe Cyber im Rahmen der hochrangigen Arbeitsgruppe ist die Russische Föderation bislang nicht eingegangen.

Die Bundesregierung tauscht sich mit der Volksrepublik China regelmäßig im Rahmen der deutsch-chinesischen Cybersicherheitskonsultationen zu böswilligen Cyberaktivitäten aus, so zuletzt im August 2019. Ein Termin für das nächste Treffen steht noch nicht fest.

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?***

Die Fragen 8 und 8 a) werden gemeinsam beantwortet. Die Bundesregierung informierte vor dem Hintergrund des im Zusammenhang mit dem Cyber-Angriff auf den Deutschen Bundestag erwirkten Haftbefehls die HWP ERCHT am 3. Juni 2020 über den Vorfall und schlug vor, EU-Sanktionen gegen verantwortliche Akteure zu verhängen. Der EU-Entscheidungsprozess hierzu dauert an.

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

Im Falle des Cyber-Angriffs auf den Bundestag hat die Bundesregierung Sanktionsvorschläge im EU-Rahmen durch Vorlage eines umfangreichen Beweispakets auf Grundlage von Ergebnissen deutscher Ermittlungsbehörden und aufgrund von nachrichtendienstlichen Informationen sowie durch öffentlich zugängliche Quellen belegt und dieses Beweispaket den anderen Mitgliedstaaten zugänglich gemacht. Im Übrigen wird auf die Antworten zu den Fragen 1 b) und 1 e) verwiesen.

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

Einrichtungen der Europäischen Union waren an der deutschen Attribuierungs-Entscheidung nicht beteiligt.

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

Die Bundesregierung hat die Beweise in der zuständigen Ratsarbeitsgruppe vorgelegt.

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

Die Bundesregierung geht davon aus, dass vom Urheber weiterhin eine Gefahr ausgeht.

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

Sowohl im Rahmen der deutsch-russischen Cybersicherheitskonsultationen 2017 als auch bei den Gesprächen der Untergruppe Nichtverbreitung von Massenvernichtungswaffen und Rüstungskontrolle der Hochrangigen Arbeitsgruppe zu Sicherheitspolitik im März 2019 wurden aus Russland stammende Cyberangriffe auf Ziele in Deutschland thematisiert.

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 Bundestag im Rahmen der Reaktion auf „böswillige Cyberaktivitäten“ bekannt gemacht werden und inwiefern will die Bundesregierung hierzu vorher wieder Hintergrundgespräche mit einzelnen Medien führen?

Die Fragen 8 g) und h) werden gemeinsam beantwortet. Sanktionen werden vom Ministerrat der EU beschlossen und im Amtsblatt der EU veröffentlicht. Zudem macht der Europäische Auswärtige Dienst üblicherweise durch Pressemitteilungen auf Sanktionsbeschlüsse aufmerksam. Die Vielzahl der Medienkontakte wird nicht dokumentiert.

9. Welche Fortschritte kann die Bundesregierung zur Entwicklung eines „Protokoll für die Notfallreaktion“ auf Cybersicherheitsvorfälle („Emergency Response Protocol“) europäischer Strafverfolgungsbehörden mitteilen (Drucksache 19/1900, Antwort auf Frage 21)?

Die Konzepte für das „EU Law Enforcement Emergency Response Protocol“ (EU LE ERP) sowie die Prozesse zur Ausrufung des Protokolls anhand eines „Initial Threat Assessment“ sind erarbeitet und umgesetzt. Das Bundeskriminalamt nimmt für Deutschland die Rolle des „National 24/7 Contact point“ im Prozess des EU LE ERP wahr und wird etwaig notwendige strafprozessuale bzw. gefahrenabwehrende Maßnahmen einleiten oder durch die Polizei-Behörden der Länder initiieren, sofern eine Betroffenheit in Deutschland vorliegt.

Im dritten Quartal 2019 erfolgte eine Übung im Kontext des EU LE ERP, die auch die Kommunikationsprüfung der 24/7 Kontaktpunkte sowie die Überprüfung des Protokollablaufs zum Gegenstand hatte.

10. Welches Ausmaß müssen IT-Störungen annehmen, um das Protokoll zu aktivieren, bzw. wie würde die Aktivierung bestimmt?

Das EU LE ERP stellt im Wesentlichen die Reaktion von Europol auf die bedeutenden Cyber-Vorfälle „WannaCry“ und „NotPetya“ aus dem Jahr 2017 dar. Fälle dieser Größenordnung (bewertet anhand einer „threat classification matrix“) wären auch zukünftig als Auslöser für das EU LE ERP anzusehen.

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?

Die Fragen 10 a) und b) werden gemeinsam beantwortet. Hierzu liegen der Bundesregierung keine Informationen vor.

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?

Gemäß öffentlich verfügbaren Quellen der EU beschäftigt die Abteilung für Strategische Kommunikation und Informationsanalyse des Auswärtigen Dienstes der Europäischen Union (StratCom) 35 Mitarbeiterinnen und Mitarbeiter (https://op.europa.eu/en/web/who-is-who/organization/-/organization/EEAS/EEAS_CRF_240841) und das „Stratcom East“ 16 Mitarbeiterinnen und Mitarbeiter (vgl. https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-). Eigene, darüber hinausgehende Kenntnisse liegen der Bundesregierung nicht vor.

a) Welcher Aufwuchs ist für das StratCom geplant?

Laut dem Aktionsplan gegen Desinformation der EU (vgl. https://ec.europa.eu/commission/sites/ beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf, Seite 6) ist bis Ende 2020 eine Entwicklung der Teams im Bereich „Strategische Kommunikation“ auf eine Gesamthöhe von 50 bis 55 Mitarbeiterinnen und Mitarbeitern geplant. Eigene darüber hinausgehende Kenntnisse liegen der Bundesregierung nicht vor.

b) Mit welchen neuen Initiativen will die Europäische Union unabhängige Medien und „Faktenprüfer“ (auch in Drittstaaten) unterstützen?

Es wird auf die Gemeinsamen Mitteilung der EU-Kommission „Bekämpfung von Desinformation im Zusammenhang mit COVID-19 – Fakten statt Fiktion“ (JOIN(2020) 8, erschienen am 10. Juni 2020, https://ec.europa.eu/info/files/joint-communication-tackling-covid-19-disinformation-getting-facts-right_de) verwiesen.

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?

Die HWP ERCHT ist insbesondere für das Thema hybride Bedrohungen zuständig, das hier als Querschnittsthema koordiniert wird und auch Cyber-Aspekte umfassen kann. Initiativen zur Bekämpfung von Cyberbedrohungen laufen jedoch in der vorrangig zuständigen „Horizontal Working Party on Cyber“.

Zum Thema Umgang mit Desinformation hat die HWP ERCHT die Umsetzung des Europäischen Aktionsplans gegen Desinformation weiter vorangetrieben (vgl. GM der EU-KOM Nr. JOIN(2018) 36 vom 2.Januar 2019). Unter kroatischem Vorsitz in der HWP ERCHT wurden insbesondere die Auswirkungen von Desinformation in den EU-Nachbarschaften bearbeitet. Zudem ist das Auftreten von Desinformation im Kontext der COVID-19-Pandemie adressiert worden. Diese Arbeit wird unter deutschem Vorsitz fortgeführt.

13. Welche Anstrengungen sind der Bundesregierung auf EU-Ratsebene bekannt, aus der Coronakrise Schlussfolgerungen für eine verbesserte Kommunikation unter den EU-Mitgliedstaaten im Falle von Krisen sowie eine verbesserte Krisenkommunikation nach außen zu ziehen?

Auf EU-Ebene koordiniert die Bundesregierung in verschiedenen Gremien mit anderen EU-Mitgliedstaaten Maßnahmen der nationalen und der gemeinsamen europäischen Krisen-kommunikation. Zentral ist hierbei der Krisenreaktionsmechanismus des Rates („Integrated Political Crisis Response“ / IPCR), in dem sich regelmäßig Vertreter/-innen von EU-Institutionen und

Mitgliedstaaten austauschen. In diesem Rahmen wurde zur Abstimmung der Krisenkommunikation ein informelles Netzwerk von Kommunikationsfachleuten aus den Mitgliedstaaten gebildet – das so genannte „Crisis Communicators Network“ (CCN). Die Abstimmung von Kommunikationsmaterialien und -kampagnen zwischen EU-Institutionen und Mitgliedstaaten findet auch in der Ratsarbeitsgruppe Information statt.

Bedingt durch die Corona-Krise wurde diese Abstimmung weiter intensiviert. EU-Institutionen und Mitgliedstaaten kommunizieren dabei in der Corona-Krise unter gemeinsam genutzten Hashtags wie #EuropeansAgainstCovid19 oder #StrongerTogether zur Solidarität zwischen EU-Mitgliedstaaten in der Corona-Krise. Die EU und ihre Mitgliedstaaten helfen außerdem im Rahmen der Initiative „Team Europe“ Partnerländern in der ganzen Welt bei der Bekämpfung der COVID-19-Pandemie, ebenfalls begleitet von einer entsprechenden Kommunikationskampagne.

14. Ist der Bundesregierung mittlerweile ein „terroristischer Cyberangriff“ in Deutschland oder der Europäischen Union bekannt geworden und falls ja, wie wurde dieser attribuiert (Drucksache 19/10273, Antwort auf Frage 2)?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.