**Deutscher Bundestag** **Drucksache 19/1419**

**19. Wahlperiode** 22.03.2018

# Kleine Anfrage

**der Abgeordneten Andrej Hunko, Brigitte Freihold, Dr. André Hahn, Niema Movassat, Norbert Müller (Potsdam), Zaklin Nastic, Dr. Alexander S. Neu, Martina Renner, Eva-Maria Elisabeth Schreiber, Dr. Petra Sitte, Friedrich Straetmanns, Katrin Werner und der Fraktion DIE LINKE.**

## Reaktion der EU auf Cyberangriffe

In einem „Cybersicherheitspaket“ will die Europäische Union ihre „Reaktionsfähigkeit auf Cyberangriffe“ verbessern (Quelle hier und im Folgenden: Pressemitteilung sowie Factsheet der Europäischen Kommission vom 19. September 2017). Als neues „Instrument zur Verbesserung des Schutzes gegen Cyberangriffe“ plant die EU-Kommission unter anderem die Einrichtung einer „EU-Agentur für Cybersicherheit“, um die bislang existierende Abwehrfähigkeit und Reaktion der EU bei Cyberattacken zu verbessern, indem die bereits existierende Agentur für Netz- und Informationssicherheit (ENISA) „gestärkt“ wird und Mitgliedstaaten beim Umgang mit Cyberangriffen unterstützt werden. Hierzu soll die ENISA mit einem ständigen Mandat ausgestattet werden. Zusätzlich zu den regelmäßig abgehaltenen „EU-Cyberübungen“ soll auch die neue Agentur jährliche europaweite „Cybersicherheitsübungen“ durchführen. Wie in der Richtlinie über die Sicherheit von Netz- und Informationssystemen vorgesehen, soll die runderneuerte ENISA dafür sorgen, dass in jedem Mitgliedstaat „schwerwiegende Cybersicherheitsvorfälle“ einer nationalen Behörde gemeldet werden müssen.

Ebenfalls geplant ist die Einrichtung eines europäischen „Forschungs- und Kompetenzzentrums für Cybersicherheit“, ein entsprechendes „Pilotzentrum“, soll noch 2018 starten, um die Mitgliedstaaten bei der Entwicklung und Nutzung von „Instrumenten und Technik“ gegen die „immer neuen Bedrohungen“ zu unterstützen. Das Zentrum könnte außerdem „um eine Cyberabwehr-Abteilung ergänzt werden“. Dessen ungeachtet stellt die Kommission ein „Kompetenzdefizit im Bereich der Cyberabwehr“ fest, dem noch 2018 mit einer „Plattform für die Ausbildung und Aufklärung im Bereich der Cyberabwehr“ begegnet werden soll. Von Cyberangriffen betroffene Mitgliedstaaten könnten ähnlich wie beim EU-Katastrophenschutzmechanismus aus einem „Cybersicherheits-Notfallfonds“ unterstützt werden, allerdings müssten diese zuvor alle nach EU-Recht vorgeschrieben Cybersicherheitsmaßnahmen „ordnungsgemäß umgesetzt haben“. Weitere neue Kapazitäten sollen für die „Enttarnung, Rückverfolgbarkeit und Verfolgung von Cyberkriminellen“ sorgen. Genannt werden jedoch keine Maßnahmen zur Bekämpfung von Cyberangriffen, sondern lediglich „Betrug und Fälschung im Zusammenhang mit bargeldlosen Zahlungsmitteln“. Ebenfalls als „Ermittlungsarbeit bei Cyberdelikten“ wird die Erleichterung des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln genannt, die eigentlich zur Beschlagnahme von Cloud-Daten im EU-Ausland dienen soll und die „Überlegungen zur Rolle der Verschlüsselung bei kriminaltechnischen Ermittlungen“.

Schließlich arbeitet die EU-Kommission an einem „Konzept, wie Europa und die Mitgliedstaaten in der Praxis gemeinsam rasch reagieren können, wenn es zu einem groß angelegten Cyberangriff kommt“. In einer bereits vorgelegten Empfehlung werden die Mitgliedstaaten und die EU-Organe aufgefordert, für die praktische Umsetzung einen EU-Rahmen für die Reaktion auf Cybersicherheitskrisen zu schaffen. Zur Verbesserung der Cyberabwehr sollen auch militärische Strukturen („Cyberabwehrprojekte“) eingebunden werden, die EU-Kommission nennt hierzu die ständige strukturierte Zusammenarbeit (PESCO) und den Europäischen Verteidigungsfonds. Insbesondere mit der NATO soll die Europäische Union die „Forschungs- und Innovationszusammenarbeit“ intensivieren. Wie in den Jahren 2017 und 2018 ist die Beteiligung an „parallelen und koordinierten Übungen“ geplant (Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 19/1212). Zur Verbesserung der internationalen Zusammenarbeit plant die EU-Kommission die Umsetzung eines „Rahmens für eine gemeinsame diplomatische Reaktion auf böswillige Cyberaktivitäten“. Auch Drittländer sollen bei der „Bewältigung von Cyberbedrohungen“ unterstützt werden.

Wir fragen die Bundesregierung:

1. Inwiefern teilt die Bundesregierung die Einschätzung der EU-Kommission, die ein „Kompetenzdefizit im Bereich der Cyberabwehr“ feststellt, und worin liegt dies begründet?
2. Ab welcher Schwelle einer „Cybersicherheitskrise“ sollten „Europa und die Mitgliedstaaten in der Praxis“ aus Sicht der Bundesregierung „gemeinsam rasch reagieren können, wenn es zu einem groß angelegten Cyberangriff kommt“?
3. Welche wesentlichen Akteure der Mitgliedstaaten und der Europäischen Union sind aus Sicht der Bundesregierung im Bereich des operativen und strategischen Krisenmanagements im Cyberraum unterrepräsentiert und müssten stärker beteiligt werden (etwa Reaktionsteams für Computersicherheitsverletzungen, Europol, der Europäische Auswärtige Dienst, die East StratCom Task Force, die Website „EUvsdisinformation“)?
4. Welche Rolle sollte eine „EU-Agentur für Cybersicherheit“ aus Sicht der Bundesregierung hinsichtlich der Abwehrfähigkeit und Reaktion der EU auf Cyberangriffe übernehmen, und welche Maßnahmen hält sie dazu für geeignet?
5. Inwiefern sollte die neue Agentur aus Sicht der Bundesregierung zusätzlich zu den regelmäßig abgehaltenen „EU-Cyberübungen“ weitere „Cybersicherheitsübungen“ durchführen, und welche Defizite sollten damit überbrückt werden?
6. Wo soll nach Kenntnis der Bundesregierung das europäische „Forschungs- und Kompetenzzentrums für Cybersicherheit“ bzw. ein entsprechendes „Pilotzentrum“ eingerichtet werden, um die Mitgliedstaaten bei der Entwicklung und Nutzung von „Instrumenten und Technik“ gegen die „immer neuen Bedrohungen“ zu unterstützen?
   a) Welche Mitgliedstaaten oder sonstigen Einrichtungen nehmen an dem Zentrum teil, und welche Kapazitäten stellt die Bundesregierung hierfür zur Verfügung?
   b) Welche Haltung vertritt die Bundesregierung zur Frage, inwiefern das Zentrum um eine „Cyberabwehr-Abteilung“ ergänzt werden sollte, und über welche Kompetenzen dieses verfügen sollte?
7. Wo soll die von der EU-Kommission angekündigte „Plattform für die Ausbildung und Aufklärung im Bereich der Cyberabwehr“ nach Kenntnis der Bundesregierung eingerichtet werden?

8. Auf welche Weise arbeiten Bundesbehörden mit dem „Incident and Threat Information Sharing EU Centre“ (ITIS-EUC) zusammen, über das „Informationen über Cyberbedrohungen und -vorfälle im Energiesektor analysiert und ausgetauscht werden“ (Ratsdokument 11539/17)?
9. Was ist der Bundesregierung über die Einrichtung einer „Cyber platform for education, training, exercise and evaluation“ (ETEE) bekannt (http://gleft.de/29D), wo wird diese installiert, und wer nimmt daran teil?
   a) Welche Ziele werden mit der ETEE verfolgt, und wie werden Doppelungen mit bestehenden Einrichtungen vermieden?
   b) Welche Kosten (auch Machbarkeitsstudien) entstehen für die ETEE, und wie werden diese übernommen?
   c) Wann soll die ETEE starten bzw. ihre volle Einsatzbefähigung erreichen?
10. Welchen neuen EU-(Rechts-)Rahmen für die Reaktion auf „Cybersicherheitskrisen“ hält die Bundesregierung für notwendig, und wie müsste dieser ausgestaltet werden?
11. Welche Haltung vertritt die Bundesregierung zur Frage, wie ein „Cybersicherheits-Notfallfonds“ ausgestaltet werden könnte, und ob Mittel hierfür aus vorhandenen Strukturen verteilt werden könnten?
12. Welche neuen Kapazitäten sollte die Europäische Union aus Sicht der Bundesregierung zur „Enttarnung, Rückverfolgbarkeit und Verfolgung von Cyberkriminellen“ entwickeln?
13. Welche Haltung vertritt die Bundesregierung zur Frage, welche militärischen EU-Strukturen („Cyberabwehrprojekte“) in die zivile Cyberabwehr eingebunden werden sollten?
   a) Was ist der Bundesregierung über Planungen bekannt, die ständige strukturierte Zusammenarbeit (PESCO) und den Europäischen Verteidigungsfonds stärker in die eigentlich zivile Cyberabwehr zu integrieren (bitte etwaige Projekte oder Initiativen aufführen)?
   b) Was ist der Bundesregierung darüber bekannt, auf welche Weise die Europäische Union und die NATO den Informationsaustausch zwischen ihren jeweiligen Cybersicherheitsgremien (laut EU-Kommission dem IT-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der EU (CERT-EU) und der Computer Incident Response Capability (NCIRC) der NATO), intensivieren, wozu die beiden Partner in den Jahren 2017 und 2018 erstmals parallele und koordinierte Übungen zur Reaktion auf ein hybrides Angriffsszenario abgehalten haben?
   c) Wie sollen die „Bemühungen um bessere Interoperabilität bei den Cybersicherheitsstandards“ umgesetzt werden?
14. Was ist der Bundesregierung über Ort und Zeitpunkt einer Cybersicherheitsübung „Cyber Europe 2018“ bekannt (sofern die Übung in einzelne Teile aufgegliedert ist, diese bitte benennen)?
   a) Wer nimmt an der Übung teil, und inwiefern soll diese im Kontext anderer Übungen, etwa der NATO, abgehalten werden?
   b) Welche Szenarien werden dort geübt?
   c) Sofern auch Szenarien wie die „Verunstaltung von Webseiten“, „Datendiebstahl von Benutzernamen und Passwörtern“, „Ausschalten der Energieversorgung eines Flughafens“, „Kontrolle über die Flugzeugbetankungsanlage“ oder die Reaktion auf das Streuen von Falschinformationen geübt werden sollen, welche Details sind der Bundesregierung hierzu bekannt?

15. Welche Szenarien werden nach Kenntnis der Bundesregierung in der militärischen Übung „Locked Shields 2018“ vom 23. bis 27. April 2018 in Tallinn geübt (Antwort der Bundesregierung auf Bundestagsdrucksache 19/1212)?

    a) Welche Staaten, mit denen Beitrittsverhandlungen zum NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) vor dem Abschluss stehen, werden eingeladen bzw. nehmen teil?

    b) Inwiefern ist mittlerweile bekannt, welche Cyberübungen, an denen sich die Bundeswehr 2018 beteiligt, an der Schwelle eines bewaffneten Angriffs operieren?

    c) An welchen Cyberübungen der Europäischen Union oder der NATO hat sich die Bundeswehr in der Vergangenheit mit „Red-Teams“ beteiligt (Antwort der Bundesregierung auf Bundestagsdrucksache 19/1212)?

    d) In welchen Cyberübungen, an denen sich die Bundeswehr 2017 beteiligt, wurde mit den Anwendungen „Cobalt Strike“, „Metasploit“ oder „Burp Proxy“ geübt?

16. Welche weiteren Anstrengungen sollte die Europäische Union aus Sicht der Bundesregierung hinsichtlich von Cyberdiplomatie und internationalen Cybernormen sowie zur Umsetzung der „Cyber Diplomacy Toolbox“ (Ratsdokument 9916/17) unternehmen?

17. Welche Drittländer außer den USA, Japan, Indien, der Republik Korea und China sollten aus Sicht der Bundesregierung für die Europäische Union zur Etablierung „starker Bündnisse“ oder zu Gesprächen über das Thema Cybersicherheit im Fokus stehen?

18. Welche Haltung vertritt die Bundesregierung zur Frage der Notwendigkeit eines „Rahmens für eine gemeinsame diplomatische Reaktion auf böswillige Cyberaktivitäten“?

19. Inwiefern bzw. nach welcher Maßgabe sollte die Europäische Union aus Sicht der Bundesregierung zukünftig mit (öffentlichen oder nichtöffentlichen) diplomatischen Verurteilungen, Erklärungen oder Ratsschlussfolgerungen an Regierungen, die als Urheber von Cyberangriffen verdächtigt werden, reagieren (Ratsdokument WK 2641/2018 INIT)?

20. Mit welchen Maßnahmen sollte die Europäische Union aus Sicht der Bundesregierung zukünftig gemeinsam auf „böswillige Cyberaktivitäten“ reagieren?

    a) Nach welcher Maßgabe fielen „böswillige Cyberaktivitäten“ unter die Regelungen der „Solidaritätsklausel“ nach Artikel 222 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV)?

    b) Inwiefern könnten als „Reaktion auf böswillige Cyberaktivitäten“ Instrumente der integrierten EU-Regelung für die politische Reaktion auf Krisen (ICPR) genutzt werden?

    c) In welchen zivilen oder militärischen Cyberübungen, an denen sich die Bundesregierung beteiligt hat, wurde der ICPR-Mechanismus bereits berücksichtigt?

    d) Inwiefern könnten sich etwaige EU-Reaktionen aus Sicht der Bundesregierung auch auf die United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) berufen, und welche Initiativen sind der Bundesregierung hierzu bekannt?

21. Wie könnte ein „Protokoll für die Notfallreaktion“ auf Cybersicherheitsvorfälle („Emergency Response Protocol”) europäischer Strafverfolgungsbehörden aus Sicht der Bundesregierung ausgestaltet und umgesetzt werden (Ratsdokument 11809/17)?

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

    b) Welche zivilen und militärischen EU-Lagezentren sollten daraufhin aktiviert werden?

    c) Welche Einrichtungen sollten mit der Überwachung offener Quellen („Open Source Monitoring” und taktischer Koordination beauftragt werden?

22. Welche Defizite sieht die Bundesregierung bei der EU-Reaktion auf die Cyberangriffe mit „Wannacry“ und „NotPetya“ („Herausforderungen, an deren Bewältigung gearbeitet wird“, Ratsdokument 11539/17), und welche Maßnahmen hält sie hierzu für erforderlich?

    a) Welche Rolle übernimmt das geheimdienstliche Lagezentrum INTCEN schon jetzt bei der Zurechnung („Attribuierung“) von Cyberangriffen, und wie sollten diese Fähigkeiten ausgebaut werden?

    b) Auf welche Weise ist das INTCEN bzgl. der Cyberangriffe mit „Wannacry“ und „NotPetya“ tätig geworden?

    c) Welche deutschen Behörden haben hierzu Lageberichte beigesteuert?

    d) Auf welche Weise sind welche EU-Agenturen oder IT-Netzwerke (etwa die Reaktionsteams für Computersicherheitsverletzungen) bzgl. der Cyberangriffe mit „Wannacry“ und „NotPetya“ tätig geworden bzw. weiterhin damit befasst?

23. Was ist der Bundesregierung darüber bekannt, welche EU-Agenturen oder IT-Netzwerke mit Ermittlungen und Analysen zu Angriffen mit der Schadsoftware „Snake“ (bzw. „Turla“, „Uroburos“), „Stuxnet“, „Black Energy“ oder „Mirai“ befasst waren oder sind?

Berlin, den 22. März 2018

**Dr. Sahra Wagenknecht, Dr. Dietmar Bartsch und Fraktion**

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.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