Deutscher Bundestag **Drucksache 19/11734**

19. Wahlperiode 17.07.2019

Kleine Anfrage

der Abgeordneten Alexander Graf Lambsdorff, Grigorios Aggelidis, Renata Alt, Nicole Bauer, Jens Beeck, Dr. Jens Brandenburg (Rhein-Neckar), Dr. Marco Buschmann, Hartmut Ebbing, Dr. Marcus Faber, Daniel Föst, Otto Fricke, Thomas Hacker, Katrin Helling-Plahr, Markus Herbrand, Torsten Herbst, Katja Hessel, Manuel Höferlin, Dr. Christoph Hoffmann, Reinhard Houben, Ulla Ihnen, Olaf in der Beek, Gyde Jensen, Dr. Christian Jung, Thomas L. Kemmerich, Karsten Klein, Dr. Marcel Klinge, Pascal Kober, Carina Konrad, Konstantin Kuhle, Ulrich Lechte, Till Mansmann, Dr. Jürgen Martens, Alexander Müller, Roman Müller-Böhm, Dr. Martin Neumann, Bernd Reuther, Matthias Seestern-Pauly, Frank Sitta, Bettina Stark-Watzinger, Dr. Marie-Agnes Strack-Zimmermann, Katja Suding, Michael Theurer, Stephan Thomae, Dr. Andrew Ullmann, Sandra Weeser, Nicole Westig und der Fraktion der FDP

„Digitaler Verteidigungsfall“

Der Inspekteur Cyber- und Informationsraum, Generalleutnant Ludwig Leinhos, führte am 8. Juni 2019 ein Interview mit der Nachrichtenagentur „AFP“. In dem Interview forderte Leinhos einen Rahmen für den Umgang mit Hackerangriffen, Propaganda und Desinformationskampagnen. In diesem Zusammenhang führte der Inspekteur Cyber- und Informationsraum aus: „Wir brauchen etwas, welches ich in der Diskussion gerne als ‚digitalen Verteidigungsfall‘ bezeichne, unterhalb der Schwelle eines klassischen Verteidigungsfalls“. Ohne das Trennungsgebot von Bundeswehr, Polizei und Geheimdiensten infrage zu stellen, bedürfe es einer Überprüfung und möglicherweise Anpassung der rechtlichen Grundlagen, zitiert „AFP“ den Generalleutnant. Leinhos ließ bei seiner Forderung nach einem „digitalen Verteidigungsfall“ aber weitestgehend offen, was unter dem Begriff genau zu verstehen sei. Auch nahm er keine klare Abgrenzung zum „klassischen Verteidigungsfall“ vor. Eine eindeutige Definition des Begriffs „digitaler Verteidigungsfall“ durch die Bundesregierung ist aus Sicht der Fragesteller aber für eine weitere öffentliche Diskussion zwingend notwendig. Darüber hinaus forderte Leinhos klare Regelungen, um einen „reibungslosen Übergang von der Cyberabwehr zur Cyberverteidigung sicher(zu)stellen“ und regte dazu eine koordinierende Rolle im Nationalen Cyber-Abwehrzentrum an. Auch in diesem Zusammenhang ist die Darlegung des konkreten Verständnisses und der Unterscheidung von „Cyberabwehr“ und „Cyberverteidigung“ durch die Bundesregierung aus Sicht der Fragesteller erforderlich.

Wir fragen die Bundesregierung:

1. Teilt die Bundesregierung die Aussage von Generalleutnant Leinhos, dass es die Kategorie „digitaler Verteidigungsfall“ für den Umgang der Bundesregierung mit Hackerangriffen, Propaganda und Desinformationskampagnen brauche?

   Wenn nein, warum nicht?

   Wenn ja, auf welchen Erkenntnissen, Erfahrungen oder aktuellen Anlässen beruht diese Forderung?

2. Was versteht die Bundesregierung konkret unter dem Begriff „digitaler Verteidigungsfall“?

3. Wie würde sich nach Auffassung der Bundesregierung ein „digitaler Verteidigungsfall“ von einem „klassischen Verteidigungsfall“ unterscheiden hinsichtlich

   a) der Intensität des Angriffs,

   b) der Intensität der Reaktion,

   c) der Attribution,

   d) des Verfahrens der Feststellung eines Verteidigungsfalls,

   e) (völker-)rechtlicher Aspekte,

   f) des Parlamentsbeteiligungsgesetzes und der Mandatierung von Gegenmaßnahmen und

   g) des Bündnisfalls auf der Grundlage des NATO-Vertrags?

4. Wäre nach Auffassung der Bundesregierung im Falle eines Hackerangriffs, der nicht die Schwelle eines bewaffneten Angriffs erreicht, die Zuständigkeit der Bundeswehr nach dem Grundgesetz (GG), insbesondere Artikel 87a GG, eröffnet?

5. Unter welchen Voraussetzungen wäre die Bundeswehr für die Abwehr von Hackerangriffen nach Ansicht der Bundesregierung zuständig?

6. Welche Institution bzw. welches Gremium soll die Federführung für die Feststellung eines „digitalen Verteidigungsfalles“ nach Auffassung der Bundesregierung haben?

7. Welche Rolle soll das Nationale Cyber-Abwehrzentrum im Zusammenhang mit der Feststellung und der Reaktion auf einen „digitalen Verteidigungsfall“ aus Sicht der Bundesregierung haben?

8. Welche rechtlichen Regelungen und gesetzgeberischen Vorgaben müssten aus Sicht der Bundesregierung zur Feststellung eines „digitalen Verteidigungsfalls“ angepasst werden?

9. Welche Auswirkungen hätte ein „digitaler Verteidigungsfall“ nach Auffassung der Bundesregierung auf die Befehls- und Kommandogewalt?

10. Wie definiert die Bundesregierung konkret den Begriff „Cyberabwehr“?

11. Wie definiert die Bundesregierung konkret den Begriff „Cyberverteidigung“?

12. Welcher konkreten gesetzlichen und organisatorischen Regelungen bedarf es nach Auffassung der Bundesregierung, um einen „reibungslosen Übergang von Cyberabwehr zur Cyberverteidigung“ sicherzustellen?

    Wie kann dabei die Wahrung des Trennungsgebotes zweifelsfrei eingehalten werden?

13. Wie ist der Übergang von „Cyberabwehr“ zur „Cyberverteidigung“ bisher geregelt (welche Institution hat die Federführung, welche Institutionen sind beteiligt, wie verläuft die Entscheidungsfindung und Koordinierung, etc.)?
14. Gibt es konkrete Pläne für strukturelle oder personelle Veränderungen im Nationalen Cyber-Abwehrzentrum (wenn ja, bitte einschließlich von Zeitplänen erläutern)?

Berlin, den 26. Juni 2019

Christian Lindner 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