Deutscher Bundestag **Drucksache 19/12235**

19. Wahlperiode 09.08.2019

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Alexander Graf Lambsdorff, Grigorios Aggelidis, Renata Alt, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/11734 –

„Digitaler Verteidigungsfall“

Vorbemerkung der Fragesteller

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.

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?

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Verteidigung vom 7. August 2019 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

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

Die Fragen 1 und 2 werden aufgrund ihres inhaltlichen Zusammenhanges zusammen beantwortet.

Der Begriff „digitaler Verteidigungsfall“ wird durch die Bundesregierung nicht verwendet, daher existiert hierfür keine festgelegte Definition. Er stellt keinen Rechtsbegriff dar, der an rechtliche Voraussetzungen anknüpft oder rechtliche Konsequenzen auslöst.

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?

Auf die Antworten zu den Fragen 1 und 2 wird verwiesen.

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?

Die Fragen 4 und 5 werden aufgrund ihres inhaltlichen Zusammenhangs zusammen beantwortet.

Auf die Antwort der Bundesregierung zu den Fragen 1 bis 3 auf Bundestagsdrucksache 19/5472 wird verwiesen.

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?

Die Fragen 6 bis 9 werden gemeinsam beantwortet.

Auf die Antworten zu den Fragen 1 und 2 wird verwiesen.

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

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

Die Fragen 10 und 11 werden aufgrund ihres inhaltlichen Zusammenhangs zusammen beantwortet.

Auf die Vorbemerkung der Bundesregierung auf Bundestagsdrucksache 19/2645 wird verwiesen.

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?

Cyber-Abwehr und Cyber-Verteidigung sind sich ergänzende Mittel zum Erreichen von Cyber-Sicherheit und damit zwei stetig wahrzunehmende Aufgabenbereiche.

Im Falle eines bewaffneten Angriffes steht der Bundesrepublik Deutschland das Recht zu, sich zu verteidigen. Dies erlaubt eine Reaktion mit allen nach Maßgabe des Völkerrechtes zulässigen militärischen Mitteln und umfasst auch den Einsatz von militärischen Cyber-Fähigkeiten. Auch in diesem Fall findet in Deutschland weiterhin zivile Cyber-Abwehr statt.

Dabei wird das Cyber-Abwehrzentrum im Sinne eines vernetzten Ansatzes als Informations-, Kooperations- und Koordinationsplattform für das gesamtstaatliche Handeln zum Erreichen von Cyber-Sicherheit agieren. Dies wird im Rahmen der kontinuierlichen Weiterentwicklung des Cyber-Abwehrzentrums berücksichtigt.

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.)?

Auf die Antworten zu den Fragen 10 bis 12 wird verwiesen.

14. Gibt es konkrete Pläne für strukturelle oder personelle Veränderungen im Nationalen Cyber-Abwehrzentrum (wenn ja, bitte einschließlich von Zeitplänen erläutern)?

Beim Cyber-Abwehrzentrum handelt es sich um eine Informations-, Koordinations- und Kooperationseinrichtung von Bundesbehörden mit Sicherheitsaufgaben, die keine eigenständige Behörde ist. Die am Cyber-Abwehrzentrum beteiligten Behörden bringen sich im Rahmen ihrer jeweiligen Zuständigkeiten sowie des ansonsten für sie geltenden Rechts ein.

Das Cyber-Abwehrzentrum unterliegt einem kontinuierlichen Weiterentwicklungsprozess. Im nächsten Schritt wird das Cyber-Abwehrzentrum u. a. das Cyber-Lagebild und die Risikobewertung zu Cyber-Gefahren weiter optimieren sowie eine intensivere Koordinierung der operativen Zusammenarbeit realisieren. Durch verbesserten Informationsaustausch, in Verbindung mit der bereits beste-

henden 24/7-Erreichbarkeit, kann zudem schneller und koordinierter auf Cyber-Angriffe reagiert werden. Die Zusammenarbeitsprozesse der am Cyber-Abwehrzentrum beteiligten Behörden werden deutlich optimiert.

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