Deutscher Bundestag **Drucksache 20/8158**

20. Wahlperiode 29.08.2023

Kleine Anfrage

der Abgeordneten Joachim Wundrak, Eugen Schmidt, Petr Bystron, Tino Chrupalla, Dr. Alexander Gauland, Markus Frohnmaier, Stefan Keuter, Steffen Kotré, Matthias Moosdorf, René Springer und der Fraktion der AfD

Cyberkriegsführung und Cyberkriegsverteidigung: rechtliche, organisatorische und politische Aspekte

Cyberkriegsführung und Cyberkriegsverteidigung spielen nicht erst seit der Nationalen Sicherheitsstrategie der Bundesregierung (2023, vgl. www.auswaertiges-amt.de/blueprint/servlet/blob/2604006/857b2e75fade2a89cc5232a59fca997b/nationale-sicherheitsstrategie-data.pdf) eine große Rolle im gesamtstaatlichen sicherheits- und verteidigungspolitischen Konzept.

Bereits durch die Einrichtung des Kommandos Cyber- und Informationsraum (KdoCIR) der Bundeswehr sowie die prominente Erwähnung in NATO-Gipfelerklärungen (beispielsweise Madrid 2022 sowie Vilnius 2023, vgl. www.nato.int/cps/en/natohq/official_texts_196951.htm sowie www.nato.int/cps/en/natohq/official_texts_217320.htm) wurde die Bedeutung der Cyberabwehr deutlich.

Nach Rechtsauffassung der Bundesregierung, niedergelegt im Arbeitspapier On the Application of International Law in Cyberspace, ist ein Cyberangriff dabei ein „Akt oder eine Aktion, die im oder durch den Cyberraum initiiert wurde, um schädigende Auswirkungen auf Kommunikation, Information oder andere elektronische Systeme zu zeitigen, auf die Information, die in diesen Systemen gespeichert oder prozessiert wird oder durch diese Systeme übertragen wird oder auf physische Objekte oder Personen“ (eigene Übersetzung; vgl. ccdcoe.org/uploads/2018/10/Germany_on-the-application-of-international-law-in-cyberspace-data_English.pdf, S. 8).

Trotz der Beteuerungen der Bundesregierung, die massive Cyberangriffe konventionellen Angriffen gleichstellt (vgl. ebd., siehe auch Erklärung zum NATO-Gipfel von Vilnius), ist auch Experten bis heute nicht klar, welche Operationen im Cyber-Raum die Bundesregierung für politisch sinnvoll, technisch machbar und rechtlich für legitim hält (vgl. www.swp-berlin.org/publications/products/studien/2020S15_she_CyberOperationen.pdf, S. 39-40). Daher dient diese Kleine Anfrage der Klärung dieses strategisch wichtigen und für die nationale Sicherheit nach Auffassung der Fragesteller essenziellen Themas.

Wir fragen die Bundesregierung:

1. Welche Staaten teilen nach Kenntnis der Bundesregierung die in dem Papier On the Application of International Law in Cyberspace (vgl. Vorbemerkung der Fragesteller) geäußerte Rechtsauffassung der Bundesregierung?

2. Welche Staaten vertreten nach Kenntnis der Bundesregierung entgegenstehende Rechtsauffassungen zum o. g. Papier, und ist der Bundesregierung deren entsprechende Begründung bekannt (wenn ja, bitte erläutern)?
3. Sind der Bundesregierung empirische Fälle bekannt, in denen Cyberangriffe in Ausmaß und Auswirkungen vergleichbar waren zu physischen (kinetischen) Angriffen, und wenn ja, welche (vgl. On the Application of International Law in Cyberspace, S. 5)?
4. Arbeitet die Bundesregierung auf eine international anerkannte Definition (Legaldefinition) von kritischer Infrastruktur hin, und wenn ja, welche diesbezüglichen Erfolge kann die Bundesregierung vorweisen (vgl.. On the Application of International Law in Cyberspace, S. 4)?
5. Hat die Bundesregierung Kenntnis von Initiativen anderer Staaten, die auf eine international verbindliche Legaldefinition von kritischer Infrastruktur abzielen, und wenn ja, welche?
6. Sind der Bundesregierung empirische Fälle bekannt, in denen bewaffnete nichtstaatliche Gruppierungen Cyberangriffe gegen einen Staat durchgeführt haben, die so weitrechend, dauerhaft und von hoher Intensität waren, dass sie als nichtstaatlicher bewaffneter Konflikt klassifiziert wurden bzw. rechtlich klassifiziert werden könnten, und wenn ja, welche (vgl. ebd., S. 7)?
7. Sind der Bundesregierung Cyberangriffe bekannt, die von nichtstaatlichen bewaffneten Gruppierungen im Auftrag, unter Kontrolle oder durch Anweisungen von Staaten gegen Einrichtungen, Bundesministerien, Behörden des Bundes durchgeführt wurden, und wenn ja, welche (vgl. ebd., S. 11)?
8. Sind der Bundesregierung Cyberangriffe bekannt, die von nichtstaatlichen bewaffneten Gruppierungen gegen Einrichtungen, Bundesministerien, Behörden des Bundes durchgeführt wurden, und wenn ja, welche (vgl. ebd., S. 11)?
9. Sind der Bundesregierung internationale Bemühungen um ein internationales Übereinkommen bekannt, die darauf abzielen, einen Verzicht auf Cyberangriffe zu erreichen bzw. völkerrechtlich bindend zu kodifizieren (z. B. Verzicht auf den Cybererstschlag), und wenn ja, von welchen Staaten, in welchem Stadium, und mit welchem Inhalt (ggf. bitte Kernpunkte darstellen)?
10. Sind der Bundesregierung andere Staaten bekannt, die Hackbacks als Mittel der Cyberabwehr prinzipiell ablehnen (Nationale Sicherheitsstrategie, S. 62), und wenn ja, welche?
11. Welche Staaten neben den USA (vgl. www.focus.de/politik/ausland/usa/usa-beanspruchen-recht-auf-cyber-erstschlag-neue-richtlinien-fuer-das-us-militaer_id_2237677.html) nehmen nach Kenntnis der Bundesregierung für sich das Recht auf einen Cybererstschlag in Anspruch, und welche Staaten haben nach Kenntnis der Bundesregierung die entsprechenden Fähigkeiten und den politischen Willen?
12. Bis wann soll das Nationale Cyberabwehrzentrum in vollem Umfang seine Arbeit aufnehmen, einschließlich der Lagebilderstellung (vgl. Nationale Sicherheitsstrategie, S. 61)?
13. Wie viele Bundeswehrangehörige sollen zum Nationalen Cyberabwehrzentrum bis wann abgeordnet werden?

14. Welche zusätzlichen Haushaltsmittel sollen gemäß der Nationalen Sicherheitsstrategie (S. 59 ff.) bis wann aus welchen Haushaltstiteln in die Cyberabwehr fließen?

15. Bis wann wird die in der Nationalen Sicherheitsstrategie (S. 62) angekündigte Prüfung der Fähigkeiten und rechtlichen Befugnisse im Bereich der Cyberabwehr voraussichtlich abgeschlossen, und in welcher Form werden die Ergebnisse der (parlamentarischen) Öffentlichkeit zugänglich gemacht?

16. Bis wann strebt die Bundesregierung die Änderung des Grundgesetzes zur Schaffung einer Bundeskompetenz zur Cyberabwehr an (vgl. Nationale Sicherheitsstrategie, S. 62)?

17. Welche Arten von Cyberoperationen, insbesondere OMCO (Offensive militärische Cyber-Operationen), sind nach Auffassung der Bundesregierung rechtlich legitim und politisch-militärisch sinnvoll (vgl. www.swp-berlin.org/publications/products/studien/2020S15_she_CyberOperationen.pdf, S. 7)?

18. Wie viele militärische und nichtmilitärische Cyberoperationen gegen Bundesministerien, Bundesbehörden und kritische Infrastruktur in Deutschland bzw. entsprechende deutsche Einrichtungen im Ausland (u. a. Botschaften und Konsulate) oder die Bundeswehr in Auslandseinsätzen wurden seit 2017 durch wen ausgeführt (bitte gemäß Fragestellung jährlich aufschlüsseln und Staaten bzw. nichtstaatliche Akteure und deren (wahrscheinliche) Auftraggeber nennen sowie nach Denial & Disruption; Zerstörung; Manipulation; Intelligence, Surveillance, Reconnaisance (ISR) sowie Informationsoperationen, (vgl. www.swp-berlin.org/publications/products/studien/2020S15_she_CyberOperationen.pdf, S. 10 bis 11) aufschlüsseln)?

19. Wie viele russische Cyberangriffe gegen ukrainische Einrichtungen (auch Ausbildungseinrichtungen ukrainischer Soldaten auf deutschem Staatsgebiet) hat es nach Kenntnis der Bundesregierung seit 2014 gegeben (bitte nach Jahresscheiben aufschlüsseln)?

20. Hat die Bundesregierung Erkenntnisse über die Anzahl der Cyberangriffe auf NATO- und EU-Verbündete durch Russland seit 2014, und wenn ja, welche (vgl. NATO-Gipfel-Erklärung von Vilnius 2023; bitte nach Jahren und Staaten aufschlüsseln)?

21. Hat die Bundesregierung Erkenntnisse über die Anzahl der Cyberangriffe auf NATO- und EU-Verbündete durch China seit 2014, und wenn ja, welche (vgl. NATO-Gipfel-Erklärung von Vilnius 2023; bitte nach Jahren und Staaten aufschlüsseln)?

22. Bei wie vielen Cyberverteidigungsübungen, an denen die Bundeswehr teilnahm, nahmen seit 2014 ukrainische Militärangehörige teil (bitte mit Titel, Zeitraum und Teilnehmern auflisten)?

23. Hat sich die Bundesregierung zur Rolle von Cyberangriffen im Ukraine-Krieg eine Auffassung gebildet, und wenn ja, wie lautet diese?

24. Wenn sich die Bundesregierung zur Rolle und Bedeutung von Cyberangriffen im Ukraine-Krieg eine Auffassung gebildet hat, welche Schlussfolgerungen zieht sie daraus für die Verteidigung Deutschlands?

25. Hat sich die Bundesregierung juristischen Rat eingeholt, wann im Rahmen von ausschließlich im Cyberraum durchgeführten Angriffen auf die Bundesrepublik Deutschland ihre politischen, militärischen, wirtschaftlichen Einrichtungen und auf die kritische Infrastruktur der Spannungsfall (Artikel 80a des Grundgesetzes (GG)) bzw. der Verteidigungsfall (Artikel 115a GG) gegeben wäre (bitte ausführen und begründen)?

26. Sind nach Auffassung der Bundesregierung reine nichtdisruptive ISR (Intelligence, Surveillance and Reconnaissance)-Operationen eine bewaffnete Unternehmung im Cyberraum, und wenn ja, welche rechtlichen und sonstigen Schlussfolgerungen zieht die Bundesregierung daraus?

27. Hat sich die Bundesregierung zur Fragestellung, ab wann Cyber- bzw. Desinformationskampagnen unterhalb der völkerrechtlichen Schwelle eines bewaffneten Konfliktes ablaufen, eine Verteidigungssituation ergeben, in der die Bundeswehr mittels Informationsoperationen „zurückschlagen“ darf, eine Auffassung gebildet, und wenn ja, wie lautet diese?

28. Hat die Bundesregierung Kenntnis, wie viele deutsche Unternehmen im Bereich Cybersicherheit bzw. Cyberverteidigung Aufträge von EU oder NATO erhalten haben, und wenn ja, wie hat sich die entsprechende Fallzahl seit 2017 bis heute entwickelt (bitte nach Fallzahl sowie Auftragsvolumen aufschlüsseln)?

29. Wie viele Dienstposten für IT-Fachkräfte sind für 2023 sowie 2024 im Bereich Cyber- und Informationsraum der Bundeswehr vorgesehen, und wie viele davon sind bzw. bleiben voraussichtlich unbesetzt (vgl. die Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 20/5597, S. 18)?

30. Wie viele Bundeswehrangehörige oder Angehörige sonstiger Bundesbehörden wurden seit Bestehen des NATO Counter Intelligence Centre of Excellence dorthin abgesandt (bitte nach Jahren aufschlüsseln und die jeweiligen Positionen aufführen)?

31. Wie viele Bundeswehrangehörige oder Angehörige sonstiger Bundesbehörden wurden seit Bestehen des Cooperative Cyber Defence Centtre of Excellence dorthin abgesandt (bitte nach Jahren aufschlüsseln und die jeweiligen Positionen aufführen)?

Berlin, den 17. August 2023

Dr. Alice Weidel, Tino Chrupalla 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.bundesanzeiger-verlag.de
ISSN 0722-8333