Deutscher Bundestag **Drucksache 20/8515**

20. Wahlperiode 27.09.2023

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Joachim Wundrak, Eugen Schmidt, Petr Bystron, weiterer Abgeordneter und der Fraktion der AfD
– Drucksache 20/8158 –

Cyberkriegsführung und Cyberkriegsverteidigung: rechtliche, organisatorische und politische Aspekte

Vorbemerkung der Fragesteller

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.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern und für Heimat vom 25. September 2023 übermittelt.

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

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)?

Die Fragen 1 und 2 werden zusammen beantwortet.

Die in dem Papier „On the Application of International Law in Cyberspace“ dargestellten Rechtsauffassungen der Bundesregierung zur Anwendung des Völkerrechts im Cyberraum in verschiedenen Fallkonstellationen sind Grundlage für unsere Bemühungen in der sog. Open-ended Working Group des 1. Ausschusses der Generalversammlung der Vereinten Nationen (OEWG) sowie in bilateralen Gesprächen mit anderen Staaten, auf eine möglichst einheitliche Auffassung der internationalen Gemeinschaft zu diesen technisch wie rechtlich komplexen Fragen hinzuarbeiten. Die Bundesregierung wirbt daher auch dafür, dass möglichst viele Staaten vergleichbare nationale Positionspapiere veröffentlichen. Diese Papiere werden von der Bundesregierung analysiert und sind entsprechend Basis weiterer Gespräche, insbesondere dort, wo ggf. im Einzelnen unterschiedliche Auffassungen zu einzelnen völkerrechtlichen Normen oder Prinzipien gegeben sind. Es ist bereits in den Vereinten Nationen konsentiert, dass Völkerrecht allgemein im Cyberraum Anwendung findet. Über Rechtsfragen zu einzelnen Normen und Anwendungsbereichen bestehen teilweise unterschiedliche Auffassungen. Wichtig zu erwähnen sind darüber hinaus nicht-verbindliche Verhaltensnormen im Cyberraum.

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)?

Die Bundesregierung erhebt und führt keine empirischen Daten im Sinne der Fragestellung

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)?

Die Bundesregierung arbeitet aktuell nicht an einer international anerkannten Definition von kritischer Infrastruktur.

5. Hat die Bundesregierung Kenntnis von Initiativen anderer Staaten, die auf eine international verbindliche Legaldefinition von kritischer Infrastruktur abzielen, und wenn ja, welche?

Der Bundesregierung sind keine Initiativen im Sinne der Frage bekannt.

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)?

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)?

10. Sind der Bundesregierung andere Staaten bekannt, die Hackbacks als Mittel der Cyberabwehr prinzipiell ablehnen (Nationale Sicherheitsstrategie, S. 62), und wenn ja, welche?

Die Fragen 6, 8 und 10 werden gemeinsam beantwortet.

Der Bundesregierung liegen keine eigenen Erkenntnisse im Sinne der Fragestellung vor.

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)?

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)?

Die Fragen 7 und 18 werden gemeinsam beantwortet.

Die Frage kann aus Gründen des Staatswohls nicht, auch nicht in eingestufter Form, beantwortet werden.

Eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde ihrer erheblichen Brisanz im Hinblick auf die Bedeutung für die Aufgabenerfüllung der Bundeswehr und des Militärischen Abschirmdienstes nicht ausreichend Rechnung tragen. Die angefragten Inhalte geben Auskunft über die Verteidigungsfähigkeit in einem sehr sensiblen Bereich, so dass eine Bekanntgabe auch gegenüber einem begrenzten Kreis von Empfängern ihrem Schutzbedürfnis nicht Rechnung tragen kann. Bei einem Bekanntwerden der schutzbedürftigen Informationen könnten feindliche Kräfte direkte Rückschlüsse auf Erfolgsaussichten weiterer Angriffe gegen die Bundesrepublik Deutschland ziehen. Es wäre ihnen möglich, Kenntnisse über die Arbeitsweise, die Lagebilderstellung und die Analysemethoden der Nachrichtendienste zu erlangen – insbesondere gilt dies vorliegend auch für die Fähigkeit, die Angreifer selbst zu identifizieren. Insgesamt würde dies die sachgerechte Erfüllung des Auftrags der Sicherheitsbehörden gefährden sowie u. a. auch die Möglichkeiten zur Informationsgewinnung einschränken.

Hieraus ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht wesentlich überwiegt. Auch ein geringfügiges Risiko des Bekanntwerdens kann unter keinen Umständen hingenommen werden. Insofern muss das Fragerecht der Abgeordneten gegenüber dem Geheimhaltungsinteresse der Bundesregierung ausnahmsweise zurückstehen. Dabei ist der Umstand, dass die Antwort verweigert wird, weder als Bestätigung noch als Verneinung des angefragten Sachverhalts zu werten.

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)?

Zu Bemühungen für ein derartiges Übereinkommen liegen der Bundesregierung keine Informationen vor.

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?

Der Bundesregierung liegen keine Informationen zur Fragestellung vor. Die Bundesregierung nimmt darüber hinaus grundsätzlich zum Verhalten und zu den Fähigkeiten von Drittstaaten keine Stellung.

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?

Die Fragen 12 und 13 werden aufgrund Sachzusammenhangs gemeinsam beantwortet.

Die Bundesregierung wird gemäß der Cybersicherheitsstrategie die Cybersicherheitsarchitektur weiterentwickeln. Sollten sich die Aufgaben und Kompetenzen des Nationalen Cyber-Abwehrzentrums im Zuge dieses Prozesses verändern, wird die aktuelle Beteiligung des Geschäftsbereiches des Bundesministeriums der Verteidigung überprüft und ggf. angepasst werden.

Aufbauend auf einem arbeitstäglichen Austausch zu Cyber-Sachverhalten wird vom Nationalen Cyber-Abwehrzentrum fortlaufend ein gemeinsames, übergreifendes Cyber-Sicherheitslagebild für Deutschland erstellt.

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

Die Bundesregierung verweist auf die laufenden Beratungen des Bundeshaushalts 2024 im Deutschen Bundestag.

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)?

Die Fragen 15 und 16 werden aufgrund Sachzusammenhangs gemeinsam beantwortet.

Das Bundesministerium des Innern und für Heimat (BMI) beabsichtigt, zu einem Entwurf des Gesetzes zur Stärkung der Cyber-Abwehr zeitnah die Ressortabstimmung einzuleiten.

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)?

Die Bundesregierung nimmt zu abstrakten Rechtsfragen keine Stellung.

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)?

Die Bundesregierung hat keine eigenen Erkenntnisse über die Zahl russischer Cyber-Angriffe gegen ukrainische Einrichtungen.

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)?

Die Fragen 20 und 21 werden aufgrund Sachzusammenhangs gemeinsam beantwortet.

Die Bundesregierung führt keine Statistik zu Anzahl und Urhebern von in anderen Staaten durchgeführten Cyber-Angriffen. Dies trifft auch auf NATO- und EU-Verbündete zu.

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

Im Verantwortungsbereich des NATO Cooperative Cyber Defence Centre of Excellence haben Ukrainer im Zusammenwirken mit einer anderen Nation im Jahre 2022 an der Cyberverteidigungsübung Locked Shields teilgenommen. Diese Übung wurde im Zeitraum 19. bis 22. April 2022 durchgeführt. Genauere Informationen bzgl. der Teilnehmer, insbesondere, ob es sich dabei um Militärangehörige gehandelt hat, liegen nicht vor.

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

Nach öffentlich verfügbaren Informationen (bspw. www.tagesschau.de/investigativ/swr/cyberkrieg-ukraine-putin-101.html) wurden kinetische Angriffe Russlands auf ukrainisches Territorium durch Cyberangriffe vorbereitet und unterstützt. Die Bundesregierung teilt diese Einschätzung.

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?

Im Zuge des Angriffskrieges Russlands gegen die Ukraine hat sich die Bedeutung von Cyberoperationen bestätigt. Die Bundesregierung wird auch vor diesem Hintergrund weiter daran arbeiten, die Cyber-Verteidigungsfähigkeit Deutschlands zu stärken.

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)?

Die Bundesregierung hat sich diesbezüglich keinen externen juristischen Rat eingeholt.

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?

Nach Auffassung der Bundesregierung sind reine nicht-disruptive ISR-Operationen keine bewaffneten Unternehmungen im Cyber-Raum.

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?

Soweit die völker- und verfassungsrechtlichen Voraussetzungen erfüllt sind, sind Informationsoperationen zum Zwecke der Verteidigung erlaubt. Die Zulässigkeit unterliegt einer rechtlichen Einzelfallbewertung.

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)?

Die Bundesregierung erhebt keine Daten im Sinne der Fragestellung.

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)?

Aktuell sind von insgesamt 5 981 Dienstposten (DP) für IT-Fachkräfte im Organisationsbereich Cyber- und Informationsraum 4 436 besetzt. Der Organisationsbereich Cyber- und Informationsraum befindet sich weiter in der Umstrukturierung, so dass auch für die Jahre 2023 und 2024 leichte Veränderungen in den DP-Umfängen zu erwarten sind. Für 2024 ist davon auszugehen, dass sich der DP-Besetzungsgrad, insbesondere durch Zuversetzung von derzeit noch in Ausbildung gebundenem Personal, leicht verbessern wird.

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)?

Die deutsche Beteiligung am NATO Counter Intelligence Centre of Excellence umfasst seit April 2015 den Posten „Branch Head Education and Training Branch“, welcher durchgängig durch den Geschäftsbereich des Bundesministeriums der Verteidigung besetzt wurde bzw. wird. Seit Juli 2023 wird zudem ein weiterer Posten in der „Education and Training Branch“ im Rahmen einer freiwilligen Abstellung besetzt.

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)?

Die deutsche Beteiligung am NATO Cooperative Cyber Defence Centre of Excellence umfasst nachstehend aufgeführte DP, welche alle durchgängig durch den Geschäftsbereich des Bundesministeriums der Verteidigung besetzt wurden bzw. werden:

Seit April 2008:	Technical Researcher
Seit Juni 2009:	Deputy Director/Chief of Staff
Seit Mai 2011:	Law Researcher

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