Deutscher Bundestag **Drucksache 19/26001**

19. Wahlperiode 15.01.2021

Kleine Anfrage

der Abgeordneten Alexander Müller, Alexander Graf Lambsdorff, Grigorios Aggelidis, Renata Alt, Nicole Bauer, Jens Beeck, Dr. Jens Brandenburg (Rhein-Neckar), Mario Brandenburg (Südpfalz), Dr. Marcus Faber, Daniel Föst, Otto Fricke, Thomas Hacker, Peter Heidt, Katrin Helling-Plahr, Markus Herbrand, Torsten Herbst, Katja Hessel, Dr. Gero Clemens Hocker, Manuel Höferlin, Reinhard Houben, Gyde Jensen, Pascal Kober, Konstantin Kuhle, Michael Georg Link, Till Mansmann, Dr. Martin Neumann, Matthias Nölke, Christian Sauter, Dr. Wieland Schinnenburg, Matthias Seestern-Pauly, Dr. Hermann Otto Solms, Bettina Stark-Watzinger, Dr. Marie-Agnes Strack-Zimmermann, Benjamin Strasser, Katja Suding, Linda Teuteberg, Stephan Thomae, Gerald Ullrich, Sandra Weeser, Nicole Westig und der Fraktion der FDP

Militärische Cyber-Operationen

Der Bereich der Cyber-Operationen wird für das Militär immer relevanter. Bedenklich erscheint, dass einige Staaten im Cyberbereich ein Allzweckschwert sehen, da ein Angriff mit vergleichbar wenig Ressourcen großen Schaden verursachen kann. Die Bundesrepublik Deutschland hat die Relevanz des Cyberbereichs erkannt und den militärischen Organisationsbereich Cyber- und Informationsraum der Bundeswehr aufgestellt. Wenig bekannt ist allerdings über die Bedrohungslage der Bundesrepublik Deutschland hinsichtlich Cyberangriffen sowie über die strategische Ausrichtung Deutschlands und die Fähigkeiten der Bundeswehr im Cyberbereich. Zudem ist eine grundrechtliche und völkerrechtliche Einordnung militärischer Cyber-Operationen seitens der Bundesregierung bisher nicht kommuniziert. Die vorliegende Kleine Anfrage hat zum Ziel, diese Informationslücken zu schließen.

Wir fragen die Bundesregierung:

1. Welche staatlichen oder staatsnahen Cyber-Operationen gegen die Bundesrepublik Deutschlandund/oder ihrer Bündnispartner in den Jahren 2014 bis 2020, aufgegliedert nach der Typisierung der Stiftung Wissenschaft und Politik (Schulze, Matthias [2020]: Militärische Cyber-Operationen. Nutzen, Limitierungen und Lehren für Deutschland. Stiftung Wissenschaft und Politik. Deutsches Institut für Internationale Politik und Sicherheit. SWP-Studie 15: Berlin), sind der Bundesregierung bekannt:

   a) defensive passiv/reaktive Maßnahmen (beispielsweise IT-Sicherheit und Resilienz),

   b) defensive pro-aktive Maßnahmen (beispielsweise Threat Hunting und Open Source Intelligence),

c) offensive passiv/reaktive Maßnahmen, also aktive Cyber-Abwehr und Hackbacks (beispielsweise Denial of Service, InfoOps und Sabotage),

d) offensive pro-aktive Maßnahmen, sogenannte Persistant Engagement oder Vorwärtsverteidigung auch Intelligence, Surveillance and Reconnaissance (ISR)?

2. Welche militärischen Cyber-Operationen gegen die Bundesrepublik Deutschland und/oder ihre Bündnispartner in den Jahren 2014 bis 2020, aufgegliedert nach der Typisierung der o. g. Stiftung Wissenschaft und Politik, sind der Bundesregierung bekannt?

3. Welche staatlichen, staatsnahen oder militärischen Cyber-Operationen gegen die Bundeswehr im Rahmen mandatierter Einsätze in den Jahren 2014 bis 2020, aufgegliedert nach der o. g. Typisierung der Stiftung Wissenschaft und Politik, sind der Bundesregierung bekannt?

4. Wie bewertet die Bundesregierung den Sinn und Zweck von militärischen Cyber-Operationen für die Landes- und Bündnisverteidigung, aufgegliedert nach der Typisierung der Stiftung Wissenschaft und Politik?

5. Wie häufig sind militärische Cyber-Operationen Gegenstand von Übungen der Bundeswehr (bitte nach der Typisierung der Stiftung Wissenschaft und Politik aufteilen)?

6. Im Verbund mit welchen Akteuren werden militärische Cyber-Operationen durch die Bundeswehr geübt (bitte nach Typisierung und Akteur aufschlüsseln)?

7. Erfüllt die Bundeswehr partiell oder vollständig die technischen und personellen Voraussetzungen zur Durchführung von militärischen Cyber-Operationen (bitte nach Typisierung der Stiftung Wissenschaft und Politik und Erfüllungsgrad der jeweiligen Fähigkeit aufgliedern)?

8. Welche Cyber-Operationen wurden im Rahmen mandatierter Einsätze der Bundeswehr durch die Bundeswehr oder für die Bundeswehr durchgeführt (bitte nach Mandat und Jahr aufschlüsseln)?

9. Wie häufig sind sogenannte InfoOps Gegenstand von Übungen der Bundeswehr?

10. Im Verbund mit welchen Akteuren werden sogenannte InfoOps geübt (bitte nach Akteur und Häufigkeit aufschlüsseln)?

11. Welche sogenannten InfoOps wurden seitens der Bundeswehr bisher durchgeführt, unterteilt nach

a) InfoOps zur Verbreitung von Informationen an Kombattanten oder Zivilbevölkerung,

b) InfoOps zur Bekämpfung von Propaganda anderer Akteure?

12. Da laut dem o. g. Papier der Stiftung Wissenschaft und Politik in der strategischen Leitlinie „Cyber-Verteidigung“ aus dem Jahr 2015 die Erstellung von Lagebildern zu gegnerischen Systemen als ein Ziel von Offensiven Militärischen Cyber-Operationen (OMCO) benannt wird, wie erfolgt eine dementsprechende aktive Cyberspionage durch die Bundeswehr oder den Bundesnachrichtendienst (BND) zur Erhebung von Schwachstellen gegnerischer Systeme, oder ist diese zukünftig vorgesehen (wenn ja, bitte aufschlüsseln, gegenüber welchen Nationen)?

a) Wie gestaltet sich der operative und rechtliche Rahmen für einen diesbezüglichen Austausch zwischen der Bundeswehr und dem BND?

b) Wird die Fähigkeit der aktiven Cyberspionage durch die Bundeswehr oder den BND zur Erhebung von Schwachstellen gegnerischer Systeme für den Verteidigungsfall geübt?

c) Wenn ja, wie häufig und im Verbund mit welchen Akteuren werden die Übungen durchgeführt?

13. Welche Vorfälle der strategischen Informationsbeeinflussung in Deutschland oder bei deutschen Staatsbürgern in den Jahren 2014 bis 2020 sind der Bundesregierung bekannt?

a) Wie viele davon kann die Bundesregierung Quellländern oder einzelnen Akteuren in Quellländern attribuieren (bitte nach Vorfall und Land aufschlüsseln)?

b) Welche Kriterien liegen einer Zuordnung zu Quellländern zugrunde?

c) Wie und durch wen wurden diese Kriterien entwickelt, und welcher Akteur ist für eine Anpassung zuständig?

14. Hat die Bundesregierung die strategische Informationsbeeinflussung durch russische Quellen in Deutschland oder bei deutschen Staatsbürgern bewertet?

Wenn ja, mit welchem Ergebnis?

Wenn nein, warum nicht?

15. Welche Maßnahmen werden zur Identifizierung strategischer Informationsbeeinflussung durch russische Quellen eingesetzt?

Welche Gegenmaßnahmen werden diesbezüglich eingesetzt?

16. Welche Maßnahmen sollen zukünftig zur Identifizierung strategischer Informationsbeeinflussung durch russische Quellen eingesetzt werden?

Welche Gegenmaßnahmen sollen zukünftig diesbezüglich eingesetzt werden?

17. Wie bewertet die Bundesregierung die strategische Informationsbeeinflussung durch chinesische Quellen in Deutschland oder bei deutschen Staatsbürgern?

18. Welche Maßnahmen werden zur Identifizierung strategischer Informationsbeeinflussung durch chinesische Quellen eingesetzt?

Welche Gegenmaßnahmen werden diesbezüglich eingesetzt?

19. Welche Maßnahmen sollen zukünftig zur Identifizierung strategischer Informationsbeeinflussung durch chinesische Quellen eingesetzt werden?

Welche Gegenmaßnahmen sollen zukünftig diesbezüglich eingesetzt werden?

20. Welche Prüfvorschriften gibt es beim Einkauf neuer Waffensysteme, und durch welche Stelle wird die Prüfung durchgeführt?

a) In welcher Regelmäßigkeit wird das IT-Sicherheitsniveau von bestehenden Waffensystemen der Bundeswehr überprüft?

b) Welche Stelle ist für die Überprüfung von bestehenden Waffensystemen zuständig?

c) Ist eine Erhöhung der Überprüfungsfrequenz geplant?

d) Wie sehen Ablauf und Inhalt einer solchen Überprüfung aus?

21. Wie stellt die Bundesregierung sicher, dass alle Soldatinnen und Soldaten die Möglichkeit haben, dienstliche Angelegenheiten auch remote über sichere Kanäle zu kommunizieren?

    a) Wann stellt die den Messenger BwChat allen Soldatinnen und Soldaten im Regelbetreib zur Verfügung, und wie sieht der Zeitplan für den Rollout aus?

    b) Erfolgt seitens der Bundesregierung eine Sensibilisierung von Soldatinnen und Soldaten hinsichtlich der Gefahr einer unsicheren Kommunikation über Messenger wie WhatsApp und Facebook Messenger?

22. Wie die Bundesregierung die grundrechtlichen und völkerrechtlichen Fragestellungen zum Einsatz von Cyber-Operationen gegen eine andere Nation bewertet (bitte nach Typisierung der Stiftung Wissenschaft und Politik aufschlüsseln)?

    Wenn ja, mit welchem Ergebnis?

    Wenn nein, warum nicht?

23. Wurden seitens der Bundesregierung die verfassungsrechtlichen Grundlagen für den Einsatz von OMCO in Friedenszeiten geprüft,

    a) wenn ja, zu welchem Schluss kam die Prüfung,

    b) wenn nein, soll eine solche Prüfung noch erfolgen?

24. Welche Schlussfolgerung zieht die Bundesregierung daraus in Bezug auf eigenen Aktivitäten in Bezug auf Übung und Anwendung von OMCO?

25. Welche Bemühungen unternimmt die Bundesregierung zur Schaffung verbindlicher völkerrechtlicher Abkommen über den Einsatz von militärischen Cyber-Operationen?

26. Wie sind die verschiedenen Arten von Cyber-Operationen völkerrechtlich einzuordnen (bitte nach Typen aufschlüsseln)?

    Wann liegt insbesondere ein Einsatz von Gewalt nach Artikel 2 Absatz 4 der Charta der Vereinten Nationen (UN-Charta) oder ein Verstoß gegen das Gebot der Nichteinmischung nach Artikel 2 Absatz 1 UN-Charta vor?

27. Unter welchen Voraussetzungen überschreitet nach Ansicht der Bundesregierung ein Cyberangriff die Schwelle zu einem bewaffneten Angriff und löst damit das in Artikel 51 der Charta der Vereinten Nationen verankerte Recht auf (militärische) Selbstverteidigung aus?

28. Wann sind die jeweiligen Arten von Cyberoperationen völkerrechtlich zulässig, einseitig und als Reaktion oder Verteidigungsmaßnahme auf Handeln eines ausländischen Staates?

29. Welche Regelungen des humanitären Völkerrechts wären aus Sicht der Bundesregierung auf die verschiedenen Cyber-Operationen anwendbar?

30. Plant die Bundesregierung das Verfassen und die Herausgabe einer Cyberdoktrin, ähnlich dem Department-of-Defense-Cyber-Strategy-Dokument?

    a) Wenn ja, wann soll ein solches Dokument erscheinen?

    b) Wenn nein, sieht die Bundesregierung einen Bedarf an einer wissenschaftlichen sowie gesellschaftlichen Debatte über Einsatz, Sinn und Zweck von militärischen Cyber-Operationen?

c) Wenn ja, welche Dokumente plant die Bundesregierung als Informationsgrundlage für eine solche Debatte zu veröffentlichen?

Berlin, den 12. Januar 2021

Christian Lindner 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.betrifft-gesetze.de
ISSN 0722-8333