Deutscher Bundestag **Drucksache 19/26855**

19. Wahlperiode 23.02.2021

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Alexander Müller, Alexander Graf Lambsdorff, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/26001 –

Militärische Cyber-Operationen

Vorbemerkung der Fragesteller

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.

Vorbemerkung der Bundesregierung

Die sichere und gesicherte sowie freie Nutzung des Cyber- und Informationsraums ist eine elementare Voraussetzung für staatliches und privates Handeln in unserer globalisierten Welt. Cyber-Verteidigung, einschließlich der Fähigkeit zu Cyber-Operationen, ist als militärischer Teil der Gesamtverteidigung verfassungsmäßiger Auftrag der Bundeswehr und stellt einen Beitrag zu einer gesamtstaatlichen Cyber-Sicherheitsarchitektur dar. Die Bundesregierung hat die Studie der Stiftung Wissenschaft und Politik [Schulze, Matthias (2020): Militärische Cyber-Operationen. Nutzen, Limitierungen und Lehren für Deutschland. Stiftung Wissenschaft und Politik (SWP). Deutsches Institut für Internationale Politik und Sicherheit. SWP-Studie 15: Berlin] zur Kenntnis genommen. Die in dieser Studie vorgenommene „Typologie militärischer Cyber-Operationen nach Nutzungszweck“ entspricht nicht den Kategorisierungen der Bundesregierung. Soweit die Fragesteller die Bundesregierung um Beantwortung der nachfolgenden Fragen spezifisch anhand der in der SWP-Studie vorgenommen Typologie ersuchen, kann die Bundesregierung diesem Ersuchen insofern nicht entspre-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Verteidigung vom 22. Februar 2021 übermittelt.

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

chen. Darüber hinaus bewertet die Bundesregierung grundsätzlich keine in Studien aufgeworfenen Fragen gutachterlich.

Die Bundesregierung hat in der Vergangenheit immer wieder an verschiedenen Stellen, u. a. im Rahmen von parlamentarischen Anfragen, Anhörungen („Rolle der Bundeswehr im Cyberraum“ 2016) und Berichten (vgl. u. a. Cybersicherheitsstrategie von 2016) zur Bedrohungslage der Bundesrepublik Deutschland von Cyber-Angriffen, zur strategischen Ausrichtung, zu den Fähigkeiten der Bundeswehr und zu den rechtlichen Rahmenbedingungen von Cyber-Operationen Stellung genommen. In dem Zusammenhang hat sie wiederholt klargestellt, dass Cyber-Operationen denselben völker- und verfassungsrechtlichen Rahmenbedingungen unterliegen wie jeder Einsatz anderer (konventioneller) militärischer Fähigkeiten auch (vgl. Antwort der Bundesregierung zu Frage 11 auf Bundestagsdrucksache 19/5472 und die Antwort der Bundesregierung zu den Fragen 2 und 18 auf Bundestagsdrucksache 18/6989).

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 proaktive 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 proaktive 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?

Die Fragen 1 bis 3 werden aufgrund des Sachzusammenhangs zusammen beantwortet.

Auf die Vorbemerkung der Bundesregierung wird verwiesen.

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?

Auf die Vorbemerkung der Bundesregierung wird verwiesen.

Für eine gesamtstaatliche Sicherheitsvorsorge einschließlich einer effektiven Landes- und Bündnisverteidigung sind Fähigkeiten zur Prävention und Abwehr von Cyberangriffen unverzichtbar. Dies umfasst auch die Fähigkeit zur Durchführung militärischer Cyber-Operationen.

Erfolgreiche Operationsführung basiert im Kern auf dem koordinierten Wirken in allen Dimensionen – Land, Luft, See, Weltraum sowie Cyber- und Informationsraum. Aufgrund der Verwundbarkeiten von Streitkräften im Cyber- und Informationsraum kommt den Operationen im Cyber- und Informationsraum auch im Rahmen der Landes- und Bündnisverteidigung eine weiterhin zunehmende Bedeutung zu. Die Anerkennung des Cyber-Raums als Operationsraum durch die NATO trägt dieser gewachsenen Bedeutung des Cyber-Raums für die Abschreckungs- und Verteidigungsfähigkeit des Bündnisses Rechnung.

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

Auf die Vorbemerkung der Bundesregierung wird verwiesen.

Auf die als „VS – Geheim“ eingestufte Anlage wird verwiesen.*

Der parlamentarische Informationsanspruch ist grundsätzlich auf die Beantwortung der gestellten Fragen in der Öffentlichkeit gerichtet. Gleichwohl ist die Bundesregierung nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Frage 5 nicht in offener Form erfolgen kann.

Die Abwägung des Aufklärungs- und Informationsrechts der Fragesteller mit den Sicherheitsinteressen der Bundesrepublik Deutschland bzw. dem Staatswohl führt zu einer höheren Gewichtung der Sicherheitsinteressen bzw. des Staatswohls. Gemäß § 2 Absatz 2 Nummer 2 der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung, VSA) sind Informationen entsprechend einzustufen, wenn die Kenntnisnahme durch Unbefugte die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährden oder ihren Interessen schweren Schaden zufügen kann.

Die in der Antwort aufgeführten Aktivitäten können unter Umständen quantitativ und qualitativ Rückschlüsse auf die Fähigkeiten der Bundeswehr und die Art und Weise, wie diese operativ zum Einsatz kommen, zulassen.

Deshalb sind diese Angaben als Verschlusssache (VS) mit dem Geheimhaltungsgrad „VS – Geheim“ eingestuft.*

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

Auf die Vorbemerkung der Bundesregierung wird verwiesen.

Auf die als „VS – Geheim“ eingestufte Anlage wird verwiesen.*

Der parlamentarische Informationsanspruch ist grundsätzlich auf die Beantwortung der gestellten Fragen in der Öffentlichkeit gerichtet. Gleichwohl ist die Bundesregierung nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Frage 6 nicht in offener Form erfolgen kann.

---

* Das Bundesministerium der Verteidigung hat die Antwort als „VS – Geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

Die Abwägung des Aufklärungs- und Informationsrechts der Fragesteller mit den Sicherheitsinteressen der Bundesrepublik Deutschland bzw. dem Staatswohl führt zu einer höheren Gewichtung der Sicherheitsinteressen bzw. des Staatswohls. Gemäß § 2 Absatz 2 Nummer 2 der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung, VSA) sind Informationen entsprechend einzustufen, wenn die Kenntnisnahme durch Unbefugte die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährden oder ihren Interessen schweren Schaden zufügen kann.

Die in der Antwort aufgeführten Aktivitäten können unter Umständen quantitativ und qualitativ Rückschlüsse auf die Fähigkeiten der Bundeswehr und die Art und Weise, wie diese operativ zum Einsatz kommen, zulassen.

Deshalb sind diese Angaben als Verschlusssache (VS) mit dem Geheimhaltungsgrad „VS – Geheim“ eingestuft.*

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)?

Auf die Vorbemerkung der Bundesregierung wird verwiesen.

Nach der Aufstellung des Zentrums für Cyber-Operationen (ZCO) im Jahr 2018 als eigenständiges, operationelles Zentrum im militärischen Organisationsbereich Cyber- und Informationsraum (CIR) soll es bis zum Jahr 2022 seine Full Operational Capability (FOC, entspricht der vollen Betriebsbereitschaft) erreichen und somit die Zielstruktur im Rahmen der ausplanbaren Dienstpostenumfänge einnehmen. Dabei soll das ZCO von derzeit rund 150 Dienstposten auf über 300 Dienstposten aufwachsen.

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)?

Auf die Antwort der Bundesregierung auf die Schriftliche Frage 58 auf Bundestagsdrucksache 19/6663 wird verwiesen.

Auf die als „VS – Geheim“ eingestufte Anlage wird verwiesen.*

Der parlamentarische Informationsanspruch ist grundsätzlich auf die Beantwortung der gestellten Fragen in der Öffentlichkeit gerichtet. Gleichwohl ist die Bundesregierung nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Frage 8 nicht in offener Form erfolgen kann.

Die Abwägung des Aufklärungs- und Informationsrechts der Fragesteller mit den Sicherheitsinteressen der Bundesrepublik Deutschland bzw. dem Staatswohl führt zu einer höheren Gewichtung der Sicherheitsinteressen bzw. des Staatswohls. Gemäß § 2 Absatz 2 Nummer 2 der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung, VSA) sind Informationen entsprechend einzustufen, wenn die Kenntnisnahme durch Unbefugte die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährden oder ihren Interessen schweren Schaden zufügen kann.

* Das Bundesministerium der Verteidigung hat die Antwort als „VS – Geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

Die in der Antwort aufgeführten Aktivitäten können unter Umständen quantitativ und qualitativ Rückschlüsse auf die Fähigkeiten der Bundeswehr und die Art und Weise, wie diese operativ zum Einsatz kommen, zulassen.

Deshalb sind diese Angaben als Verschlusssache (VS) mit dem Geheimhaltungsgrad „VS – Geheim“eingestuft.*

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)?

Die Fragen 9 und 10 werden aufgrund des Sachzusammenhangs zusammen beantwortet.

Informations-Operationen (InfoOps) sind eine koordinierende Stabsfunktion, die grundsätzlich in allen Stäben ab der Divisionsebene wahrgenommen wird.

Insbesondere in den multinationalen Großverbänden ab Korpsebene ist diese Aufgabe funktional in den jeweiligen Stäben vorhanden und findet somit Anwendung in nahezu allen Übungen.

Das Zentrum Operative Kommunikation der Bundeswehr (ZOpKomBw) hat als zentrale zuständige Stelle für InfoOps in der Bundeswehr im Jahr 2018 an sechs, im Jahr 2019 an sieben und im Jahr 2020 an zwei Übungen teilgenommen, in denen mindestens Teile des Aufgabenspektrums InfoOps abgebildet wurden. Pandemiebedingt ist das Übungsaufkommen 2020 nicht repräsentativ.

Das ZOpKomBw unterstützt auf Anforderung die jeweiligen Großverbände und Dienststellen der Bundeswehr (Einsatzführungskommando der Bundeswehr und Divisionen) und multinationale Verbände, darunter ein NATO Joint Forces Command oder die Very High Readiness Joint Task Force der NATO.

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?

Grundsätzlich sind InfoOps im Verständnis von NATO und Bundeswehr als Stabsfunktion im Führungsprozess immer Gegenstand von Übungen und Einsätzen. Es handelt sich somit nicht, wie hier impliziert, um separate Operationen, so dass auch keine Statistiken hierzu vorliegen.

* Das Bundesministerium der Verteidigung hat die Antwort als „VS – Geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

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?

Die Fragen 12 und 12a werden zusammen beantwortet.

Der Austausch von Informationen zwischen Bundeswehr und dem Bundesnachrichtendienst (BND) ist derzeit rechtlich in § 23 Absatz 1 des Gesetzes über den Bundesnachrichtendienst (BNDG) (Übermittlung an den BND) sowie in § 24 Absatz 1 und 3 BNDG (Übermittlung durch den BND) geregelt. Der BND darf Informationen grundsätzlich an inländische öffentliche Stellen übermitteln, wenn dies zur Erfüllung seiner Aufgaben erforderlich ist oder wenn der Empfänger die Daten für erhebliche Zwecke der öffentlichen Sicherheit benötigt.

    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?

Die Fragen 12b und 12c werden aufgrund des Sachzusammenhangs zusammen beantwortet.

Die Erstellung von Lagebildern ist ein grundsätzlicher Bestandteil von Übungen auch für den Verteidigungsfall.

Darüber hinaus wird auf die Antworten der Bundesregierung zu Frage 11 auf Bundestagsdrucksache 18/6989 und zu Frage 18 auf Bundestagsdrucksache 19/3420 verwiesen.

Die Frage betrifft im Übrigen solche Informationen, die in besonders hohem Maße das Staatswohl berühren und daher selbst in eingestufter Form nicht beantwortet werden können.

Das verfassungsmäßig verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung wird durch schutzwürdige Interessen von Verfassungsrang begrenzt, wozu auch und insbesondere Staatswohlerwägungen zählen. Eine Offenlegung der angeforderten Informationen und Auskünfte birgt die konkrete Gefahr, dass Einzelheiten zu der Methodik und zu besonders schutzwürdigen spezifischen Fähigkeiten des BND bekannt würden, infolgedessen sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf die konkreten Vorgehensweisen und Methoden des BND ziehen könnten.

Dies würde für den BND eine höchst folgenschwere Einschränkung der Informationsgewinnung bedeuten, wodurch der gesetzliche Auftrag des BND, die Sammlung und Auswertung von Informationen über das Ausland, die von außen- und sicherheits-politischer Bedeutung für die Bundesrepublik Deutschland sind (§ 1 Absatz 2 BNDG), nicht mehr sachgerecht erfüllt werden könnte. Die Gewinnung und Auswertung auslandsspezifischer Informationen durch den BND ist jedoch für die Sicherheits- und Außenpolitik der Bundesrepublik Deutschland unerlässlich. Würde der BND in seinen Möglichkeiten der Infor-

mationsgewinnung beeinträchtigt, drohten empfindliche Informationslücken im Hinblick auf die Sicherheitslage der Bundesrepublik Deutschland.

Eine VS-Einstufung und Hinterlegung der angefragten Informationen bei der Geheimschutzstelle des Deutschen Bundestages würde im vorliegenden Fall nicht ausreichen, um der erheblichen Sensibilität der angeforderten Informationen im Hinblick auf die Bedeutung für die Aufgabenerfüllung des BND ausreichend Rechnung zu tragen. Die angefragten Inhalte beschreiben die Fähigkeiten und Arbeitsweisen des BND so detailliert, dass eine Bekanntgabe auch gegenüber nur einem begrenzten Empfängerkreis ihrem Schutzbedürfnis nicht Rechnung tragen kann. Schon bei dem Bekanntwerden der schutzbedürftigen Informationen wäre kein Ersatz durch andere Instrumente der Informationsgewinnung mehr möglich.

Aus dem Vorgesagten ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, aufgrund derer das Staatswohl gegenüber dem parlamentarischen Informationsrecht wesentlich überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber dem Geheimhaltungsinteresse der Bundesregierung zurückstehen. Dabei ist der Umstand, dass die Antwort verweigert wird, weder als Bestätigung noch als Verneinung des angefragten Sachverhaltes zu werten.

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)?

Die Fragen 13 und 13a werden zusammen beantwortet.

Bezüglich Vorfällen der strategischen Informationsbeeinflussung in Deutschland oder bei deutschen Staatsbürgern in den Jahren 2014 bis 2020 ist die Bundesregierung nach sorgfältiger Abwägung zu der Auffassung gelangt, dass dieser Teil der Frage nicht – auch nicht in eingestufter Form – beantwortet werden kann. Eine VS-Einstufung und Hinterlegung der angefragten Informationen bei der Geheimschutzstelle des Deutschen Bundestages würde im vorliegenden Fall nicht ausreichen, um der erheblichen Sensibilität der angeforderten Informationen ausreichend Rechnung zu tragen. Gegenstand der Frage sind solche Informationen, die in besonderem Maße das Staatswohl berühren. Das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung wird durch schutzwürdige Interessen – gleichfalls von Verfassungsrang – wie das Staatswohl begrenzt.

Eine Beantwortung würde weitgehende Rückschlüsse auf die Erkenntnislage zulassen und damit mittelbar auch auf das Aufklärungspotenzial der Sicherheitsbehörden schließen lassen. Daraus folgt, dass die erbetenen Informationen derartig schutzbedürftige Geheimhaltungsinteressen berühren, so dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt. In der Abwägung des Informationsrechts und -interesses der Abgeordneten einerseits und den Geheimhaltungsinteressen andererseits muss das Recht der Abgeordneten daher ausnahmsweise zurückstehen. Dabei ist der Umstand, dass die Antwort verweigert wird, weder als Bestätigung noch als Verneinung des angefragten Sachverhaltes zu werten.

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?

Die Fragen 13b und 13c werden aufgrund des Sachzusammenhangs zusammen beantwortet.

Die fachliche Analyse und eine darauf aufbauende Zuordnung von Quellenländern hängt vom Einzelfall ab und kann Erkenntnisse der Nachrichtendienste des Bundes, forensische Befunde aus dem Cyberbereich, Erkenntnisse aus öffentlich zugänglichen Informationen und Erkenntnisse aus Ermittlungsverfahren beinhalten, die je nach konkreter Fallgestaltung unterschiedlich in eine wertende Gesamtbetrachtung einfließen. Die zugrunde liegende Methodik wird kontinuierlich weiterentwickelt.

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?

Russische Akteure haben in einzelnen Fällen Maßnahmen der Informationsbeeinflussung durchgeführt. Vor diesem Hintergrund sieht die Bundesregierung auch für die Zukunft eine Gefahr in einer solchen strategischen Informationsbeeinflussung.

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?

Die Fragen 15 und 16 werden aufgrund des Sachzusammenhangs zusammen beantwortet.

Die Bundesregierung nutzt die rechtlich zulässigen Mittel der offenen sowie verdeckten Informationsbeschaffung, um strategische Informationsbeeinflussung zu identifizieren.

Maßnahmen zur Abwehr strategischer Informationsbeeinflussung erfolgen seitens der Bundesregierung auf Basis von Einzelfallentscheidungen. Ergänzend können präventive Maßnahmen, u. a. zur Sensibilisierung der Öffentlichkeit für entsprechende Bedrohungen, zum Einsatz kommen.

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

Chinesische Akteure haben in Einzelfällen Maßnahmen der Informationsbeeinflussung durchgeführt. Vor diesem Hintergrund sieht die Bundesregierung auch für die Zukunft eine Gefahr in einer solchen strategischen Informationsbeeinflussung.

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?

Die Fragen 18 und 19 werden aufgrund des Sachzusammenhangs zusammen beantwortet.

Auf die Antwort zu den Fragen 15 und 16 wird verwiesen.

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?

Die Fragen 20 bis 20b werden aufgrund des Sachzusammenhangs zusammen beantwortet.

Waffensysteme werden grundsätzlich mit der Einführung sowie vor Einsätzen und Übungen nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) akkreditiert, wenn sie Informationen ab „VS – Nur für den Dienstgebrauch“ verarbeiten. Zudem werden sie in regelmäßigen, dreijährlich stattfindenden Inspektionen sowie bei Ablauf von Fristen zur Abstrahlsicherheit untersucht. Davon unbenommen erfolgen regelmäßige Kontrollen und Prüfungen durch die zuständigen Informationssicherheitsbeauftragten.

Für die Überprüfung von Waffensystemen sind unterschiedliche Stellen zuständig. Die Prüfgruppe IT-Sicherheit der Wehrtechnischen Dienststelle 81 in Greding unterstützt die jeweiligen Projektleiter im Rahmen der Realisierung von Waffensystemen.

Die Akkreditierung bei der Übernahme zur Nutzung und in der Nutzungsphase bzw. bei Einsätzen und Übungen erfolgt durch die Deutsche militärische Security Accreditation Authority (DEUmilSAA) nach den Vorgaben des BSI mit Unterstützung aus dem Bereich Schwachstellenanalyse im Zentrum für Cybersicherheit der Bundeswehr (ZCSBw). In ausgewählten Fällen wird eine erweiterte Überprüfung auch durch einen Penetrations-Test durchgeführt.

    c) Ist eine Erhöhung der Überprüfungsfrequenz geplant?

Auf Grundlage einer fachlichen Bewertung ist eine Erhöhung der Überprüfungsfrequenz nicht vorgesehen.

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

Der Akkreditierungsprozess gliedert sich in Phasen:

– Durchführung eines Akkreditierungsplanungsgesprächs mit der Festlegung des Prüfumfangs und Prüftiefe durch den Akkreditierenden.
– Prüfung der Informationssicherheitsdokumentation durch die DEUmilSAA.

– Überprüfung der in der Informationssicherheitsdokumentation beschriebenen Informationssicherheitsmaßnahme auf ihre Umsetzung im System in seiner Einsatzumgebung, auch mittels Schwachstellenanalysen.
– Ausstellung einer Akkreditierungsbescheinigung bzw. eines sogenannten „Statement of Compliance (SoC)“ nach erfolgreich abgeschlossener Prüfung durch die DEUmilSAA.

Der Ablauf von Vor-Ort-Inspektionen erfolgt anhand einer durch den Chief Information Security Officer der Bundeswehr (CISOBw) vorgegebenen bundeswehreinheitlichen Prüfliste, die die Inhalte des IT-Grundschutzes berücksichtigt und weitere Vorgaben macht. Diese Prüfliste ist modular aufgebaut. Der Inhalt der Prüfliste wird in regelmäßigen Abständen aktualisiert.

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?

Die Fragen 21 und 21a werden gemeinsam beantwortet.

Die Bundeswehr hat zum 31. Dezember 2020 den auf Basis stashcat pilotierten Messenger BwChat durch einen auf Open Source basierenden BwMessenger ersetzt, der auf Bw-eigener IT-Infrastruktur durch die BWI GmbH betrieben wird.

Der BwMessenger ist für alle Bundeswehr-Angehörigen auf dienstlichen Endgeräten seit April 2020 und auf privaten Endgeräten seit November 2020 im Regelbetrieb verfügbar und kann bei steigenden Nutzerzahlen bedarfsgerecht erweitert werden.

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

Die Beschäftigten werden durch ihre Dienststelle zum sicheren Umgang mit Informationen und Daten in Social Media und mit Messengern hinreichend geschult, sensibilisiert und belehrt. Anlassbezogene Belehrungen finden beim Wechsel der Dienststelle, bei Aufnahme von sicherheitsempfindlichen Tätigkeiten und vor Einsätzen statt.

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?

Auf die Vorbemerkung der Bundesregierung wird verwiesen.

Das Völkerrecht findet – wie bei jeder anderen militärischen Operation – auch auf Cyber-Operationen gegen einen anderen Staat Anwendung. Sollten von Cyber-Operationen gegen einen anderen Staat auch private Dritte bzw. potenzielle Grundrechtsträger betroffen sein, sind die gegebenenfalls anwendbaren und einschlägigen Grundrechte zu beachten. Insofern ist es eine Frage des Ein-

zelfalls und es lässt sich nicht pauschal beantworten, welche völker- bzw. grundrechtlichen Regeln auf eine militärische Operation Anwendung finden.

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?

Aufgrund des Sachzusammenhangs werden die Fragen 23 und 24 gemeinsam beantwortet.

Die verfassungsrechtlichen Grundlagen für Cyber-Operationen in Friedenszeiten wurden seitens der Bundesregierung geprüft. Die verfassungsrechtliche Zulässigkeit hängt maßgeblich davon ab, ob eine solche Operation als Wahrnehmung des Verfassungsauftrags der Streitkräfte zur Verteidigung nach Artikel 87a Absatz 1 und 2 des Grundgesetzes (GG) bzw. im Rahmen eines Systems gegenseitiger kollektiver Sicherheit im Sinne des Artikel 24 Absatz 2 GG erfolgt und erfordert eine Prüfung des Einzelfalls.

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

Das geltende Völkerrecht zur Einhegung militärischer Maßnahmen, darunter u. a. die Charta der Vereinten Nationen und das humanitäre Völkerrecht, ist auch in Bezug auf den Einsatz von militärischen Cyber-Operationen anwendbar. Insoweit gibt es keine Regelungslücke.

Die Bundesregierung setzt sich auf internationaler Ebene aktiv dafür ein, ein gemeinsames Verständnis darüber zu schaffen, wie die bereits existierenden und geltenden völkerrechtlichen Regeln auf Cyber-Operationen Anwendung finden. Auf die Antworten der Bundesregierung zu Frage 10b auf Bundestagsdrucksache 17/6971 und zu Frage 18 auf Bundestagsdrucksache 19/2307 wird verwiesen.

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?

Auf die Vorbemerkung der Bundesregierung wird verwiesen.

Grundsätzlich ist ein Verstoß gegen das Gewaltverbot gemäß Artikel 2 Absatz 4 der Charta der Vereinten Nationen (UN-Charta) im Falle einer Cyber-Operation dann gegeben, wenn diese nach Umfang und Wirkung mit einer traditionellen kinetischen Gewaltanwendung vergleichbar ist. Hinsichtlich des völkergewohnheitsrechtlich geltenden und aus Artikel 2 Absatz 1 UN-Charta ableitbaren Interventionsverbots, welches eine Einmischung in die inneren Angelegenheiten (sog. domaine réservé) eines anderen Staates unter Anwendung von Zwang verbietet, gilt im Grundsatz Ähnliches: Das Interventionsverbot

kann dann verletzt sein, wenn eine Einmischung in die inneren Angelegenheiten mit einer Zwangsausübung einhergeht, die in Umfang und Wirkung mit herkömmlichen, also nicht cyber-bezogenen Zwangsmaßnahmen vergleichbar ist. Wann jeweils konkret eine entsprechende Vergleichbarkeit nach Umfang und Wirkung gegeben ist, ist eine Frage des Einzelfalls und lässt sich nicht pauschal beantworten.

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?

Auf die Antwort der Bundesregierung zu Frage 27 auf Bundestagsdrucksache 18/6989 wird verwiesen.

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

Auf die Vorbemerkung der Bundesregierung sowie auf die Antwort der Bundesregierung zu Frage 20 auf Bundestagsdrucksache 19/2307 wird verwiesen.

Es gilt, eine Cyber-Operation darf sich nicht außerhalb der durch das Gewaltverbot und das Interventionsverbot sowie durch andere ggf. einschlägige völkerrechtliche Normen – wie z. B. menschenrechtliche und humanitär-völkerrechtliche Verpflichtungen – gesetzten Grenzen bewegen. Maßstab für die völkerrechtliche Zulässigkeit von Cyber-Operationen eines Staates, die als Reaktion auf gegen diesen Staat gerichtete Maßnahmen und unter Eingriff in Rechte des (Ziel-)Staats erfolgen, ist das Vorliegen von völkerrechtlich anerkannten Umständen, welche die Rechtswidrigkeit ausschließen (vgl. Artikel 20 ff. der Artikelentwürfe über die Verantwortlichkeit der Staaten für völkerrechtswidrige Handlungen der International Law Commission).

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

Auf die Vorbemerkung der Bundesregierung wird verwiesen.

Soweit das humanitäre Völkerrecht auf eine Cyber-Operation im gegebenen Einzelfall Anwendung findet, die Cyber-Operation also im Kontext eines bewaffneten Konflikts erfolgt, sind dies z. B. das Unterscheidungsgebot, das Verbot exzessiver ziviler Begleitschäden und das Gebot, Vorsichtsmaßnahmen zum Schutz der Zivilbevölkerung bei der Planung eines Angriffs zu ergreifen.

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?

Die Fragen 30 und 30a werden zusammen beantwortet.

Die Bundesregierung plant derzeit eine Aktualisierung der Cyber-Sicherheitsstrategie 2016. Auf dieser Basis wird eine Aktualisierung der Strategischen Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg erfolgen. Die Veröf-

fentlichung einer Cyber-Doktrin, die dem Department of Defense Cyber Strategy-Dokument ähnelt, ist derzeit nicht geplant.

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

Eine gesellschaftliche und wissenschaftliche Debatte über militärische Cyber-Operationen findet aus Sicht der Bundesregierung bereits statt. Diese wird von der Bundesregierung auch befürwortet.

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

Die Bundesregierung wird weiterhin aktiv an der Debatte teilnehmen und etwa im Rahmen von öffentlichen Anhörungen über ihre Arbeit informieren.

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