Deutscher Bundestag **Drucksache 19/3420**

19. Wahlperiode 17.07.2018

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Agnieszka Brugger, Dr. Konstantin von Notz, Dr. Tobias Lindner, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
– Drucksache 19/2618 –

Aktivitäten der Bundeswehr im digitalen Raum und gesetzgeberische Maßnahmen der Bundesregierung

Vorbemerkung der Fragesteller

Im April 2017 wurde das Kommando Cyber- und Informationsraum (KdoCIR) der Bundeswehr aufgestellt. In diesem Kommando wurden bereits vorhandene und neue IT-Strukturen der Bundeswehr gebündelt. Mit diesem strukturell-organisatorischen Schritt will die Bundesministerin der Verteidigung, Dr. Ursula von der Leyen, auf die sicherheitspolitischen Herausforderungen im digitalen Raum reagieren. Auch ein Jahr nach der Aufstellung des KdoCIR sind zentrale Fragen im Zusammenhang mit dem Aufbau, den rechtlichen Grundlagen, dem Vorhalten und der potenziellen Anwendung von digitalen Einsatzfähigkeiten der Bundeswehr unbeantwortet.

Die Bundeswehr muss sich auf die sicherheitspolitischen Herausforderungen im digitalen Raum und damit verbundene neue Bedrohungslagen einstellen. Zwingend notwendig sind ein verbesserter Eigenschutz und die Härtung der IT-Infrastrukturen der Bundeswehr. Dieser verbesserte Schutz muss sowohl der Sicherung der eigenen Systeme im Rahmen der Landes- und Bündnisverteidigung als auch dem Schutz von Soldatinnen und Soldaten sowie Auslandseinsätzen der Bundeswehr dienen.

Anstatt sich jedoch auf den wichtigen Schutz der eigenen IT-Infrastruktur zu konzentrieren, hatte Bundesverteidigungsministerin Dr. Ursula von der Leyen bereits im Weißbuch 2016 angekündigt, die Bundeswehr offensive Fähigkeiten nicht nur üben und entwickeln zu lassen. Auch der Inspekteur Cyber- und Informationsraum, Generalleutnant Ludwig Leinhos, spricht in einem Interview von der Notwendigkeit, „Angriffe auch offensiv abwehren zu können“ (www.handelsblatt.com/politik/deutschland/cyber-general-ludwig-leinhos-die-bedrohung-aus-dem-netz-ist-real-und-sie-wird-zunehmen/21182502.html).

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Verteidigung vom 13. Juli 2018 übermittelt.

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

Im September 2016 berichtete „SPIEGEL ONLINE“ über eine im Herbst 2015 erfolgte Operation der damaligen Einheit „Computer Netzwerk Operationen“ (CNO), bei der in das System eines afghanischen Mobilfunkbetreibers eingedrungen wurde (vgl.: www.spiegel.de/politik/ausland/cyber-einheit-bundeswehr-hackte-afghanisches-mobilfunknetz-a-1113560.html).

Ein solches Vorgehen birgt aus Sicht der Fragesteller erhebliche Gefahren und gefährdet zudem die Entwicklung eines freien und sicheren Internets. Es stellen sich zahlreiche rechtliche und verfassungsrechtliche Fragen, die bis heute nicht ausreichend beantwortet sind. Der fortwährende Verweis auf die Besonderheiten des Cyber- und Informationsraums und die daraus resultierenden speziellen sicherheitspolitischen Herausforderungen, wie der oftmals fehlende oder unklare rechtliche Rahmen oder der Bedeutungsverlust nationaler Grenzen im digitalen Raum, entbindet die Bundesregierung nicht davon, die notwendigen rechtlichen Grundlagen für ein verfassungsgemäßes Handeln der Bundeswehr zu schaffen.

Dies gilt auch und besonders für die parlamentarische Kontrolle durch den Deutschen Bundestag beim Einsatz von digitalen Einsatzkapazitäten der Bundeswehr, analog zu den bereits bestehenden Regeln beim Einsatz militärischer Kräfte. Für eine effektive demokratische Kontrolle der Parlamentsarmee ist es aus Sicht der Fragesteller unerlässlich, dass der Deutsche Bundestag in Zukunft über die konkreten Details von Operationen der Bundeswehr im digitalen Raum besser und transparenter informiert wird. Nur so kann eine wirksame parlamentarische Kontrolle der Aktivitäten der Bundeswehr im digitalen Raum gewährleistet werden.

Während die weltweite Zahl an IT-Angriffen kontinuierlich steigt und zivile und staatliche digitale Infrastrukturen immer wieder attackiert werden, gibt es derzeit keine wirklichen Fortschritte bei der Erarbeitung konkreter internationaler Vereinbarungen zum Schutz digitaler Infrastrukturen und zur Gewährleistung einer effektiven IT-Sicherheit im Netz. Es reicht nicht, lediglich festzustellen, dass die Prozesse mit Blick auf international verbindliche Regelwerke oder vertrauens- und sicherheitsbildende Maßnahmen höchst schleppend vorangehen und wenig konkrete Ergebnisse erzielen konnten. Stattdessen sollte sich die Bundesregierung auf internationaler Ebene beispielsweise entschieden für einen Verhaltenskodex einsetzen, der u. a. eine Selbstverpflichtung enthält, zivile (Netz-)Infrastruktur nicht für militärische Angriffe durch digitale Angriffskapazitäten zu nutzen oder selbst zum Angriffsziel zu machen.

Vorbemerkung der Bundesregierung

In der „Cybersicherheitsstrategie für Deutschland 2016“ werden die Cyber-Abwehr (FF Bundesministerium des Innern, für Bau und Heimat – BMI), die Cyber-Außen/und -Sicherheitspolitik (FF Auswärtiges Amt – AA) und die Cyber-Verteidigung (Bundesministerium der Verteidigung – BMVg) als drei sich ergänzende Mittel zum Erreichen von Cyber-Sicherheit festgehalten.

Die Cyber-Abwehr bezieht sich auf die Abwehr aller rechtswidriger Beeinträchtigungen, welche die Verfügbarkeit, Integrität und Vertraulichkeit von informationstechnischen Systemen durch informationstechnische Mittel manipulieren, beeinflussen oder stören.

Die Cyber-Verteidigung umfasst die in der Bundeswehr im Rahmen ihres verfassungsmäßigen Auftrages und dem völkerrechtlichen Rahmen vorhandenen defensiven und offensiven Fähigkeiten zum Wirken im Cyber-Raum, die zur Einsatz- und Operationsführung geeignet und erforderlich sind oder zur Abwehr von (militärischen) Cyber-Angriffen und damit dem Schutz eigener Informationen, IT,

sowie Waffen- und Wirksysteme dienen. Dazu gehört auch die Nutzung und Mitgestaltung von Strukturen, Prozessen und Meldewesen der Cyber-Abwehr unter verteidigungsrelevanten Aspekten und Situationen.

Die Aufgaben der Bundeswehr im Cyber- und Informationsraum sind durch das ressortgemeinsame Handeln aller verantwortlichen deutschen Behörden und Organisationen mit Sicherheitsaufgaben (BOS) in eine umfassende nationale Sicherheitsvorsorge eingebunden.

Dabei gelten für den Einsatz von Streitkräften im Cyber-Raum stets die gleichen rechtlichen Voraussetzungen wie beim Einsatz anderer Fähigkeiten. Hierzu wird auf die Antwort der Bundesregierung zu Frage 2 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/6989 verwiesen.

Die parlamentarische Kontrolle der Bundeswehr erfolgt im Rechtsrahmen, der durch das Grundgesetz gesteckt wird. Dies betrifft Cyber-Wirkmittel in gleicher Weise wie die anderen militärischen Fähigkeiten der Bundeswehr. Somit unterliegen die Cyber-Fähigkeiten der Bundeswehr derselben parlamentarischen Kontrolle wie die klassischen Einsatzmittel. Defizite bei der parlamentarischen Kontrolle, die Anlass für darüber hinausgehende spezifische Verfahren hinsichtlich von Cyber-Mitteln gäben, kann die Bundesregierung nicht erkennen.

Die Bundesregierung plant keine Änderung des im Grundgesetz verankerten Handlungsrahmens der Bundeswehr, noch besteht aus ihrer Sicht ergänzender Rechtsetzungsbedarf für den Einsatz der Streitkräfte im Cyber-Raum.

1. Wie definiert die Bundesregierung einen „Cyber-Angriff“?

   Nach welchen Kategorien erfolgt eine solche Klassifizierung?

   Welche Standards hat die Bundesregierung für Reaktionen auf solche Angriffe festgelegt, und bei welchen Stellen liegt die diesbezügliche Entscheidungsgewalt?

Nach der im Jahr 2016 vom Bundesministerium des Innern herausgegebenen Cyber-Sicherheitsstrategie für Deutschland wird unter einem Cyber-Angriff eine Einwirkung auf ein oder mehrere andere informationstechnische Systeme im oder durch den Cyber-Raum verstanden, die zum Ziel hat, deren IT-Sicherheit durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen. Mit dem Begriff können somit verschiedenste Konstellationen mit unterschiedlicher Qualität, Wirkungsweise und Zielsetzung (von Kriminalität, Spionage, Terrorismus über die gezielte Beeinträchtigung nationaler Souveränität bis hin zum Einsatz als militärisches Wirkmittel) bezeichnet werden. Hiervon hängt die jeweilige rechtliche Bewertung ab. Der Begriff des „Cyber-Angriff“, wie ihn die Cyber-Sicherheitsstrategie als technischen Sammelbegriff verwendet, ist nicht identisch mit dem völkerrechtlichen Begriff des (bewaffneten) Angriffs im Sinne von Artikel 51 der Charta der Vereinten Nationen. Anders als dort handelt es sich mithin nicht um einen Begriff, mit dem von vornherein festgelegte Konsequenzen oder bestimmte staatliche Zuständigkeiten verbunden sind. Die auf einen Cyber-Angriff in Betracht kommenden Reaktionen wie auch die hierfür zuständigen staatlichen Behörden und Dienststellen hängen vielmehr rechtlich und tatsächlich von dem jeweiligen Einzelfall ab.

2. Auf welcher Ebene wird innerhalb der Bundesregierung aufgrund von welchen Rechtsgrundlagen entschieden, welche Stellen mit welcher Maßnahme auf eine Bedrohung oder einen Angriff auf die IT-Infrastruktur reagieren oder ob gar in fremde Netze gewirkt wird?

   Wie sieht hier die Aufgabenteilung insbesondere zwischen dem Bundesministerium des Innern, für Bau und Heimat und seinen Stellen bzw. Behörden, dem Bundesministerium der Verteidigung und seinen Stellen und den Nachrichtendiensten aus?

Die innerstaatliche Kompetenzverteilung und Aufgabenabgrenzung folgt den aktuell geltenden rechtlichen Vorgaben und Entscheidungsverfahren. Hierzu wird auf die Antwort der Bundesregierung zu Frage 1 der Kleinen Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/2645 verwiesen. Auf diesen Grundlagen ist die Bundesrepublik Deutschland auch im Bereich der Cyber-Sicherheit umfassend handlungsfähig. Ob gleichwohl in Bezug auf Bedrohungen aus und durch den Cyber- und Informationsraum Anpassungen angebracht sind, ist Gegenstand aktueller rechtlicher und tatsächlicher Prüfungen der Bundesregierung. Diese sind noch nicht abgeschlossen. Hinsichtlich der Bundeswehr wird auf die Vorbemerkung der Bundesregierung zu dieser Anfrage verwiesen.

3. Wie viele IT-Angriffe gab es jeweils in den letzten fünf Jahren und bisher im Jahr 2018 auf die Bundeswehr im Inland?

   a) Wie viele der IT-Angriffe sind als zielgerichtete Attacken auf die Systeme der Bundeswehr einzustufen?

   b) Bei wie vielen dieser Angriffe ist ein Angreifer tatsächlich in Rechner oder Netzwerke der Bundeswehr eingedrungen?

      Wie viele dieser Angriffe beinhalteten gezieltes Kontaktieren oder Ausspionieren von Bundeswehrangehörigen, sogenanntes Social Engineering?

   c) Wie viele Angriffe konnten jeweils in den letzten fünf Jahren und im Jahr 2018 bereits durch übliche Schutzeinrichtungen wie Firewalls etc. abgewehrt werden?

   d) Welche Schäden wurden durch diese IT-Angriffe tatsächlich jeweils bewirkt?

Die Fragen 3 bis 3d werden aufgrund ihres inhaltlichen Zusammenhangs gemeinsam beantwortet.

Die Informationssicherheitsorganisation der Bundeswehr erkennt an ihren Sensoren unerwünschtes Verhalten, sogenannte „Incidents“, und blockt dieses. Gemäß der Antwort zu Frage 1 sind erkannte Incidents auf Cyber-Angriffe zurückzuführen. Zu Art und Umfang der Cyber-Angriffe wird auf die Antwort der Bundesregierung auf die Schriftliche Frage 87 des Abgeordneten Alexander Graf Lambsdorff auf Bundestagsdrucksache 19/2922 verwiesen.

4. Wie viele der bis 2022 geplanten 15 000 Stellen des Kommandos Cyber- und Informationsraumes (KdoCIR) sind bis zum gegenwärtigen Zeitpunkt tatsächlich bereits besetzt?

   Wie viele der derzeit vorgesehenen Dienstposten im KdoCIR sind aktuell aus welchen Gründen nicht besetzt?

Im Organisationsbereich Cyber- und Informationsraum sind derzeit 13 989 besetzungsrelevante Dienstposten eingerichtet, von denen 10 364 Dienstposten besetzt sind. Daneben befindet sich, bedingt durch die Neuaufstellung des Organisationsbereiches zum 1. April 2017, noch Personal in der Ausbildung, das, nach Erreichen der notwendigen Qualifikationen, auf unbesetzten Dienstposten eingesetzt wird.

5. Wie weit ist der Aufbau einer „Cyber-Reserve“ fortgeschritten?

   Wie viele Dienstposten für Reservistinnen und Reservisten sind für die „Cyber-Reserve“ eingeplant, und wie viele dieser Posten sind aktuell tatsächlich bereits besetzt?

Der Aufbau der Cyber-Reserve vollzieht sich in mehreren Schritten. Zunächst wurden Interessenten für eine Tätigkeit in der „Cyber-Reserve“ erfasst und nach fachlichen Kriterien und Verfügbarkeit geordnet. Bislang wurden 635 Personen erfasst.

Ab Mitte dieses Jahres wird geeignetes Personal mit Cyber-/IT-Expertise zur Vertiefung und Verbreitung des bundeswehreigenen Fachwissens zur Cyber-Verteidigung bedarfsorientiert eingesetzt. Ziel ist es, den Aufbau und Einsatz einer hoch qualifizierten und schlagkräftigen „Cyber-Reserve“ zur bedarfsorientierten Unterstützung des aktiven Cyber-Personals der Bundeswehr bis Ende 2019 zu erreichen.

Grundsätzlich gibt es keine Obergrenze an Dienstposten für die „Cyber-Reserve“. Derzeit liegt der Fokus im Organisationsbereich Cyber- und Informationsraum auf circa 460 Beorderungsdienstposten mit „MINT“-Hintergrund (MINT: Mathematik, Informatik, Naturwissenschaften, Technik).

6. Welche konkreten Fähigkeiten meint die Bundesministerin der Verteidigung, Dr. Ursula von der Leyen, wenn sie, wie auf der Bundeswehrtagung am 14. Mai 2018, davon spricht, dass man für die Bundeswehr ein „volles Fähigkeitenspektrum im Bereich Cybersicherheit“ wolle?

Unter einem vollen Fähigkeitenspektrum im Bereich Cyber-Sicherheit werden die Fähigkeiten verstanden, die zum Schutz eigener Informationen, IT sowie Waffen- und Wirksystemen dienen oder mit denen im Rahmen der Einsatz- und Operationsführung im und durch den Cyber- und Informationsraum gewirkt wird.

7. Welche konkreten Fähigkeiten meint nach Ansicht der Bundesregierung der Inspekteur Cyber- und Informationsraum, Generalleutnant Ludwig Leinhos, wenn er von benötigten Optionen für die offensive Abwehr von IT-Angriffen spricht (Quelle siehe Vorbemerkung der Fragesteller)?

   Sind hierunter auch aktive Angriffe auf fremde Server („Hackback“) zu verstehen?

Cyber-Verteidigung umfasst die in der Bundeswehr im Rahmen ihres verfassungsmäßigen Auftrages und den völkerrechtlichen Rahmen vorhandenen Fähigkeiten zum Wirken im Cyber-Raum, die zur Einsatz- und Operationsführung geeignet und erforderlich sind oder zur Abwehr von (militärischen) Cyber-Angriffen und damit dem Schutz eigener Informationen, IT sowie Waffen- und Wirksysteme dienen. Die Bundeswehr verfügt auch im Cyber-Raum, wie zu Lande, zu Luft sowie auf und unter Wasser, über reaktive und aktive Fähigkeiten, die für rechtmäßige Maßnahmen genutzt werden können.

8. Wie definiert die Bundesregierung einen „Hackback“, und auf welche Szenarien bezieht sie sich, wenn von einem solchen die Rede ist?

   Welche konkreten Fähigkeiten für „Hackbacks“ will die Bundesregierung in welchen Sicherheitsbehörden oder der Bundeswehr ansiedeln (vgl. beispielhaft die Äußerung vom Präsident des Bundesamts für Verfassungsschutz Hans Georg Maaßen im ARD-Interview, www.tagesschau.de/inland/maassen-cyberangriffe-103.html)?

In der Bundesregierung gibt es keine festgelegte Definition für den Begriff „Hackback“. Umgangssprachlich werden unter dem Begriff „Hackback“ zivile Maßnahmen verstanden, die zum Ziel haben, die bei einem Angriff genutzten informationstechnischen Systeme mit informationstechnischen Mitteln zu manipulieren oder zu stören. Maßnahmen in diesem Sinne bezeichnet die Bundesregierung als aktive Cyber-Abwehr.

Zu der Aufgabenverteilung bei der Cyber-Abwehr und der Cyber-Verteidigung auf die Stellen des Bundes wird auf die Antwort der Bundesregierung zu Frage 1 der Kleinen Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/2645 verwiesen.

9. Wie bewertet die Bundesregierung die Frage nach der Verfassungskonformität von aktiven Angriffen auf fremde Server („Hackback“) durch die Bundeswehr?

Generell sind auf völkerrechtswidrige Aktivitäten gegen die Bundesrepublik Deutschland Reaktionen der Bundeswehr innerhalb des völker- und verfassungsrechtlich gesteckten Rahmens möglich. Auf die Antwort zu Frage 41 sowie auf die Antwort der Bundesregierung zu Frage 20 der Kleinen Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/2307 wird verwiesen.

10. Teilt die Bundesregierung die Ansicht der Fragestellenden, dass es für aktive Angriffe auf fremde Server („Hackback“) heute keine ausreichende Rechtsgrundlage gibt?

Im Hinblick auf Cyber-Verteidigung sind die Rechtsgrundlagen ausreichend. Es wird auf die Antwort der Bundesregierung zu Frage 20 der Kleinen Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/2307 verwiesen.

Im Hinblick auf die aktive Cyber-Abwehr wird auf die Antwort der Bundesregierung zu Frage 16 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 19/2643 verwiesen.

11. Plant die Bundesregierung die Schaffung einer Rechtsgrundlage für aktive Angriffe auf fremde Server („Hackback“)?

    Falls ja, bis wann soll eine solche erarbeitet werden?

Zur Schaffung von Rechtsgrundlagen wird auf die Antwort zu Frage 8 sowie auf die Antwort der Bundesregierung zu Frage 16 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 19/2643 verwiesen.

12. Ist die Bundesregierung der Ansicht, dass ein aktiver Angriff auf fremde Server („Hackback“) durch die Bundeswehr vom Deutschen Bundestag mandatiert werden muss, und wenn nein, warum nicht?

Militärische Maßnahmen im Cyber-Raum unterliegen dem gleichen rechtlichen Rahmen wie andere militärische Maßnahmen auch. Nach dem Parlamentsbeteiligungsgesetz unterliegen bewaffnete Einsätze der Streitkräfte außerhalb des Geltungsbereichs des Grundgesetzes grundsätzlich der vorherigen konstitutiven Zustimmung des Deutschen Bundestages. Ob ein Vorgehen der Bundeswehr im Cyberraum diese Voraussetzung erfüllt, kann nur für den jeweiligen Einzelfall entschieden werden.

13. Wie beurteilt die Bundesregierung im Kontext der vorausgegangenen Fragen die Attributions-Problematik bei IT-Angriffen und ihrer Abwehr?

Im Hinblick auf die aktive Cyber-Abwehr ist diese Frage Gegenstand laufender Prüfungen der Bundesregierung. Diese sind noch nicht abgeschlossen.

Im Hinblick auf die Cyber-Verteidigung müssen sich grundsätzlich sämtliche Verteidigungsmaßnahmen gegen den Angreifer richten, der für diesen Zweck hinreichend identifiziert sein muss.

14. Wie will man gegebenenfalls verhindern, dass bei einem „Hackback“ und anderen Maßnahmen auch zivile Infrastrukturen in Mitleidenschaft gezogen werden?

    Welche Schutzmechanismen sind hier aus Sicht der Bundesregierung denkbar und notwendig, und wie sind diese in der Praxis umsetzbar?

Zur Vermeidung ungewollter Auswirkungen im Rahmen der Cyber-Verteidigung wird auf die Antwort zu Frage 24 verwiesen.

Für den Teil der Cyber-Abwehr wird auf die Antwort der Bundesregierung zu Frage 10 der Kleinen Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/2645 verwiesen.

Im Übrigen wird auf die Antwort zu Frage 8 verwiesen.

15. Wie bewertet die Bundesregierung das Risiko, dass eine präventive Infiltrierung bzw. Kompromittierung von fremden Servern (welche in bestimmten Szenarien eine technische Voraussetzung für einen „Hackback“ darstellen kann) ihrerseits von ausländischen Streitkräften oder Geheimdiensten als offensiver Akt gewertet werden könnte?

Die aktive Cyber-Abwehr umfasst Reaktionen auf bereits erfolgte rechtswidrige Beeinträchtigungen informationstechnischer Systeme. Die Cyber-Verteidigung ergibt sich aus dem Verteidigungsauftrag der Bundeswehr als Reaktion auf bereits erfolgte völkerrechtswidrige Handlungen fremder Staaten.

16. Welche Reaktionsszenarien auf IT-Angriffe werden durch welche Einheiten des Kommandos Cyber- und Informationsraum (KdoCIR) geübt?

Die IT-Sicherheitsorganisation der Bundeswehr, verortet im Kommando Cyber- und Informationsraum, übt Maßnahmen zur Aussperrung von Angreifern und zur Bereinigung der Netze und Systeme.

17. Welche konkreten Fortschritte wurden seit der Aufstellung des KdoCIR in der Härtung der Infrastruktur und der Systeme der Bundeswehr gemacht?

Unabhängig von der Aufstellung des Kommando Cyber- und Informationsraum haben die zuständigen Stellen seit jeher die Infrastruktur und die Systeme gehärtet. Mit Aufstellung des Kommando Cyber- und Informationsraum wurde begonnen, den Fokus auf die Informationssicherheit der Infrastrukturen und auf die Identifikation von Schwachstellen zu stärken. Dadurch wurde bei den jeweils Verantwortlichen eine Erhöhung des Stellenwerts von Maßnahmen zur Steigerung der Informationssicherheit erzielt, die eine Härtung von Infrastruktur und Systemen bewirken.

18. Wie ist der Umgang mit Sicherheitslücken in fremden oder eigenen Systemen, die durch die Bundeswehr im Rahmen von Operationen und Übungen national wie international entdeckt werden?

Werden entdeckte Sicherheitslücken gemeldet?

Wenn ja, an wen, und wie oft kam das bisher vor (bitte konkret aufschlüsseln)?

Wenn nein, warum nicht?

Die von der Bundeswehr verwendete Definition von Sicherheitslücken umfasst, gemäß der Allgemeinen Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 Absatz 6 des BSI-Gesetzes neuartige Sicherheitslücken oder Schwachstellen in IT-Produkten, die durch den Meldenden aufgedeckt wurden.

Die durch die Informationssicherheitsorganisation der Bundeswehr in den eigenen Systemen identifizierten Sicherheitslücken werden an den jeweils zuständigen Informationssicherheitsbeauftragten des/der betroffenen Projekte und der betroffenen Dienststelle/n zur Abstellung gemeldet. Diese setzen als Ergebnis einer Risikoanalyse zusätzliche Maßnahmen zur Mitigation um. In Abhängigkeit von der Sicherheitslücke können dies personelle, organisatorische, technische und/oder infrastrukturelle Maßnahmen sein. Die Umsetzung der Maßnahmen wird in den jeweiligen Informationssicherheitsdokumentationen der Projekte bzw. Dienststellen nachgewiesen, jedoch nicht in einer übergreifenden Statistik. Entdeckte Sicherheitslücken werden gemäß § 4 des BSI-Gesetzes ebenfalls an das Bundesamt für Sicherheit in der Informationstechnik gemeldet.

Der parlamentarische Informationsanspruch ist grundsätzlich für die Beantwortung gestellter Fragen in der Öffentlichkeit ausgelegt. Die Bundesregierung ist allerdings nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Frage 18 nicht vollständig in offener Form erfolgen kann. Für die weitere Beantwortung der Frage 18 wird auf den „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil verwiesen.

Die Einstufung der Antwort auf die Frage 18 als Verschlusssache (VS) mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ wird im Hinblick auf das Staatswohl als erforderlich erachtet, da die in der Antwort aufgeführten Informationen unter Umständen Rückschlüsse auf die Fähigkeiten der Informationssicherheitsorganisation der Bundeswehr zulassen. Nach § 3 Nummer 4 der Allgemeinen Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlusssachen (Verschlusssachenanweisung, VSA) sind Informationen, deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein können, entsprechend einzustufen. Im vorliegenden Fall werden diese Informationen daher als „VS – Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.[1]

19. Plant die Bundesregierung eine gesetzliche Regelung zur Schaffung einer Meldepflicht von Sicherheitslücken durch staatliche Stellen?

    Falls ja, wie soll diese konkret ausgestaltet sein?

    Falls nein, warum nicht?

§ 4 Absatz 3 des BSI-Gesetzes regelt die gesetzliche Meldepflicht von Stellen des Bundes gegenüber dem Bundesamt für Sicherheit in der Informationstechnik. Ob weitere gesetzliche Meldepflichten z. B. für Betreiber kritischer Infrastrukturen geschaffen werden sollten, wird derzeit geprüft. Die Prüfungen sind noch nicht abgeschlossen.

20. Inwieweit hält es die Bundesregierung für rechtlich zulässig, sogenannte Zero-Day-Lücken zu erwerben, um sie gegebenenfalls selbst zu nutzen?

    Hat die Bundesregierung Kenntnis davon, ob so ein Erwerb durch staatliche Organisationen oder Behörden bereits stattgefunden hat oder geplant ist (bitte detailliert und einzeln aufführen)?

    Wenn ja, unter welchen Rahmenbedingungen und zu welchem Zweck hält die Bundesregierung ein solches Vorgehen für legitim, erforderlich und rechtskonform?

Im Hinblick auf die Rahmenbedingungen und Nutzung von sogenannten Zero-Day-Lücken wird auf die Antworten der Bundesregierung auf die Schriftliche Frage 25 des Abgeordneten Andrej Hunko auf Bundestagsdrucksache 18/13696 sowie zu Frage 21 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 19/1867 verwiesen.

Im Hinblick auf die nachfolgend nicht explizit genannten Sicherheitsbehörden des Bundes wird zum Erwerb von sogenannten Zero-Day-Lücken auf die Antwort auf die Schriftliche Frage 20 des Abgeordneten Andrej Hunko auf Bundestagsdrucksache 18/3361 verwiesen.

[1] Das Bundesministerium der Verteidigung hat einen Teil der Antwort zu Frage 18 als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

Eine Beantwortung der Frage 20 zum Erwerb von sogenannten Zero-Day-Lücken kann für das BAMAD und die Bundeswehr nicht in offener Form erfolgen. 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. Detaillierte Angaben zu spezifischen technischen Fähigkeiten des BAMAD und der Bundeswehr sind lediglich für den parlamentarischen Bereich, nicht jedoch für die Kenntnisnahme einer breiten Öffentlichkeit bestimmt. Eine solche Bekanntgabe würde der Öffentlichkeit und damit möglicherweise fremdem Nachrichtendiensten und Streitkräften Informationen über Arbeitsweisen des BAMAD und der Bundeswehr offenlegen bzw. Rückschlüsse auf technische Fähigkeiten und operative Einsatzmöglichkeiten bzw. Vorgehensweisen zulassen. Das würde dem staatlichen Geheimhaltungsinteresse in diesen Bereichen evident widersprechen und die Auftragserfüllung der betroffenen Dienststellen gefährden. Da die Kenntnisnahme durch Unbefugte insoweit für die Interessen der Bundesrepublik Deutschland schädlich sein kann, wurden die angefragten Informationen gemäß § 3 Nummer 3 der allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) mit dem Geheimhaltungsgrad „VS – Vertraulich“ eingestuft und in der Geheimschutzstelle des Deutschen Bundestages hinterlegt.[2]

21. Teilt die Bundesregierung die Auffassung der Fragestellenden, dass Sicherheitslücken, die nicht schnellstmöglich geschlossen werden, immer auch Dritten offenstehen, die diese für IT-Angriffe nutzen können, wodurch sich signifikante Probleme für die IT-Sicherheit insgesamt ergeben?

Die Bundesregierung vertritt die Auffassung, dass zum Erreichen bestmöglicher Cyber-Sicherheit, Schwachstellen, deren Nutzung weitreichende Auswirkungen auf die Sicherheit der Bevölkerung bzw. des Staates haben, gemeldet werden sollen und gleichzeitig die zuständigen Behörden die Mittel zur Verfügung haben, die sie für die Erfüllung ihrer Aufgaben, auch im Cyber-Raum, benötigen.

22. Wie viele Schwachstellen in Netzwerken von Dienststellen der Bundeswehr konnten bisher durch Angehörige des KdoCIR aufgedeckt und geschlossen werden?

Wie viele dieser entdeckten Schwachstellen wurden im Rahmen von Übungen bzw. während der Abwehr von tatsächlichen IT-Angriffen entdeckt?

Seit Bestehen des Kommandos Cyber- und Informationsraum hat das zuständige Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw) 25 Untersuchungen zur Ermittlung technischer Schwachstellen an Systemen und Projekten der Bundeswehr durchgeführt. Dabei wurden verschiedene Schwachstellen in den Bereichen Systemarchitektur, Update-Management, Systemkonfiguration und Schutz gegen Schadsoftware identifiziert und an die für das Schließen zuständigen Verantwortlichen übermittelt. Eine statistische Erfassung erkannter technischer Schwachstellen erfolgt bei der Bundeswehr nicht.

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

23. Welche konkreten Regelungen und datenschutzrechtlichen Bestimmungen kommen nach Auffassung der Bundesregierung für die Verarbeitung aller Verfahren und Prozesse der Bundeswehr, insbesondere auch im Rahmen von Cybersicherheitsaktivitäten, zur Anwendung (bitte im Einzelnen auflisten)?

Die Aktivitäten der Bundeswehr im Cyber-Raum unterliegen denselben rechtlichen Voraussetzungen wie jede andere Verwendung deutscher Streitkräfte. In der Bundeswehr finden die EU-Datenschutzgrundverordnung sowie das Bundesdatenschutzgesetz Anwendung. Deren Umsetzung ist durch interne Weisungen konkretisiert.

24. Inwiefern analysiert die Bundeswehr im Rahmen von Übungen die möglichen Auswirkungen auf Zivilistinnen und Zivilisten und zivile Infrastruktur von Operationen im digitalen Raum?

a) Ist diese Analyseperspektive festintegrierter Bestandteil jedes Übungsszenarios?

Wenn nein, warum nicht?

b) Durch welche konkreten Mechanismen wird sichergestellt, dass das Unterscheidungsgebot zwischen Kombattantinnen und Kombattanten und der Zivilbevölkerung bei Operationen im digitalen Raum (im konkreten Einsatz- und im Übungsfall) stets beachtet wird?

Die Fragen 24 bis 24b werden aufgrund ihres inhaltlichen Zusammenhanges gemeinsam beantwortet.

Der Aspekt „Collateral Damage Estimation (CDE)“, d. h. die Berücksichtigung nicht intendierter Begleitschäden, ist genereller Bestandteil jeder militärischen Operation, also auch im digitalen Raum.

Im Übungsfall werden eigens für die Übung zur Verfügung gestellte und zugleich von anderen öffentlichen Netzwerken gekapselte Netzwerke genutzt, um Auswirkungen außerhalb dieser Netzwerke zu vermeiden. Die Vermeidung von ungewollten Schäden ist auch Teil der Übungsszenarien.

Im Einsatzfall erfolgt eine Eingrenzung auf einsatzrelevante, militärische Systeme durch gezielte Aufklärung im Vorfeld von Operationen.

Dabei dient der Einsatz von Cyber-Fähigkeiten immer dem Erreichen definierter militärischer Operationsziele und Effekte. Er erfolgt kontrolliert, unter unmittelbarer Einbindung von Rechtsberatern, ist präzise, skalierbar und in der Regel reversibel.

25. Wie hoch waren 2017 und 2018 die Kosten für die speziell auf eine Nachwuchsgewinnung für das KdoCIR ausgerichtete Öffentlichkeitsarbeit?

Es wurden 2017 und 2018 keine personalwerblichen Maßnahmen durchgeführt, die speziell auf das Kommando Cyber- und Informationsraum ausgerichtet waren.

26. Wie viele Studienplätze gibt es im Studiengang „Cyber-Sicherheit“ der Universität der Bundeswehr in München, und wie hoch sind die gegenwärtige Auslastung sowie die Abbruchquote innerhalb dieses Studiengangs?

Am 1. Januar 2018 haben acht Studierende das Studium im ersten Jahrgang des neu eingerichteten Studiengangs „Cyber-Sicherheit“ aufgenommen.

Die Studienplatzkapazität des neuen Studiengangs wird von anfangs 20 (2018) über 50 (2019) auf 121 (2020) Studienplätze aufwachsen.

Aufgrund des gerade erst begonnenen Studienbetriebs gibt es noch keine feststellbare Abbruchquote.

27. Wie viele IT-Angriffe gab es in den letzten fünf Jahren und im Jahr 2018 im Rahmen der Auslandseinsätze auf die Systeme der Bundeswehr (bitte nach Jahren und den einzelnen Auslandseinsätzen der Bundeswehr aufschlüsseln)?

a) Sofern sich ein Muster erkennen lässt, worauf zielten diese IT-Angriffe im Speziellen ab?

b) Wie viele dieser Angriffe wurden von Einheiten der Bundeswehr erkannt und abgewehrt?

Welche Bundesbehörden oder staatlichen Stellen waren in die Abwehr dieser Angriffe in welcher Form involviert?

Welche Stellen und Behörden anderer Staaten waren in die Abwehr dieser Angriffe in welcher Form involviert?

c) Welche Schäden wurden verursacht?

Für die Fragen 27 bis 27c wird auf die Antwort zu Frage 3 verwiesen.

28. Im Rahmen welcher Auslandseinsätze der Bundeswehr kamen welche Kräfte des KdoCIR bisher in welcher konkreten Form zum Einsatz?

Der parlamentarische Informationsanspruch ist grundsätzlich für die Beantwortung gestellter Fragen in der Öffentlichkeit ausgelegt. Die Bundesregierung ist allerdings nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Frage 28 nicht vollständig in offener Form erfolgen kann.

Die Einstufung der Antwort zu Frage 28 als Verschlusssache (VS) mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ wird im Hinblick auf das Staatswohl als erforderlich erachtet, da die in der Antwort aufgeführten Fähigkeiten unter Umständen Rückschlüsse auf den in den aufgeführten Einsätzen zur Verfügung stehenden Fähigkeitsumfang zulassen. Nach § 3 Nummer 4 der Allgemeinen Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlusssachen (Verschlusssachenanweisung, VSA) sind Informationen, deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein können, entsprechend einzustufen. Im vorliegenden Fall werden diese Informationen daher als „VS – Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.[3]

[3] Das Bundesministerium der Verteidigung hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft.
Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

29. Gab es bis heute – jenseits der Presseberichterstattung über das Eindringen in die internen Netze eines afghanischen Mobilfunkbetreibers im Jahr 2015 (vgl.: www.spiegel.de/politik/ausland/cyber-einheit-bundeswehr-hackte-afghanisches-mobilfunknetz-a-1113560.html) – Aktivitäten der Bundeswehr, im Rahmen derer in fremde oder gegnerische Netze eingegriffen oder gewirkt wurde?

Wenn ja, welche (bitte konkret aufschlüsseln)?

Der parlamentarische Informationsanspruch ist grundsätzlich für die Beantwortung gestellter Fragen in der Öffentlichkeit ausgelegt. Die Bundesregierung ist allerdings nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Frage 29 nicht vollständig in offener Form erfolgen kann.

Die Einstufung der Antwort zu Frage 29 als Verschlusssache (VS) mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ wird im Hinblick auf das Staatswohl als erforderlich erachtet, da die in der Antwort aufgeführten Aktivitäten unter Umständen Rückschlüsse auf die Fähigkeiten der Bundeswehr zulassen. Nach § 3 Nummer 4 der Allgemeinen Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlusssachen (Verschlusssachenanweisung, VSA) sind Informationen, deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein können, entsprechend einzustufen. Im vorliegenden Fall werden diese Informationen daher als „VS – Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.[4]

30. Welche staatlichen und nichtstaatlichen Akteure werden über das Cyber Innovation Hub miteinander vernetzt (bitte aufschlüsseln)?

Vernetzt werden Bereiche der Bundeswehr (Bedarfsträger, Universität der Bundeswehr) mit Start-ups und sonstigen Akteuren des Start-up-Ökosystems wie etwa Venture Capital Gesellschaften, Verbänden (z. B. Bundesverband Deutsche Startups e. V., Bitkom e. V.) sowie anderen Digital Innovation Units der deutschen Wirtschaft (z. B. Deutsche Bahn AG) und verbündeter Streitkräfte.

31. Inwieweit wurden bisher Partnerschaften, gemeinsame Vorhaben, Verträge oder sonstige Kooperationen seitens der Bundeswehr mit welchen Akteuren vereinbart bzw. sind in Zukunft geplant?

Um ein Innovationsnetzwerk aufzubauen und Dual-Use-Technologien zu entwickeln und zu fördern, soll der Cyber Innovation Hub strategische Partner (in erster Linie große Unternehmen, die vor vergleichbaren Herausforderungen stehen oder einen vergleichbaren Bedarf haben), Innovations-Partner (andere Digital Innovation Units verbündeter Streitkräfte oder der deutschen Wirtschaft) und Netzwerk-Partner (Akteure an der Schnittstelle zwischen Cyber/IT, digitaler Transformation und Innovation) gewinnen.

Bislang gibt es in diesem Rahmen formlose, temporäre Kooperationen in Gestalt von gemeinsamen Veranstaltungen wie Pitch-Events oder Workshops mit den vorstehend genannten Akteuren.

[4] Das Bundesministerium der Verteidigung hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft.
Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

32. Was sind die konkreten Ergebnisse der bisherigen Zusammenarbeit mit Start-ups im Rahmen des Cyber Innovation Hub?

Es wird auf die Antwort zu den Fragen 32a und 32b verwiesen.

a) Zu welchen konkreten Vereinbarungen ist es bis heute durch dieses Kooperationsinstrument gekommen?

Der Cyber Innovation Hub hat seit dem ersten Pitch-Event am 20. Juni 2017 bis heute insgesamt 41 theoretisch mögliche Projekte mit Start-ups identifiziert.

Nach näherer Prüfung haben sich einige Projekte als nicht realisierbar herausgestellt, andere wurden zurückgestellt, da die hierfür marktverfügbaren Start-ups Qualitätsvorgaben (noch) nicht erfüllten.

Bislang konnten vier Verträge mit Start-ups als Grundlage für die Durchführung von Anwendungstests abgeschlossen werden. Weitere Vertragsschlüsse sind in Arbeit.

b) Welche Innovationen haben durch das Cyber Innovation Hub Eingang in das KdoCIR oder andere Organisationsbereiche der Bundeswehr gefunden?

Alle Projekte des Cyber Innovation Hubs werden zusammen mit Nutzern aus der Bundeswehr durchgeführt.

Die jeweiligen Testphasen für die laufenden Projekte (Vergleich Antwort zu Frage 32a) sind noch nicht abgeschlossen, so dass noch keine Entscheidungen über eine endgültige bzw. flächendeckende Einführung entsprechender Innovationen in die Bundeswehr initiiert wurden.

33. Inwiefern hat das Cyber Innovation Hub Projekte durchgeführt, die sich mit sozialen Medien befassen oder diese bedienen?

Falls ja,

Ein entsprechendes Projekt des Cyber Innovation Hubs befindet sich in der Testphase.

a) was ist für die Bundeswehr ein Anwendungsfall für die Analyse von sozialen Medien,

Ein Anwendungsfall ist das systematische Erfassen der öffentlich zugänglichen Berichterstattung im vorjournalistischen Raum und in den digitalen Medien sowie das Aufzeigen sprunghafter Veränderungen in digitaler Kommunikation als Ergänzung der traditionellen Presseauswertung.

b) wurden Daten deutscher Staatsbürgerinnen und Staatsbürger im Rahmen dieser Projekte verwendet,

Das Analysetool stützt sich ausschließlich auf öffentlich zugängliche Quellen. Soweit deutsche Staatsbürgerinnen und Staatsbürger Daten öffentlich zugänglich gemacht haben, wurden und werden diese im Rahmen des Testlaufs verwendet. Die gesetzlichen Vorgaben des Datenschutzes werden eingehalten.

c) wurden diese Projekte ausgeschrieben?

Die Anforderungen des Vergaberechts wurden beachtet.

34. Inwiefern bestehen Compliance-Regeln für Beschäftigte des Cyber Innovation Hubs, die etwa den Besitz von Anteilen an Unternehmen betreffen, mit denen das Cyber Innovation Hub Geschäftsbeziehungen unterhält oder aufzubauen plant?

Unterscheiden sich diese von denen, die im Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) oder der BWI GmbH gelten?

Ist es bisher zu Verstößen gegen diese Regeln gekommen?

Aktuell sind im Cyber Innovation Hub (CIH) ca. jeweils zur Hälfte Mitarbeiterinnen und Mitarbeiter mit einem Anstellungsvertrag der BWI GmbH sowie Soldatinnen und Soldaten beschäftigt.

Für CIH-Mitarbeiterinnen und Mitarbeiter mit BWI-Vertrag gelten die Business Conduct Guidelines der BWI GmbH. Die Business Conduct Guidelines enthalten die Verpflichtung, direkte oder indirekte Beteiligungen (größer 5 Prozent) an Wettbewerbsunternehmen mit der Möglichkeit der Einflussnahme auf das Management offenzulegen. Für im Cyber Innovation Hub eingesetzte Soldatinnen und Soldaten gelten die gleichen Regelungen, die für alle anderen Soldatinnen und Soldaten der Bundeswehr Anwendung finden.

Zusätzlich hat der Cyber Innovation Hub eigene, erweiterte Richtlinien eingeführt, im Rahmen derer sowohl die Arbeitnehmerinnen und Arbeitnehmer als auch die Soldatinnen und Soldaten sämtliche Beteiligungen, Geschäftsverbindungen oder Ehrenämter offenlegen müssen und ein laufendes Monitoring bezüglich etwaiger Interessenskonflikte stattfindet.

Verstöße gegen diese Compliance-Regeln sind nicht bekannt.

35. Wie viele Dienstposten hat das Cyber Innovation Hub, und wie viele dieser Dienstposten sind bereits besetzt?

Im Jahr 2018 stehen dem Cyber Innovation Hub 21 Planstellen zur Verfügung, die durch die BWI GmbH besetzt werden. Davon sind aktuell 14 besetzt. Zusätzlich stehen dem Cyber Innovation Hub im Jahr 2018 insgesamt 15 Vollzeitäquivalente für Reservistendienst Leistende zur Verfügung. Aktuell sind 15 Soldaten zum Cyber Innovation Hub kommandiert.

a) Wie viele der Dienstposten sind mit einem Absolventen oder einer Absolventin mit universitärem Abschluss in einem MINT-Fach (MINT = Mathematik, Informatik, Naturwissenschaft und Technik) besetzt?

Derzeit sind drei Dienstposten mit einem Absolventen oder einer Absolventin mit universitärem Abschluss in einem MINT-Fach besetzt. Aufgabe des Cyber Innovation Hubs ist nicht die technologische Forschung oder Entwicklung, sondern das Projektmanagement und die unternehmerische Umsetzung von Innovationen sowie generell die Verfügbarmachung von Kompetenzen aus dem Start-up-Ökosystem für die Bundeswehr. Abschlüsse in MINT-Fächern oder vergleichbare fachliche Qualifikationen sind daher mit Blick auf das Anforderungsprofil willkommen, aber nicht zwingend erforderlich.

b) Welches Anforderungsprofil sollen Angestellte des Cyber Innovation Hub erfüllen?

Bewerberinnen und Bewerber mit eigener unternehmerischer Erfahrung oder Führungserfahrung in der Digitalwirtschaft stehen im Fokus. Der Cyber Innovation Hub legt darüber hinaus Wert auf Diversität der Abschlüsse (derzeit u. a. Betriebs- und Volkswirte, Juristen, Geisteswissenschaftler), Erfahrungen (z. B. Gründung, Bundeswehr) und Lebenswege (z. B. Studienabbrecher mit Gründungserfahrung, Auslandserfahrung).

c) Inwiefern wurden außertarifliche Vereinbarungen für Angestellte des Cyber Innovation Hubs getroffen?

Die BWI GmbH, bei der die zivilen Mitarbeiterinnen und Mitarbeiter des Cyber Innovation Hub angestellt sind, unterliegt keiner Tarifbindung. Insofern gibt es keine Unterscheidung zwischen tariflichen und außertariflichen Vereinbarungen bzw. Leistungen.

36. In welcher Liegenschaft ist das Cyber Innovation Hub untergebracht, und Kosten in welcher Höhe sind für die Unterbringung des Hubs bisher, und werden voraussichtlich bis zum Ende der Pilotphase anfallen?

Der Cyber Innovation Hub ist in einem von der BWI GmbH angemieteten Objekt in den Gebauer-Höfen in 10587 Berlin untergebracht.

Die Bruttomiete inklusive Nebenkosten und Umsatzsteuer für das angemietete Objekt betrug für den bisherigen Anmietungszeitraum (1. Mai 2017 bis 31. Mai 2018) 526 153,73 Euro. Bis zum voraussichtlichen Ende der Pilotphase (1. Mai 2017 bis 31. Dezember 2019) werden insgesamt 1 331 063,71 Euro anfallen. Die genannte Bruttomiete umfasst die Miete für Büro-, Projekt-, Co-Working- und Veranstaltungsräumlichkeiten, die teilweise auch für sonstige Akteure aus dem Bereich der Bundeswehr nutzbar sind, und Parkplätze.

37. Wo sieht die Bundesregierung rechtlichen Regelungsbedarf für den Einsatz der Bundeswehr im digitalen Raum, und welche Initiativen sind hierzu ggf. geplant?

Derzeit sieht die Bundesregierung keinen zusätzlichen Regelungsbedarf für den Einsatz der Bundeswehr und deren militärische Maßnahmen im digitalen Raum.

38. Erachtet die Bundesregierung die gegenwärtigen parlamentarischen Aufsichts- und Kontrollstrukturen sowie die bisherige Unterrichtungspraxis über das Eindringen, Wirken oder Angreifen in fremde Netze durch die Bundeswehr im digitalen Raum als ausreichend?

Die Bundeswehr unterliegt einer umfassenden, verfassungsrechtlich vorgegebenen parlamentarischen Kontrolle. Dies umfasst auch militärische Maßnahmen im Cyber-Raum. Es gelten die gleichen Informations- und Kontrollrechte wie für sonstige Maßnahmen der Streitkräfte. Die Bundesregierung informiert regelmäßig den Deutschen Bundestag im Rahmen der vorgesehenen Verfahren über geplante und durchgeführte militärische Maßnahmen, dies schließt Maßnahmen im Cyber-Raum ein.

a) In welchem Gremium bzw. welchem Gremien berichtet die Bundesregierung durch wen dem Parlament vollumfänglich über das Eindringen, Wirken oder Angreifen in fremde Netze durch die Bundeswehr oder durch staatliche Stellen der Bundesebene und ihrer Behörden im digitalen Raum?

Die Bundesregierung unterrichtet das Parlamentarische Kontrollgremium über die Tätigkeit der Nachrichtendienste des Bundes, wie im Kontrollgremiumgesetz vorgegeben.

Im Übrigen wird auf die Antwort zu Frage 38 verwiesen.

b) Wie stellt die Bundesregierung eine umfassende, konsistente und zeitnahe Unterrichtung des Parlaments über das Eindringen, Wirken oder Angreifen in fremde Netze durch die Bundeswehr im digitalen Raum sicher?

Es wird auf die Antwort zu Frage 38 verwiesen.

c) Hat die Bundesregierung in der Vergangenheit das Parlament vollumfänglich und mit Blick auf alle erfolgten Operationen der Bundeswehr über ein Eindringen, Wirken oder Angreifen in fremde Netze durch die Bundeswehr im digitalen Raum unterrichtet?

Wenn ja, in welchem Gremium hat sie dies getan?

Es wird auf die Antwort zu Frage 38 verwiesen.

39. Erachtet die Bundesregierung angesichts der zunehmenden Bedeutung des digitalen Raums für militärische Operationen eine Anpassung der rechtlichen Grundlagen für notwendig?

Wenn ja, in welchen konkreten Punkten?

Wenn nein, warum nicht?

Auf die Antwort zu den Fragen 12, 37 und 41 wird verwiesen.

40. Definiert die Bundesregierung eine Abgrenzung zwischen defensiven und offensiven Operationen und Fähigkeiten der Bundeswehr?

Wenn ja, entlang welcher Kriterien?

Im Rahmen einschlägiger Rechtsgrundlagen wird nicht zwischen defensiven und offensiven Operationen unterschieden, vielmehr haben Operationen stets im Einklang mit geltendem nationalen und internationalem Recht zu erfolgen und dem Grundsatz der Verhältnismäßigkeit zu entsprechen. Vor diesem Hintergrund werden die jeweiligen Fähigkeiten eingesetzt.

41. Unter welchen konkreten Voraussetzungen erachtet die Bundesregierung den Einsatz von Fähigkeiten zum Eindringen, Wirken oder Angreifen in fremde Netze durch die Bundeswehr im digitalen Raum als möglich und notwendig, und auf welcher rechtlichen Grundlage tut sie das?

Der Einsatz von Cyber-Fähigkeiten kann, wie der anderer militärischer Fähigkeiten auch, notwendig sein, weil nur so das Erreichen eines definierten Operationsziels unter Beachtung politischer und rechtlicher Vorgaben, der Verhältnismäßigkeit des Einsatzes, der Kräfteökonomie im Sinne der Aufwand-/Nutzen-Relation, und der Verfügbarkeit von Kräften nach Zeit und Raum möglich ist.

Der Einsatz von Fähigkeiten der Streitkräfte im Cyber-Raum unterliegt den gleichen rechtlichen Voraussetzungen wie der Einsatz anderer militärischer Fähigkeiten. Rechtsgrundlagen für den Einsatz von Streitkräften mit Bezug zum Cyberraum sind damit einerseits die verfassungsrechtlichen Vorgaben für den Einsatz von Streitkräften, andererseits die allgemeinen Regelungen des Völkerrechts, insbesondere Artikel 51 der Charta der Vereinten Nationen, Entscheidungen des Sicherheitsrates nach Kapitel VII der VN-Charta, das humanitäre Völkerrecht sowie anwendbare Menschenrechtsübereinkommen. Diese finden grundsätzlich auch für den Cyber-Raum Anwendung.

42. Wie stellt die Bundesregierung eine Abgrenzung von Innerer und Äußerer Sicherheit im Cyber- und Informationsraum im Rahmen der gesetzlichen Grundlagen sicher?

Welche Einschränkungen ergeben sich hieraus für den Einsatz der Bundeswehr im digitalen Raum?

Die fortschreitende Digitalisierung führt dazu, dass heute eine Vielzahl von staatlichen Stellen in Bund und Ländern mit Fragen der Cyber-Sicherheit befasst ist. Dies ändert nichts an den verfassungsrechtlich vorgegebenen Kompetenzzuweisungen. Die Einsatzmöglichkeiten der Streitkräfte sind im Grundgesetz aufgeführt und gelten auch in Bezug auf den digitalen Raum. Im Übrigen wird auf die Antwort zu den Fragen 1 und 41 verwiesen.

43. Wie wird die ressortübergreifende Kooperation zur Abwehr von IT-Angriffen durch die Bundesregierung bewertet?

Wo und in welchem Umfang soll diese verbessert werden?

Wann ist mit der Vorlage des im Koalitionsvertrags zwischen CDU, CSU und SPD angekündigten zweiten IT-Sicherheitsgesetzes zu rechnen?

Eine operative ressortübergreifende Kooperation zur Abwehr von IT-Angriffen ist zum Erreichen gesamtstaatlicher Cyber-Sicherheit von grundlegender Bedeutung. Diese findet im nationalen Cyber-Abwehrzentrum (Cyber-AZ) statt.

Das Cyber-AZ ist die zentrale Stelle für den Informationsaustausch und die Koordinierung der mit Cyber-Abwehr befassten Stellen.

Im Cyber-AZ sind das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Bundesamt für Verfassungsschutz (BfV), das Bundeskriminalamt (BKA), der Bundesnachrichtendienst (BND), das Bundespolizeipräsidium (BPOL), die Bundeswehr, das Bundesamt für den Militärischen Abschirmdienst (BAMAD) und das Zollkriminalamt (ZKA) vertreten. Mit der geplanten Weiterentwicklung des Cyber-AZ wird insbesondere auch eine Möglichkeit zur stärkeren Einbindung der Länder eröffnet.

Das zweite IT-Sicherheitsgesetz befindet sich derzeit in der Erarbeitung. Ein Abschluss in der ersten Hälfte dieser Legislaturperiode ist geplant.

Ergänzend wird auf die Antwort der Bundesregierung zu Frage 3 der Kleinen Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/2645 verwiesen.

44. Wie weit sind die von der Bundesministerin der Verteidigung, Dr. Ursula von der Leyen, am 14. Mai 2018 bei der Bundeswehrtagung angekündigten Pläne zur Schaffung einer Agentur für Disruptive Innovation für Cybersicherheit (ADIC) fortgeschritten, und was sollen die konkreten Aufgaben dieser Agentur sein?

Mit Einrichtung eines gemeinsamen, ressortübergreifenden Aufbaustabs verfolgen das Bundesministerium der Verteidigung und das Bundesministerium des Innern, für Bau und Heimat derzeit das Ziel, die Rahmenbedingungen für die Einrichtung einer übergreifenden Forschungs- und Innovationsagentur für Disruptive Innovationen in Cyber-Sicherheit und Schlüsseltechnologien vertiefend zu untersuchen. Die vorläufigen Ergebnisse dieser Untersuchungen werden derzeit innerhalb des Bundesministeriums der Verteidigung und des Bundesministeriums des Innern, für Bau und Heimat hinsichtlich ihrer Umsetzbarkeit geprüft. Eine Entscheidung zum weiteren Vorgehen steht derzeit aus.

Ziel und Zweck der Agentur soll es sein, Forschungs- und Entwicklungsvorhaben mit hohem Innovationspotenzial auf dem Gebiet der Cyber-Sicherheit und Schlüsseltechnologien zu fördern und finanzieren, soweit an diesen ein Interesse des Bundes besteht.

45. Welche Kenntnisse hat die Bundesregierung über Operationen und Fähigkeiten der NATO im digitalen Raum?

Die NATO verfolgt den Schutz der eigenen Netzwerke durch Stärkung der Resilienz und Robustheit sowie der Revision von etablierten Verfahren im Falle eines Angriffes auf die eigenen Netzwerkstrukturen. Dazu gehört auch die Verbesserung des Lagebildes über die eigenen Netzwerke.

46. Wie weit sind nach Kenntnis der Bundesregierung die Planungen für das „Cyber Operations Center“ der NATO inzwischen fortgeschritten?

Während des NATO-Gipfels 2016 in Warschau beschlossen die Mitgliedstaaten die Anerkennung des Cyber-Raumes als zusätzliche Dimension der Operationsführung. Gleichzeitig wurde während des Gipfels die Notwendigkeit zur Anpassung der NATO-Kommandostruktur an die neuen sicherheitspolitischen Realitäten festgestellt.

Das geplante „Cyberspace Operations Centre“ auf Ebene des Supreme Allied Command Operations ist Teil der bereits durch die NATO-Verteidigungsminister gebilligten Erneuerung der NATO-Kommandostruktur. Dieses Element wird die planerische und operative Umsetzung des Cyber-Raumes als fünfte Dimension abbilden.

Für die weitere Beantwortung der Frage 46 wird auf den „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil verwiesen.

Der parlamentarische Informationsanspruch ist grundsätzlich für die Beantwortung gestellter Fragen in der Öffentlichkeit ausgelegt. Die Bundesregierung ist allerdings nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Frage 46 nicht vollständig in offener Form erfolgen kann.

Die Einstufung der Antwort zu Frage 46 als Verschlusssache (VS) mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ wird als erforderlich erachtet, da die in der Antwort aufgeführten Informationen von der NATO als „NATO RESTRICTED“ eingestuft wurden. Im vorliegenden Fall werden diese Informationen daher als „VS – Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.[5]

a) Mit welchen konkreten Zielen und Beiträgen bringt sich die Bundesregierung aktuell und in Zukunft in der weiteren Ausplanung der konkreten Aufgaben des „Cyber Operations Center“ der NATO ein?

Im Rahmen der Anpassung der NATO-Kommandostruktur plant Deutschland, sich personell angemessen im „Cyberspace Operations Centre“ einzubringen. Deutschland verfolgt den Grundgedanken, den Cyber-Raum gleichwertig zu den anderen Dimensionen der Operationsführung zu verankern.

b) Durch welche konkreten Maßnahmen hat sich die Bundesregierung bisher innerhalb der NATO dafür eingesetzt, dass Aspekte wie politische Kontrolle und Einhaltung des internationalen Rechts im Ausplanungsprozess beachtet werden?

Deutschland setzt sich im Rahmen des Gestaltungsprozesses in verschiedenen NATO-Gremien gemeinsam mit anderen Nationen dafür ein, den Cyber-Raum gleichwertig zu den anderen Dimensionen der Operationsführung zu verankern. Dazu gehören nach Auffassung der Bundesregierung die gleichen, bewährten Mittel der politischen Kontrolle und der Einhaltung internationalen Rechtes, welche bereits bei der konventionellen Operationsführung zum Einsatz kommen.

47. Wie bewertet die Bundesregierung die Gefahr einer fortschreitenden Militarisierung im digitalen Raum, und welche konkreten Maßnahmen hinsichtlich einer Anpassung des Instrumentariums der Rüstungskontrolle an veränderte technologische und sicherheitspolitische Rahmenbedingungen plant sie bis wann zu ergreifen?

Im Jahr 2013 hat das Institut für Abrüstungsforschung der Vereinten Nationen (UNIDIR) ein Dokument mit dem Titel „Cyber Index“ veröffentlicht. Die Angaben in dieser Studie werden derzeit mit finanzieller Unterstützung der Bundesregierung aktualisiert. Es sind jedoch auch die alten Angaben interessant: UNIDIR

[5] Das Bundesministerium der Verteidigung hat einen Teil der Antwort zu Frage 46 als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

stellte bereits im Jahr 2013 fest, dass es weltweit 114 nationale Cyber-Sicherheitsprogramme gab. In den Cyber-Sicherheitsprogrammen von 47 Staaten war dabei auch eine Involvierung der jeweiligen Streitkräfte vorgesehen. Die Bundesregierung geht davon aus, dass sich diese Zahlen seither erhöht haben. Dieser Entwicklung trägt die Bundesregierung im Rahmen ihrer Außen- und Sicherheitspolitik Rechnung.

Das Instrumentarium der Rüstungskontrolle kann Cyber-Fähigkeiten nur schwer erfassen, da eine Verifikation vereinbarter Maßnahmen kaum möglich ist. Bewährte Instrumente der Rüstungskontrolle können insofern zukünftig kaum als Blaupausen für die neuen Herausforderungen im Cyber-Raum herangezogen werden – wenn überhaupt, dann nur sehr bedingt. Im Kontext neuer Technologien werden derzeit vor allem Möglichkeiten diskutiert, verloren gegangenes Vertrauen wiederherzustellen und zugleich auch neue (nichtstaatliche) Akteure in zu schaffende Regelwerke einzubinden. Auf die Antwort zu Frage 49 wird verwiesen.

48. Welche konkreten Initiativen hat die Bundesregierung bis heute selbst angestoßen oder wesentlich unterstützt, um ein internationales Regelwerk für das Handeln von Streitkräften und Nachrichtendiensten im digitalen Raum auf den Weg zu bringen (bitte einzeln darstellen)?

Die Bundesregierung unterstützt Anstrengungen in den Vereinten Nationen, ein internationales Einverständnis der Staatengemeinschaft über die Regeln für verantwortungsvolles Staatenverhalten im Cyber-Raum zu schaffen. Seit 2005 hat die Generalversammlung der Vereinten Nationen eine Reihe von fünf Expertengruppen beauftragt, an diesem Thema zu arbeiten. Als einziger Staat, der nicht ständig dem Sicherheitsrat angehört, war Deutschland an allen diesen Gruppen beteiligt; in einer der Gruppen hat der deutsche Experte den Vorsitz geführt.

Nach Abschluss der Diskussionen in der letzten Expertengruppe im Juni 2017 wird in den Vereinten Nationen aktuell diskutiert, wie die Arbeit fortgesetzt werden kann. Gemeinsam mit der Schweiz und Mexiko hat die Bundesregierung vorgeschlagen, eine Arbeitsgruppe zu beauftragen, die die Umsetzung der bisher vorgelegten Expertenempfehlungen bezüglich vertrauensbildender Maßnahmen überprüfen, Ansätze zu ihrer weiteren Umsetzung entwickeln und einen Konsensbericht hierüber vorlegen soll, der auf im Rahmen von regelmäßigen Konsultationen mit allen VN-Mitgliedstaaten und anderen interessierten Akteuren gewonnenen Erkenntnissen basieren soll.

Die Bundesregierung hat außerdem gemeinsam mit Brasilien seit 2013 mehrere Resolutionen in der Generalversammlung der Vereinten Nationen und im Menschenrechtsrat zum Schutz des Rechts auf Privatheit im digitalen Zeitalter eingebracht, die alle im Konsens angenommen wurden. Auch die Einsetzung des VN-Sonderberichterstatters zum Recht auf Privatheit ist ein Ergebnis dieser Initiative.

49. Welche konkreten Vorstellungen hat die Bundesregierung in Anbetracht der technologischen Entwicklung und der Zunahme von Angriffen und militärischen Operationen im digitalen Raum für eine Neu- und Weiterentwicklung von Rüstungskontrollinstrumenten als Teil einer modernen und zukunftsorientierten Sicherheitspolitik?

Rüstungskontrollinstrumente können Cyber-Fähigkeiten mangels Verifikationsmöglichkeiten nur schwer erfassen. Die Bundesregierung setzt daher darauf, Einigkeit über die Regeln für das verantwortungsvolle Staatenverhalten im Cyber-Raum herzustellen, Vertrauen zu schaffen, dass Staaten sich an diese Regeln halten, und erforderlichenfalls Staaten auch beim Aufbau der Fähigkeit zu unterstützen, sich regelgerecht und vertrauenswürdig zu verhalten.

Die Arbeit an Regeln für das verantwortungsvolle Staatenverhalten im Cyber-Raum verfolgt die Bundesregierung in den Vereinten Nationen (auf die Antwort zu Frage 48 wird verwiesen). Zur Herstellung von Vertrauen, dass Staaten sich an diese Regeln halten, unterstützt die Bundesregierung auch entsprechende Arbeiten in Regionalorganisationen weltweit. Sie hat insbesondere den deutschen Vorsitz in der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) im Jahr 2016 für erhebliche Fortschritte genutzt, die sich in der Vereinbarung konkreter vertrauensbildender Maßnahmen (VBM) und einem Beschluss des Ministerrats von Hamburg niedergeschlagen haben. Die Bundesregierung unterstützt außerdem ausgewählte Partner beim Auf- und Ausbau ihrer Cyber-Sicherheitsfähigkeiten, damit diese in die Lage versetzt werden, sich regelgerecht und vertrauenswürdig zu verhalten. Zur weiteren Unterstützung dieser Bemühungen beabsichtigt die Bundesregierung die Gründung eines deutschen Instituts für internationale Cyber-Sicherheit, wie in der Cyber-Sicherheitsstrategie der Bundesregierung aus dem Jahr 2016 dargestellt.

50. Welches internationale Forum erachtet die Bundesregierung als geeigneten Rahmen, um international breit getragene Verhaltensnormen zu verhandeln?

Welche Initiativen hat die Bundesregierung an diesen Stellen wann angeschoben?

Auch im Cyber-Raum ist das Völkerrecht anzuwenden und unverzichtbar für die Wahrung von Frieden und Stabilität. Das geeignete Forum zur Diskussion über die Frage, was dies im Einzelnen bedeutet, sowie über weitere, völkerrechtlich nicht bindende, aber politisch bedeutsame Normen für das verantwortungsvolle Staatenverhalten im Cyber-Raum sind die Vereinten Nationen.

Im Übrigen wird auf die Antwort zu Frage 48 verwiesen.

51. Welche Pläne gibt es seitens der Bundesregierung, sich auf internationaler Ebene für Vereinbarungen zur Sorgfaltsverantwortung für ein friedliches Miteinander im digitalen Raum einzusetzen und, sollte es hier noch keine Pläne geben, warum nicht, und welche alternativen Maßnahmen will man ergreifen?

Regelungen zur Sorgfaltsverantwortung fallen in den Bereich des Völkerrechts. Diesbezüglich wird auf die Antwort zu den Fragen 48 und 50 verwiesen.

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