



Bundesministerium
der Verteidigung

-1880022-V124-

Bundesministerium der Verteidigung, 11055 Berlin

Präsidenten des Deutschen Bundestages
Herrn Prof. Dr. Norbert Lammert, MdB
Parlamentssekretariat
Platz der Republik 1
11011 Berlin

Markus Grübel

Parlamentarischer Staatssekretär
Mitglied des Deutschen Bundestages

HAUSANSCHRIFT Stauffenbergstraße 18, 10785 Berlin
POSTANSCHRIFT 11055 Berlin

TEL +49 (0)30 2004-22400
FAX +49 (0)30 2004-22441
E-MAIL BMVgBueroParlStsGruebel@BMVg.Bund.de

BETREFF **Kleine Anfrage der Abgeordneten Dr. Alexander S. Neu, Andrej Hunko u. a. sowie der Fraktion DIE LINKE. vom 16. Oktober 2015 eingegangen beim BKAm am 28. Oktober 2015
BT-Drucksache 18/6496 vom 16. Oktober 2015
Krieg im „Cyber-Raum“ – offensive und defensive Cyberstrategie des Bundesministeriums der Verteidigung**
ANLAGE Antwort der Bundesregierung auf die oben genannte Kleine Anfrage

Berlin, **9.** Dezember 2015

Sehr geehrter Herr Bundestagspräsident,

beigefügt übersende ich die Antwort der Bundesregierung auf die oben genannte Kleine Anfrage.

Auf die Einstufung eines Teils der Antwort zu der Frage 20 als „VS – VERTRAULICH“ erlaube ich mir hinzuweisen.

Mit freundlichen Grüßen

Markus Grübel

Antwort der Bundesregierung auf die Kleine Anfrage Dr. Alexander S. Neu, Andrej Hunko u. a. sowie der Fraktion DIE LINKE. vom 16. Oktober 2015

BT-Drucksache 18/6496 vom 16. Oktober 2015

Krieg im „Cyber-Raum“ – offensive und defensive Cyberstrategie des Bundesministeriums der Verteidigung

Vorbemerkung der Fragesteller

Das Schlagwort "Cyberwar" steht für militärische IT-Angriffe auf computergestützt betriebene Systeme anderer Staaten. Hierbei kann es sich um mittelbare und unmittelbare Einwirkungen auf Waffen- oder sonstige militärische Systeme handeln, aber auch um (ggf. völkerrechtswidrige) Angriffe mit Auswirkungen auf wichtige zivile Infrastruktureinrichtungen wie Krankenhäuser oder Energieversorgungssysteme. Der Begriff des Cyberangriffs ist dabei weit gefasst und meint z. B. auch Daten-Spionage, das Zerstören von Hardware oder das Einschleusen schadhafter oder kompromittierter Hard- und Software in fremde Systeme. Neben sogenannten offensiven Strategien, die darauf zielen, die Systeme anderer Staaten anzugreifen, sie zu sabotieren, die Kontrolle über sie zu erlangen, sie außer Kraft zu setzen oder Fehlfunktionen hervorzurufen, geht es zudem darum, durch sogenannte defensive Ansätze die eigenen IT-Strukturen, Kommunikations- und Waffensysteme zu sichern und aufrechtzuerhalten, und sie vor Einwirkungen und Angriffen zu schützen.

Auch die Bundeswehr soll nach dem Willen der Bundesregierung künftig stärker auf derartige-Aktivitäten fokussieren. Der "Cyber-Raum" wird zum "Operationsraum" der Bundeswehr erklärt. Nach Definition der Bundesregierung ist „Cyber-Raum“ der „virtuelle Raum aller auf Datenebene vernetzten IT-Systeme im globalen Maßstab“, dem das Internet als „universelles und öffentlich zugängliches Verbindungs- und Transportnetz“ zugrunde liegt, ergänzt durch „beliebige andere“ Datennetze, „die über Schnittstellen verfügen“, ansonsten aber vom Internet separiert betrieben werden.

So ist Cyberwar ein Gegenstand des im Februar 2015 gestarteten und noch bis Frühjahr 2016 laufenden "Weißbuch-Prozesses", mit dem die Bundesregierung unter Federführung des Bundesministeriums der Verteidigung u.a. mit einer Reihe nicht inklusiver "Expertengespräche" – Gesprächsrunden mit Akteurinnen und Akteuren aus dem militärischen und sicherheitspolitischen Bereich, die entgegen anderslautender öffentlicher Postulate aufgrund ihrer Konzeption als geschlossene Veranstaltungen der kritischen Öffentlichkeit tatsächlich nicht zugänglich sind – "Grundzüge, Ziele, und Rahmenbedingungen deutscher Sicherheitspolitik, die Lage der

Bundeswehr und die Zukunft der Streitkräfte" darstellen will (www.bmvg.de vom 2. September 2015 „Was ist ein Weißbuch“). Eine Gesprächsrunde zum Thema Cyberwar fand im Rahmen des Weißbuch-Prozesses am 17. September 2015 in Berlin statt.

Bereits am 16. April 2015 erließ Bundesministerin der Verteidigung Dr. Ursula von der Leyen eine „Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich des BMVg“. Das Strategiepapier wurde zunächst unter Verschluss gehalten, und erst im Sommer 2015, nachdem Medien über seine Existenz berichtet hatten, einzelnen Bundestagsabgeordneten auf ausdrückliche Nachfrage zur Verfügung gestellt. Inzwischen dokumentiert die Plattform Netzpolitik das Dokument im Internet (Netzpolitik vom 30. Juli 2015: www.netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/).

Nach dem Willen des BMVg soll die Bundeswehr im Rahmen dieser Cyberstrategie „einen Beitrag zur gesamtstaatlichen Sicherheitsvorsorge“ leisten. "Cyberattacken auf Wirtschaft und Staat in Deutschland", "die allgemeine Bedrohungs- und Gefährdungslage im Cyber-Raum sowohl für staatliche Institutionen als auch für die Wirtschaft und den privaten Bereich", „Gefährdungen“ für privatwirtschaftliche und staatliche mögliche Angriffsziele – all das wird in der Cyberstrategie gleichrangig genannt, das BMVg differenziert weder zwischen Eingriffen in militärische und zivile Strukturen, noch danach, ob es sich bei „Angreifen“ um staatliche oder private, zivile oder militärische Akteure handelt.

Die Cyberstrategie des BMVg bezieht sich zwar nominal auf die Cybersicherheitsstrategie des Bundesministeriums der Innern (BMI), in dessen Verantwortungsbereich der Schutz ziviler Netze fällt, erhebt aber dennoch den Anspruch der kooperativen Zuständigkeit der Bundeswehr für die „gesamtstaatliche Abwehr von Cyber-Angriffen“ im „Cyber-Raum“. Vorgeschlagen wird sogar, die Bundeswehr könne Netze für andere Behörden betreiben. Wie sich derartige Ideen und Zuständigkeiten (verfassungs-) rechtlich fundieren ließen, bleibt hingegen völlig unklar.

Zugleich werden – ungeachtet fehlender völkerrechtlicher Vereinbarungen für diesen Bereich – offensive Strategien verfolgt: Die Cyberstrategie hebt ausdrücklich auf die verstärkte Abhängigkeit „eines potenziellen Gegners“ von Informationstechnik ab. Einrichtungen des BMVg und der Bundeswehr sollen in der Lage sein, selbst offensiv tätig zu werden, d. h. "Cyber-Angriffe" in fremden Netzen auszuführen. Verbrämt wird das durch die in der Cyberstrategie des BMVg aufgestellte Forderung, die Bundeswehr müsse in der Lage sein, Bedrohungen „ggf. auch aktiv abzuwehren“.

Vorbemerkung der Bundesregierung

Politik, Wirtschaft, Behörden, Kritische Infrastrukturen, die Gesellschaft insgesamt und auch die Bundeswehr sind als Teil einer zunehmend vernetzten Welt auf verlässliche Informations- und Kommunikationstechnik angewiesen. Deren Verfügbarkeit sowie die Vertraulichkeit und Integrität der darin gespeicherten,

übertragenen und verarbeiteten Daten haben besondere Bedeutung für die nationale Sicherheit, Wirtschaft und das öffentliche bzw. private Leben. Der Cyber-Raum ist nicht nur zu einem wesentlichen staatlichen und öffentlichen Raum geworden, sondern er hat sich auch zu einem internationalen strategischen Handlungsraum entwickelt. Jenseits des nationalen Bezugsrahmens sind Cyber-Sicherheit und die Sicherheit wichtiger kritischer Ressourcen des Cyber-Raums sowie der darin gespeicherten, verarbeiteten und übertragenen Informationen eine globale Herausforderung für alle Gesellschaften des 21. Jahrhunderts.

Gleichzeitig mit der gesellschaftlichen und wirtschaftlichen Bedeutung des Cyber-Raums ist auch das Schädigungs- bzw. auch Missbrauchspotenzial durch staatliche und nichtstaatliche Akteure in diesem Raum stetig angewachsen. Als eine Folge der Durchdringung öffentlichen und privaten Lebens wie auch des Staates durch die vernetzte Informations- und Kommunikationstechnik hat sich auch gezeigt, dass im Cyber-Raum (erweitert verstanden auch als Informationsraum) die Grenzen von Krieg und Frieden, innerer und äußerer Sicherheit sowie kriminell und politisch motivierten Angriffen auf die Souveränität eines Staates zunehmend verschwimmen. Cyberfähigkeiten sind in den letzten Jahren überdies zu einem wichtigen Mittel einiger staatlicher und nichtstaatlicher Akteure geworden, um politische Ziele auf illegitime Art durchzusetzen (bspw. als Teil der hybriden Kriegsführung).

Unverändert bleibt es Aufgabe der Sicherheits- und Verteidigungspolitik, die territoriale Unversehrtheit und die Souveränität Deutschlands und seiner Verbündeten auch im Informationsraum zu wahren. Die Verteidigungsaspekte im Rahmen gesamtstaatlicher Cyber-Sicherheit (Cyber-Verteidigung) fallen in den Geschäftsbereich des Bundesministeriums der Verteidigung (BMVg). Die Aufgabe der Bundeswehr ist es insbesondere, im Cyber-Raum folgende Beiträge zur gesamtstaatlichen Sicherheitsvorsorge zu leisten:

- Die Verteidigung gegen Cyber-Angriffe, die einen bewaffneten Angriff auf Deutschland darstellen bzw. einen solchen vorbereiten oder begleiten können.
- Die Ausübung von Cyberfähigkeiten im Rahmen von Auslandseinsätzen nach Art. 24 Absatz 2 Grundgesetz.

Die Unterstützung bei der gesamtstaatlichen Abwehr von Cyber-Angriffen durch Maßnahmen, die von der technischen Unterstützung im Rahmen von Amtshilfe bis

hin zum Einsatz der Bundeswehr zur Bewältigung eines besonders schweren Unglücksfalls, insbesondere hinsichtlich Kritischer Infrastrukturen reichen können.

Auch innerhalb des Verteidigungsressorts sind die stark vernetzten, hochtechnisierten militärischen Plattformen und Waffensysteme auf die Nutzung von Informations- und Kommunikationssystemen angewiesen. Für die Bundeswehr ist neben den klassischen Räumen Land, Luft, See und Weltraum der Cyber-Raum zu einem Operationsraum geworden, in dem sie über geeignete personelle und operative Fähigkeiten sowie über eine entsprechende Ausrüstung verfügen muss, um die auftretenden Herausforderungen zu bewältigen.

Um sich diesen Aufgaben im Cyber- und Informationsraum zukünftig möglichst wirkungsvoll zu stellen, wird sich das Verteidigungsressort im Cyber- und Informationsraum neu aufstellen und zum einen die über alle Ebenen und Organisationsbereiche fragmentierten Zuständigkeiten und Strukturen zur Cyber-Verteidigung zusammenführen sowie zum anderen die IT-Fähigkeiten bündeln.

Bezugsrahmen für die Neuaufstellung des Verteidigungsressorts im Bereich Cyber ist auch der Weißbuchprozess, der im Rahmen seiner ausdrücklich inklusiven und partizipativen Umsetzung ebenfalls die Thematik Cybersicherheit in den Blick genommen hat. Hierzu wurde am 17. September 2015 mit zahlreichen Akteuren aus Politik, Wirtschaft und Zivilgesellschaft ein Experten-Workshop mit dem Titel „Perspektiven Cybersicherheit“ durchgeführt, der allen Teilnehmern die Möglichkeit bot, sich einzubringen. Die Ergebnisse und Thesen des Workshops wurden noch am selben Tag der Öffentlichkeit präsentiert und zur Diskussion gestellt.

Der Experten-Workshop „Perspektiven Cybersicherheit“ war darüber hinaus so konzipiert, dass er eine durchgehende Teilnahme von Vertretern der themenbezogenen parlamentarischen Ausschüsse (Verteidigungsausschuss, Auswärtiger Ausschuss, Innenausschuss, Ausschuss Digitale Agenda) vorsah. Zudem bestand für eine breite Öffentlichkeit die Möglichkeit, die nicht den Chatham-House-Regeln unterliegenden Anteile per Live-Video-Stream zu verfolgen.

1. *Mit welchen „Wirkmöglichkeiten“ und „Wirkmitteln“ für den Cyberwar soll die Bundeswehr nach den Vorstellungen der Bundesregierung ausgerüstet werden, um „eigene Wirkung zu entfalten“?*

„Cyberwar“ ist kein Konzept für die Bundeswehr. Wirkmittel und Wirkmöglichkeiten im Cyberraum richten sich nach den Operationszielen eines Einsatzes der Streitkräfte und den gegebenen politischen, rechtlichen und operativen Rahmenbedingungen zum Zeitpunkt der Entscheidung.

Aufgrund der hohen Entwicklungsgeschwindigkeit von Veränderungen im Cyberraum und des hohen Anpassungsbedarfs müssen sich entsprechende Aktivitäten an den gegebenen technischen Möglichkeiten zum Zeitpunkt eines Einsatzes orientieren.

2. *Unter welchen Voraussetzungen soll die Bundeswehr nach Vorstellung der Bundesregierung offensive Cyber-Fähigkeiten einsetzen dürfen?*

Der Einsatz militärischer Cyber-Fähigkeiten durch die Bundeswehr unterliegt denselben rechtlichen Voraussetzungen wie jeder andere Einsatz deutscher Streitkräfte. Grundlagen für Einsätze der Bundeswehr sind die einschlägigen Regelungen des Grundgesetzes sowie des Völkerrechts, Maßnahmen des Sicherheitsrates nach Kapitel VII der VN-Charta (Mandate), völkerrechtliche Vereinbarungen mit dem betreffenden Staat und das Parlamentsbeteiligungsgesetz. Im Falle eines Einsatzes im bewaffneten Konflikt gilt das humanitäre Völkerrecht.

3. *Inwieweit wird angestrebt, Cyber-Fähigkeiten neben oder anstelle anderer Waffen einzusetzen (komplementär bzw. ergänzend, unterstützend oder substituierend)?*

In militärischen Konflikten werden verschiedene militärische Wirkmittel im Verbund eingesetzt. Cyberfähigkeiten kommen in diesem Wirkverbund – abhängig von den Operationszielen und der aktuellen Lage – eine Rolle zum Schutz der eigenen Kräfte (Force Protection) oder zur Erhöhung eigener Wirkung zu, sie können damit andere Waffensysteme in einer konkreten Lage womöglich substituieren.

4. *Mit welchen konkreten taktischen Ansätzen soll nach Vorstellung der Bundesregierung „zur Unterstützung von militärischen Einsätzen“ ermöglicht werden, die „Nutzung des Cyber-Raums durch gegnerische Kräfte einzuschränken, ggf. sogar zu unterbinden [...] und eigene Wirkung zu entfalten“?*

Ein konkreter taktischer Ansatz kann erst bei Vorliegen konkreter Operationspläne erfolgen, welche die Operationsziele, Möglichkeiten und Grenzen eigenen Handelns definieren.

5. *Inwiefern sollen auch Trojaner bzw. Malware sowie Stealth-Techniken zum Einsatz kommen?*

Auf die Antwort zu Frage 1 wird verwiesen.

6. *Inwiefern sollen die Bundeswehr oder sonstige staatliche Stellen auch letale bzw. letal wirkende Cyber-Angriffe ausführen (mit Blick auf die Darlegung in der Cyber-Strategie, wonach Cyber-Fähigkeiten „in der Regel nicht-letal“ – im Umkehrschluss also ggf. doch letal – „wirken“ sollen)?*

Auf die Antwort zu Frage 4 wird verwiesen.

7. *Welche Erwartungen hat die Bundesregierung an die Präzision von Cyberangriffen, d. h. inwieweit geht sie davon aus, dass die mit Cyber-Fähigkeiten zu realisierenden Ein- oder Auswirkungen von vornherein (räumlich oder von der Wirkungsweise) konkret bestimmbar und eingrenzbar sein können, und dass im Ergebnis die erwarteten Auswirkungen den realen Auswirkungen entsprechen werden?*

Der Einsatz von Cyber-Wirkmitteln richtet sich nach denselben Kriterien wie der Einsatz anderer militärischer Wirkmittel. Falls ein Einsatz im Verbund mit anderen Wirkmitteln vorgesehen ist, setzt dies voraus, dass die Wirkungsweise von vornherein konkret bestimmbar und eingrenzbar ist.

8. *Inwiefern teilt die Bundesregierung die Einschätzung des Chaos Computer Club, wonach „digitale Angriffe den Charakter von Streubomben [haben], die große Teile des Internets betreffen und damit auch ein hohes Risiko für weite Bereiche der Zivilbevölkerung darstellen“ und es unmöglich ist, „Ziele mit einer ‚hohen Präzision‘ auszumachen“ (Netpolitik vom 30. Juli 2015)?*

Dieser Vergleich wird den spezifischen Charakteristiken des Internets nicht gerecht. Streubomben haben signifikant andere Auswirkungen – insbesondere für die körperliche Unversehrtheit eines Menschen – als digitale Maßnahmen.

9. *Wie ist nach Einschätzung der Bundesregierung ein „präzises“, „punktgenaues“ Einwirken auf nicht selbst kontrollierte IT-Netzwerke realisierbar?*

Viele ausgewertete Computerangriffe zeigen, dass durch die Anwendung bestimmter Maßnahmen eine Kontrolle über Netze oder Netzelemente erreicht werden konnte und bestimmte Funktionen für eigene Zwecke genutzt werden konnten.

10. *Inwiefern und ggf. in welchem Maße hält die Bundesregierung „Kollateralschäden“ durch nicht punktgenaue Eingriffe in fremde IT-Systeme mit für Menschen letale Auswirkungen oder sonstigen ursprünglich nicht beabsichtigten Auswirkungen von Cyber-Einsätzen deutscher Kräfte für hinnehmbar?*

Die Bundeswehr ist im bewaffneten Konflikt, unabhängig davon, ob Cyber-Fähigkeiten eingesetzt werden, an die humanitär-völkerrechtlichen Regelungen zur Vermeidung von Kollateralschäden gebunden.

11. *Bezüglich welcher Staaten soll im Sinne der Cyberstrategie ein „Lagebild über die Fähigkeiten, Verwundbarkeiten und möglichen Angriffsvektoren“ erstellt werden?*

Ein zukünftiges Lagebild im Sinne der "Strategischen Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg" soll neben eigenen Kräften, Mitteln und Einrichtungen sowie Verfahren, die Fähigkeiten, Verwundbarkeiten und möglichen Angriffsvektoren von und gegen mögliche Gegner darstellen. Die Definition "mögliche Gegner" umfasst dabei sowohl gegnerische Streitkräfte als auch nicht staatlich legitimierte bzw. nicht als militärisch klassifizierte Gegner, gegen die aufgrund der politischen und rechtlichen Rahmenbedingungen militärisch vorgegangen werden kann. Deren konkrete Benennung und genaue Zuordnung – soweit dies technisch im Cyber-Raum möglich ist – innerhalb des zu erstellenden Lagebildes unterliegt jedoch der jeweils aktuellen Lage bzw. Lageentwicklung in diesem Operationsraum und ist für Einsätze der Bundeswehr abhängig vom jeweiligen Mandat.

12. *Inwiefern handelt es sich dabei um Staaten, die als "Gegner" betrachtet werden?*

Seitens der Bundesregierung werden derzeit keine Staaten als Gegner eingestuft.

13. *Inwieweit sollen entsprechende „Lagebilder“ zu „Fähigkeiten, Verwundbarkeiten und möglichen Angriffsvektoren“ auch bzgl. EU- oder NATO-Mitgliedstaaten, sonstigen Partnerstaaten oder Staaten, mit denen Kooperationen geplant sind bzw. bestehen, erstellt werden (bitte auch mitteilen, um welche Staaten es sich dabei handelt)?*

Die Erstellung von Lagebildern über die Fähigkeiten, Verwundbarkeiten und möglichen Angriffsvektoren bezieht sich im Sinne der "Strategischen Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg" auf "mögliche Gegner" und nicht auf EU- oder NATO-Mitgliedstaaten, sonstige Partnerstaaten oder Staaten, mit denen Kooperationen geplant sind bzw. bestehen.

14. *Welche Abteilungen der Bundeswehr, der Bundeswehrverwaltung, des BMVg oder sonstiger staatlicher Stellen, einschließlich der Nachrichtendienste, sind hiermit befasst und wann sollen welche Ergebnisse vorliegen?*

Im Nationalen Cyber-Abwehrzentrum arbeiten seit April 2011 das federführende Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie Bundeskriminalamt (BKA), Bundespolizei (BPOL), Bundesamt für Verfassungsschutz (BfV), Bundesnachrichtendienst (BND), Militärischer Abschirmdienst (MAD), Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), Zollkriminalamt (ZKA) und die Bundeswehr im Rahmen ihrer gesetzlichen Aufgaben und Befugnisse zusammen, um eine Optimierung der operativen Zusammenarbeit aller staatlichen Stellen und eine bessere Koordinierung von Schutz- und Abwehrmaßnahmen gegen IT-Vorfälle zu erreichen. Diese Mitwirkung dient der Bundeswehr zur Ableitung von Schutzmaßnahmen für die eigenen Netze. Im Sinne der Strategischen Leitlinie Cyber-Verteidigung sollen die Prozesse der Datengewinnung und -aufbereitung zu einem kohärenten Lagebild weiterentwickelt werden. Innerhalb der Bundeswehr tragen letztlich sämtliche Stellen hierzu bei.

15. Welche Programme oder Szenarien sollen auf der Basis dieser Erkenntnisse und Daten erstellt oder erarbeitet werden?

Die Mitwirkung am Nationalen Cyber-Abwehrzentrum dient der Bundeswehr zur Ableitung von Schutzmaßnahmen für die eigenen Netze. Auf Basis dieser Erkenntnisse werden Informationsprogramme zur Erhöhung der digitalen Kompetenz von Mitarbeitern (Security Awareness) erarbeitet und durchgeführt bzw. Szenarien im Rahmen von Übungen erstellt, welche die Resilienzfähigkeiten an aktuellen Bedrohungsszenarien üben.

16. Mit welchen Verfahren sollen die Erkenntnisse und Daten in nicht selbst betriebenen Netzen gesammelt werden?

Die militärische Aufklärung orientiert sich an den konkreten Anforderungen, der jeweiligen Ausgangslage und den verfügbaren technischen Möglichkeiten zum Zeitpunkt einer militärischen Operation im vorher definierten politischen und rechtlichen Rahmen.

17. Auf welcher rechtlichen Grundlage sollen in nicht selbst betriebenen Netzen Erkenntnisse und Daten gesammelt werden?

Erkenntnisse und Daten werden gesammelt, soweit dies verfassungsrechtlich erlaubt ist und völkerrechtliche Regeln nicht entgegenstehen.

18. *Welche Rechtsgrundlage legitimiert nach Einschätzung der Bundesregierung Eingriffe der Bundeswehr oder sonstiger staatlicher Stellen in die IT-Infrastruktur anderer Staaten (bitte konkret bezeichnen, ggf. unter Angabe des einschlägigen Gesetzes, der völkerrechtlichen Vereinbarung bzw. des Rechtsinstituts)?*

Die rechtlichen Grundlagen für Einsätze und Verwendungen der Streitkräfte unterscheiden sich nicht im Hinblick auf deren unterschiedliche Fähigkeiten und deren jeweiliges besonderes militärisches Einsatzspektrum. Rechtsgrundlage für die Einsätze und Verwendungen der Bundeswehr sind die einschlägigen Regelungen des Völkerrechts und des Grundgesetzes sowie des Parlamentsbeteiligungsgesetzes. Im Übrigen wird auf die Antwort zu Frage 2 verwiesen.

19. *Wo liegt im "Cyber-Raum" die Grenze (technisch und rechtlich) zwischen Verteidigung und Angriff?*

In völkerrechtlicher Hinsicht ist zu unterscheiden zwischen einem bewaffneten Angriff im Sinne von Art. 51 VN-Charta, der das Recht auf individuelle und kollektive Selbstverteidigung auslöst, und dem Begriff des Angriffs im Sinne des humanitären Völkerrechts, der jede offensive und defensive Gewaltanwendung gegen den Gegner erfasst (Art. 49 Abs. 1 ZP I zu den Genfer Abkommen). Insoweit differenziert das humanitäre Völkerrecht nicht zwischen offensiven und defensiven Gewaltanwendungen. Hinsichtlich der Bestimmung eines bewaffneten Angriffs nach Art. 51 VN-Charta wird auf die Antwort zu Frage 27 verwiesen. Das Grundgesetz verbietet auch im Cyber-Raum den Angriffskrieg (Art. 26 Abs. 1 GG).

20. *Welche Aktivitäten der Bundeswehr oder sonstiger deutscher Stellen, bei denen mit Cyber-Fähigkeiten in fremde oder gegnerische Netze bzw. IT-Systeme eingegriffen wurde, gab es bislang?*

Eine zur Veröffentlichung bestimmte Antwort der Bundesregierung auf diese Frage würde spezifische Informationen zu operativen Verfahren und Fähigkeiten, insbesondere zum Modus Operandi der Sicherheitsbehörden einem nicht eingrenzbaaren Personenkreis – auch der Bundesrepublik Deutschland möglicherweise gegnerisch gesinnten Kräften – nicht nur im Inland, sondern auch im Ausland zugänglich machen. Durch die Kenntnis über die Methodik würde die Möglichkeit gegeben, aus den Informationen Rückschlüsse auf die Arbeitsweise zu gewinnen. Dabei könnte die Gefahr einer nachhaltigen Beeinträchtigung oder Unterbindung von Informationskanälen und -zugängen erwachsen. Im Ergebnis

könnte dies für die Interessen der Bundesrepublik Deutschland schädlich sein oder aber die Sicherheit der Bundesrepublik Deutschland gefährden.

Daher muss bei der Beantwortung dieser Frage eine Abwägung der verfassungsrechtlich garantierten Informationsrechte des Deutschen Bundestages und seiner Abgeordneten einerseits mit den dargestellten negativen Folgen sowie der daraus resultierenden Gefährdung der Sicherheit der Bundesrepublik Deutschland andererseits erfolgen. Bezogen auf die vorgenannte Frage führt die gebotene Abwägung zum Vorrang der Geheimhaltungsinteressen. Gleichwohl wird die Bundesregierung nach gründlicher Abwägung dem Informationsrecht des Parlaments unter Wahrung berechtigter Geheimhaltungsinteressen nachkommen. Zur Beantwortung hinsichtlich der Bundeswehr wird auf eine Unterrichtung der Obleute des Verteidigungsausschusses und des Auswärtigen Ausschusses vom 18. November 2015 durch das BMVg verwiesen.

Zur Beantwortung bezogen auf sonstige deutsche Stellen wird auf die Hinterlegung einer ergänzenden, VS-Vertraulich eingestuften Antwort, in der Geheimschutzstelle des Deutschen Bundestages verwiesen.

21. *Welche offensiven und defensiven Szenarien werden bzw. wurden in der Vergangenheit von der Bundeswehr oder sonstigen deutschen Stellen bereits geübt?*

Die Bundeswehr beteiligt sich an der durch das NATO Cooperative Cyber Defence Center of Excellence jährlich durchgeführten Übung „Locked Shields“. Im Rahmen dieser Übung wird in einer virtuellen Testumgebung eine vorgegebene IT-Infrastruktur gegen einen fiktiven Angreifer verteidigt. Im Rahmen der jährlichen NATO Cyber Defence Übung „Cyber Coalition“ werden Prozesse und Verfahren zum Schutz der eigenen IT-Systeme mit der NATO und den teilnehmenden Staaten auf Basis ebenfalls rein fiktiver Szenarien geübt.

Die Abteilung Computer Network Operations (CNO) des Kommandos Strategische Aufklärung der Bundeswehr übt mit der ihr zur Verfügung stehenden Ausbildungs- und Trainingsanlage das Wirken gegen und in gegnerischen Netzen in bewaffneten Konflikten ebenfalls nur anhand fiktiver Szenarien, um ihre Einsatzbereitschaft sicherzustellen.

22. *Welche konkreten „zielgerichteten und koordinierten Maßnahmen zur Beeinträchtigung von fremden Informations- und Kommunikationssystemen sowie der darin verarbeiteten Informationen“*

sollen Kräfte der Bundeswehr sowie sonstige staatliche Stellen, einschließlich der Nachrichtendienste, nach Vorstellung der Bundesregierung im Konfliktfall bzw. Cyber-Konflikt ergreifen?

Alle Maßnahmen der Bundesregierung richten sich nach den jeweils aktuellen politischen, rechtlichen und operativen Rahmenbedingungen.

23. *Stellt nach Einschätzung der Bundesregierung das Eindringen in fremde oder gegnerische IT-Netzwerke, um dort Schwachstellen auszukundschaften, „aufzuklären“ oder Funktionen zu stören, einen Angriff dar? Wo verortet die Bundesregierung ggf. die Grenze, ab der ein derartiges Vorgehen zum Angriff wird?*

Auch im Cyber-Raum sind Aktivitäten staatlicher Stellen am geltenden Recht zu messen. In friedensvölkerrechtlicher Hinsicht sind dies das Interventions- und Gewaltverbot sowie die davon nach dem Völkerrecht bestehenden Ausnahmen. Die Frage, inwieweit die für eine Ausnahme vom Interventions- oder Gewaltverbot notwendigen Voraussetzungen erfüllt sind oder nicht, ist im Einzelfall zu prüfen. Im Hinblick auf das Verfassungsrecht und das humanitäre Völkerrecht wird auf die Antwort zur Frage 19 verwiesen.

24. *Inwieweit kann es nach Einschätzung der Bundesregierung überhaupt einen Eingriff der Bundeswehr oder anderer staatlicher Stellen, einschließlich der Nachrichtendienste, in ausländische oder gegnerische IT-Netze geben, der nicht als Souveränitätsverletzung und in der Folge als „Angriff“ zu definieren ist?*

Ob eine rechtswidrige Souveränitätsverletzung gegeben ist, kann nur im Einzelfall unter Beachtung des einschlägigen Völkerrechts und der Gesamtumstände (z.B. Zustimmung des betroffenen Staates, Vorliegen von Resolution des VN-Sicherheitsrats oder anderer Rechtfertigungsgründe) bewertet werden.

25. *Inwiefern betrachtet die Bundesregierung Aktivitäten mit dem Ziel der Informationsabschöpfung oder Spionage als Aktivitäten, die eine Reaktion von IT-Kräften oder konventionellen Kräften der Bundeswehr rechtfertigen, wenn diese Aktivitäten*
- a. von nicht-staatlichen Stellen bzw. Akteuren,*
 - b. von zivilen staatlichen Stellen bzw. Akteuren (einschließlich der Nachrichtendienste),*
 - c. von militärischen Akteuren ausgehen?*

Die Sammlung und Auswertung von Informationen über sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Inland für eine fremde Macht fallen in den durch § 1 Abs. 1 des MADG beschriebenen Zuständigkeitsbereich des Militärischen

Abschirmdienstes, wenn sich diese Tätigkeiten gegen Personen, Dienststellen oder Einrichtungen im Geschäftsbereich des Bundesministeriums der Verteidigung richten und von Personen ausgehen oder ausgehen sollen, die diesem Geschäftsbereich angehören oder in ihm tätig sind.

Darüber hinaus obliegt dem Militärischen Abschirmdienst gemäß § 1 Abs. 2 MADG zur Beurteilung der Sicherheitslage die Auswertung von Informationen über geheimdienstliche Tätigkeiten gegen Dienststellen und Einrichtungen des Geschäftsbereichs des Bundesministeriums der Verteidigung, auch soweit sie von Personen ausgehen oder ausgehen sollen, die nicht diesem Geschäftsbereich angehören oder in ihm tätig sind.

Im Übrigen wird auf die Antworten zu den Fragen 2 und 18 verwiesen.

26. *Inwiefern betrachtet die Bundesregierung Einwirkungen auf das IT-Netz als Aktivitäten, die eine Reaktion von IT-Kräften oder konventionellen Kräften der Bundeswehr rechtfertigen, wenn diese Einwirkungen*
- a. *von nicht-staatlichen Stellen bzw. Akteuren,*
 - b. *von zivilen staatlichen Stellen bzw. Akteuren (einschließlich der Nachrichtendienste),*
 - c. *von militärischen Akteuren ausgehen?*

Der Bundeswehr obliegt der Schutz der eigenen IT-Netze vor Einwirkungen unabhängig davon, von welchen Akteuren diese ausgehen.

Im Übrigen wird auf die Antwort zu Frage 25 verwiesen.

27. *Ab welchem Intensitätsgrad betrachtet die Bundesregierung Einwirkungen auf das IT-Netz als „(bewaffneten) Angriff“ im Sinne der UN-Charta, wenn diese Einwirkungen*
- a. *von nicht-staatlichen Stellen bzw. Akteuren,*
 - b. *von zivilen staatlichen Stellen bzw. Akteuren (einschließlich der Nachrichtendienste),*
 - c. *von militärischen Akteuren ausgehen?*

Um die Schwelle des bewaffneten Angriffs zu überschreiten, muss der Cyber-Angriff mit Blick auf Umfang bzw. Wirkung dem Einsatz konventioneller Waffen und kriegerischen Handlungen gleichkommen. Inwieweit eine Aktivität diese Voraussetzungen erfüllt, kann nur im Einzelfall bewertet werden.

Ob der erforderliche Intensitätsgrad im Hinblick auf den jeweiligen Akteur zu differenzieren ist, lässt sich nicht abstrakt bewerten, sondern kann nur unter Berücksichtigung aller Umstände im Einzelfall bewertet werden.

28. *Wie definiert die Bundesregierung in diesem Kontext die Begriffe „hybride Bedrohung“ und „hybride Kriegführung“?*

Der Begriff „hybride Bedrohung“ wird vornehmlich im EU-Rahmen benutzt, wohingegen die NATO von „hybrider Kriegführung“ spricht. Es handelt sich dabei um ein Phänomen, das sich nur schwer eindeutig von anderen Konfliktformen abgrenzen lässt, da eines seiner Hauptmerkmale gerade darin besteht, unterschiedliche Formen und Methoden des Konfliktaustrags und der Kriegführung miteinander zu kombinieren. „Hybride Bedrohungen“ oder „hybride Kriegführung“ können sich auf verschiedene Weise manifestieren: Die Verbindung staatlicher und nicht-staatlicher Akteure, militärischer und nicht-militärischer Mittel, asymmetrische Einsatzformen, Propaganda und Desinformation oder auch Cyberattacken und -sabotage und die Nutzung des Cyber-Informationsraums, um nur einige mögliche Elemente eines „hybriden Szenarios“ zu nennen. Häufige Begleiterscheinung „hybrider Bedrohungen“ oder „hybrider Kriegführung“ ist das Bestreben, Urheberschaft und Verantwortlichkeiten gezielt zu verschleiern und dabei Grenzen u.a. zwischen Krieg und Frieden oder auch zwischen innerer und äußerer Sicherheit zu verwischen.

29. *Welche Vorkehrungen werden getroffen, um eine "Aufrüstungsspirale" im Bereich militärischer Nutzung der IT zu vermeiden?*

Die Bundesregierung setzt sich auch international für breit getragene Verhaltensnormen zur Förderung von Sicherheit und Verfügbarkeit des Cyber-Raumes ein. Dazu begleitet die Bundesregierung Debatten in relevanten Foren im Rahmen der EU, NATO, OSZE und VN und gestaltet sie aktiv, insbesondere durch Förderung vertrauensbildender Maßnahmen.

30. *Wie beabsichtigt die Bundesregierung mit Blick auf das völkerrechtliche Gebot, Kombattanten äußerlich erkennbar und so von der Zivilbevölkerung unterscheidbar zu machen (Unterscheidungsgebot), zu gewährleisten, dass bei Cyberangriffen der Bundeswehr für die jeweiligen Gegner erkennbar wird, von wo bzw. wem der Angriff ausging (d. h., ob es sich um einen staatlichen, militärischen oder um einen von nichtstaatlichen, zivilen Akteurinnen oder Akteuren ausgehenden Angriff handelte)?*

Die Streitkräfte der Bundeswehr sind im internationalen bewaffneten Konflikt verpflichtet, sich von der Zivilbevölkerung zu unterscheiden, insbesondere durch das

Tragen von Uniform. Das völkerrechtliche Unterscheidungsgebot erfordert aber bei der Nutzung technischer Einrichtungen und Aktivitäten im Cyber-Raum nicht, die Zurechenbarkeit zu einem bestimmten Staat offen zu legen.

31. *Welche Vorstellungen hat die Bundesregierung dazu, welche Anforderungen an die Erkennbarkeit eines möglichen digitalen Angreifers zu stellen sind, um zu (nach der UN-Charta erlaubten) Selbstverteidigungsmaßnahmen gegen unter Umständen nicht eindeutig identifizierbare Angreifer zu greifen?*

Ein Staat, der das Ziel einer Cyberoperation geworden ist, die nach Umfang und Wirkung einem bewaffneten Angriff gleichkommt (vgl. hierzu die Antwort zu Frage 27), ist zur Ausübung des Rechts auf individuelle oder kollektive Selbstverteidigung berechtigt, einschließlich Cyber-Operationen gegen den Staat oder nichtstaatlichen Akteur, dem der bewaffnete Angriff zuzurechnen ist. Inwieweit eine Aktivität diese Voraussetzungen erfüllt, ist wiederum einer Bewertung im Einzelfall unterlegen.

32. *Welche Konsequenzen zieht die Bundesregierung hinsichtlich ihrer Cyberstrategie im Geschäftsbereich des BMVg und mögliche daran orientierte (auch offensive) Aktivitäten der Bundeswehr und sonstiger staatlicher Stellen aus dem Fehlen einer völkerrechtlichen Vereinbarung oder sonstigen Grundlage für „Cyber-Einsätze“ (laut Cyberstrategie existiert „kein cyber-spezifisches Völkerrecht“)?*

Die Streitkräfte können im Cyber-Raum auf Grundlage derselben völker- und verfassungsrechtlichen Regelungen, die auch ansonsten den Einsatz und die Verwendung von Streitkräften ermöglichen, eingesetzt werden. Im Übrigen wird auf die Antworten zu den Fragen 2 und 18 verwiesen.

33. *Welche Konsequenzen für ihre Cyberstrategie im Geschäftsbereich des BMVg und mögliche daran orientierte (auch offensive) Aktivitäten der Bundeswehr oder sonstiger staatlicher Stellen zieht die Bundesregierung aus dem Fehlen einer völkerrechtlichen Vereinbarung und einer Definition ab wann ein Cyberangriff ggf. die (Erheblichkeits-) Schwelle eines bewaffneten Angriffs erreicht oder überschreitet (und somit das Recht auf militärische Selbstverteidigung auslöst), sowohl*
- a. *bzgl. einer Befugnis zur „Verteidigung“ deutscher Stellen gegen Cyberangriffe, als auch,*
 - b. *bzgl. der Frage, ab welcher Intensität von der Bundeswehr oder sonstigen deutschen staatlichen Stellen ausgehende Cyberaktivitäten militärische Gewalt oder einen „bewaffneten Angriff“ i.S. der UN-Charta darstellen?*

Die Ausübung des Rechts zur individuellen und kollektiven Selbstverteidigung der Bundesrepublik Deutschland gegen Cyberangriffe richtet sich nach den allgemeinen völkerrechtlichen Grundsätzen.

Im Übrigen wird auf die Antworten zu den Fragen 27, 31 und 32 verwiesen.

34. *In welcher Form beabsichtigt die Bundesregierung sicherzustellen, dass beim Einsatz offensiver militärischer IT-"Wirkmittel" durch die Bundeswehr oder sonstige deutsche staatliche Stellen das völkerrechtliche Prinzip der Unterscheidung zwischen militärischen und zivilen Zielen eingehalten wird, und keine unterschiedslosen Angriffe ausgeführt werden, die (kritische) zivile Infrastrukturen und damit auch Zivilistinnen und Zivilisten treffen (Kollateralschäden)?*

Es werden die gleichen Verfahren angewendet wie beim Einsatz anderer militärischer Wirkmittel. Dabei wird den technischen Eigenheiten von IT-Fähigkeiten Rechnung getragen.

Auf die Antworten zu den Fragen 2, 4, 7 und 10 wird verwiesen.

35. *Inwiefern hält die Bundesregierung, angesichts der Tatsache, dass eine sichere technische oder politisch belastbare Feststellung der Urheberchaft eines Angriffs im "Cyber-Raum" und Zuordnung zu einem klar zu benennenden Angreifer nach Auffassung der Fragesteller kaum zu erbringen ist, es überhaupt für rechtlich und politisch vertretbar, auf mutmaßliche Cyber-Angriffe mit Gegenangriffen (sei es mit IT-Aktivitäten oder mit Waffengewalt) zu reagieren?*

Ob ein Cyberangriff einem Urheber zugeordnet werden kann, lässt sich nur im Einzelfall feststellen.

36. *In welcher Form beabsichtigt die Bundesregierung sicherzustellen, dass bei offensiven Cybereinsätzen der Bundeswehr oder sonstiger staatlicher Stellen der Parlamentsvorbehalt eingehalten wird?*

Der Einsatz der Bundeswehr außerhalb des Geltungsbereichs des Grundgesetzes unterliegt im Falle der Einbeziehung oder zu erwartenden Einbeziehung der eingesetzten Soldatinnen und Soldaten in bewaffnete Unternehmungen der Zustimmungspflicht durch den Bundestag nach dem Parlamentsbeteiligungsgesetz.

37. *Welche Überlegungen gibt es zur ausdrücklichen Berücksichtigung von Cyberaktivitäten im Parlamentsbeteiligungsgesetz?*

Seitens der Bundesregierung gibt es derzeit keine Überlegungen im Sinne der Fragestellung. Auf die Antwort zu Frage 36 wird verwiesen.

38. *Sollen nach Einschätzung der Bundesregierung – angesichts der Gleichstellung von staatlichen und privaten Akteuren, zivilen oder militärischen „Angreifern“ sowie von Eingriffen in militärische oder zivile Strukturen, in der von Netzpolitik dokumentierten „Strategischen Leitlinie Cyber-Verteidigung“ – die Bundeswehr oder Stellen der Bundeswehrverwaltung auch Zuständigkeiten bzgl. „Gefährdungen“ für zivile Infrastrukturen erhalten, die von nicht-militärischen Akteuren (wobei insbesondere zu berücksichtigen ist, dass es sich auch bei „Terroristen“ nicht um militärische Akteure handelt) ausgehen?*

Das Bundesamt für die Sicherheit in der Informationstechnik ist nach § 3 Abs. 1, Satz 2 Nr. 17 BSIG zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen.

39. *Auf welcher Rechtsgrundlage soll dies ggf. fußen?*

Auf die Antwort zu Frage 38 wird verwiesen.

40. *Inwiefern handelt es sich bei Einsätzen der Bundeswehr gegen von nicht-militärischen Akteuren ausgehenden „Gefährdungen“ für zivile IT-Infrastrukturen nach Einschätzung der Bundesregierung um Bundeswehr-Einsätze im Inneren?*

Gemäß Art. 35 Abs. 1 Grundgesetz leisten sich alle Behörden des Bundes und der Länder gegenseitig Amtshilfe. In diesem Rahmen kann die Bundeswehr - wie andere Behörden auch - Unterstützung leisten zur Abwehr von „Gefährdungen“ für zivile IT-Netze. Ein Einsatz der Bundeswehr liegt dabei nicht vor.

41. *Wie soll – mit Blick auf das Trennungsgebot – bei Einsätzen der Bundeswehr gegen von nicht-militärischen Akteuren ausgehende „Gefährdungen“ für zivile IT-Infrastrukturen nach Einschätzung der Bundesregierung die Trennung polizeilicher und militärischer Aufgaben, Zuständigkeiten und Strukturen gewährleistet werden, und wie soll insoweit eine Abgrenzung erfolgen?*

Die Zuständigkeiten der Sicherheitsbehörden sind in den jeweiligen Fachgesetzen geregelt.

42. *Sofern die Bundesregierung der Auffassung ist, ein „Beitrag“ der Bundeswehr oder von Stellen der Bundeswehrverwaltung „zur gesamtstaatlichen Sicherheitsvorsorge“ solle „ressortübergreifend“ (wie in der von Netzpolitik dokumentierten „Strategischen Leitlinie Cyber-Verteidigung“ dargestellt) auf der rechtlichen Grundlage der sog. Amtshilfe geleistet werden, wie gedenkt die Bundesregierung zu berücksichtigen, dass Amtshilfe entsprechend verfassungsrechtlicher Vorgaben immer nur in Ausnahmefällen und nur punktuell geleistet werden kann, um eine andere Behörde, die für anfallende Aufgaben nicht über die erforderliche*

Ausstattung verfügt, kurzzeitig zu unterstützen – nicht aber institutionell und/oder auf Dauer?

Im Geschäftsbereich des Bundesministeriums der Verteidigung schließen Dienstvorschriften aus, dass im Rahmen von Amtshilfe eine regelmäßige, auf Dauer angelegte, institutionalisierte Zusammenarbeit zwischen Bundeswehr und zivilen Behörden ohne weitere Rechtsgrundlage stattfindet.

43. *Welche Cyberwar- bzw. Cyberdefence-Projekte sind der Bundesregierung derzeit auf Ebene der EU, der NATO sowie der Mitglied- oder Partnerstaaten dieser Organisationen bekannt, und auf welchem Stand befinden sich diese jeweils?*
- a. *Mit welchen mit "Cyber-Aktivitäten" befassten Einrichtungen oder Stellen der EU bzw. der EU-Mitgliedstaaten kooperieren welche deutschen Stellen hinsichtlich derartiger Aktivitäten oder tauschen entsprechende Erkenntnisse oder Daten aus (bitte auch mitteilen, wenn dies für die Zukunft geplant ist)?*

Zur Umsetzung der Ziele des „EU-Politikrahmens für Cyber-Verteidigung“ beteiligt sich die Bundeswehr mit dem Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) im Projektteam Cyber Defence (PT CD) der European Defence Agency (EDA).

Schwerpunkte sind:

- Schutz der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP)- Kommunikationsinfrastruktur (für GSVP-Missionen und -Operationen sowie alle Strukturen, die GSVP-Informationen verarbeiten),
- Zivil-militärische Zusammenarbeit und Synergien mit anderen EU-Politikbereichen und –Akteuren,
- Training, Ausbildung und Übungen (Standards für Fähigkeitsentwicklung und Training, Pooling&Sharing von Ausbildungskapazitäten),
- Unterstützung der Mitgliedstaaten bei der Fähigkeitsentwicklung im Bereich Cyber-Verteidigung und
- Ausbau der Zusammenarbeit mit relevanten internationalen Partnern (insbesondere NATO), Wissenschaft und Wirtschaft.

Die Umsetzung des Politikrahmens für Cyber-Verteidigung erfolgt durch konkrete Einzelmaßnahmen, u.a. zur Erstellung eines gemeinsamen Cyber-Lagebildes (Projekt Cyber Situational Awareness Package) und zur Realisierung einer multinationalen Übungs- und Ausbildungsplattform (Projekt Cyber Ranges).

- b. *Mit welchen mit "Cyber-Aktivitäten" befassten Einrichtungen oder Stellen der NATO bzw. der NATO-Mitgliedstaaten kooperieren welche deutschen Stellen hinsichtlich derartiger Aktivitäten oder tauschen entsprechende Erkenntnisse oder Daten aus? (bitte auch mitteilen, wenn dies für die Zukunft geplant ist)*

Die Bundeswehr beteiligt sich an den NATO „Smart Defence“-Projekten „Cyber Defence Education and Training“ sowie „Malware Information Sharing Platform“. Das Projektmanagement für die Projekte liegt bei der NATO Communications and Information Agency (NCIA). Seitens der Bundeswehr liegt die Federführung beim BAAINBw.

- c. *Inwieweit ist nach Kenntnis der Bundesregierung eine Verschränkung der "Cyber-Aktivitäten" von NATO und EU angestrebt, und wie positioniert die Bundesregierung sich dazu?*

Sowohl die auf dem NATO-Gipfeltreffen am 4. und 5. September 2014 von den Staats- und Regierungschefs angenommene Enhanced NATO Cyber Defence Policy als auch das vom Rat der Europäischen Union (Verteidigungsminister) am 18. November 2014 verabschiedete Cyber Defence Policy Framework sehen eine stärkere Zusammenarbeit zwischen der NATO und der EU vor.

44. *Inwiefern ist – mit Blick auf die Unkompromittiertheit von Komponenten – der ausnahmslose Bezug der für die Umsetzung der Cyberstrategie benötigten IT-Hard- und Softwarekomponenten von inländischen Herstellern gewährleistet?*

Die Bundeswehr strebt an, soweit technisch möglich, bei allen für die Umsetzung der Cyberstrategie benötigten IT-Hard- und Softwarekomponenten sicherzustellen, dass diese ausschließlich von inländischen Herstellern stammen. Oftmals existiert in Deutschland die dazu erforderliche Industrie nicht (z.B. im Bereich der Fertigung von Halbleiterchips mit sehr hoher Komplexität). In solchen Fällen sind das potenzielle Risiko sowie die damit in Verbindung stehenden möglichen Konsequenzen zu bewerten. Handelt es sich um IT-Sicherheitsprodukte, die im Bereich des nationalen Geheimschutzes eingesetzt werden, erfolgte eine vorherige Prüfung und Zulassung durch das BSI. Sofern in Ausnahmefällen keine geeigneten zugelassenen IT-Sicherheitsprodukte existieren, wird im Rahmen der Umsetzung einer auf den Einzelfall bezogenen Risikoanalyse durch eine Kaskadierung von Sicherheitsmaßnahmen die Reduzierung des Sicherheitsrisikos auf ein tragfähiges Niveau angestrebt.

45. *In welcher Form werden die Sicherheit und Unkompromittiertheit von IT-Hard- oder Software-Komponenten gewährleistet werden, die aus Drittstaaten geliefert werden oder an deren Produktion oder Konzeption (staatliche oder nichtstaatliche) Akteure aus Drittstaaten beteiligt waren?*

Auf die Antwort zu Frage 44 wird verwiesen.

46. *Welches Konzept konkret verfolgt die Bundesregierung mit Blick auf IT-Hard- oder Software-Komponenten, die aus Staaten (wie den USA oder Großbritannien) bezogen werden oder an deren Produktion oder Konzeption (staatliche oder nichtstaatliche) Akteure in bzw. aus Staaten beteiligt sind, deren Geheimdienste in großem Umfang in Deutschland, auch in Form einer Ausforschung staatlicher Infrastruktur, aktiv sind?*

Unabhängig von ihrer Herkunft sollte die Integrität von IT-Sicherheitsprodukten durch ein Zertifizierungsverfahren nachgewiesen werden. Das BSI als nationale Zertifizierungsstelle hat hier in wichtigen Teilbereichen eine weltweite Führungsrolle. Die Zertifizierung von Produkten gemäß einer geeigneten Anforderungsliste ist das bevorzugte Konzept für den Nachweis unabhängig geprüfter und damit sicherer Hard- und Software.

47. *Inwiefern sollen derartige geheimdienstliche Aktivitäten und daraus potentiell resultierende Kompromittierungen von Systemkomponenten oder andere Sicherheitslücken bei einer gemeinsamen Nutzung von IT-Einrichtungen zur Kommunikation mit und Steuerung von (Waffen-) Systemen, auch z. B. mit Blick auf multinationale Einsätze, Berücksichtigung finden?*

Die Sicherheit der IT in Waffensystemen wird bei der Konzeption, Entwicklung und Nutzung entsprechend des jeweiligen Schutzbedarfs der mit der IT verarbeiteten, übertragenen und gespeicherten Information umfänglich berücksichtigt. Sie ist konkreter Bestandteil des Materialentstehungsprozesses in der Bundeswehr. Ein wichtiger Faktor ist dabei – nicht zuletzt zur Wahrnehmung von Gewährleistungsansprüchen – die jeweilige Festschreibung und Überwachung des Konstruktions- und Konfigurationsstandes bzw. des Patchstandes.

48. *In welcher Höhe beabsichtigt die Bundesregierung im Kontext des Cybersicherheitskonzepts und der Cyberstrategie in den Jahren 2016 bis 2020 Haushaltsmittel aufzuwenden (bitte nach Haushaltsjahren und unter konkreter Angabe der jeweiligen Einzelpläne und Titel aufschlüsseln)?*

Das BMVg plant derzeit, die Bundeswehrstrukturen anzupassen, um den heutigen und zukünftigen Bedrohungen im Cyber-Raum optimal begegnen zu können. Dazu wird derzeit ein Vorschlag zur Ausgestaltung des Gesamtbereichs Cyber erarbeitet.

49. *Inwiefern wird von der Bundesregierung im Kontext des Cybersicherheitskonzepts und der Cyberstrategie eine Zusammenarbeit mit Universitäten, sonstigen Forschungseinrichtungen sowie der Wirtschaft oder Industrie auf dem Gebiet Forschung und Entwicklung befürwortet, geplant oder in Erwägung gezogen?*

Die mögliche Zusammenarbeit mit Universitäten, sonstigen Forschungsrichtungen oder der Wirtschaft ist Gegenstand der laufenden Überlegungen. Diese Frage befindet sich derzeit in der ressortübergreifenden Abstimmung.

50. *Inwiefern beabsichtigt die Bundesregierung, mit dem Cybersicherheitskonzept und der Cyberstrategie auch Ansätze zur Industrie- bzw. Wirtschaftsförderung in Schlüsseltechnologien zu verbinden?*

Die Bundesregierung beabsichtigt mit der "Cyber-Sicherheitsstrategie für Deutschland" die Stärkung der technologischen Souveränität und wissenschaftlichen Kapazität in Deutschland und Europa über die gesamte Bandbreite strategischer IT-Kernkompetenzen. Mit dem Strategiepapier zur Stärkung der Verteidigungsindustrie hat die Bundesregierung wehrtechnische Schlüsseltechnologien u.a. auch im Bereich Cyber und IT definiert. In der Folge beabsichtigt die Bundesregierung, ihre Anstrengungen zur Förderung verteidigungsrelevanter Technologien u.a. im Bereich Cyber/IT auf nationaler und europäischer Ebene zu erhöhen. Der Förderung mittelständischer Unternehmen wird dabei besonderes Augenmerk gewidmet werden. Die Ausgestaltung ist Gegenstand laufender Abstimmungen.