Deutscher Bundestag **Drucksache 18/6496**

18. Wahlperiode 16.10.2015

Kleine Anfrage

der Abgeordneten Dr. Alexander S. Neu, Andrej Hunko, Wolfgang Gehrcke, Christine Buchholz, Annette Groth, Heike Hänsel, Inge Höger, Katrin Kunert, Kathrin Vogler und der Fraktion DIE LINKE.

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

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 (gegebenenfalls 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 sich 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 (BMVg) 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 die 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 dessen 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 „Angreifern“ um staatliche oder private, zivile oder militärische Akteure handelt.

Die Cyberstrategie des BMVg bezieht sich zwar nominal auf die Cybersicherheitsstrategie des Bundesministeriums des Innern (BMJ), 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“.

Wir fragen die Bundesregierung:

1. Mit welchen „Wirkmöglichkeiten“ und „Wirkmitteln“ für den Cyberwar soll die Bundeswehr nach den Vorstellungen der Bundesregierung ausgerüstet werden, um „eigene Wirkung zu entfalten“?
2. Unter welchen Voraussetzungen soll die Bundeswehr nach Vorstellung der Bundesregierung offensive Cyber-Fähigkeiten einsetzen dürfen?
3. Inwieweit wird angestrebt, Cyber-Fähigkeiten neben oder anstelle anderer Waffen einzusetzen (komplementär bzw. ergänzend, unterstützend oder substituierend)?
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“?
5. Inwiefern sollen auch Trojaner bzw. Malware sowie Stealth-Techniken zum Einsatz kommen?
6. Inwiefern sollen die Bundeswehr oder sonstige staatliche Stellen auch letale bzw. letal wirkende Cyberangriffe 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)?

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?
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“ (Netzpolitk vom 30. Juli 2015)?
9. Wie ist nach Einschätzung der Bundesregierung ein „präzises“, „punktgenaues“ Einwirken auf nicht selbst kontrollierte IT-Netzwerke realisierbar?
10. Inwiefern und gegebenenfalls 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?
11. Bezüglich welcher Staaten soll im Sinne der Cyberstrategie ein „Lagebild über die Fähigkeiten, Verwundbarkeiten und möglichen Angriffsvektoren“ erstellt werden?
12. Inwiefern handelt es sich dabei um Staaten, die als „Gegner“ betrachtet werden?
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)?
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?
15. Welche Programme oder Szenarien sollen auf Basis dieser Erkenntnisse und Daten erstellt oder erarbeitet werden?
16. Mit welchen Verfahren sollen die Erkenntnisse und Daten in nicht selbst betriebenen Netzen gesammelt werden?
17. Auf welcher rechtlichen Grundlage sollen in nicht selbst betriebenen Netzen Erkenntnisse und Daten gesammelt werden?
18. Welche Rechtsgrundlage legitimiert gegebenenfalls nach Einschätzung der Bundesregierung Eingriffe der Bundeswehr oder sonstiger staatlicher Stellen in die IT-Infrastruktur anderer Staaten (bitte konkret bezeichnen, gegebenenfalls unter Angabe des einschlägigen Gesetzes, der völkerrechtlichen Vereinbarung bzw. des Rechtsinstituts)?
19. Wo liegt im "Cyber-Raum" die Grenze (technisch und rechtlich) zwischen Verteidigung und Angriff?
20. Gab es bislang Aktivitäten der Bundeswehr oder sonstiger deutscher Stellen, bei denen mit Cyber-Fähigkeiten in fremde oder gegnerische Netze bzw. IT-Systeme eingegriffen wurde, und wenn ja, welche?
21. Welche offensiven und defensiven Szenarien werden bzw. wurden in der Vergangenheit von der Bundeswehr oder sonstigen deutschen Stellen bereits geübt?

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?

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 gegebenenfalls die Grenze ab der ein derartiges Vorgehen zum Angriff wird?

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, welcher nicht als Souveränitätsverletzung und in der Folge als „Angriff“ zu definieren ist?

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?

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?

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?

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

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

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, sodass

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)?

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?

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“)?

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 gegebenenfalls 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?

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)?

35. Inwiefern hält die Bundesregierung, angesichts der Tatsache, dass eine sichere technische oder politisch belastbare Feststellung der Urheberschaft 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 Cyberangriffe mit Gegenangriffen (sei es mit IT-Aktivitäten oder mit Waffengewalt) zu reagieren?

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

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

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 bezüglich „Gefährdungen“ für zivile Infrastrukturen erhalten,

die von nicht-militärischen Akteuren (wobei insbesondere zu berücksichtigen ist, dass es sich bei „Terroristen“ nicht um militärische Akteure handelt) ausgehen?

39. Auf welcher Rechtsgrundlage soll dies gegebenenfalls fußen?

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

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?

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 sogenannten Amtshilfe geleistet werden, wie gedenkt die Bundesregierung zu berücksichtigen, dass die Bundeswehr 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?

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)?

    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)?

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

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

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 nichtsstaatliche) Akteure aus Drittstaaten beteiligt waren?

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 nichtsstaatliche) Akteure in bzw. aus Staaten beteiligt sind, deren Geheimdienste in großem Umfang in Deutschland, auch in Form einer Ausforschung staatlicher Infrastruktur, aktiv sind?

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?

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)?

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 von Forschung und Entwicklung befürwortet, geplant oder in Erwägung gezogen?

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

Berlin, den 16. Oktober 2015

Dr. Sahra Wagenknecht, Dr. Dietmar Bartsch und Fraktion

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