Deutscher Bundestag **Drucksache 18/3963**

18. Wahlperiode 06.02.2015

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Jan van Aken, Andrej Hunko, Christine Buchholz, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/3799 –

Elektronische Kampfführung der Bundeswehr

Vorbemerkung der Fragesteller

Laut Angaben der Bundesregierung hat die Bundeswehr bereits im Jahr 2007 die Gruppe „Computer Netzwerk Operationen“ (CNO) innerhalb des Kommandos Strategische Aufklärung eingerichtet (vgl. Mündliche Frage 8 des Abgeordneten Andrej Hunko vom 19. Februar 2014, Plenarprotokoll 18/16). In der Ausgabe 02/2014 der Zeitschrift „Technology Report“ gibt der Leiter dieser Spezialeinheit einen Einblick in die Arbeit der dort tätigen Mitarbeiterinnen und Mitarbeiter (www.heise.de/tr/artikel/Die-deutschen-Cyber-Krieger-2192518.html).
Demnach ist die CNO grundsätzlich auch zu offensiven Operationen in der Lage und führt diese durch, unter anderem durch den Einsatz von „Stealth-Techniken“, durch die Angriffe und Angriffsversuche getarnt werden. Ob und wie derartige Operationen durchgeführt werden, hänge lediglich von politischen Willensbildungsprozessen ab.

Vorbemerkung der Bundesregierung

Als Hintergrund zur Beantwortung der Anfrage wird auf den Bericht zum Themenkomplex Cyber-Verteidigung vom 12. September 2012 – VS – Nur für den Dienstgebrauch –, übermittelt an die Vorsitzende des Verteidigungsausschusses am 21. September 2012, und die Beratung im Verteidigungsausschuss am 30. Januar 2013 verwiesen. Auf Wunsch der Mitglieder des Verteidigungsausschusses wurde dieser Bericht im Einstufungsgrad – offen – am 26. April 2013 an die Vorsitzende des Verteidigungsausschusses übermittelt, um den Fraktionen des Deutschen Bundestages den freien Zugang zu ermöglichen.

1. Welche sind die rechtlichen Grundlagen von Operationen der Einheit CNO?

Die rechtlichen Grundlagen für Einsätze und Verwendungen der Streitkräfte unterscheiden sich nicht im Hinblick auf unterschiedliche Fähigkeiten. Grund-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Verteidigung vom 5. Februar 2015 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

lagen sind die einschlägigen Regelungen des Völkerrechts, des Grundgesetzes und das Parlamentsbeteiligungsgesetz.

2. Verfügt oder verfügte die Einheit über etwaige Sonderrechte für geplante und bzw. oder durchgeführte Einsätze?

   Wenn ja, welche und mit welcher konkreten Begründung wurden diese wann verliehen?

Nein. Ergänzend wird auf die Antwort zu Frage 1 verwiesen.

3. Welchem Kommando ist die CNO unterstellt, und welche Rücksprachen, Befehlswege und Unterrichtungsroutinen mit politischen Entscheidungsträgern der Bundesregierung gibt es?

Die CNO-Kräfte sind dem Kommando Strategische Aufklärung unterstellt. Ein Einsatz erfolgt unter denselben rechtlichen Rahmenbedingungen wie der Einsatz anderer militärischer Wirkmittel. In jedem Fall geht dem möglichen Einsatz eine umfangreiche Prüfung politischer, rechtlicher und operativer Faktoren voraus.

4. Inwiefern lassen sich die grundsätzlichen rechtlichen Vorgaben für die Einheit CNO für die Durchführung von offensiven Cyberangriffen nutzen?

Es wird auf die Antwort zu Frage 1 verwiesen.

5. Welches sind nach Einschätzung der Bundesregierung grundsätzlich legitime Ziele von Cyberangriffen der Einheit CNO?

Als legitime militärische Ziele in einem bewaffneten Konflikt kommen grundsätzlich nur solche Objekte in Betracht, die aufgrund ihrer Beschaffenheit, ihres Standorts, ihrer Zweckbestimmung oder ihrer Verwendung wirksam zu militärischen Handlungen beitragen und deren gänzliche oder teilweise Zerstörung, deren Inbesitznahme oder Neutralisierung unter den im betreffenden Zeitpunkt des Angriffs gegebenen Umständen einen eindeutigen militärischen Vorteil darstellen.

6. Wie viele und welche Angriffe durch verbündete Staaten der Bundesrepublik Deutschland wurden seit Bestehen der Einheit durch diese unterstützt, bzw. an welchen Angriffen beteiligte sie sich (bitte Einsatzziel, Einsatzdatum und durchführenden Hauptakteur angeben)?

Es gab weder Unterstützung noch Beteiligung der CNO-Kräfte bei eventuellen Angriffen verbündeter Staaten.

7. Welcher der bisherigen Einsätze der CNO ist nach Einschätzung der Bundesregierung durch ein bestehendes Mandat des Deutschen Bundestages zum Einsatzzeitpunkt gedeckt gewesen (bitte Einsatz, Zeitpunkt und entsprechendes Mandat angeben)?

8. Für welchen Einsatz hat die Bundesregierung keine Mandatierung der Spezialeinheit CNO laut Parlamentsbeteiligungsgesetz beantragt, und aus welchen Gründen wurde hiervon ggf. abgesehen?

9. Was sind seit Bestehen der Einheit Ziele von Cyberangriffen der Einheit CNO geworden (bitte Einsatzziel und Einsatzdatum angeben)?

Die Fragen 7, 8 und 9 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Die CNO-Kräfte wurden bisher nicht eingesetzt.

10. Welche weiteren Einheiten bestehen bei Bundeswehr, Nachrichtendiensten oder anderen Einrichtungen des Bundes, die in der Lage sind, offensive Operationen der elektronischen Kriegsführung bzw. Sabotage durchzuführen?

11. Welche offensiven Operationen durch Einheiten, die nicht Bestandteil der CNO sind, haben auf welcher rechtlichen Grundlage seit dem Jahr 2000 stattgefunden (bitte Einheit, Datum und Angriffsziel angeben)?

Die Fragen 10 und 11 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Es gibt keine Einheiten der deutschen Sicherheitsbehörden zur Durchführung elektronischer Kriegsführung und Sabotage. Die CNO-Kräfte sind die einzigen Kräfte der Bundeswehr zum Wirken gegen und in gegnerischen Netzen in bewaffneten Konflikten.

12. In welchen Fällen waren Angehörige der Spezialeinheit CNO oder anderer Einheiten außerhalb von Deutschland an der Ausführung von defensiven Operationen im Einsatz beteiligt (bitte Einsatzzeitraum, Einsatzort, Operationsbeschreibung und Anzahl von eingesetztem Personal angeben)?

Der Schutz der IT-Systeme der Bundeswehr im In- und Ausland einschließlich in den Einsatzgebieten der Bundeswehr wird durch ständige Maßnahmen der IT-Sicherheit gewährleistet, die durch die IT-Sicherheitsorganisation vorgegeben und überwacht werden. Die Implementierung und Überwachung von IT-Sicherheitsmaßnahmen in den Einsatzgebieten ist Bestandteil der Aufgaben der vor Ort befindlichen Kräfte. Diese werden durch Kräfte im Wesentlichen des Computer Emergency Response Teams der Bundeswehr (CERTBw) aus Deutschland heraus und bei Bedarf im Einsatzgebiet unterstützt.

Eine Unterstützung durch CNO-Kräfte zur Wiederherstellung der IT-Sicherheit in den betroffenen IT-Systemen fand bislang im Einsatz nicht statt.

13. In welchen Fällen waren Angehörige der Spezialeinheit CNO oder anderer Einheiten außerhalb von Deutschland an der Ausführung von offensiven Operationen im Einsatz (bitte Einsatzzeitraum, Einsatzort, Operationsbeschreibung und Anzahl von eingesetztem Personal angeben)?

Es wird auf die Antworten zu den Fragen 7 und 10 verwiesen.

14. Schließt die Bundesregierung aus, dass durch Cyberangriffe deutscher Soldaten bzw. Angehöriger der Einheit CNO unbeteiligte Zivilisten bzw. Personen zu Schaden gekommen sind?

15. Wie viele feindliche Kämpferinnen und Kämpfer, Soldatinnen und Soldaten und wie viel feindliches Militärpersonal sind seit Bestehen der Einheit CNO durch von ihr ausgeführte Cyberangriffe zu Schaden gekommen?

16. In welchen Fällen ist es zu Schäden an nichtmilitärischer und bzw. oder ziviler Infrastruktur gekommen (bitte Einheit, Datum, Angriffsziel und Schadensbeschreibung angeben)?

Die Fragen 14 bis 16 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Auf die Antwort zu Frage 7 wird verwiesen.

17. Wie beabsichtigt die Bundesregierung grundsätzlich, Schäden an unbeteiligten Personen und/oder Zivilisten sowie an nichtmilitärischer, ziviler In frastruktur durch Cyberangriffe zu vermeiden?

18. Wie wird vonseiten der Bundesregierung sichergestellt, dass keine Ziele mit völkerrechtlichen Schutzzeichen durch einen Cyberangriff beschädigt bzw. zerstört werden?

Die Fragen 17 und 18 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Es wird nach den grundsätzlich geltenden Regeln zur Vermeidung dieser Schäden wie bei anderen Wirkmitteln verfahren. Dabei werden die besonderen Aspekte des Cyber-Raums berücksichtigt.

19. Strebt die Bundesregierung den Ausbau der elektronischen Kriegsführungsfähigkeiten – insbesondere die der Einheit CNO – an (bitte finanzielle, personelle und logistische Konsequenzen dieser Bestrebungen konkret angeben)?

Es gibt keine Planungen, die sich nach diesen Kriterien konkretisieren lassen.

20. Betrachtet die Bundesregierung die Einsatzmittel der Spezialeinheit als Wirkmittel im Sinne von Waffensystemen, die dazu beschafft und vorbereitet werden, bei ihrem Einsatz die Handlungsfähigkeit eines Gegners (nachhaltig) zu beeinträchtigen oder zu eliminieren?

21. Wenn nein, wie lautet die grundsätzliche Definition dieser offensiven Wirkmittel durch die Bundesregierung?

Die Fragen 20 und 21 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Die CNO-Kräfte werden als militärische Wirkmittel betrachtet. CNO-Kräfte sind dazu aufgestellt, im Rahmen des verfassungsgemäßen Auftrages der Bundeswehr Fähigkeiten zum Wirken im Cyber-Raum bereitzustellen.

22. Welche rechtlichen und/oder völkerrechtlichen Implikationen besitzen diese Definitionen von Wirkmitteln der elektronischen Kriegsführung nach Einschätzung der Bundesregierung?

Auf die Antworten zu den Fragen 1 und 5 wird verwiesen.

23. Sind die bei der Spezialeinheit CNO tätigen Mitarbeiterinnen und Mitarbeiter sowie Soldatinnen und Soldaten nach Einschätzung der Bundesregierung Kombattanten im Sinne des Völkerrechts, wenn sie sich an offensiven Angriffen beteiligen, und wenn nein, warum nicht?

Der Kombattantenstatus ist grundsätzlich auf Angehörige der Streitkräfte in internationalen bewaffneten Konflikten begrenzt. Sofern CNO-Kräfte, die im Rahmen eines internationalen bewaffneten Konflikts, in dem Deutschland Konfliktpartei ist, eingesetzt werden, sind diese als Kombattanten zu qualifizieren.

24. Wenn ja, tragen die bei der Spezialeinheit CNO tätigen Mitarbeiterinnen und Mitarbeiter sowie Soldatinnen und Soldaten die für Kombattanten im Sinne des Völkerrechts üblichen hoheitlichen Abzeichen der Bundesrepublik Deutschland sichtbar an ihrer Arbeitskleidung bzw. Uniform?

Ja. Zum Kombattantenbegriff wird auf die Antwort zu Frage 23 verwiesen.

25. Werden im Falle offensiver Angriffe oder Abwehrmaßnahmen technische Einrichtungen genutzt, die sicherstellen, dass die hoheitliche Zugehörigkeit der bei der Spezialeinheit CNO tätigen Mitarbeiterinnen und Mitarbeiter sowie Soldatinnen und Soldaten gegenüber dem Gegner sichtbar und erkennbar ist (bitte technische Einrichtungen, Maßnahmen etc. angeben)?

Nein. Ein Unterscheidungserfordernis analog zur Kennzeichnungspflicht von Kombattanten (vgl. dazu die Antwort zu Frage 24) besteht für technische Einrichtungen nicht.

26. Wurden Fähigkeiten, Aufgaben und Kapazitäten der Spezialeinheit CNO oder Teile davon an private Auftragnehmer ausgelagert (bitte den Zeitpunkt, die Arbeitsbereiche und die Auftragnehmer nennen)?

27. Bestehen aufseiten der Bundesregierung oder der Bundeswehr Pläne, Fähigkeiten, Aufgaben und Kapazitäten der Spezialeinheit CNO oder Teile davon an private Auftragnehmer auszulagern (bitte den geplanten Zeitpunkt, die konkreten Arbeitsbereiche und den Auftragnehmer nennen)?

28. Wie ist nach Einschätzung der Bundesregierung die völkerrechtliche Einordnung von Mitarbeiterinnen und Mitarbeitern privater Unternehmen, die ausgelagerte Fähigkeiten, Aufgaben und Kapazitäten der Spezialeinheit CNO oder Teile davon übernehmen?

29. Sind die Mitarbeiterinnen und Mitarbeiter privater Unternehmen, die ausgelagerte Fähigkeiten, Aufgaben und Kapazitäten der Spezialeinheit CNO oder Teile davon übernehmen, nach Einschätzung der Bundesregierung völkerrechtlich als Kombattanten zu betrachten?

Die Fragen 26 bis 29 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Nein.

30. Sind sogenannte Stealth-Techniken zur Tarnung von Cyberangriffen grundsätzlich dazu geeignet, über die Zugehörigkeit von Akteuren zu einer bestimmten Konfliktpartei zu täuschen?

Ja.

31. Werden durch Einheiten der Bundeswehr zur elektronischen Kriegsführung wie der CNO sogenannte Stealth-Techniken zur Tarnung von Cyberangriffen eingesetzt?

Stealth-Techniken sind Tarnungstechniken und damit den völkerrechtlich grundsätzlich erlaubten Kriegslisten zuzuordnen. Bislang wurden keine Cyber-Angriffe durch die Bundeswehr durchgeführt.

32. Wie beurteilt die Bundesregierung grundsätzlich den Einsatz von sogenannten Stealth-Techniken zur Tarnung über die Zugehörigkeit von Akteuren vor dem Hintergrund des völkerrechtlichen Perfidieverbots?

33. Unter welchen Umständen sind nach Auffassung der Bundesregierung sogenannte Stealth-Techniken grundsätzlich Verstöße gegen das völkerrechtliche Perfidieverbot?

Die Fragen 32 und 33 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Die Nutzung so genannter Stealth-Techniken verletzt das Heimtückeverbot nicht, da ihr Einsatz keine Handlung darstellt, durch die ein Gegner in der Absicht, sein Vertrauen zu missbrauchen, verleitet wird, darauf zu vertrauen, dass er nach den Regeln des in bewaffneten Konflikten anwendbaren Völkerrechts Anspruch auf Schutz hat oder verpflichtet ist, Schutz zu gewähren.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333