Deutscher Bundestag **Drucksache 19/9592**

19. Wahlperiode 23.04.2019

Kleine Anfrage

der Abgeordneten Dr. Alexander S. Neu, Heike Hänsel, Andrej Hunko, Christine Buchholz, Zaklin Nastic, Tobias Pflüger, Helin Evrim Sommer und der Fraktion DIE LINKE.

Fähigkeiten der „Cyber-Truppe“ der Bundeswehr

Der „Cyber-Raum“ gehört in den letzten Jahren zu den heißen Themen der Militärberichterstattung (http://augengeradeaus.net/2018/10/cyber-cyber-die-meldungen-nur-eines-tages/#more-31555).

Dabei bleibt nicht nur die Gewinnung geeigneter IT-Kräfte schwierig und die Definition der Einsatzspektren vage. Wie beim Einsatz militärischer IT-Kräfte das Völkerrecht eingehalten werden kann, z. B. was die verlässliche Attribution von Angriffen und die klare Unterscheidung ziviler und militärischer Angriffsziele angeht, ist noch nicht erkennbar. Bis jetzt fehlt es außerdem an einer nachvollziehbaren Darstellung, inwieweit die Bundesregierung gewährleisten kann, dass bei einem Einsatz ihrer „Cyber-Krieger“ der verfassungsrechtliche Parlamentsvorbehalt nicht verletzt wird – und das nicht nur dann, wenn es darum geht, bereits vor einem Bundeswehreinsatz fremde Netze zu infiltrieren. In keinem Mandatsantrag der Bundesregierung fand bislang der Einsatz von IT-Kräften bei Bundeswehreinsätzen auch nur Erwähnung.

Wir fragen die Bundesregierung:

1. Welche Einsätze von IT-Kräften der Bundeswehr, insbesondere der CNO-Einheit sowie deren Nachfolgeinstitutionen, wie dem Zentrum Cyber-Operationen, gab es seit Gründung der CNO (Computer-Netzwerk-Operationen) im Jahr 2006?
2. Welche Kräfte innerhalb des Kommando CIR (Cyber- und Informationsraum) sind für die kontinuierliche Lagebildaufklärung im „Cyber-Raum“ zuständig?
3. Welche anderen Bereiche bzw. Einheiten der Bundeswehr sowie externer Stellen wie beispielsweise der Nachrichtendienste sind an der Lagebildaufklärung im „Cyber-Raum“ beteiligt, und in welchem Umfang?
4. Inwieweit werden im Rahmen der Vorfeldaufklärung in Friedenszeiten bzw. außerhalb nur im bewaffneten Konflikt geltender spezifischer Befugnisse auch fremde IT-Systeme analysiert?
5. Wodurch wird dabei der völkerrechtlich gebotenen Differenzierung zwischen staatlichen und privaten Akteuren bzw. IT-Systemen Rechnung getragen?

6. Welche Kooperationen von IT-Kräften der Bundeswehr, des Kommando CIR, der CNO-Einheit sowie deren Nachfolgeinstitutionen wie dem Zentrum Cyber-Operationen mit anderen deutschen staatlichen Stellen bzw. Nachrichtendiensten gab und gibt es?

   In welchen Anteilen wurden und werden hier welche Aufgaben erfüllt, und zu welchen Zwecken?

7. Inwieweit wurden und werden durch IT-Kräfte der Bundeswehr, das Kommando CIR, die CNO-Einheit sowie deren Nachfolgeinstitutionen wie das Zentrum Cyber-Operationen oder andere Stellen im Geschäftsbereich des Bundesministeriums der Verteidigung Exploits bzw. Schwachstellen in IT-Produkten (Soft- und Hardware) mit dem Ziel der Ausnutzung dieser Schwachstellen für Aufklärung oder offensives Wirken im „Cyber-Raum“

   a) eigenständig gesucht,

   b) angekauft (bitte unter nachvollziehbarer, präziser Angabe der zugrunde gelegten Haushaltstitel auflisten) bzw.

   c) durch Kooperationen mit anderen Diensten oder Staaten bereitgestellt?

8. Inwieweit existiert derzeit eine Praxis im Geschäftsbereich des Bundesverteidigungsministeriums und nachgeordneter Stellen, erkannte Schwachstellen in IT-Produkten (Soft- und Hardware) zu melden bzw. veröffentlichen?

9. Inwieweit und unter welchen Bedingungen werden Sicherheitslücken – sofern sie verwendet werden – zurückgehalten für eine spätere Nutzung?

   Inwiefern findet ein kontinuierlicher Prozess der Abwägung über deren Veröffentlichung statt (im Sinne eines Vulnerabilities Equities Process)?

10. Welche Ansätze im Zuständigkeitsbereich der gesamten Bundesregierung gibt es, im Interesse der IT-Sicherheit darauf hinzuwirken, dass

    a) ausnahmslos alle bekannt werdenden Sicherheitslücken gemeldet und geschlossen werden und nicht zur Infiltration von Netzen genutzt werden dürfen, und

    b) an diese Verpflichtungen auch staatliche Stellen – einschließlich Geheimdiensten und Stellen im Geschäftsbereich des Bundesverteidigungsministeriums und nachgeordneter Behörden – gebunden werden, d. h. die Meldepflichten auch für diese gelten und ihnen die Nutzung von Exploits bzw. Schwachstellen untersagt wird?

11. Welche Kooperationen oder Bedarfsmeldungen gibt es seitens des Kommando CIR an die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) sowie an die neue Agentur für Innovation in der Cybersicherheit?

12. Welche Einsatzszenarien wurden und werden durch die CNO-Einheit sowie deren Nachfolgeinstitutionen wie das Zentrum Cyber-Operationen geübt?

    Für welche strategischen Aufgaben und Ziele planen diese IT-Kräfte?

13. Welche Einheiten im Geschäftsbereich des Bundesverteidigungsministeriums außer der CNO-Einheit sowie deren Nachfolgeinstitution Zentrum Cyber-Operationen verfügen über Fähigkeiten zum „Wirken im Cyber-Raum“?

14. In welchem quantitativen und qualitativen Verhältnis steht bei der Aus- oder Fortbildung von IT-Kräften, im Kommando CIR, bei der CNO-Einheit sowie deren Nachfolgeinstitutionen wie dem Zentrum Cyber-Operationen der Bundeswehr das Vermitteln offensiver Fähigkeiten und Fähigkeiten zum „Wirken in fremden Netzen“ zum Erwerb und der Vermittlung von Fähigkeiten zur Härtung von IT-Systemen?

15. Inwieweit und konkret durch welche Verfahrensschritte wird bei der Auswahl von Bewerberinnen und Bewerbern, der Nachqualifikation von Mannschaften und der Ausbildung aller (zukünftigen) IT-Kräfte im Geschäftsbereich des Bundesverteidigungsministeriums darauf geachtet und sichergestellt, dass diese qualifiziertes Fachwissen über Stabilität, Sicherheit, Zuverlässigkeit von IT-Systemen und auch darüber besitzen bzw. erwerben, wie typische Angriffe auf die IT-Infrastruktur funktionieren und wie Hard- und Software schon bei der Entwicklung dagegen geschützt werden kann?

16. Welche Planungen – sowohl personell als auch hinsichtlich technischer Fähigkeiten – gibt es im Kommando CIR über 2021 hinaus?

17. Inwieweit ist beabsichtigt, das Parlament über die offensiven Fähigkeiten bzw. Fähigkeiten zum „Wirken im Cyber-Raum“ zu unterrichten, die erworben werden durch IT-Kräfte der Bundeswehr, das Kommando CIR, die CNO-Einheit sowie deren Nachfolgeinstitutionen wie das Zentrum Cyber-Operationen oder andere Stellen im Geschäftsbereich des Bundesverteidigungsministeriums?

    In welcher Form und in welchem Detailumfang?

18. In welcher Form konkret ist eine Beteiligung des Parlaments vor dem Einsatz offensiver Fähigkeiten bzw. Fähigkeiten zum „Wirken im Cyber-Raum“ durch IT-Kräfte der Bundeswehr, das Kommando CIR, die CNO-Einheit sowie deren Nachfolgeinstitutionen wie das Zentrum Cyber-Operationen oder andere Stellen im Geschäftsbereich des Bundesverteidigungsministeriums realisiert oder beabsichtigt?

19. Welche Fähigkeiten aus dem IT-Bereich sollen der NATO zur Verfügung gestellt werden (vgl. www.zeit.de/news/2019-02/14/deutschland-stellt-nato-mittel-fuer-militaerische-cyber-einsaetze-zur-verfuegung-20181004-doc-19r778)?

Berlin, den 12. April 2019

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