Bundesministerium
der Verteidigung

Ludwig Leinhos
Leiter Aufbaustab CIR

HAUSANSCHRIFT Stauffenbergstraße 18, 10785 Berlin
POSTANSCHRIFT 11055 Berlin

TEL +49 (0)30 18-24-70130
FAX +49 (0)30 18-24-
E-MAIL BMVgAufbaustabCIR@bmvg.bund.de

-1880066-V459-

Bundesministerium der Verteidigung, 11055 Berlin

Deutscher Bundestag
Petitionsausschuss
Referat Pet 1
OAR'in Martina Swanson
Platz der Republik 1

11011 Berlin

BETREFF **Eingabe der Teilnehmer der 44.0ten Konferenz der Informatikfachschaften, Techn. Universität Darmstadt, 64289 Darmstadt, vom 12. Mai 2016 (Petition Nr.: 1-18-14-553-032622)**

BEZUG 1. Schreiben Deutscher Bundestag – Petitionsausschuss vom 6. Juni 2016

Berlin, 18. Juli 2016

Sehr geehrte Frau Swanson,

für Ihr Schreiben vom 6. Juni 2016, in dem Sie um Stellungnahme zur Petition der Teilnehmer/innen der "44,0ten Konferenz der Informatikfachschaften, Technische Universität Darmstadt" (KIF 44,0) bitten, danke ich Ihnen. In ihrer Petition fordert die KIF 44,0,

- dass Deutschland auf eine offensive Cyberstrategie verzichtet,
- dass sich Deutschland verpflichtet, keine Cyber-Waffen zu entwickeln, zu beschaffen und zu verwenden und
- dass internationale Abkommen zu einem weltweiten Bann von Cyber-Waffen angestrebt werden.

Das Bundesministerium der Verteidigung (BMVg) nimmt hierzu wie folgt Stellung:

Die Verfügbarkeit des Cyber-Raums und die Integrität, Authentizität und Vertraulichkeit der darin vorhandenen Daten sind zu einer bestimmenden Frage des 21. Jahrhunderts geworden. Wie die anderen Dimensionen Land, Luft, See und Weltraum weist auch der Cyber-Raum eine verteidigungspolitische und militärische Dimension

auf. Internationale bzw. grenzüberschreitend relevante Konflikte werden zunehmend auch im Cyber-Raum ausgetragen. Damit muss sich auch die Bundesrepublik Deutschland auf Angriffe im und durch den Cyber-Raum einstellen.
Die Bedenken des Petenten in Bezug auf die IT-Sicherheit von „IT-Systemen" sind bereits durch das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), welches im Juli 2015 in Kraft getreten ist, aufgegriffen worden. Das IT-Sicherheitsgesetz leistet einen Beitrag dazu, die IT-Systeme und digitalen Infrastrukturen Deutschlands zu den sichersten weltweit zu machen.
Hinsichtlich der Bedenken des Petenten, dass Know-How beim Militär ohne Nutzen für die Zivilgesellschaft gebündelt würde, ist entgegenzuhalten, dass angesichts der steigenden Cyber-Gefahren die Bundesbehörden, die sich mit den relevanten Facetten dieses Themas beschäftigen, enger zusammenarbeiten. Hierzu wurde unter der Federführung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) das gemeinsame Cyber-Abwehrzentrum (Cyber-AZ) geschaffen.
Die Cyber-Sicherheitsstrategie für Deutschland erkennt an, dass hinter Cyber-Angriffen auch militärische Operationen stehen können. Dem Cyber-Raum wird somit zunehmend operative Bedeutung bei militärischen Auseinandersetzungen aller Art zukommen.
Die Bundeswehr ist dabei auf drei unterschiedlichen Ebenen betroffen:

1. Vergleichbar jeder anderen öffentlichen und zivilen Institution nutzt die Bundeswehr den Cyber-Raum und informationstechnische Systeme im täglichen Dienstbetrieb und hat somit die Sicherheit und Funktionsfähigkeit des IT-Systems der Bundeswehr zu gewährleisten.
2. Der Bundeswehr obliegt der verfassungsrechtliche Auftrag zur Verteidigung der Bundesrepublik Deutschland und ihrer Bürger.
3. Angesichts der Abhängigkeit moderner Waffensysteme und militärischer Kommunikationsmittel vom Cyber-Raum müssen diese zur Gewährleistung eigener Handlungs- und Führungsfähigkeit zuverlässig verfügbar sein. Gegnerische Maßnahmen gegen diese Funktionen und Komponenten sind daher möglichst vorbeugend zu verhindern oder abzuschwächen.

Für die Bundeswehr steht folglich zunächst der Schutz der eigenen IT-Systeme und Netzwerke im Vordergrund und ihre Strategie ist daher entsprechend den Grundsätzen der Gesamtverteidigung der Bundesrepublik Deutschland **defensiv ausgerichtet**. Da jedoch auch ein militärischer Gegner von der Nutzung des Cyber-Raums ab-

hängig ist, kann es im Rahmen eines militärischen Einsatzes erforderlich werden, ihn darin zu behindern oder sie ihm gegebenenfalls völlig zu verwehren. So war und ist die Unterbrechung und Beeinträchtigung beispielsweise von Kommunikationswegen des Gegners ein klassisches Mittel militärischer Operationsführung.
Ein Einsatz der Streitkräfte bleibt jedoch auch in Bezug auf Cyber-Sicherheit immer an die gegebenen verfassungsrechtlichen und völkerrechtlichen Voraussetzungen gebunden. Dies schließt das Verbot von unterschiedslosen und unverhältnismäßigen Beeinträchtigungen von Zivilpersonen und ziviler digitaler Infrastruktur mit ein, die den Petenten offenbar besonders bewegen.

Hinsichtlich der Forderung des Petenten nach einem **Einsatz Deutschlands für internationale Abkommen** und einem Bann von „Cyber-Waffen" ist festzuhalten, dass Deutschland in den verschiedensten internationalen Gremien vertreten ist, die sich um mehr Sicherheit und Grundsätze verantwortlichen Staatenhandelns im Cyberraum bemühen. Herauszuheben ist hier u.a. die Expertenarbeitsgruppe der Vereinten Nationen zu Cyber und internationaler Sicherheit, für die Deutschland bereits zum fünften Mal als Mitglied ausgewählt wurde und die beginnend ab August 2016 wieder tagen wird.[1] Diese Gruppe hat sich in der Vergangenheit auch mit Vorschlägen für völkerrechtliche Verträge über die Nutzung des Cyber-Raums für militärische Operationen befasst, konnte sich aber nicht auf einen Vorschlag für ein Abrüstungs- oder Rüstungskontrollabkommen einigen. Unter anderem weisen Implementierungs- und Verifikationsprobleme, die **Definition von „Cyber-Waffen"** sowie das Problem der völkerrechtlichen Zurechnung (Attribuierbarkeit von Angriffen) erhebliche Schwierigkeiten auf.
In der Organisation für die Sicherheit und Zusammenarbeit in Europa OSZE setzt sich Deutschland seit Jahren erfolgreich für sicherheits- und vertrauensbildend Maßnahmen ein. Unter deutschem Vorsitz wurde nach schwierigen Verhandlungen im März 2016 ein Satz zusätzlicher solcher Maßnahmen verabschiedet und Deutschland ist es gelungen, die Diskussion zu Cybersicherheit über die politisch-militärische Dimension hinaus im Sinne eines umfassenden Sicherheitsbegriffs auf andere Dimensionen auszuweiten.

---

[1] Group of Governmental Experts On Developments in the Field of Information and Telecommunications In the Context of International Security

Hierbei bringt sich das Bundesministerium der Verteidigung im Rahmen der Cyber-Außen- und Sicherheitspolitik, die in der Federführung des Auswärtigen Amtes liegt, aktiv ein.

Im Auftrag

Leinhos

Generalmajor