„Die Rolle der Bundeswehr im Cyberraum“
Anhörung im Bundestag am 22.02.2016
Intro Sts’in Dr. Suder

Lage: Neue Qualität der Cyber-Bedrohung

- Man könnte Cyber als „eine Steuer auf die Digitalisierung“ bezeichnen: Staat, Wirtschaft und Gesellschaft sind in einer zunehmend digitalisierten Welt für Angriffe im Cyber-Raum verwundbarer geworden.
- Diese digitale Verwundbarkeit haben sich in den letzten Jahren staatliche und nichtstaatliche Akteure zu Nutze gemacht:
    1. Cyber ist kostengünstig und effektiv – erzielt also asymmetrische Wirkung. Häufig um Ziele - unterhalb der Schwelle eines militärischen Angriffs - durchzusetzen.
    2. Cyber-Angriffe umfassen Spionage, Informationsmanipulation, mögliche Cyber-Terrorakte bis hin zu groß angelegten Sabotage-Attacken bspw. bei Kritischer Infrastruktur.
    3. Proliferation und exponentielle IT-Entwicklung verstärken den Trend
- Wir erleben dies bereits heute im Rahmen der „hybriden Kriegsführung“.
- Doch nicht nur die Quantität, vor allem die Qualität der Bedrohung hat sich spürbar gewandelt.
    - Die Entwicklung von einfachen Viren hin zu komplexen, schwer erkennbaren Attacken (Advanced Persistant Threats) stellt einen Qualitätssprung dar. Es werden im Schnitt über 200 Tage benötigt, einen APT zu erkennen und in der Regel dauert es mehr als 1 Monat, das Problem zu beheben.
    - Solche Cyber- Angriffe auf Staaten und Kritische Infrastrukturen sind schon lange keine Fiktion mehr sondern Realität. Bekannte Beispiele sind:
        - der „STUXNET-Angriff“ mit physischen Schäden an einer iranischen Uranzentrifuge (2010) - eines der Themen der Berlinale diesen Monat,
        - der „OPM-Breach“ mit einem Datenabfluss in den USA von ca. 20 Millionen personenbezogener Staatsangestellten (2014/2015),
        - der „Bundestaghack“, mit Schadsoftware auf Rechnern des Bundestags (2015).
    - Zwar können vereinzelt Vorgehensmuster erkannt werden. Dennoch sind die modernen Hochwertangriffe meist auf das jeweilige Zielsystem maßgeschneidert.
- So hat sich der Cyber-Raum zu einem internationalem und strategischen Handlungsraum entwickelt, der sich jedoch klassischen Kategorien entzieht.
    - Im Cyber-Raum existieren keine Grenzen, Angriffe können weltweit wirken, werden stetig weiterentwickelt und verfeinert.
    - Hierdurch verschwimmen die Grenzen zwischen Krieg und Frieden, innerer und äußerer Sicherheit sowie kriminell und politisch motivierten Angriffen.
    - Die Schwierigkeit der Attribution, also der zweifelsfreien Zurückführung von Angriffen auf Verursacher, verstärkt die gefühlte Grenzenlosigkeit des Cyber-Raums.
    - Aber auch hier verfügen wir über einen klarer Rechtsrahmen.

Vernetze Bedrohungen des Cyber-Raums ist nur gesamtstaatlich zu begegnen

- Innere und äußere Sicherheit fallen in wenigen Bereichen so eng zusammen wie hier. Und deshalb erfordert es eine ganzheitliche, gesamtstaatliche Betrachtung.
- In enger Abstimmung werden sich deshalb BMI und BMVg komplementär und eng verzahnt für die Cyber-Sicherheit und –Verteidigung aufstellen. BMI und BMVg sind sich einig:
    1. Die Wahrung der Cyber-Sicherheit ist eine gesamtstaatliche Aufgabe, die nur gemeinsam zu bewältigen ist.
    2. Dazu gehört auch der gemeinsame Schutz der kritischen Infrastrukturen.
    3. Verteidigungsaspekte sind originäre Aufgaben von BMVg und Bundeswehr.
- Ähnliche Kooperationen gibt es bereits im Bereich Sicherheit im Luftraum.
- Gemeinsam gilt es, die gesamte Kette von Prävention zu Reaktion sowie einfachen bis komplexen Angriffen zu beherrschen.
    1. Zur Sicherung der inneren Sicherheit bedarf es bspw. der Steigerung der allgemeinen „Cyber-Hygiene“ – also der erhöhten „Cyber-Awareness“ und „Cyber-Resilienz“ bei Bürgern, Wirtschaft und natürlich auch beim Staat. Hier setzen die unabdingbaren Maßnahmen des BMI zur Steigerung der IT-Sicherheit und des Grundschutzes an.
    2. Gleichzeitig müssen wir aber auch für die neue Qualität von Cyber-Hochwertangriffen gerüstet sein, gegen die einfache Maßnahmen wie Firewalls und Detektions-Fähigkeiten nicht ausreichen; gerade weil die Bundeswehr ein solches Hochwertziel für staatliche wie nicht-staatliche Organisationen ist.
- Und deshalb brauchen wir vor allem defensive aber auch offensive Hochwertfähigkeiten, die es kontinuierlich zu üben und weiterzuentwickeln gilt.
- Dabei gelten für den Einsatz von Streitkräften im Cyber-Raum stets die gleichen rechtlichen Voraussetzungen wie beim Einsatz anderer Fähigkeiten: Es gibt keine Einsatz von Cyber-Kräften ohne entsprechende Einsatzmandatierung im Sinne des Parlamentsbeteiligungs-gesetzes durch den Deutschen Bundestag.

Bundeswehr für den Cyber-Raum aufstellen und kontinuierlich weiterentwickeln

- Was gilt es angesichts der Lage und der Aufgaben zu tun?
    1. Cyber-Sicherheit:
        - Eigene Cyber-Fähigkeiten sind auszubauen, dabei ist die Sicherheitsarchitektur des IT-Systems der Bundeswehr zu konsolidieren und resilienter zu machen („**Hygienemaßnahmen**“),
        - Waffensysteme und Gefechtsstände sowie Lieferketten in der Rüstung sind u.a. durch den gezielten Rückgriff auf nationale Schlüsseltechnologien zu härten („**APT-Schutz**“).
    2. Gesamtstaatlichen Cyber-Fähigkeiten:
        - Wir müssen ressortübergreifend viel enger kooperieren und uns mit Wissenschaft, Industrie und Partnern stärker vernetzen („**Resilenzprozesse**“ & „**Cyber-Cluster**“).

3. Struktur (Kontext: Großorganisation mit ca. 280.000 IT-Nutzern):
    - Das Verteidigungsressort wird einen neuen Organisationsbereich „Cyber- und Informationsraum“ aufstellen.
    - Im Ministerium wird die neue Relevanz der Digitalisierung der Streitkräfte durch ein neues Element „IT/ Cyber“ mit einem Chief Information Officer (CIO) an der Spitze abgebildet („**Strukturelle Signifikanz**“).
4. Personal:
    - Spitzenpersonal ist durch Schaffung attraktiver Cyber-Karrierepfade und innovativer Personalgewinnungsstrategien zu rekrutieren („**Die besten Köpfe**“).

- Ich bin darüber hinaus der Überzeugung, die Bundeswehr muss sich insgesamt für Partner weiter öffnen, um den zukünftigen Herausforderungen des Cyber-Raums gewachsen zu sein.