

Nationalrat

Conseil national

Consiglio nazionale

Cussegl naziunal



17.3507 s Mo. Ständerat (Dittli). Ein Cyberdefence-Kommando mit Cybertruppen für die Schweizer Armee

Bericht der Sicherheitspolitischen Kommission vom 30. Oktober 2017

Die Sicherheitspolitische Kommission des Nationalrates hat an ihrer Sitzung vom 30. Oktober 2017 die von Ständerat Josef Dittli am 15. Juni 2017 eingereichte und vom Ständerat am 25. September 2017 angenommene Motion vorberaten.

Die Motion beauftragt den Bundesrat, bei der Schweizer Armee ein militärisch ausgerichtetes Cyberdefence-Kommando mit Cybertruppen in angemessener Stärke aufzubauen. Das Kommando soll aus 100 bis 150 Berufsmilitärs bestehen, die IT-/Cyberspezialisten sind. Die Cybertruppen wiederum sollen etwa 400 bis 600 Angehörige der Milizarmee umfassen, die beispielsweise in Cyberbataillons organisiert sind. Für die Ausbildung der Cybertruppen soll eine Cyber-RS angeboten werden. Schliesslich präzisiert der Motionär auch, welche Aufgaben das Cyberdefence-Kommando und die entsprechenden Truppen mindestens übernehmen sollen.

Antrag der Kommission

Die Kommission beantragt einstimmig, die Motion in der geänderten Fassung (vgl. Ziff. 4 des Berichts) anzunehmen.

Berichterstattung: Dobler (d), Golay (f)

Im Namen der Kommission
Die Präsidentin:

Corina Eichenberger-Walther

Inhalt des Berichtes

- 1 Text und Begründung
- 2 Stellungnahme des Bundesrates vom 6. September 2017
- 3 Verhandlungen und Beschluss des Erstrates
- 4 Änderungsantrag der Kommission
- 5 Erwägungen der Kommission



1 Text und Begründung

1.1 Text

Der Bundesrat wird beauftragt, zur Erfüllung der Armeeaufträge (gemäss Art. 58 der Bundesverfassung) bei der Schweizer Armee ein militärisch ausgerichtetes Cyberdefence-Kommando mit Cybertruppen (Angehörige der Armee) in angemessener Stärke aufzubauen. Das Kommando soll professionalisiert aus 100 bis 150 IT-/Cyberspezialisten bestehen, und die milizmässig aufgebauten Cybertruppen sollen etwa 400 bis 600 Angehörige der Armee umfassen, z. B. organisiert als Cyberbataillon. Für die Ausbildung der Cybertruppen soll eine Cyber-RS angeboten werden. Das neue Cyberdefence-Kommando der Schweizer Armee mit den Miliz-Cybertruppen soll mindestens:

1. permanent und in allen Lagen seine eigenen Systeme und Infrastrukturen vor Cyberangriffen schützen;
2. für den Verteidigungsfall befähigt sein, als Truppenkörper oder mit Teilen davon eigenständige Cyberoperationen durchzuführen (Cyberaufklärung, Cyberverteidigung, Cyberangriff);
3. im Rahmen des Nachrichtendienstgesetzes (NDG) den Nachrichtendienst des Bundes (NDB) subsidiär unterstützen und dessen Systeme schützen;
4. die Betreiber kritischer Infrastrukturen subsidiär unterstützen;
5. die zivilen Behörden des Bundes und der Kantone bei Cyberangelegenheiten subsidiär unterstützen.

Zu diesem Zweck soll die Schweizer Armee:

6. eine enge Kooperation mit den Hochschulen (z. B. ETHZ, EPFL), der IT-Wirtschaft und Vertretern der potenziell gefährdeten Infrastrukturen (Energie, Verkehr, Banken usw.) eingehen;
7. die notwendigen organisatorischen Konzeptionen wie Gliederung und Aufbau des Kommandos, Einsatzdoktrin, Anwerbung von IT-/Cyberspezialisten, Rekrutierung von IT-/Cybersoldaten, Ausbildung, Ressourcenbeschaffung usw. rasch vorantreiben.

1.2 Begründung

Mit der NCS-Strategie hat die Schweiz ein gutes übergeordnetes Konzept. Mit Melani besitzt die zivile Seite auch ein erstes gut funktionierendes Instrument. Aufseiten der Armee sind die Mittel nicht in ausreichendem Masse vorhanden, um im Rahmen der Armeeaufträge den Bedrohungen angemessen begegnen zu können. Wie der Luftraum oder das terrestrische Staatsgebiet muss, in der normalen Lage bis hin zum Verteidigungsfall, auch der Cyberraum verteidigt werden können. Dazu sind Mittel, Kompetenzen (Expertise, Wissen und Erfahrung) und Kapazitäten (Experten) in der Armee aufzubauen. Mit dem professionellen Teil der neuen Formation sollen schergewichtig die sicherheitspolitischen Cyberbedürfnisse in der normalen Lage gewährleistet sowie die Führung des Kommandos sichergestellt werden. Mit den milizmässig aufgebauten Cybertruppen (z. B. Milizbataillon) soll der Cyberraum im Verteidigungsfall behauptet werden können, und sie sollen in allen Lagen subsidiär den NDB und die zivilen Behörden unterstützen.

2 Stellungnahme des Bundesrates vom 6. September 2017

Aufgrund der Entwicklung der Cyberbedrohungen, des Bedarfs, der sich aus der Umsetzung des Nachrichtendienstgesetzes und des Militärgesetzes ergibt, sowie aufgrund der Erwartungen an die Armee im Rahmen der nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) hat das



VBS im Rahmen seiner Kompetenzen und Mittel den Aktionsplan Cyberdefence ausgearbeitet, über den der Bundesrat am 12. April 2017 informiert worden ist.

Der Aktionsplan, dessen Umsetzung bis Ende 2020 andauern wird, erfüllt die Forderungen der Motion zum grössten Teil, insbesondere in Bezug auf die ständige Verfügbarkeit, die Stärke der Truppen und den Einbezug der Miliz. Er deckt auch die Bedürfnisse im Bereich der Unterstützung ziviler Behörden bei der Verteidigung von kritischen Infrastrukturen (einschliesslich der Subsidiarität der Armee - das Thema wird in die laufende Revision der NCS Eingang finden) sowie für den Verteidigungsfall und die Unterstützung militärischer Operationen ab. Schliesslich sieht der Aktionsplan eine enge Zusammenarbeit mit den Hochschulen sowie die Stärkung der Mittel des Nachrichtendienstes des Bundes vor. Die zur Umsetzung erforderlichen Ressourcen können im Übrigen über das Budget des VBS abgewickelt werden.

Einige Elemente der Motion können jedoch nicht wie vorgeschlagen umgesetzt werden. Aus Sicht des Bundesrates ist eine "Cyber-RS" nicht zweckdienlich, da die Ausbildung der benötigten Spezialistinnen und Spezialisten mit den traditionellen Ausbildungsmodellen der Armee nicht zu realisieren ist. Aus diesem Grund ist das VBS bereits daran, mit den Hochschulen geeignete Lösungen zu erarbeiten. Im Rahmen der Weiterentwicklung der Armee hat das Parlament entschieden, ein Unterstützungskommando zu schaffen. Das von der Motion gewünschte Cyberdefence-Kommando kann in dieses Projekt integriert werden, seine endgültige Form hängt jedoch von den anstehenden Arbeiten ab.

Gemäss Bundesrat ist die Motion demzufolge in ihrer heutigen Form abzulehnen.

Wenn der erstbehandelnde Rat die Motion annimmt, hat das VBS die Möglichkeit, dem Zweirat einen Änderungsvorschlag zu unterbreiten.

Der Bundesrat beantragt die Ablehnung der Motion.

3 Verhandlungen und Beschluss des Erstrates

Der Ständerat nahm die Motion am 25. September 2017 mit 34 zu 7 Stimmen an. Bei den Rednerinnen und Rednern herrschte Einigkeit darüber, dass die Cyberdefence-Mittel weiter ausgebaut werden sollten, um gegen die aktuellen und künftigen Bedrohungen in diesem Bereich vorgehen zu können. Sie hielten fest, dass ein Cyberdefence-Kommando und entsprechende Einheiten geschaffen werden sollten. Der Vorsteher des VBS, Bundesrat Guy Parmelin, liess verlauten, dass der Bundesrat in der Zwischenzeit mit den Anliegen der Motion einverstanden ist, mit Ausnahme von zwei Punkten: der Einführung einer Cyber-RS und der Schaffung von Cyberbataillons. Er gab zu verstehen, dass der Bundesrat im Falle der Annahme der Motion einen Änderungsantrag in diesem Sinne unterbreiten würde.

4 Änderungsantrag der Kommission

Die Kommission beantragt einstimmig, die Motion wie folgt zu ändern:

Der Bundesrat wird beauftragt, zur Erfüllung der Armeeaufträge (gemäss Art. 58 der Bundesverfassung) bei der Schweizer Armee eine militärisch ausgerichtete Cyberdefence-Organisation mit Cybertruppen (Angehörigen der Armee) in angemessener Stärke aufzubauen. Die Organisation soll professionalisiert aus 100 bis 150 IT- /Cyberspezialisten bestehen, und die milizmässig aufgebauten Cybertruppen sollen etwa 400 bis 600 Angehörige der Armee umfassen. Für die Ausbildung der Cybertruppen soll ab Rekrutenschule eine fachspezifische Cyberausbildung organisiert werden. Die neue Cyberdefence-Organisation der Schweizer Armee mit den Milizcybertruppen soll mindestens:



1. ...
2. für den Verteidigungsfall befähigt sein, Cyberoperationen durchzuführen (Cyberaufklärung, Cyberverteidigung, Cyberangriff);
- 3.-6. ...
7. die notwendigen organisatorischen Konzeptionen wie Gliederung und Aufbau, Einsatzdoktrin, Anwerbung von IT-/Cyberspezialisten, Rekrutierung von IT-/Cybersoldaten, Ausbildung, Ressourcenbeschaffung usw. rasch vorantreiben.

5 Erwägungen der Kommission

Die Kommission führte mit den Experten des VBS für Cybersicherheit ausführliche Diskussionen. Dabei nahm sie Kenntnis von den laufenden Arbeiten in Zusammenhang mit dem Aktionsplan des VBS. Die Kommission begrüsst diese Arbeiten und ist der Auffassung, dass sich die Motion bestens in die bereits unternommenen langfristigen Anstrengungen einfügt.

Die Kommission unterstützt die Schaffung einer auf Cyberdefence spezialisierten Armeeorganisation mit Cybertruppen. Sie hat davon Kenntnis genommen, dass diese Organisation gemäss VBS aus 100 bis 150 IT-/Cyberspezialisten, die Berufsmilitärs sind, bestehen soll, denen 400 bis 600 Angehörige der Milizarmee zur Seite gestellt werden. Ebenfalls zur Kenntnis genommen hat die Kommission, dass im Rahmen der Weiterentwicklung der Armee per 1. Januar 2018 aus einer bereits bestehenden Einheit eine Cyberkompanie geschaffen werden soll.

Die Kommission spricht sich klar für die von der Motion geforderte Stossrichtung aus und befürwortet, dass dieser Organisation die vorgeschlagenen Aufgaben übertragen werden. Sie beantragt allerdings, den Motionstext in folgenden Punkten zu ändern:

- Die Kommission beantragt, anstelle des Begriffs "Kommando" den Begriff "Organisation" zu verwenden, damit die Armee über den nötigen Handlungsspielraum verfügt und die Art der Organisationseinheit nicht bereits festgelegt ist.
- Sie beantragt, den Begriff "Cyberbataillon" fallen zu lassen, da er dahingehend verstanden werden könnte, dass er autonome Formationen umfasst. Es ist jedoch vorgesehen, dass IT-Spezialisten der Militärverwaltung und der Milizarmee zusammen zum Einsatz kommen und nicht, dass Formationen wie Kompanien oder Bataillons selbstständig operieren.
- Sie beantragt, auf eine Rekrutenschule, die ihren Schwerpunkt einzig auf Cyberdefence-Aspekte legt (Cyber-RS), zu verzichten. In den Augen der Kommission ist dies nicht die beste Lösung. Rekruten, die in diesem Bereich Talent mitbringen, sollen vielmehr ab der Rekrutenschule eine fachspezifische Cyberausbildung erhalten, bevor sie einer Cybereinheit zugeteilt werden (Ausbildung). Auch muss die Zuteilung der Armeeangehörigen mit Fachwissen jederzeit geändert werden können – selbst wenn diese die Rekrutenschule in einer anderen Truppengattung absolviert haben. Das Ausbildungs- und Einsatzkonzept für eine fachspezifische Cyberausbildung soll nicht nur aus einer Grundausbildung bestehen. Es sind auch verschiedene Kaderlehrgänge und Weiterbildungslehrgänge vorgesehen. Der Begriff "Cyber-RS" wäre für diesen Ausbildungsbereich zu restriktiv.

Aus all diesen Gründen beantragt die Kommission einstimmig, die Motion in der geänderten Fassung anzunehmen.