Ständerat

Conseil des Etats

Consiglio degli Stati

Cussegl dals stadis

17.3199 n Mo. Nationalrat (Grüter). Ausbau der Cyberabwehrkompetenzen

Bericht der Sicherheitspolitischen Kommission vom 13. August 2018

Die Sicherheitspolitische Kommission des Ständerates hat an ihrer Sitzung vom 13. August 2018 die von Nationalrat Franz Grüter (SVP, LU) am 16. März 2017 eingereichte und vom Nationalrat am 6. März 2018 angenommene Motion vorberaten.

Mit der Motion wird der Bundesrat beauftragt, innerhalb der folgenden zwei Jahre alle sicherheitspolitischen Cyberabwehrkompetenzen des Bundes auszubauen und an geeigneter Stelle innerhalb der Armee oder beim Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) als eigenständiges Cyberkommando zu bündeln. Die notwendigen Aufwendungen sollen zusätzlich im Rüstungsbudget berücksichtigt werden. In den nächsten Jahren ist zudem bei den Rüstungsbeschaffungen und im Bereich BFI auch ein Schwerpunkt auf das Thema Cybersicherheit zu legen. Die dafür notwendigen Gesetzesanpassungen sind einzuleiten.

Antrag der Kommission

Die Kommission beantragt mit 10 zu 2 Stimmen, die Motion abzulehnen.

Berichterstattung: Dittli

Im Namen der Kommission
Der Präsident:

Josef Dittli

Inhalt des Berichtes

1 Text und Begründung

1.1 Text

Der Bundesrat wird beauftragt, innerhalb der folgenden zwei Jahre alle sicherheitspolitischen Cyberabwehrkompetenzen des Bundes auszubauen und an geeigneter Stelle innerhalb der Armee oder beim Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) als eigenständiges Cyberkommando zu bündeln. Die notwendigen Aufwendungen sollen zusätzlich im Rüstungsbudget berücksichtigt werden. In den nächsten Jahren ist zudem bei den Rüstungsbeschaffungen und im Bereich BFI auch ein Schwerpunkt auf das Thema Cybersicherheit zu legen. Die dafür notwendigen Gesetzesanpassungen sind einzuleiten.

1.2 Begründung

Wirtschaftsspionage, verbotener Nachrichtendienst, Informationsoperationen und organisierte Kriminalität finden in der Schweiz zunehmend im Cyberraum statt. Aktuelle und wiederkehrende Enthüllungen und Angriffe zeigen, dass die Schweiz und der Bund hier nicht gewappnet und verletzlich sind. Der militärische und geheimdienstliche Ausbau vieler Länder von Fähigkeiten im Bereich Cyber beweist, dass diese Bedrohung real ist und zunimmt. Die Digitalisierung der Gesellschaft und Wirtschaft macht uns im virtuellen Raum immer anfälliger für Sabotage und Manipulation. Zudem ist die Schweiz einer der wichtigsten Datenstandorte in Europa. Der Bund hat gemäss Artikel 2 Absatz 1 der Bundesverfassung den Auftrag, die Sicherheit des Landes zu wahren. Dazu gehört auch die Cybersicherheit!
Die bereits vorhandenen, jedoch verzettelten Kompetenzen bei der Armee, beim Nachrichtendienst, beim Bakom, beim Bundesamt für Informatik und Telekommunikation, beim Justiz- und Polizeidepartement (EJPD) und in anderen Departementen sollen straffer geführt und gebündelt werden, denn Redundanzen, Ineffizienzen und Koordinationsaufwand müssen reduziert werden. Hierfür kommt gemäss internationalen Vergleichen ein ausgebautes Cyberkommando innerhalb der Armeestrukturen infrage oder beispielsweise ein eigentliches Bundesamt für Cybersicherheit beim VBS. Die Ressourcen sollen einerseits durch die Bündelung der Kräfte aus den jeweiligen Departementen freigemacht werden, andererseits durch Einsparungen bei den Departementszentralen. Bei der Armee muss zudem ein Umdenken stattfinden, und so oder so braucht es mehr Personal und Rüstung im Bereich Cyberverteidigung. Das Informationszeitalter braucht auch in der sicherheitspolitischen Architektur der Schweiz ein den Umständen und Bedrohungen entsprechendes Pendant. Die Schweiz darf auch aus neutralitätspolitischen Überlegungen hier nicht zu einem Vakuum werden und muss eigenständig die Sicherheit auch im Cyberraum gewährleisten können.

2 Stellungnahme des Bundesrates vom 17. Mai 2017

Mit der Umsetzung der nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) konnten die Fähigkeiten des Bundes im Bereich Cyber gestärkt werden. Mit der Konzeptstudie Cyberdefence der Armee von 2013 und dem Aktionsplan Cyberdefence des VBS werden zudem die Cyberfähigkeiten in der Armee, insbesondere im Bereich der Rüstung und beim Nachrichtendienst des Bundes, weiter verstärkt. Der Bundesrat teilt die Einschätzung des Motionärs, dass die Fähigkeiten im Bereich Cyber angesichts der Entwicklung der Bedrohungslage und der schnell fortschreitenden Digitalisierung von Wirtschaft und Bevölkerung weiterhin substanziell gestärkt und die entsprechende Forschung und Bildung verstärkt werden müssen.
Cyberrisiken betreffen neben der Armee alle Bereiche der Verwaltung, Wirtschaft und Bevölkerung. Dementsprechend müssen verschiedenste Behörden in ihren Zuständigkeitsbereichen den Schutz vor Cyberrisiken wahrnehmen. Das sind etwa die Polizei und die Strafverfolgung, der zivile und der militärische Nachrichtendienst, die verschiedenen sektoriellen Aufsichtsbehörden (Energie, Finanz,

Kommunikation, Verkehr, Gesundheit usw.) wie auch die Betreiber kritischer Infrastrukturen. Zu Letzteren gehört auch der Betrieb der Informatik in der Verwaltung. Dafür benötigen diese Stellen die entsprechenden Fähigkeiten und personellen sowie finanziellen Ressourcen. Diese können nicht ausgegliedert und in ein Cyberkommando der Armee überführt werden. Stattdessen ist eine übergreifende und abgestimmte, auf die jeweiligen Rollen basierte Zusammenarbeit notwendig. Dies hat sich auch im Rahmen der Umsetzung der NCS bewährt. Die vom Motionär erwähnten Cyberkommandos z. B. in Frankreich oder Deutschland betreffen im Übrigen durchwegs nur die Streitkräfte. Sie können nicht als Beispiele für eine durchgehende Zentralisierung aller sicherheitspolitischen Cyberabwehrkompetenzen eines Landes gelten.
Es gilt aber sicherzustellen, dass die verfügbaren Mittel schlagkräftig und aufeinander abgestimmt organisiert sind. Im Rahmen der Weiterentwicklung der NCS beabsichtigt der Bundesrat deshalb auch, mögliche Konzentrationen von Cyberkompetenzen zu prüfen sowie die Zusammenarbeit zwischen den zivilen Stellen und der Armee einschliesslich ihrer Zuständigkeiten zu klären.

Der Bundesrat beantragt die Ablehnung der Motion.

3 Verhandlungen und Beschluss des Erstrates

Der Nationalrat hat die Motion am 6. März 2018 mit 134 zu 47 Stimmen bei 9 Enthaltungen angenommen.

4 Erwägungen der Kommission

Wie der Motionär stuft auch die Kommission die Prävention und Bekämpfung der Cyber-Bedrohungen als prioritär ein. Sie verweist jedoch auf verschiedene Arbeiten, die im Zuge der von den Räten überwiesenen Motionen 17.3507, "Ein Cyberdefence-Kommando mit Cybertruppen für die Schweizer Armee", und 17.3508, "Schaffung eines Cybersecurity-Kompetenzzentrums auf Stufe Bund", bereits im Gange sind. Insbesondere hat der Bundesrat am 4. Juli 2018 im Hinblick auf den Aufbau eines Cyber-Kompetenzzentrums erste Grundsatzentscheide gefällt und verschiedene Aufträge erteilt (siehe Medienmitteilung vom 4. Juli 2018). Gemäss dessen Vorentscheiden soll das Kompetenzzentrum im Eidgenössischen Finanzdepartement (EFD) angesiedelt werden und nicht wie vom Motionär verlangt im VBS oder bei der Armee zentralisiert werden. Weiter verabschiedete der Bundesrat am 18. April 2018 die zweite Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (2018-2022), die gemeinsam mit Wirtschaft, Kantonen und Hochschulen erarbeitet wurde (siehe Medienmitteilung vom 19. April 2018).

Die Kommission begrüsst diese Arbeiten und die verstärkte Koordination im Cyber-Bereich. Eine komplette Zentralisierung, wie vom Motionär befürwortet, würde dem eingeschlagenen Weg und den bisherigen Beschlüssen des Parlaments und Bundesrates jedoch grundsätzlich widersprechen. Es handle sich um eine Schnittstellen-Thematik, die unterschiedliche Departemente und Akteure betreffe und sowohl militärische wie auch zivile Komponenten beinhalte. Entsprechend wäre eine Zentralisierung nicht zielführend und würde vielmehr dazu führen, dass Kompetenzen an wichtigen dezentralen Stellen verloren gehen. Zum jetzigen Zeitpunkt gelte es den eingeschlagenen Weg der verstärkten Koordination entschieden weiterzuführen und die konkreten Massnahmen umzusetzen.

Weiter bringt die Kommission auch ordnungspolitische Überlegungen hervor: Es obliege der Exekutive und nicht der Legislative, die Kompetenzen an geeigneter Stelle einzusetzen und Federführungen zu bestimmen. Zumal die Melde- und Analysestelle Informationssicherung MELANI bereits jetzt beim EFD angesiedelt sei, mache es auch Sinn, das Kompetenzzentrum und die Federführung dort einzusetzen. So könne auf Bestehendes aufgebaut werden – eine Verlagerung hin zum VBS und zur Armee könnte hingegen zu grossem Zeitverlust führen. Nicht zuletzt bedürfte dies auch einer Anpassung des Verteidigungsauftrages der Armee.