

Sélection d'article sur la politique suisse

processus

Cyberdefence-Kommando (Mo. 17.3507)

Imprimer

Éditeur

Année Politique Suisse
Institut für Politikwissenschaft
Universität Bern
Fabrikstrasse 8
CH-3012 Bern
www.anneepolitique.swiss

Contributions de

Porcellana, Diane
Schubiger, Maximilian

Citations préféré

Porcellana, Diane; Schubiger, Maximilian 2025. *Sélection d'article sur la politique suisse: Cyberdefence-Kommando (Mo. 17.3507), 2017 – 2021*. Bern: Année Politique Suisse, Institut de science politique, Université de Berne. www.anneepolitique.swiss, téléchargé le 30.04.2025.

Sommaire

Chronique générale	1
Eléments du système politique	1
Ordre juridique	1
Sécurité extérieure	1
Criminalité	2

Abréviations

VBS	Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport
SiK-SR	Sicherheitspolitische Kommission des Ständerates
SiK-NR	Sicherheitspolitische Kommission des Nationalrates
AdA	Angehörige(r) der Armee
RS	Rekrutenschule
NDB	Nachrichtendienst des Bundes
	(bis 2010: Strategischer Nachrichtendienst und Dienst für Analyse und Prävention)

DDPS	Département fédéral de la défense, de la protection de la population et des sports
CPS-CE	Commission de la politique de sécurité du Conseil des Etats
CPS-CN	Commission de la politique de sécurité du Conseil national
Militaire	Militaire
ER	École de recrues
SRC	Service de renseignement de la Confédération
	(à 2010: Service de renseignement stratégique et Service d'analyse et de prévention)

Chronique générale

Eléments du système politique

Ordre juridique

Sécurité extérieure

MOTION
DATE: 25.09.2017
MAXIMILIAN SCHUBIGER

Josef Dittli (fdp, UR) schlug mit seinem Vorschlag, innerhalb der Armee ein **Cyberdefence-Kommando** einzurichten, einen eigentlichen Paradigmenwechsel vor. Bereits seit Jahren war der Bund bestrebt, im Bereich Cyber-Kriminalität neue Wege zu gehen und den sich verändernden technologischen Entwicklungen Rechnung zu tragen, indem beispielsweise die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) lanciert wurde. Eine eigentliche Cyber-Armee wurde jedoch in diesen Prozessen noch nicht konzipiert. Mit der fortschreitenden Digitalisierung und den damit ausgelösten Datenverschiebungen müssen Sicherheitsaspekte im Cyber-Bereich jedoch zunehmend angesprochen sowie entsprechende Massnahmen vorgesehen werden. Dittli wollte innerhalb des VBS und der Armee eine eigene Truppe zur Cyberabwehr aufbauen. Er leitete die Notwendigkeit seines Vorschlags aus dem Verfassungsauftrag an die Armee ab. Ein professionalisiertes Kommando mit 100 bis 150 Cyberspezialisten soll, flankiert von einer 400-600 AdA-starken Cybertruppe, die sensiblen Infrastrukturen schützen. Die Ausbildung dieser Spezialisten soll über eine eigens zu schaffende Cyber-RS erfolgen. Sieben Punkte führte der Motionär an, die eine solche Cyber-Einheit erfüllen können muss: Eigene Systeme jederzeit schützen; eigenständige Cyberoperationen durchführen (z. B. Cyberaufklärung, -verteidigung, aber auch -angriff); den NDB unterstützen; Unterstützungsleistungen weiterer Betreiber kritischer Infrastrukturen; zivile Behörden in Cyberangelegenheiten unterstützen. Dafür soll die Armee einerseits Kooperationen mit dem Forschungsplatz, aber auch dem Hochschulbereich eingehen und andererseits Vorbereitungen treffen, damit eine solche militärische Cyber-Einheit konzipiert werden kann. Dittli schlug also eine eigentliche Cyber-Armeeinheit vor, daneben war auch eine Motion von Ständerat Eder (fdp, ZG) hängig, der sich im Cyber-Bereich ein Kompetenzzentrum wünschte. Diese Motion wurde vom Ständerat bereits dem Zweitrat überwiesen.

Der Bundesrat zeigte sich in seiner Antwort auf den Vorstoss skeptisch. Elemente der Zielvorgabe würden gegenwärtig mit einem Aktionsplan Cyberdefence angegangen, dieser erfülle weite Teile der Motion. Bezüglich der Anliegen die Truppe betreffend (Verfügbarkeit, Stärke, Milizprinzip) seien daher die nächsten Schritte in der Umsetzung des Aktionsplans, wie sie bis 2020 vorgesehen sind, abzuwarten. Hinsichtlich der Einrichtung eines eigenen Kommandos zeigte sich die Regierung offener, man müsse aber auch hier abwarten, wie sich solche Leitungsstrukturen in ein Gesamtgefüge integrieren liessen. So sprach sich der Bundesrat noch gegen die Motion aus, hielt sich aber die Möglichkeit offen, bei einer allfälligen Annahme im Erstrat via das VBS zuhanden des Zweitrats noch auf den Motionstext Einfluss zu nehmen.

Die Ratsdebatte wurde mit einem Ordnungsantrag Hêche (sp, JU) eröffnet, der die Motion der zuständigen SiK zur Vorprüfung zuweisen wollte. Hêche wollte nicht mehrspurig fahren und nicht neben den Prozessen um den Aktionsplan des Bundesrates und der zuvor angenommenen Motion Eder (fdp, ZG) zusätzlich auch noch einen Prozess zur Schaffung einer Cyber-Armee anstossen. Der Motionär entgegnete jedoch, dass sich die Ziele der Motion Eder nicht mit denjenigen seiner eigenen überschneiden würden, da er sich eben auf den Bereich Armee beschränke. Im Übrigen hätte sich ja die Regierung offen gegenüber der Motion gezeigt und einzig an der Cyber-RS Anstoss genommen. Der Ordnungsantrag wurde nicht angenommen, damit konnte der Vorstoss materiell behandelt werden.

Der Motionär verteidigte sein Anliegen mit der Einschätzung, dass nicht klar sei, was der Bundesrat und das VBS im Cyber-Bereich erreichen wollen. Zwar werde viel unternommen, auch gerade bezüglich der Rollendefinition der Armee und ihrer Funktionen in der Cyberabwehr, offen sei jedoch, wie die Stärken der Miliz einbezogen werden können. Der Aktionsplan Cyberdefence sei laut Dittli (fdp, UR) „in Ordnung“, jedoch sei kaum etwas über seinen Inhalt bekannt. Dass ein wesentlicher Teil seiner Motion bereits in anderen Prozessen umgesetzt wird, begrüßte er, aber das wichtige und titelgebende Anliegen seines Vorstosses, ein Cyber-Kommando in die Armeestrukturen einzubinden, sei eben noch nicht angedacht. Ebenso fehle in der Debatte über die Möglichkeiten, IT-Spezialisten zu finden und auszubilden, die Prüfung einer Cyber-RS. Es gebe schliesslich bereits IT-Spezialisten in den Rechenzentren von Bund und VBS, eine systematische armeenaher Cyber-Ausbildung fehle jedoch komplett.

Er sah denn auch einen Steilpass in der geäusserten Bereitschaft der Regierung, im Falle einer Annahme seiner Motion noch Änderungsvorschläge zuhanden der SiK-NR zu machen. Diesen Steilpass müsste der Ständerat „also der Sache zuliebe annehmen“. Ratskollege Ettlin (cvp, OW) blies ins gleiche Horn. Es gebe bereits heute monatlich tausende Cyberangriffe auf diverse kritische Strukturen und er finde die Argumentation der Regierung, eine Cyber-RS sei nicht möglich, da sie sich nicht in die bestehenden Ausbildungsmodelle der Armee einfügen lasse, „speziell“. Die Annahme neuer Herausforderungen, auch im Bereich (Cyber-)Verteidigung sei wichtig, so der Obwaldner weiter.

Verteidigungsminister Parmelin argumentierte vergeblich mit den bestehenden Arbeiten und der Bereitschaft, den Weg der Cyberabwehr weiter gehen zu wollen. Das Ratsplenum nahm die Motion mit 34 zu 7 Stimmen deutlich an.¹

MOTION

DATE: 12.12.2017

MAXIMILIAN SCHUBIGER

Ein **Cyberdefence-Kommando** innerhalb der Strukturen der Armee zu etablieren, stiess bei der SiK des Nationalrates grundsätzlich auf Zustimmung. Jedoch sahen die Sicherheitspolitikerinnen und -politiker noch Präzisierungspotenzial beim Text der Motion Dittli (fdp, UR). So soll statt von einem Kommando von einer «Cyber-Organisation» die Rede sein. Ferner sei der Begriff «Cyber-Bataillon» unzutreffend, weil dadurch suggeriert werde, dass eine autonome Formation errichtet würde. Hingegen sei vorgesehen, dass IT-Spezialisten der Verwaltung und des Militärs zusammen zum Einsatz kommen würden. Schliesslich wollte die Kommission darauf verzichten, eigens eine Cyber-RS durchzuführen. Stattdessen sollten AdA, die ein Talent im Cyber-Bereich hätten, erst später eine armee(fach)spezifische Cyberausbildung erhalten und in einem weiteren Schritt einer Cyber-Einheit zugeteilt werden. Mit diesen Änderungen gelangte die SiK einstimmig ans Ratsplenum.

In der Nationalratsdebatte folgten nur die nötigsten Wortmeldungen. Kommissionssprecher Dobler (fdp, SG) fasste die zentralen Punkte zusammen. Weil die von der Kommission vorgeschlagenen Änderungen vom Bundesrat angeregt worden waren und in der Kommission Einigkeit geherrscht hatte, konnte der St. Galler auf die Unterstützung seiner Kommissionskolleginnen und -kollegen zählen. Dem Verteidigungsminister blieb nur übrig, die nunmehr von der Regierung mitgetragenen Änderungen zur Annahme zu empfehlen und die Abkehr von der zuvor herrschenden, ablehnenden Meinung bekannt zu geben. In der Folge wurde die Motion im Nationalrat angenommen, wobei sie in der kleinen Kammer aufgrund der vorgenommenen Änderungen nochmals traktandiert werden musste.²

MOTION

DATE: 06.03.2018

MAXIMILIAN SCHUBIGER

In der Frühjahrssession 2018 des Ständerates war die Beschlussfassung zu einem **Cyberdefence-Kommando** nur noch Formsache. Der Motionär selbst, aber auch die ständerätliche SiK, zeigten sich mit der vom Nationalrat veränderten Fassung einverstanden. Weil der Ständerat selbst zuvor bereits einmal dem Anliegen zugestimmt hatte und nun auch in der Ständekammer seitens des Verteidigungsministers grünes Licht gegeben wurde, galt die Motion schon beinahe als angenommen. Ohne Gegenstimme wurde sie denn auch abgesegnet.³

Criminalité

L'Assemblée fédérale a décidé, sur proposition du Conseil fédéral, de classer la motion demandant la **création d'un commandement de cyberdéfense dans l'armée suisse**. En effet, le Conseil fédéral l'a informée qu'avec la révision planifiée en 2023 de la loi du 3 février 1995 sur l'armée et de l'organisation de l'armée, il répondra aux demandes formulées.

MOTION

DATE: 10.06.2021

DIANE PORCELLANA

1) AB SR, 2017, S. 701 ff.; SGT, 26.9.17

2) AB NR, 2017, S. 2138 f.; Bericht SiK-NR vom 30.10.2017

3) AB SR, 2018, S. 110 f.; Bericht SiK-SR vom 30.10.2017; CdT, 7.3.18