

# Ausgewählte Beiträge zur Schweizer Politik

Suchabfrage	<b>18.04.2024</b>
Thema	<b>Keine Einschränkung</b>
Schlagworte	<b>Ausländische Bevölkerung, Äussere Sicherheit, Innere Sicherheit</b>
Akteure	<b>Dobler, Marcel (fdp/plr, SG) NR/CN</b>
Prozesstypen	<b>Keine Einschränkung</b>
Datum	<b>01.01.1990 - 01.01.2020</b>

# Impressum

## Herausgeber

Année Politique Suisse  
Institut für Politikwissenschaft  
Universität Bern  
Fabrikstrasse 8  
CH-3012 Bern  
[www.anneepolitique.swiss](http://www.anneepolitique.swiss)

## Beiträge von

Schubiger, Maximilian

## Bevorzugte Zitierweise

Schubiger, Maximilian 2024. *Ausgewählte Beiträge zur Schweizer Politik: Ausländische Bevölkerung, Äussere Sicherheit, Innere Sicherheit, 2017 - 2019*. Bern: Année Politique Suisse, Institut für Politikwissenschaft, Universität Bern. [www.anneepolitique.swiss](http://www.anneepolitique.swiss), abgerufen am 18.04.2024.

# Inhaltsverzeichnis

<b>Allgemeine Chronik</b>	1
<b>Grundlagen der Staatsordnung</b>	1
Rechtsordnung	1
Äussere Sicherheit	1
Innere Sicherheit	2

## Abkürzungsverzeichnis

<b>SiK-NR</b>	Sicherheitspolitische Kommission des Nationalrates
<b>AdA</b>	Angehörige(r) der Armee
<b>RS</b>	Rekrutenschule
<b>NCS</b>	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken

---

<b>CPS-CN</b>	Commission de la politique de sécurité du Conseil national
<b>Militaire</b>	Militaire
<b>ER</b>	École de recrues
<b>SNPC</b>	Stratégie nationale de protection de la Suisse contre les cyberrisques

# Allgemeine Chronik

## Grundlagen der Staatsordnung

### Rechtsordnung

#### Äussere Sicherheit

#### MOTION

DATUM: 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.<sup>1</sup>

#### POSTULAT

DATUM: 06.03.2018  
MAXIMILIAN SCHUBIGER

Angesichts der vielen Vorstösse im Bereich Cyber-Kriminalität und -Abwehr und trotz bereits laufender Projekte (Aktionsplan Cyber-Defence, Nationale Cyber-Strategie) sah die sicherheitspolitische Kommission des Nationalrates in dieser Hinsicht noch Handlungsbedarf. Auch wenn die Arbeiten in der NCS begrüsst würden, brauche es **eine klare Cyber-Gesamtstrategie für den Bund**. Was bisher lanciert wurde, entspreche noch keinem Gesamtkonzept, so die Auffassung der Kommission. Fünf konkrete Aufgaben wurden dem Bundesrat gestellt. Dazu gehörte eine präzise Umschreibung des Auftrags der Armee im Bereich der Cyberverteidigung und des Zuständigkeitsbereichs der zivilen Cyberbehörden. Im Lichte der gewonnenen Erkenntnisse sollte darauf basierend eine Abgrenzung der Kompetenzen vorgenommen und ein entsprechendes Organigramm erstellt werden. Bezüglich Finanzierung sollte man sich ferner Gedanken machen über den Ressourcenbedarf, einschliesslich des Personalbedarfs. Abschliessend wurde vorgeschlagen, dass sich die Schweiz auch am Ausland orientieren möge, wenn es um die Cyberabwehr gehe.

Die Regierung räumte ein, dass längere Zeit unzureichend über dieses Thema nachgedacht und es zeitweise gar unterschätzt worden war. Daher wurde eine solche Gesamtstrategie für unabdingbar erklärt, deutlich unterstützte der Bundesrat also dieses Postulat. Eine «Zerstückelung» des Themas, weil diverse Aktionspläne in unterschiedlichen Departementen erstellt würden, sei nicht wünschenswert.

Im Nationalrat war die Angelegenheit klar, das Postulat wurde angenommen. Kommissionssprecherin Mazzone (gp, GE) und Kommissionssprecher Dobler (fdp, SG) unterstrichen die Wichtigkeit einer koordinierten Vorgehensweise und Dobler äusserte überdies den Eindruck, dass bisher erst wenig geschehen sei, obwohl sich um die 90 Personen in der Bundesverwaltung bereits mit Cyber-Themen befassten. Dies wurde jedoch von Bundesrat Maurer sogleich bestritten. Der Magistrat betonte, dass die Planung weiter fortgeschritten sei, als es vom Vorredner dargestellt worden sei, und er stellte in Aussicht, dass bereits im Budget 2019 erste Positionen für die Umsetzung einer Gesamtstrategie beantragt werden sollten.<sup>2</sup>

## Innere Sicherheit

«Haben wir die Hard- und Softwarekomponenten bei unseren kritischen Infrastrukturen im Griff?», fragte Marcel Dobler (fdp, SG) mit einem im Frühjahr 2019 eingereichten Postulat. Damit griff Dobler Sorgen auf, die bei grösseren IT-Beschaffungen immer wieder geäussert werden. Unter anderem geht es dabei namentlich um ICT-Systeme, die in diversen sensiblen Bereichen eingesetzt werden und die von ausländischen Herstellern produziert und bereitgestellt werden. Solche «digitale[n] Lieferobjekte», die in ihrer Komplexität zu Cyberrisiken führen können, stehen im Fokus seines Vorstosses. Der Bundesrat sollte folglich beauftragt werden, zu prüfen, ob und wie nationale und internationale Standards angewendet werden können, um die Risiken zu vermindern.

Der Bundesrat zeigte sich mit der Stossrichtung des Postulats einverstanden und beantragte dessen Annahme, jedoch seien die Forderungen in einen Bericht aufzunehmen, der bereits mit der Annahme zweier anderer Postulate (Po. 18.3376 und Po. 18.3233) in Auftrag gegeben worden war, erklärte er.

Der Nationalrat sollte sich in der Sommersession 2019 damit befassen, da jedoch auf jegliche Wortmeldungen verzichtet wurde, überwies der Rat das Postulat stillschweigend.<sup>3</sup>

---

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

2) AB NR, 2018, S. 210 f.

3) AB NR, 2019, S. 1324