année politique suisse

DOKUMENTATION · ANALYSE · DIFFUSION

Ausgewählte Beiträge zur Schweizer Politik

Suchabfrage	**17.04.2024**
Thema	**Keine Einschränkung**
Schlagworte	**Cyberkriminalität**
Akteure	**Dobler, Marcel (fdp/plr, SG) NR/CN, Hochuli, Susanne (AG, gp/verts)**
Prozesstypen	**Keine Einschränkung**
Datum	**01.01.1965 - 01.01.2021**

Impressum

Herausgeber

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

Beiträge von

Frick, Karin
Porcellana, Diane
Schmid, Catalina
Schubiger, Maximilian

Bevorzugte Zitierweise

Frick, Karin; Porcellana, Diane; Schmid, Catalina; Schubiger, Maximilian 2024. *Ausgewählte Beiträge zur Schweizer Politik: Cyberkriminalität, 2017 - 2020*. Bern: Année Politique Suisse, Institut für Politikwissenschaft, Universität Bern. www.anneepolitique.swiss, abgerufen am 17.04.2024.

Inhaltsverzeichnis

Abkürzungsverzeichnis

VBS	Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport
RK-SR	Kommission für Rechtsfragen des Ständerates
SiK-NR	Sicherheitspolitische Kommission des Nationalrates
AdA	Angehörige(r) der Armee
RS	Rekrutenschule
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken

DDPS	Département fédéral de la défense, de la protection de la population et des sports
CAJ-CE	Commission des affaires juridiques du Conseil des Etats
CPS-CN	Commission de la politique de sécurité du Conseil national
Militaire	Militaire
ER	École de recrues
SNPC	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. [1]

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 sicherheitpolitische 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. [2]

Innere Sicherheit

POSTULAT
DATUM: 21.06.2019
MAXIMILIAN SCHUBIGER

«**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. [3]

Kriminalität

MOTION
DATUM: 29.09.2017
KARIN FRICK

Vor dem Hintergrund der wachsenden Bedrohung durch Cyberkriminalität forderte eine im Sommer 2017 eingereichte Motion Dobler (fdp, SG) die **Schaffung einer zentralen Anlauf- und Koordinationsstelle zur Bekämpfung der organisierten und international tätigen Computerkriminalität**. Der zunehmenden Komplexität und Vielschichtigkeit dieser Art von Bedrohung sei die föderal fragmentierte Strafverfolgung in der Schweiz nicht gewachsen, weshalb es einer zentralen Anlaufstelle beim Bund bedürfe, um die Zusammenarbeit in der Strafverfolgung operativ zu koordinieren, so die Begründung des Motionärs. Dem Antrag des Bundesrates folgend, stimmte der Nationalrat in der Herbstsession 2017 dem Vorstoss stillschweigend zu. [4]

MOTION
DATUM: 14.03.2018
CATALINA SCHMID

Nach der einstimmigen Annahme im Nationalrat kam die Motion Dobler (fdp, SG), welche eine **zentrale Anlauf- und Koordinationsstelle zur Bekämpfung der organisierten und international tätigen Computerkriminalität** forderte, im Frühjahr 2018 zur Behandlung in den **Ständerat**. Die Bekämpfung der immer grösser werdenden Herausforderung der digitalen Kriminalität verlange eine stärkere Zentralisierung und Koordinierung bei der Beweiserhebung und -sicherung, begründete die RK-SR ihren einstimmigen Antrag auf Annahme. Wie Justizministerin Simonetta Sommaruga im Rat zustimmend anfügte, betreffe eine solche Anlauf- und Koordinationsstelle sowohl den Bund als auch die Kantone. Aus diesem Grund sei es sinnvoll, diese Zusammenarbeit gesetzlich zu verankern. Im Rahmen des Bundesgesetzes über polizeiliche Massnahmen zur Bekämpfung von Terrorismus (PMT), welches bereits in Vernehmlassung sei, sei eine gesetzliche Grundlage für die Bekämpfung der digitalen Kriminalität zudem vorgesehen. Diese Stossrichtung werde durch die Motion Dobler bestärkt; aus diesem Grund beantrage auch der Bundesrat deren Annahme. Der Ständerat folgte diesen Empfehlungen und nahm die Motion stillschweigend an. [5]

MOTION
DATUM: 19.06.2020
CATALINA SCHMID

Im Sommer 2020 **schrieb das Parlament** die Motion Dobler (fdp, SG) für eine **zentrale Anlauf- und Koordinationsstelle zur Bekämpfung der organisierten und international tätigen Computerkriminalität ab**, da der Bundesrat das Anliegen des Vorstosses in seiner Vorlage zum Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus (PMT) umgesetzt hatte. [6]

Landesverteidigung

Landesverteidigung

POSTULAT
DATUM: 21.06.2019
DIANE PORCELLANA

Le Conseil national a adopté le postulat de Marcel Dobler (plr, SG) visant à ce que le Conseil fédéral analyse les **standards applicables à la gestion des risques du fournisseur et la sécurité des composants cyberphysiques de l'armée**. Il est également attendu du Conseil fédéral qu'il juge si les mesures actuelles permettent d'identifier les risques et de les ramener à un niveau acceptable.
Dans sa réponse, le Conseil fédéral proposait d'accepter le postulat, pour que la sécurité soit contrôlée lors des acquisitions. [7]

Militärorganisation

POSTULAT
DATUM: 16.06.2017
MAXIMILIAN SCHUBIGER

Armee 2.0 – unter dieses Schlagwort setzte Postulant Dobler (fdp, SG) die Forderungen aus seinem Vorstoss. Die Schweiz müsse das **Technologie-Know-how fördern und sichern** und entsprechend auch im Bereich der Landesverteidigung Modifikationen vornehmen, erklärte er. Fünf Punkte wurden vom St. Galler umschrieben: Das Armeepersonal müsse in Anbetracht des technologischen und wissenschaftlichen Kompetenzbedarfs rekrutiert werden; der Personalbedarf im Bereich Cyberabwehr müsse abgeklärt werden; der Bundesrat solle prüfen, inwiefern mit Bildungsinstitutionen und der Wirtschaft zusammengearbeitet werden könne; Armeeangehörigen sollten diverse neue Typen von Ausbildungen und Einsätzen angerechnet werden können; sowie, fünftens, sollten neue Kriterien der Diensttauglichkeit formuliert werden („differenzierte Tauglichkeit"). Dobler reihte sich damit in eine Gruppe von Parlamentariern ein, welche die Armee bezüglich neuerer Bedrohungsszenarien aus dem Cyberspace und durch computergestützte Systeme besser aufstellen möchte. Technologie und Wissenschaft seien immer wichtiger für die Armee und solch hoch innovativer Themen müsse sich das Militär zuwenden, so der Postulant in seiner Begründung. Einzelne Möglichkeiten zur Anrechenbarkeit von Praktika bei Bundesbetrieben oder Hochschulen an die Dienstleistung seien zwar bereits gegeben, man müsse aber noch weitere Anreize schaffen. Im Fokus stünden dabei Projekte, die für das Militär einen Verwendungszweck haben. Der Bundesrat teilte offensichtlich die Stossrichtung des Postulats und beantragte dessen Annahme. Als es im Sommer 2017 im Nationalrat behandelt wurde, gab es keine Debatte, das Geschäft wurde diskussionslos angenommen. [8]

BERICHT
DATUM: 11.12.2020
DIANE PORCELLANA

En exécution du postulat Dobler, le Conseil fédéral a présenté son rapport dans lequel il décrit les mesures pour **garantir les compétences de l'armée dans les nouvelles technologies**. Parmi les mesures déjà entreprises, l'accent a notamment été mis sur la formation et le perfectionnement internes, afin de faciliter l'accès des futurs spécialistes à l'administration militaire. Les militaires qualifiés dans le civil pourront être promus au rang d'officiers spécialistes ou comme spécialistes. Les spécialistes en informatique participant au stage de formation «cyber» de l'armée pourront obtenir le brevet fédéral de spécialiste en cybersécurité. Le campus cyberdéfense, la collaboration avec les partenaires suisses et étrangers, l'engagement de l'économie privée au développement des technologies liées à la sécurité, permettent de développer et conserver les connaissances technologiques. Dans le futur, le DDPS prévoit de conclure et de consolider les partenariats dans le domaine, de soutenir la recherche et le développement des technologies, ainsi que de recruter et conserver un personnel (de milice) disposant de connaissances technologiques. [9]

---

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
4) AB NR, 2017, S. 1685
5) AB SR, 2018, S. 209 f.; Bericht RK-SR vom 12.2.18
6) BBl, 2019, S. 4751 ff.
7) BO CN, 2019, p.1324
8) AB NR, 2017, S. 1196
9) Rapport du Conseil fédéral du 11.12.2020