

Ausgewählte Beiträge zur Schweizer Politik

Suchabfrage	20.04.2024
Thema	Keine Einschränkung
Schlagworte	Cyberkriminalität
Akteure	Eder, Joachim (fdp/plr, ZG) SR/CE
Prozesstypen	Keine Einschränkung
Datum	01.01.1965 - 01.01.2024

Impressum

Herausgeber

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

Beiträge von

Bühlmann, Marc
Porcellana, Diane
Schubiger, Maximilian

Bevorzugte Zitierweise

Bühlmann, Marc; Porcellana, Diane; Schubiger, Maximilian 2024. *Ausgewählte Beiträge zur Schweizer Politik: Cyberkriminalität, 2017 – 2019*. Bern: Année Politique Suisse, Institut für Politikwissenschaft, Universität Bern. www.anneepolitique.swiss, abgerufen am 20.04.2024.

Inhaltsverzeichnis

Allgemeine Chronik	1
Grundlagen der Staatsordnung	1
Rechtsordnung	1
Äussere Sicherheit	1
Institutionen und Volksrechte	4
Regierungspolitik	4

Abkürzungsverzeichnis

EJPD	Eidgenössisches Justiz- und Polizeidepartement
EFD	Eidgenössisches Finanzdepartement
VBS	Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport
SiK-SR	Sicherheitspolitische Kommission des Ständerates
GPK	Die Geschäftsprüfungskommissionen
ETH	Eidgenössische Technische Hochschule
SiK-NR	Sicherheitspolitische Kommission des Nationalrates
FINMA	Eidgenössische Finanzmarktaufsicht
EDI	Eidgenössisches Departement des Inneren
MELANI	Melde- und Analysestelle Informationssicherheit
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
WBF	Eidgenössisches Departement für Wirtschaft, Bildung und Forschung
AdA	Angehörige(r) der Armee
RS	Rekrutenschule
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
NDB	Nachrichtendienst des Bundes
	(bis 2010: Strategischer Nachrichtendienst und Dienst für Analyse und Prävention)

DFJP	Département fédéral de justice et police
DFF	Département fédéral des finances
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
CdG	Les Commissions de gestion
EPF	École polytechnique fédérale
CPS-CN	Commission de la politique de sécurité du Conseil national
FINMA	Autorité fédérale de surveillance des marchés financiers
DFI	Département fédéral de l'intérieur
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information
DFAE	Département fédéral des affaires étrangères
DEFR	Département fédéral de l'économie, de la formation et de la recherche
Militaire	Militaire
ER	École de recrues
SNPC	Stratégie nationale de protection de la Suisse contre les cyberrisques
SRC	Service de renseignement de la Confédération
	(à 2010: Service de renseignement stratégique et Service d'analyse et de prévention)

Allgemeine Chronik

Grundlagen der Staatsordnung

Rechtsordnung

Rechtsordnung

POSTULAT
DATUM: 28.11.2019
DIANE PORCELLANA

Le Conseil fédéral a présenté son **rapport sur l'organisation de la Confédération pour la mise en œuvre de la Stratégie nationale de protection de la Suisse contre les cyberrisques** (SNPC), dans lequel il fournit également une réponse au postulat 18.3003 et à la motion Eder 17.3508. Depuis la transmission des interventions parlementaires, il a déjà adopté le plan de mise en œuvre de la SCNP 2018-2022, déterminé l'organisation de la Confédération dans le domaine des cyberrisques, défini les compétences et les responsabilités de la cyberdéfense militaire et a contribué à la création d'un centre de compétences pour la cybersécurité.

Les sept objectifs stratégiques et les 29 mesures à prendre dans les dix différents champs d'action sont détaillés dans la SNCP 2018-2022. Au sein de l'Administration fédérale, Délégation Cyber du Conseil fédéral surveillera la mise en œuvre de la stratégie. Le délégué de la Confédération à la cybersécurité se chargera, d'une part, de la direction stratégique et d'autre part, il chapeautera le Groupe Cyber – responsable de la coordination des domaines – et le comité de pilotage de la SNCP. Le centre de compétences assumera la direction stratégique de la cybersécurité de la Confédération, du guichet unique national, du service spécialisé de sécurité informatique et du pool de compétences pour la cybersécurité. L'armée formera ses cadres et membres en matière de cybersécurité. Avec les autorités civiles, elle devra définir les conditions-cadres de son soutien lors de cyberincidents et le déroulement de son intervention. Trois projets propices à l'innovation seront mis en œuvre afin de réduire la dépendance à l'égard de prestataires et de fabricants de logiciels et de matériel étrangers. Pour la réalisation, des ressources financières et en personnel supplémentaires seront nécessaires. D'après l'étude du Center for Security Studies de l'EPF de Zurich, les structures dans le domaine de la cybersécurité en Suisse se retrouvent à l'étranger. Aucun des pays étudiés ne possède d'organisation unique pour la réalisation des travaux liés aux cyberrisques et n'a confié à son armée la responsabilité d'assurer la protection contre ce type de danger.¹

Äussere Sicherheit

MOTION
DATUM: 19.09.2017
MAXIMILIAN SCHUBIGER

Zeitgleich mit Josef Dittli (cvp, UR) reichte auch Ständerat Eder (fdp, ZG) eine Motion zu Cyber-Fragen ein. Er fokussierte jedoch nicht auf Armeestrukturen, sondern regte generell die **Schaffung eines Cybersecurity-Kompetenzzentrums auf Stufe Bund** an. Im Laufe der Überprüfung der NCS sollte der Bund Massnahmen in die Wege leiten, um eine solche Organisationseinheit zu schaffen. Eder schwebte eine Koordinationsstelle vor, die bundesweit die Vorgänge im Bereich der Cybersicherheit überwacht und fördert, die jedoch ferner auch eine Weisungsbefugnis gegenüber den Ämtern erhalten sollte. Die Notwendigkeit einer solchen Stelle leitete Eder aus früheren parlamentarischen Vorstössen sowie dem Geschäftsbericht des Bundesrates über das vergangene Jahr ab, wo klar geworden sei, dass noch zu wenig für die Cybersicherheit gemacht werde. Wie sein Ratskollege Dittli regte Eder eine Zusammenarbeit mit Wissenschaft und Hochschulen sowie der IT-Branche an.

Der Bundesrat teilte die Auffassung, dass der Cyberbereich eine Koordinationsstelle braucht. Zusammen mit MELANI sei eine solche Stelle jedoch bereits geschaffen worden. Das Know-how sei vorhanden und die geforderte Weisungsbefugnis sei auch bereits erteilt worden. Bei grösseren Cybervorfällen würden departementsübergreifende Task-Forces eingesetzt, um Kräfte zu bündeln. Die Bedrohung werde zunehmen – dessen war sich auch die Regierung sicher – und die Anforderungen an die Durchhaltefähigkeit der zuständigen Stellen steige im Ereignisfall. Ein Koordinationszentrum, wie es in der Motion gefordert wird, sei entsprechend fachlich und personell weiterzuentwickeln. Genau dies werde in der Weiterentwicklung der NCS angestrebt, weswegen der Bundesrat die Ablehnung der Motion beantrage.

Anders sah dies der Ständerat. Die Motion wurde mit 41 zu 4 Stimmen deutlich angenommen. Der Abstimmung ging jedoch eine längere Debatte voraus, die rasch verdeutlichte, dass der Bundesrat allein auf weiter Flur stand. Der Motionär selbst eröffnete die Beratungen mit seiner Erstaunensbekundung: Zwar sage die Regierung,

sie wolle die Kompetenzen zur Cyberabwehr verstärken und koordinieren, aber die Motion wolle sie nicht zur Annahme empfehlen. Das passe nicht zusammen und das gehe auch für andere Mitunterzeichnende (22 an der Zahl) nicht auf. Verdeutlichen konnte er sein Anliegen mit eben bekannt gewordenen Angriffen auf zwei Departemente. Die Meinung, dass die Meldestelle MELANI bereits Aufgaben im Cyberbereich wahrnehme, teilte der Motionär nicht. Deren Arbeit stellte er nicht infrage, aber in der noch gültigen Cyberstrategie des Bundes komme das Wort "Cybersecurity-Kompetenzzentrum nicht ein einziges Mal vor." Daraufhin hielt er ein eigentliches Plädoyer für die Sache, man müsse endlich handeln – die beiden ETH stünden bereit. Weitere Redner pflichteten Eder (fdp, ZG) bei. Besonders Vertreter der SP sprachen sich dabei für einen Ausbau der Cyberabwehr aus, durchaus auch zu Lasten von anderen Abwehrprogrammen (Rüstung). Erich Ettlin (cvp, OW) fand die Debatte dann "fast schon langweilig", weil sich alle einig waren. Alle ausser Bundesrat Maurer, der die Regierung vertrat. Sein langes Votum – im Wesentlichen zeigte er die bisher angewendeten Vorgänge und Massnahmen auf und die Tatsache, dass kaum eine Bundesratssitzung ohne Cyber-Thema abgehalten werde – schloss er mit dem Appell, man solle die Regierung und MELANI nicht unterschätzen. Das Plenum wollte jedoch ganz offensichtlich ein Zeichen setzen und die Arbeiten im Cyberbereich dergestalt bündeln, dass eine zentrale Stelle die Koordination übernimmt.²

MOTION
DATUM: 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 armeenahere 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 Ettlín (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.³

MOTION

DATUM: 07.12.2017

MAXIMILIAN SCHUBIGER

Die **Schaffung eines Cybersecurity-Kompetenzzentrums auf Stufe Bund** war im Ständerat kaum bestritten und auch im Vorfeld an die Plenardebatte in der grossen Kammer wurden die Zeichen auf grün gesetzt. Das auf eine Motion Eder (fdp, ZG) zurück gehende Anliegen fand einstimmige Unterstützung in der sicherheitspolitischen Kommission des Nationalrates. Sie kam nach Gesprächen mit Cybersicherheits-Fachpersonen aus der Bundesverwaltung sowie unter Berücksichtigung der bereits laufenden Arbeiten im Bereich der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) und dem entsprechenden Aktionsplan zum Schluss, dass die Motion unterstützt werden soll, denn tiefer greifende Koordination sei im Cyberbereich notwendig. Ein Kompetenzzentrum für Cybersicherheit sei hierzu der richtige Weg.

Kommissionssprecher Glättli (gp, ZH) präziserte in seiner Einleitung zur Debatte, dass die MELANI nur über beschränkte Personalressourcen verfüge und zudem ihr Auftrag limitiert sei. MELANI, als verwaltungsinterne Koordinationsstelle auch für Cyberkriminalität zuständig, leiste gute Arbeit, so Glättli weiter, es bedürfe aber weiter reichender Kompetenzen für ein eigentliches Kompetenzzentrum. Der anwesende Bundesrat Maurer vertrat auch im Nationalrat die ablehnende Haltung des Siebnerkollegiums: Es werde bereits viel im Cyberbereich unternommen und diverse Expertengruppen würden bald ihre Arbeiten abschliessen. Insofern bat Maurer die Nationalrätinnen und Nationalräte, nicht vorzugreifen. Im Wesentlichen zielten die gegenwärtig angestossenen Prozesse in die gleiche Richtung, wie der Motionär vorgebe, und dies ohne Aufblähung der Verwaltung. Letzteres befürchtete Maurer, falls eine zusätzliche Verwaltungseinheit geschaffen werden müsste. Kommissionssprecher Glättli entgegnete hierauf, dass mit der Motion noch keine operativen Beschlüsse gefasst und die Ausgestaltung und Umsetzung eines solchen Cyber-Kompetenzzentrums Gegenstand weiterer Diskussionen sein würden.

Das Ratsplenum folgte seiner Kommission und hiess die Motion mit 177 zu 2 Stimmen ohne Enthaltungen deutlich gut.⁴

MOTION

DATUM: 06.03.2018

MAXIMILIAN SCHUBIGER

Mit 58 Mitunterzeichnenden aller Parteien im Rücken forderte Franz Grüter (svp, LU) den Bundesrat mittels Motion auf, den **Ausbau der Cyberabwehrkompetenzen** voranzutreiben. Innerhalb zweier Jahre sollen alle sicherheitspolitischen Kompetenzen im Bereich Cyberabwehr zudem gebündelt werden und innerhalb der Verwaltung von einer einzigen Stelle koordiniert werden können. Dabei wurde offen gelassen, ob diese Einheit innerhalb der Armee geschaffen oder dem VBS angegliedert werden soll. Jedoch sah der Motionär eine Finanzierung via das Rüstungsbudget vor. Ferner sollte auch bezüglich künftiger Beschaffungen ein Augenmerk auf Cybersicherheit gelegt werden. Grüter schlug damit in die gleiche Kerbe wie Ständerat Dittli (fdp, UR), der seinerseits ein Cyberdefence-Kommando anregte, und Ständerat Eder (fdp, ZG), der die Schaffung

eines Kompetenzzentrums für Cyberfragen verlangte. Begründet wurde die Motion mit den neuen Bedrohungsszenarien im digitalen Raum sowie mit der Erfahrung kürzlich stattgefundener Angriffe auf die Computerinfrastruktur von Bund und Wirtschaft. Der Luzerner wollte darüber hinaus ebenfalls – dieses Anliegen deckt sich mit den Bestreben der beiden Motionen aus der kleinen Kammer – die Zuständigkeit neu regeln und nur eine Verwaltungsstelle mit der Aufsicht betrauen, um «Redundanzen, Ineffizienzen und Koordinationsaufwand» reduzieren zu können.

Der Bundesrat, der sich also bereits wiederholt mit ähnlichen Vorstössen konfrontiert sah, beharrte auf der Ablehnung dieser Forderungen. Im Grunde sei er ja nicht gegen einen Ausbau im Cyberbereich, jedoch sollte den Prozessen der NCS nicht vorgegriffen werden, erklärte er. Eine einzige Stelle für diese Oberaufsicht werde geprüft.

Dieser bundesrätlichen Zurückhaltung stand, wie auch in den anderen diesbezüglichen Geschäften, eine wohlwollende Parlamentskammer gegenüber. Im Wissen um die bereits genehmigten anderen beiden Motionen Dittli und Eder hiess der Nationalrat auch die vorliegende Motion gut. Grüter gelang es, Druck aufzubauen, in dem er auf der Einrichtung einer zentralen Koordinationsstelle beharrte. Dabei bot er in der Ratsdebatte bereits Hand zu einer Lösung: Melani könne diese Aufgabe übernehmen, es brauche also nicht einmal eine neue Verwaltungseinheit, schlug er vor. Jedoch müsse dort mehr investiert und sowohl personell als auch finanziell mehr Aufwand betrieben werden. Zudem müsse der Auftrag an Melani neu verfasst werden. Bundesrat Maurer vertrat die ablehnende Haltung der Regierung, auch mit Verweis auf ein kurz zuvor angenommenes SiK-Kommissionspostulat, vergeblich. Die grosse Kammer überwies den Vorstoss mit 134 zu 47 Stimmen und 9 Enthaltungen der Ständekammer.⁵

Institutionen und Volksrechte

Regierungspolitik

BUNDESRATSGESCHÄFT
DATUM: 17.06.2019
MARC BÜHLMANN

Der **Geschäftsbericht des Bundesrats 2018** wurde von den Räten in der Sommersession 2019 beraten. Im Geschäftsbericht legt die Regierung Rechenschaft über die Schwerpunkte ihrer Tätigkeiten in einem Berichtsjahr ab. In den Ratsdebatten berichten die Vertreterinnen und Vertreter der Aufsichtskommissionen über die Beratungen, die sie mit den Bundesrätinnen und Bundesräten zum Geschäftsbericht geführt haben. National- und Ständerat nehmen dann in Form eines Bundesbeschlusses Kenntnis von diesem Bericht.

Für die GPK berichteten Anne Seydoux-Christe (cvp, JU) im Ständerat und Doris Fiala (fdp, ZH) im Nationalrat. Die GPK hätten mit der Regierung zwei Querschnittsthemen behandelt, deren Auswertungen noch ausstünden: den Umgang der Departemente mit Kritik durch Bürgerinnen und Bürger bei Aufsichtsbeschwerden sowie die Ferien- und Zeitguthaben der Topkader in der Bundesverwaltung. Die Fragen der GPK seien vom Bundesrat zufriedenstellend beantwortet worden und man beantrage deshalb die Genehmigung des Geschäftsberichts.

In der Folge berichteten Subkommissionssprecherinnen und -sprecher gestützt auf den Geschäftsbericht über die einzelnen Departemente. Sowohl im Ständerat als auch im Nationalrat stand dabei die Cyberabwehr im VBS im Zentrum. Er könne mit Genugtuung feststellen, dass sich der Bund der Dringlichkeit dieses Themas bewusst sei, führte Damian Müller (fdp, LU) im Ständerat aus. Insbesondere durch die Cyberattacke auf die RUAG sei das VBS sensibilisiert worden und habe den Aktionsplan Cyberdefence ausgearbeitet, berichtete hierzu Ida Glanzmann (cvp, LU) in der grossen Kammer. Beim EDA stand die Frage «Wie weiter mit dem Brexit?» im Zentrum. Damien Müller führte aus, dass ein geordneter Übergang mit insgesamt fünf unterzeichneten Abkommen möglich sein sollte. Ida Glanzmann berichtete bei der Präsentation des EDA über die Diskussionen um den aufgeschobenen Beitritt der Schweiz zum Kernwaffenverbotvertrag. Entgegen einer angenommenen Motion Sommaruga (sp, GE; Mo. 17.4241) wolle man im Moment nur einen Beobachterstatus anstreben, um die Neutralität der Schweiz nicht zu gefährden. Beim WBF wurde in beiden Räten über den ETH-Bereich berichtet. Gegenstand waren die medial begleiteten Vorwürfe gegen verschiedene Personen an der ETH Zürich, Mobbing, Korruption sowie Amts- und Machtmissbrauch betrieben zu haben. Die GPK sei nach intensiven Gesprächen mit den Verantwortlichen der ETH zur Überzeugung gelangt, dass es einen Kulturwandel brauche, führte Yvonne Feri (sp, AG) im Nationalrat aus. Die Oberaufsicht über die ETH unterliege Bundesrat Parmelin und der sei sich der Situation bewusst, versicherte Joachim Eder (fdp, ZG) im Ständerat. Ein weiteres WBF-Thema in beiden Räten waren die Kriegsmaterialausfuhren. Man habe ja manchmal das Gefühl, die Schweiz liefere Waffen an Schurkenstaaten, so Joachim Eder in der kleinen Kammer. Dies sei aber

mitnichten der Fall. Vielmehr stehe die Schweiz hinsichtlich Transparenz von Waffenexporten international an erster Stelle. Man habe aber Fragen im Zusammenhang mit Medienberichten über Schweizer Handgranaten und Sturmgewehre, die angeblich im Jemen-Krieg aufgetaucht seien, klären können – so Yvonne Feri im Nationalrat. Beim EFD wurden die Rolle der Finma und die Cyberrisiken für den Finanzplatz Schweiz diskutiert. Die Finma nehme ihre Aufsicht gut wahr und das «interdepartementale Kompetenzgerangel» beim Thema Cyberrisiken habe sich erledigt: Die Federführung und die Koordination liegen beim EFD, das VBS ist zuständig für die Cyberdefence und das EJPD für die Cyberkriminalität. Von speziellem Interesse war die Postauto-Affäre, auf die der Bundesrat im Geschäftsbericht auf Geheiss der GPK in einem eigenen Kapitel eingehen musste. Diesem Auftrag sei die Exekutive nachgekommen, berichtete Claude Hêche (sp, JU) im Ständerat. Die Aufarbeitung der Affäre sei jedoch noch nicht abgeschlossen. Darüber hinaus erwähnte Hêche bei der Berichterstattung zum EDI die Gesundheitskosten, deren Wachstum als problematisch betrachtet werde. Gesundheitsminister Alain Berset habe aber alle Fragen der GPK beantworten können. Peter Föhn (svp, SZ) und Valérie Piller Carrard (sp, FR) berichteten schliesslich über die Bundeskanzlei und das EJPD. Bei der Bundeskanzlei standen Fragen zur Entwicklung bei Vote Electronique im Vordergrund. Die GPK würden die Problematik eng begleiten, so die Subkommissionssprecherin bzw. der Subkommissionssprecher. Hauptthema beim EJPD war die Terrorismusbekämpfung. Es gebe nach wie vor ein Sicherheitsrisiko für die Schweiz und die Kantone; mit verschiedenen Projekten und vor allem dem anstehenden neuen Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus würde hier aber viel unternommen.

In beiden Räten fasste Ueli Maurer in seiner Funktion als Bundespräsident ein paar der erreichten Ziele im Rahmen der drei Leitlinien (Wohlstandsicherung; nationaler Zusammenhalt und internationale Zusammenarbeit; Sicherheit und verlässliche internationale Partnerschaften) zusammen. Er bedankte sich am Schluss für die sehr offene und konstruktive Zusammenarbeit mit den GPK. Der Bundesrat profitiere sehr von den Fragen und Hinweisen einer Kommission, «die sehr oft unterhalb des Radars arbeitet, das aber sehr intensiv und gut macht».⁶

1) Plan de mise en oeuvre de la SNPC 2018-2022; Rapport CF du 27.11.19

2) AB SR, 2017, S. 661 ff.; LZ, TA, 20.9.17

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

4) AB NR, 2017, S. 1994 ff.; Bericht SiK-NR vom 30.10.2017; SGT, TA, TG, 8.12.17

5) AB NR, 2018, S. 217 f.

6) AB NR, 2019, S. 1138 ff.; AB SR, 2019, S. 402 ff.; BBI, 2019, S. 4651; Geschäftsbericht des Bundesrates 2018 (I); Geschäftsbericht des Bundesrates 2018 (II)