année politique suisse

DOKUMENTATION · ANALYSE · DIFFUSION

Ausgewählte Beiträge zur Schweizer Politik

Suchabfrage	**17.04.2024**
Thema	**Keine Einschränkung**
Schlagworte	**Cyberkriminalität**
Akteure	**Keine Einschränkung**
Prozesstypen	**Bundesratsgeschäft**
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
Frick, Karin
Heidelberger, Anja
Hirter, Hans
Magnin, Chloé
Porcellana, Diane
Schubiger, Maximilian

Bevorzugte Zitierweise

Bühlmann, Marc; Frick, Karin; Heidelberger, Anja; Hirter, Hans; Magnin, Chloé; Porcellana, Diane; Schubiger, Maximilian 2024. ***Ausgewählte Beiträge zur Schweizer Politik: Cyberkriminalität, Bundesratsgeschäft, 1991 - 2023***. Bern: Année Politique Suisse, Institut für Politikwissenschaft, Universität Bern. www.anneepolitique.swiss, abgerufen am 17.04.2024.

Inhaltsverzeichnis

Abkürzungsverzeichnis

EJPD	Eidgenössisches Justiz- und Polizeidepartement
EFD	Eidgenössisches Finanzdepartement
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
VBS	Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport
AHV	Alters- und Hinterlassenenversicherung
SiK-SR	Sicherheitspolitische Kommission des Ständerates
GPK	Die Geschäftsprüfungskommissionen
ETH	Eidgenössische Technische Hochschule
SiK-NR	Sicherheitspolitische Kommission des Nationalrates
GPK-SR	Geschäftsprüfungskommission des Ständerates
FINMA	Eidgenössische Finanzmarktaufsicht
EU	Europäische Union
EDI	Eidgenössisches Departement des Inneren
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
GPDel	Geschäftsprüfungsdelegation
BJ	Bundesamt für Justiz
RK MZF	Regierungskonferenz Militär, Zivilschutz und Feuerwehr
KMU	Kleine und mittlere Unternehmen
BWIS	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
WBF	Eidgenössisches Departement für Wirtschaft, Bildung und Forschung
SGV	Schweizerischer Gewerbeverband
MG	Bundesgesetz über die Armee und die Militärverwaltung (Militärgesetz)
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
BK	Bundeskanzlei
AO	Verordnung der Bundesversammlung über die Organisation der Armee
IZA	Internationale Zusammenarbeit
Fedpol	Bundesamt für Polizei
NCSC	Nationales Zentrum für Cybersicherheit
ISG	Informationssicherheitsgesetz

DFJP	Département fédéral de justice et police
DFF	Département fédéral des finances
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication
DDPS	Département fédéral de la défense, de la protection de la population et des sports
AVS	Assurance-vieillesse et survivants
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
CDG-CE	Commission de gestion du Conseil des Etats
FINMA	Autorité fédérale de surveillance des marchés financiers
UE	Union européenne
DFI	Département fédéral de l'intérieur
PFPDT	Préposé fédéral à la protection des données et à la transparence
DélCDG	Délégation des Commissions de gestion
OFJ	Office fédéral de la justice
CG MPS	Conférence gouvernementale des affaires militaires, de la protection civile et des sapeurs-pompiers
PME	petites et moyennes entreprises
LMSI	Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure
DFAE	Département fédéral des affaires étrangères
DEFR	Département fédéral de l'économie, de la formation et de la recherche
USAM	Union suisse des arts et métiers

LAAM	Loi fédérale sur l'armée et l'administration militaire (Loi sur l'armée)
SNPC	Stratégie nationale de protection de la Suisse contre les cyberrisques
ChF	Chancellerie fédérale
OOrgA	Ordonnance de l'Assemblée fédérale sur l'organisation de l'armée
CI	coopération internationale
Fedpol	Office fédéral de la police
NCSC	Centre national pour la cybersécurité
LSI	Loi fédérale sur la sécurité de l'information

Allgemeine Chronik

Grundlagen der Staatsordnung

Rechtsordnung

Innere Sicherheit

BUNDESRATSGESCHÄFT
DATUM: 29.11.2009
MARC BÜHLMANN

Im Berichtsjahr standen nach wie vor die Bekämpfung bzw. Schaffung von Instrumenten zur Ermittlung von Internetkriminalität im Vordergrund. Der Ständerat nahm den Entwurf des Bundesrats zur Umsetzung des Übereinkommens des Europarates über die **Cyberkriminalität** einstimmig an. Das internationale Übereinkommen richtet sich gegen die Computer- und Netzwerkkriminalität. Damit erübrige sich aber laut der Kleinen Kammer die Motion Darbellay (cvp, VS; Mo. 09.4307), die eine rasche Ratifizierung des Übereinkommens verlangt hat und vom Nationalrat in der Frühjahrssession angenommen wurde. [1]

BUNDESRATSGESCHÄFT
DATUM: 16.10.2014
KARIN FRICK

Um den komplexer und dynamischer werdenden Bedrohungen für die Informationsgesellschaft Rechnung zu tragen, beabsichtigte der Bundesrat, ein **Bundesgesetz über die Informationssicherheit (ISG)** zu schaffen. Angriffe auf Informationssysteme des Bundes hätten wiederholt gezeigt, dass der Schutz von Informationen Lücken aufweise, welche unter anderem auf unzeitgemässe und inkohärente Rechtsgrundlagen zurückzuführen seien. Mit dem neuen Gesetz sollen einheitliche gesetzliche Grundlagen für das Management der Informationssicherheit beim Bund geschaffen und somit Schwachstellen des geltenden Rechts behoben werden. Den Begriff der Informationssicherheit definierte der Bundesrat im erläuternden Bericht als «sämtliche Anforderungen und Massnahmen, die zum Schutz der Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit von Informationen dienen, und zwar unabhängig davon, ob die Informationen elektronisch, mündlich oder in Papierform bearbeitet werden.» Die im bestehenden System sektoriell angelegten Rechtsgrundlagen und organisatorischen Zuständigkeiten seien nicht effizient und sollten daher durch eine einheitliche Regelung ersetzt werden.

Bei der im Jahr 2014 durchgeführten Vernehmlassung waren überwiegend positive Rückmeldungen eingegangen. Von den insgesamt 55 Vernehmlassungsteilnehmerinnen und -teilnehmern standen unter anderen 17 Kantone, die CVP und die SP, Economiesuisse sowie die Bundesanwaltschaft und ihre Aufsichtsbehörde dem Entwurf grundsätzlich positiv gegenüber, brachten jedoch einige Änderungsvorschläge an. Diese bezogen sich vor allem auf die Zusammenarbeit zwischen Bund und Kantonen, die Präzisierung von im Gesetzestext verwendeten Begriffen sowie auf die Schnittstellen zwischen Informationssicherheit, Datenschutz und Öffentlichkeitsprinzip. Sieben Kantone, die FDP sowie drei weitere Teilnehmende, darunter das Bundesgericht, sprachen ihre vorbehaltlose Zustimmung zur Vorlage aus. Vollumfänglich ablehnend äusserte sich einzig die SVP, die im neuen Gesetz keinen Mehrwert gegenüber gezielten Verbesserungen am heutigen System sah. Von den drei Teilnehmenden, die dem Entwurf grundsätzlich skeptisch gegenüberstanden, würde der Kanton Bern dem Entwurf nur unter der Voraussetzung zustimmen, dass die kantonalen und kommunalen Behörden bei der Anwendung des ISG auf die im Gesetz vorgesehenen Fachstellen des Bundes zurückgreifen können und sie diese nicht selber aufbauen müssen. Der SGV kritisierte indessen den «irreführenden Titel» sowie die mangelhafte Qualität der erläuternden Materialien. Nach seinem Vorschlag sollte das Gesetz besser «Bundesgesetz über die Informationssicherheit in Bundesbehörden und ähnlichen Organisationen» genannt werden, da es sich nicht um ein gesamtgesellschaftliches Regelwerk zu Information und Informationssicherheit handle. Im Ergebnisbericht des Vernehmlassungsverfahrens folgerte das Generalsekretariat des VBS, dass die überwiegende Mehrheit der Vernehmlasserinnen und Vernehmlasser die Schaffung eines Informationssicherheitsgesetzes begrüsst. [2]

BUNDESRATSGESCHÄFT
DATUM: 04.12.2017
KARIN FRICK

In seiner dem Parlament im Februar 2017 unterbreiteten Botschaft stellte der Bundesrat den Entwurf zum neuen **Informationssicherheitsgesetz** (ISG) vor. Im Zentrum des Gesetzgebungsprojektes stehen mit der Zusammenführung der wichtigsten Rechtsgrundlagen im Bereich der Informations- und Informatikmittelsicherheit des Bundes in einen einzigen Erlass sowie mit der Einführung einer einheitlichen Regelung für alle Behörden und Organisationen des Bundes zur Erreichung eines möglichst einheitlichen Sicherheitsniveaus zwei ambitiöse Ziele. Dazu sollen im neuen Gesetz insbesondere das Risikomanagement, die Klassifizierung von Informationen, die Sicherheit beim Einsatz von Informatikmitteln, die personellen Massnahmen und der physische Schutz von Informationen und Informatikmitteln geregelt werden. Ausdrücklich festgehalten werden soll auch der Vorrang des Öffentlichkeitsgesetzes, um zu betonen, dass das Öffentlichkeitsprinzip in der Verwaltung weiterhin uneingeschränkte Geltung haben wird. Überdies überführte der Bundesrat die Regelungen über die Personensicherheitsprüfung vom BWIS in das neue ISG und erweiterte den Geltungsbereich des militärischen Betriebssicherheitsverfahrens auf zivile Beschaffungen, um die Informationssicherheit bei der Vergabe von sicherheitsempfindlichen Aufträgen an Dritte zu gewährleisten. Die Kantone sind vom neuen Gesetz insofern betroffen, als sie bei der Bearbeitung von klassifizierten Informationen des Bundes und beim Zugriff auf seine Informatikmittel für eine gleichwertige Informationssicherheit sorgen müssen. Dazu sollen sie in einem Koordinationsorgan Einsitz nehmen.

Mit einem langen Votum eröffnete Ständerat Isidor Baumann (cvp, UR) als Sprecher der vorberatenden SiK-SR in der Wintersession 2017 die Debatte im Erstrat. Er gab dem Ratsplenum einen Einblick in die Arbeiten der Kommission und legte dar, wie sie im Verlaufe von vier Sitzungen zu ihren Entscheidungen gelangt war. Zum grossen und sehr grundsätzlichen Diskussionspunkt der Gesetzesentschlackung führte er aus, man habe sich von der Verwaltung erklären lassen, dass Umfang und Dichte der vorgeschlagenen Regulierung – der Gesetzesentwurf umfasst immerhin 92 Artikel – notwendig seien, weil die Bestimmungen für verschiedenste Behörden, darunter auch das Bundesgericht und die Nationalbank, gelten sollen und eine solche einheitliche Lösung nur auf Gesetzes- und nicht auf Verordnungsstufe erlassen werden könne. Um sich ein besseres Bild von den Auswirkungen des neuen Gesetzes machen zu können, hatte die Kommission bei der Bundesverwaltung weitere Unterlagen angefordert, so beispielsweise eine Liste der zu schliessenden rechtlichen Lücken, eine Auflistung der indirekten Auswirkungen auf die Kantone und genauere Angaben zu personellen und finanziellen Folgen. Darüber hinaus hatte sie Professor Markus Müller, Leiter der Expertengruppe, die am Anfang dieses Gesetzgebungsprojektes gestanden hatte, EDÖB Adrian Lobsiger, RK-MZF-Generalsekretär Alexander Krethlow sowie Vertreterinnen und Vertreter des Bundesgerichts, der Parlamentsdienste, der Nationalbank und der Wirtschaft angehört. Der integrale Ansatz und die angestrebte Vereinheitlichung seien am Gesetzgebungsprojekt von allen Eingeladenen gelobt worden und auch der Handlungsbedarf sei unbestritten anerkannt worden. Kritisiert worden sei die Vorlage vor allem von der Wirtschaftsvertretung, welche das Gesetz auf seine KMU-Tauglichkeit überprüft und mit der laufenden Revision des Bundesgesetzes über das öffentliche Beschaffungswesen abgestimmt wissen wollte. Krethlow habe indes als Kantonsvertreter die Forderung platziert, dass die Kantone für ihre Tätigkeiten im Zusammenhang mit dem Informationssicherheitsgesetz vollumfänglich vom Bund entschädigt werden sollten. Zusammen mit einer Stellungnahme des VBS hatten die in den Anhörungen vorgebrachten Vorschläge und Empfehlungen der Kommission als Grundlage für die Detailberatung gedient. Noch unklar war die Höhe der Umsetzungskosten gewesen, weil das anzustrebende Sicherheitsniveau von den Bundesbehörden erst im Rahmen des Vollzugs festgelegt werde. Der Bundesrat habe sich jedoch einverstanden gezeigt, die SiK-SR zu allen kostenrelevanten Umsetzungsstrategien und Vollzugserlassen zu konsultieren. Die SiK-SR hatte dem Entwurf sodann einstimmig zugestimmt. Nach diesen umfangreichen Erläuterungen trat der Ständerat ohne Gegenantrag auf die Vorlage ein.

In der Detailberatung zeigte sich die Unbestrittenheit der Vorlage: Zu keinem der zahlreichen Änderungsanträge der SiK-SR fand eine Diskussion statt und auch der Bundesrat zeigte sich mit allen Anpassungen einverstanden. Trotz der vielen Anträge, die alle stillschweigend angenommen wurden, änderte sich inhaltlich nur wenig am Entwurf des Bundesrates. So wurde die Trinkwasserversorgung explizit in die Liste der kritischen Infrastrukturen aufgenommen und die systematische (und nicht nur vorübergehende) Verwendung der AHV-Nummer zur Identifikation von Personen, die Zugang zu Informationen, Informatikmitteln, Räumlichkeiten und anderen Infrastrukturen des Bundes haben, erlaubt. Die Bestimmung, wonach Umsetzung,

Zweckmässigkeit, Wirksamkeit und Wirtschaftlichkeit des ISG periodisch überprüft werden muss, ergänzte der Ständerat dahingehend, dass diese Überprüfung durch eine unabhängige Stelle, namentlich durch die Eidgenössische Finanzkontrolle, zu geschehen habe. Des Weiteren nahm er das Personal von Fedpol und Bundesanwaltschaft einerseits sowie dolmetschende und übersetzende Personen im Asylbereich andererseits in den Kreis jener Personen auf, die unabhängig davon, ob sie Zugang zu geschützten Informationen oder Informatiksystemen des Bundes haben, einer Sicherheitsprüfung unterzogen werden können. Ins Muster der fehlenden Kontroverse fügte sich schliesslich auch die Gesamtabstimmung ein, bei der die kleine Kammer die Vorlage einstimmig (bei vier Enthaltungen) annahm. [3]

BUNDESRATSGESCHÄFT
DATUM: 13.03.2018
KARIN FRICK

Wie im vergangenen Dezember schon der Ständerat und dessen sicherheitspolitische Kommission stellte im Frühjahr 2018 auch die SiK-NR Handlungsbedarf im Informationssicherheitsmanagement des Bundes fest. Anders als ihre Schwesterkommission, der die kleine Kammer widerstandslos gefolgt war, zweifelte die nationalrätliche Kommission jedoch am Mehrwert, den das **Informationssicherheitsgesetz** mit sich brächte. Die bedeutendsten Unbekannten im Gesetzgebungsprojekt waren nach wie vor die Kosten und der Personalaufwand im Zusammenhang mit der Umsetzung. Während sich der Ständerat mit der Zusicherung zufriedengegeben hatte, zu den Kosten später noch einmal konsultiert zu werden, beauftragte die SiK-NR die Verwaltung, die Kosten und den Personalaufwand für verschiedene mögliche Sicherheitsniveaus zu beziffern. Es wurden also drei mögliche Szenarien vorgestellt: Ambitionsniveau 1 mit Kosten von CHF 5 Mio. und 9,5 bis 15,5 zusätzlichen Stellen, Ambitionsniveau 2 mit Kosten von CHF 33 bis 58 Mio. und 42 zusätzlichen Stellen sowie Ambitionsniveau 3 mit Kosten von CHF 62 bis 87 Mio. und 78 zusätzlichen Stellen. Für die Kommissionsmehrheit standen diese beträchtlichen Kosten in einem ungenügenden Verhältnis zum Ertrag und darüber hinaus befürchtete sie, der neu geschaffene, komplexe Informationsschutzapparat könnte eine Eigendynamik entwickeln und sich zunehmend der Kontrolle durch das Parlament entziehen. Aus diesen Gründen beantragte die Mehrheit der SiK-NR ihrem Rat Nichteintreten. Eine Minderheit erachtete hingegen den gesamtheitlichen Ansatz der Vorlage als zentral, um die Informationssicherheit beim Bund zu verbessern. Sie hielt die Kosten für vertretbar, da dadurch Sicherheitslücken geschlossen und die Koordination erheblich verbessert werden könne. Einen drohenden Kontrollverlust des Parlaments sah sie nicht und beantragte folglich Eintreten. Die Eintretensdebatte gestaltete sich dementsprechend umfangreich, kontrovers und emotionsgeladen.

Die bürgerlichen Fraktionen machten sich – mit Ausnahme der BDP – für den Nichteintretensantrag stark. Die Kosten entsprächen einer «Blackbox» und es sei «unseriös», nur auf Annahmen gestützt zu entscheiden; anstatt Experimente zu machen, sollten besser bestehende Gesetze angepasst werden, um die Sicherheit zu gewährleisten, so Ida Glanzmann-Hunkeler (cvp, LU) als Vertreterin der CVP-Fraktion. David Zuberbühler (svp, AR) legte die Ansicht der SVP-Fraktion dar: Das Gesetz sei ein neues «Bürokratiemonster», biete nur «Scheinsicherheit» und sei einen konkreten Nutzennachweis bisher schuldig geblieben, weshalb es «brandgefährlich» sei, darauf einzutreten. Für die FDP-Fraktion waren vor allem die Bedenken bezüglich der Kostenfolgen ausschlaggebend dafür, dass man nicht auf das überladene Gesetz und den damit verbundenen «Blindflug» eintrete. Demgegenüber stellte BDP-Fraktionssprecherin Rosmarie Quadranti (bdp, ZH) Eintreten als alternativlos dar; angesichts des Handlungsbedarfs sei Nichtstun jetzt «fahrlässig». Priska Seiler Graf (sp, ZH) hielt als Vertreterin der SP-Fraktion eine regelrechte Brandrede für Eintreten: Das Gesetz werde dringend benötigt und es sei «fatal», dass anstelle der Sicherheitsfragen vielmehr die finanziellen Folgen im Zentrum der Beratungen in der sicherheitspolitischen Kommission gestanden hätten. Sie warf der SiK «Arbeitsverweigerung» vor und wies darauf hin, dass man nach dem Eintreten die Möglichkeit hätte, das – je nach Ansicht überladene, unberechenbare oder lückenhafte – Gesetz zu «entrümpeln». Arbeitsscheue sei in diesem Fall jedoch «geradezu verantwortungslos», denn auch ein Versäumnis ziehe unbezifferbare Kosten nach sich. Ins gleiche Horn blies auch der Grünen-Vertreter Balthasar Glättli (gp, ZH), indem er Nichteintreten als «Dienstverweigerung» bezeichnete und argumentierte, dass Informationssicherheitslecks sowohl Reputations- als auch Finanzschäden zur Folge hätten. Auch Beat Flach (glp, AG) als Sprecher der GLP-Fraktion erschien es unverständlich, weshalb trotz erkanntem Handlungsbedarf nicht eingetreten werden sollte; ein weiteres Mal fiel das Wort «Arbeitsverweigerung». Die Abstimmung ergab schliesslich 117 zu 68 Stimmen für Nichteintreten (8 Enthaltungen). Obschon die Fraktionen der BDP, der SP, der Grünen und der GLP geschlossen für Eintreten

votierten, besiegelte die geballte Stimmkraft des SVP-/FDP-/CVP-Blocks mit nur drei Abweichlern den Nichteintretensentscheid. [4]

BUNDESRATSGESCHÄFT
DATUM: 26.09.2018
KARIN FRICK

Mit zwölf zu einer Stimme beantragte die SiK-SR ihrem Rat im Herbst 2018, am Eintreten auf das **Informationssicherheitsgesetz** festzuhalten. Das Gesetz sei im Auftrag des Parlamentes entstanden und berücksichtige klare Vorgaben der GPK und der GPDel, erklärte Kommissionssprecher Isidor Baumann (cvp, UR) vor dem Ratsplenum. Er fügte eine Liste von Gründen an, weshalb das Gesetz notwendig sei: Es brauche das Gesetz, um bei allen Bundesbehörden einen einheitlichen, minimalen Sicherheitsstandard zu gewährleisten, um die Kantone bei der Zusammenarbeit mit dem Bund denselben Sicherheitsvorschriften zu unterstellen, um durch die Verwendung biometrischer Daten unberechtigte Zugriffe auf die Informationssysteme des Bundes besser zu verhindern und um Personensicherheitsüberprüfungen bei Betreibenden oder Verwaltenden der kritischen Informationssysteme des Bundes durchführen zu können. Darüber hinaus könnten damit die Vertrauenswürdigkeit von Unternehmen, die sensible Aufträge für den Bund ausführten, sowie die Einhaltung der Sicherheitsstandards während der Auftragserfüllung kontrolliert werden. Das inhaltlich abgestimmte Gesetz ermögliche gegenüber dem heutigen System einen Bürokratieabbau, indem es Verantwortlichkeiten und Prozesse vereinfache und Massnahmen standardisiere, hob Baumann die Vorteile des Projektes hervor. Auch Bundesrat Guy Parmelin betonte noch einmal die Bedeutung dieses Gesetzes für die Schweiz. Stillschweigend hielt der Ständerat am Eintretensentscheid fest, womit sich nun erneut der Nationalrat mit dem Geschäft befassen wird. [5]

BUNDESRATSGESCHÄFT
DATUM: 09.10.2018
KARIN FRICK

Nachdem der Ständerat in der Herbstsession 2018 am Eintreten auf das **Informationssicherheitsgesetz** (ISG) festgehalten hatte, beriet die SiK-NR die Vorlage im Oktober desselben Jahres zum zweiten Mal. Diesmal trat sie zwar mit 17 zu 8 Stimmen bei einer Enthaltung darauf ein, beschloss dann aber mit 17 zu 9 Stimmen die Sistierung des Geschäftes. Unterdessen soll das VBS bis im Juni 2019 Verbesserungsvorschläge für das Gesetzgebungsprojekt ausarbeiten. Neben der inhaltlichen Abstimmung des ISG auf die NCS und der Berücksichtigung eines zukünftigen Kompetenzzentrums für Cybersicherheit verlangte die Kommission eine klare Ausweisung und Limitierung sowie die departementsübergreifende Kompensation der Umsetzungskosten. Weiter muss das VBS aufzeigen, welche Kosten im Bereich der Betriebssicherheitsverfahren auf die öffentlichen und privaten Unternehmen in der Schweiz zukommen bzw. wie eine Belastung der Unternehmen durch das neue Gesetz vermieden werden kann. Generell erwartet die Kommission einen konkreteren, einfacheren und strafferen Gesetzesentwurf. [6]

BUNDESRATSGESCHÄFT
DATUM: 30.10.2019
KARIN FRICK

Im Lichte der Zusatzinformationen zur Abstimmung auf die NCS, zu den Kostenfolgen sowie zu weiteren möglichen Verbesserungen der Vorlage, die die SiK-NR im Oktober 2018 vom VBS angefordert hatte, beriet die Kommission im Spätsommer 2019 das **Informationssicherheitsgesetz** (ISG) im Detail und nahm einige Modifikationen vor. Mit 14 zu 8 Stimmen bei einer Enthaltung wollte sie aus Gründen des Persönlichkeitsschutzes auf die vom Ständerat vorgesehene systematische Verwendung der AHV-Nummer verzichten. Als weitere Differenz zur Kantonskammer beantragte sie ihrem Rat mit 20 zu 2 Stimmen, den Bundesrat im Gesetz ausdrücklich zu verpflichten, seine Ziele und die Kosten für die Informationssicherheit den Sicherheitspolitischen Kommissionen zur Konsultation vorzulegen. Damit wollte sie verhindern, dass die Umsetzung des ISG zu hohe finanzielle und personelle Ressourcen beansprucht. Überdies entschied die Kommission einstimmig, dass die Personensicherheitsüberprüfung auch auf Dritte, die in kritischen Funktionen für die nationale Netzgesellschaft Swissgrid eingesetzt werden, angewandt werden kann, jedoch nicht auf gewählte, angehende kantonale Magistratspersonen. [7]

BUNDESRATSGESCHÄFT
DATUM: 04.06.2020
KARIN FRICK

In der Sommersession 2020 beugte sich der Nationalrat, nachdem er bei seiner ersten Beratung im Frühling 2018 nicht auf das Geschäft eingetreten war, zum zweiten Mal über den Entwurf zum **Informationssicherheitsgesetz** (ISG). Die SiK-NR hatte in der Zwischenzeit die angeforderten Verbesserungsvorschläge vom VBS bezüglich der Kosten für öffentliche und private Unternehmen, zur verstärkten Kontrolle des Parlaments bei der Anwendung und Überwachung des Gesetzes, zur Abstimmung des ISG auf die Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken sowie zur Möglichkeit, den Bereich Personensicherheitsüberprüfung in einen separaten Erlass auszulagern, erhalten und diskutiert. Sie beantragte ihrem Rat nun, auf die Vorlage einzutreten. Vertreterinnen und Vertreter sämtlicher Fraktionen ausser der SVP – deren Sprecher David Zuberbühler (svp, AR) das Gesetz als «umfangreiches und komplexes Bürokratiemonster» bezeichnete und die hohen Umsetzungskosten kritisierte – betonten unisono die dringende Notwendigkeit des Gesetzes im Zeitalter der Digitalisierung und sahen die Kosten angesichts des hohen Schadenspotenzials bei Cyberangriffen als verhältnismässig an. Auch Bundesrätin Viola Amherd hob hervor, dass die Kosten zur Umsetzung des ISG «im Verhältnis zu dessen Nutzen gering und gerechtfertigt» seien, denn das ISG werde «zahlreiche wesentliche Sicherheitslücken schliessen, Einheitlichkeit schaffen und gleichzeitig die Effizienz und Wirksamkeit der bestehenden Sicherheitsmassnahmen erhöhen». Nicht zuletzt sei auch die international tätige Wirtschaft auf das Gesetz angewiesen, da sich die entsprechenden Unternehmen sonst nicht mehr zertifizieren lassen und keine Aufträge im sicherheitsrelevanten Bereich mehr ausführen könnten; «das wäre dann der Schaden für die Wirtschaft, nicht die etwas vermehrten Kosten, die sich durch dieses Gesetz ergeben», so die VBS-Chefin weiter. So trat der Nationalrat diesmal ohne Gegenantrag auf die Vorlage ein.
In der Detailberatung schuf die grosse Kammer zwei Differenzen zum Ständerat. Erstens ergänzte sie auf Antrag ihrer Kommission einen Absatz, wonach der Bundesrat seine Ziele und die Kosten für die Informationssicherheit den sicherheitspolitischen Kommissionen vorlegen muss. Damit sollen diese auf jeden Fall zu einem allfällig geplanten Wechsel des Sicherheits-Ambitionsniveaus, das vom Bundesrat festgelegt wird, konsultiert werden, weil der Wechsel auf eine höhere Sicherheitsstufe beträchtliche Mehrkosten nach sich ziehen würde. Der Bundesrat hatte diese Änderung abgelehnt, weil sie angesichts der ohnehin umfassenden Kontrollrechte des Parlaments über den Bundesrat und die Verwaltung in seinen Augen überflüssig sei, unterlag mit diesem Antrag jedoch deutlich. Zweitens schloss sich der Nationalrat in der Frage der Verwendung der AHV-Nummer als Personenidentifikator wieder dem Entwurf des Bundesrats an, nachdem der Ständerat hier weiter gegangen war und die systematische Verwendung der AHV-Nummer hatte erlauben wollen. In der bundesrätlichen Version, für die sich die Kommissionsmehrheit stark gemacht hatte, darf die AHV-Nummer einmalig zur Personenidentifikation verwendet werden, muss nach der Erzeugung einer nicht zurückrechenbaren Personennummer aber gelöscht werden. Eine Minderheit Keller-Inhelder (svp, SG), die gar keine Verwendung der AHV-Nummer erlauben wollte, und eine Minderheit Flach (glp, AG), die den ständerätlichen Beschluss stützte, blieben chancenlos – letztere sogar, obwohl sich der Bundesrat mittlerweile ebenso für die systematische Verwendung der AHV-Nummer aussprach, weil diese mit einer Revision des AHV-Gesetzes sowieso eingeführt werden sollte. Mit diesen zwei inhaltlichen Änderungen sowie einigen redaktionellen Anpassungen übergab der Nationalrat die Vorlage in der Gesamtabstimmung mit 131 zu 53 Stimmen bei einer Enthaltung – sämtliche Opposition aus der SVP-Fraktion – wieder an den Ständerat. [8]

BUNDESRATSGESCHÄFT
DATUM: 23.09.2020
KARIN FRICK

Nachdem der Nationalrat im zweiten Anlauf im Sommer 2020 doch noch auf das Geschäft eingetreten war, widmeten sich die eidgenössischen Räte in der Herbstsession der **Differenzbereinigung beim Informationssicherheitsgesetz**. Der Ständerat, der als Erstes an der Reihe war, zeigte sich in zwei Punkten nicht bereit, den Beschlüssen des Nationalrats zu folgen. Mit stillschweigender Zustimmung strich er erstens den von der Volkskammer eingefügten Absatz, dass der Bundesrat seine Ziele und die Kosten für die Informationssicherheit zwingend den sicherheitspolitischen Kommissionen zur Konsultation vorlegen muss, wieder aus dem Gesetz. Nach Ansicht der SiK-SR war diese Bestimmung überflüssig, was auch Bundesrätin Viola Amherd bekräftigte: Die Fachkommissionen könnten wie die Finanzkommission und die Finanzdelegation jederzeit verlangen, dass sie zu einem Thema konsultiert würden, und dieser Forderung werde immer nachgekommen. Zweitens hielt die Kantonskammer an ihrem Beschluss fest, dass die AHV-Nummer systematisch zur Personenidentifikation im Rahmen des Informationssicherheitsgesetzes verwendet werden darf. Eine Minderheit Zopfi (gp, GL) hatte beantragt, den Beschluss des Nationalrats zu übernehmen, dass die AHV-Nummer nur vorübergehend zur Erzeugung einer nicht

zurückrechenbaren Personennummer verwendet werden darf, unterlag jedoch mit 31 zu 10 Stimmen bei einer Enthaltung klar. VBS-Vorsteherin Viola Amherd hatte dem Rat in Erinnerung gerufen, dass er im Juni der Änderung des AHV-Gesetzes zugestimmt habe, das den Behörden generell die systematische Verwendung der AHV-Nummer erlaube; es mache darum keinen Sinn, hier jetzt eine andere Regelung festzuschreiben. In den übrigen, redaktionellen Differenzen schloss sich der Ständerat stillschweigend dem Nationalrat an.
Die zwei vom Ständerat aufrechterhaltenen Differenzen waren anschliessend im Nationalrat hochumstritten. Während die Mehrheit der SiK-NR sich bereit erklärte, auf die ausdrückliche Erwähnung der Konsultationspflicht des Bundesrates zu verzichten, beantragte eine Minderheit Hurter (svp, SH) deren Beibehaltung. Es handle sich dabei um eine «Notbremse», um zu verhindern, dass die Kosten aus dem Ruder laufen, und er verstehe nicht, so Hurter, «warum Sie sich weigern, Informationen zu erhalten». Abgesehen von der geschlossenen SVP-Fraktion und drei Abweichlern aus der Mitte hielt die grosse Kammer diesen Passus jedoch für unnötig und strich ihn endgültig aus dem Gesetz. Während sich eine Minderheit Riniker (fdp, AG) für die systematische Verwendung der AHV-Nummer und damit die Bereinigung auch dieser Differenz starkmachte, wollte die Kommissionsmehrheit am Beschluss festhalten, dass die AHV-Nummer nur einmalig zur Erzeugung einer nicht zurückrechenbaren Identifikationsnummer verwendet werden darf und aus Gründen des Datenschutzes nachher gelöscht werden muss. Die Grundsatzfrage der systematischen Verwendung der AHV-Nummer durch alle Behörden solle im Rahmen der entsprechenden Revision des AHV-Gesetzes geklärt und nicht bereits hier vorweggenommen werden, argumentierte etwa Grünen-Sprecher Balthasar Glättli (gp, ZH). Äusserst knapp mit 90 zu 87 Stimmen bei 9 Enthaltungen erhielt die grosse Kammer diese Differenz aufrecht, womit sich der Ständerat noch einmal damit befassen muss. [9]

BUNDESRATSGESCHÄFT
DATUM: 18.12.2020
KARIN FRICK

Im Rahmen der **Differenzbereinigung zum Informationssicherheitsgesetz (ISG)** befasste sich der Ständerat in der Wintersession 2020 abermals mit der Frage, ob zur Personenidentifikation im Zusammenhang mit dem ISG die AHV-Nummer verwendet werden darf. Schon in der ersten Beratung im Dezember 2017 hatte der Ständerat die systematische Verwendung der AHV-Nummer im ISG festschreiben wollen – ein Entscheid, der vom Nationalrat seither zweimal wieder umgestossen worden war, zuletzt im September 2020, jedoch nur noch mit sehr knapper Mehrheit. Eine Minderheit Zopfi (gp, GL) beantragte im Ständerat erneut, aus Datenschutzgründen auf die direkte Verwendung der AHV-Nummer zu verzichten und stattdessen eine aus der AHV-Nummer abgeleitete Identifikationsnummer zu verwenden. Mit 30 zu 10 Stimmen bei einer Enthaltung hielt der Ständerat jedoch an seinem Beschluss fest, die Nutzung der AHV-Nummer als Identifikator zu erlauben. Die gleiche Konstellation – die Kommissionsmehrheit beantragte Zustimmung zur Verwendung der AHV-Nummer, eine Minderheit Porchet (gp, VD) deren Ablehnung – zeigte sich daraufhin auch im Nationalrat. Nachdem dieser aber zwei Tage zuvor der Revision des AHV-Gesetzes zugestimmt hatte, das neu allen Behörden die systematische Verwendung der AHV-Nummer als Identifikator erlaubt, machte eine andere Entscheidung beim ISG nicht mehr viel Sinn. Diese Geschichte sei «leider gelaufen» und die Abstimmung jetzt nur noch «für die Galerie», fasste Thomas Hurter (svp, SH) als Sprecher der SVP-Fraktion, die sich bislang auch gegen die Verwendung der AHV-Nummer ausgesprochen hatte, die Lage zusammen. So schloss sich die grosse Kammer mit 140 zu 46 Stimmen dem Beschluss des Ständerates an und räumte die letzte Differenz aus. In den Schlussabstimmungen nahm der Ständerat das ISG einstimmig an, der Nationalrat hiess es mit 141 zu 53 Stimmen bei einer Enthaltung gut. Abgelehnt hatte es die geschlossene SVP-Fraktion, weil sie die Unklarheit über die Umsetzungskosten bemängelte. [10]

Kriminalität

BUNDESRATSGESCHÄFT
DATUM: 18.06.1991
HANS HIRTER

Der Bundesrat legte im April die Botschaft für eine Änderung des Strafrechts im Bereich der **strafbaren Handlungen gegen das Vermögen und Urkundenfälschungen** vor. Damit leitete er nicht nur eine weitere Etappe der Strafrechtsreform ein, sondern ergänzte – nach der Schaffung von Strafnormen gegen Insidergeschäfte und die Geldwäscherei – auch das Konzept des Kampfs gegen Wirtschaftskriminalität und organisiertes Verbrechen um ein weiteres Element. Während sich diese Revision bei einer Vielzahl von Bestimmungen eher auf Redaktionelles beschränkt, werden im Bereich der elektronischen Datenverarbeitung neue Straftatbestände geschaffen. Grundsätzlich sollen neu auch Aufzeichnungen auf elektronischen Daten- oder Bildträgern als Urkunden anerkannt werden. Das unberechtigte Eindringen in Datenverarbeitungsanlagen (sogenanntes «**Hacken**») will der Bundesrat in Zukunft ebenso bestrafen wie die unerlaubte Aneignung von Computerdaten (inkl. Programme) oder deren Beschädigung. Von grosser Bedeutung für die Bekämpfung der Wirtschaftskriminalität sind ebenfalls die neuen Vorschriften über betrügerische Manipulationen von Datenverarbeitungsvorgängen, welche mit der Absicht vorgenommen werden, sich selber oder andere zu bereichern.
Eine Anpassung des Strafrechts an die modernen Formen der Kriminalität stellen auch die in derselben Botschaft enthaltenen neuen Bestimmungen über die missbräuchliche Verwendung von Check- und Kreditkarten dar. Der Bundesrat schlägt vor, dass sich künftig bereits strafbar macht, wer derartige Karten verwendet, obschon er zahlungsunfähig oder -unwillig ist.

Die zuständige Nationalratskommission bezeichnete die Vorlage als notwendig und dringlich und beschloss einstimmig, darauf einzutreten. [11]

BUNDESRATSGESCHÄFT
DATUM: 01.04.1992
HANS HIRTER

Die vorberatende Kommission des Nationalrats stimmte der vom Bundesrat im Vorjahr vorgeschlagenen Strafbarkeit des Missbrauchs von Check- und Kreditkarten zu. Im Bereich der neuen Bestimmungen über die Computerkriminalität nahm sie eine **Differenzierung** zwischen dem spielerischen Eindringen in Computersysteme (**Hacking**) und dem – strenger zu bestrafenden – unerlaubten Datenzugriff mit Bereicherungsabsichten vor. [12]

BUNDESRATSGESCHÄFT
DATUM: 08.12.1993
HANS HIRTER

Als Erstrat befasste sich der **Nationalrat** mit den vom Bundesrat 1991 vorgeschlagenen **Änderungen des Strafrechts in bezug auf nicht erlaubte Handlungen gegen das Vermögen und auf das Fälschen von Urkunden**. In der Eintretensdebatte begrüssten sämtliche Fraktionen diese Rechtsanpassung an die neuen Formen der Wirtschaftskriminalität. In der Detailberatung stimmte der Rat der von der Kommission vorgeschlagenen weniger strengen Bestrafung von Personen, welche ohne Bereicherungsabsichten in ein Computersystem eindringen (sog. Hacking) zu. Einen von Vertretern der SP unterstützten Antrag auf vollständige Straffreiheit für derartige Aktivitäten lehnte er hingegen ab. Mit Stichentscheid des Präsidenten abgelehnt wurde auch ein von der SP, der GP, dem LdU und Teilen der CVP unterstützter Antrag, es dem Richter zu erlauben, bei Bagatelldelikten von einer Strafverfolgung abzusehen (sog. Opportunitätsprinzip). Im übrigen nahm der Rat eine Reihe von Korrekturen am Regierungsentwurf vor, ohne allerdings Wesentliches zu verändern. Im Anschluss an seine Debatte überwies der Nationalrat oppositionslos eine Motion (Mo. 93.3037), welche die Vorlage eines Bundesgesetzes über die wirtschaftliche Strafrechtspflege in Kriegszeiten verlangt. Der Ständerat stimmte den neuen Bestimmungen in der Wintersession zu, schuf aber doch einige Differenzen zum Nationalrat. Insbesondere nahm er als zusätzlichen strafbaren Tatbestand auch noch das Einschleusen von Viren in Computersysteme sowie die Herstellung und Verbreitung derartiger Programme in das Gesetz auf. [13]

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 Querschnittthemen 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 Kernwaffenverbotsvertrag. 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 Funkion 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». [14]

BUNDESRATSGESCHÄFT
DATUM: 17.06.2021
MARC BÜHLMANN

Nicht wie im Vorjahr erst in der Herbstsession, sondern wie gewohnt in der Sommersession nahmen National- und Ständerat Kenntnis vom **Geschäftsbericht 2020 des Bundesrates**. In diesem Bericht legt die Regierung jahrweise einen Soll-Ist-Vergleich zwischen Legislaturplanung, Jahreszielen und im entsprechenden Jahr erledigten oder angegangenen Geschäften vor. Covid-19 war nicht nur schuld an der Verschiebung der Beratung im Jahr 2020, sondern auch weiterhin zentraler Gegenstand im Bericht und der parlamentarischen Beratung darüber. So bot der Bundesrat in einem eigenen Kapitel des Berichts eine Übersicht über die Entwicklungen der Pandemie und über alle rund 250 im Jahr 2020 dazu gefällten Bundesratsbeschlüsse. Er leitete den Bericht zudem mit dem Hinweis ein, dass zahlreiche Projekte wegen der Coronapandemie nicht so weit gediehen seien, wie geplant.

Im **Ständerat** erörterte Maya Graf (gp, BL) den Bericht für die GPK-SR. Das Management der Covid-19-Krise ziehe sich wie ein roter Faden durch den Bericht. Sie erinnere zudem daran, dass eine von der GPK einberaumte Inspektion zur Bewältigung der Pandemie am Laufen sei. Die GPK würden den Bericht und die Anhörungen der Departementsvorsteherinnen und -vorsteher jeweils mit Querschnittthemen versehen. Beim ersten Querschnittthema «Krisenmanagementstrukturen» habe sich die GPK informiert, ob solche Strukturen in Normalzeiten geplant gewesen seien, jetzt eingesetzt würden und wie gut dies funktioniere. Beim Thema «Cybersicherheit» habe sich die GPK zur IT-Sicherheit in den Departementen erkundigt und dazu, wo es diesbezüglich Verbesserungen brauche. Im Anschluss an die Ausführungen der GPK-Präsidentin ergriffen die Präsidenten der verschiedenen Subkommissionen das Wort, die basierend auf dem Geschäftsbericht jeweils zwei Departemente sowie die Bundeskanzlei genauer unter die Lupe genommen hatten.
Charles Juillard (mitte, JU) berichtete über das VBS und das EDA. Hier hob der Sprecher den Aktionsplan für die Cyberverteidigung hervor, bei dem praktisch alle Ziele erreicht worden seien. Hinsichtlich Nachhaltigkeit und Klimaschutz habe das VBS, das insbesondere aufgrund der Luftwaffenflotte und der schweren Militärfahrzeuge jährlich Emissionen von 200'000 Tonnen CO2 verursache, verschiedene Massnahmen ergriffen, um das 40-Prozent-Reduktionsziel bis 2030 zu erreichen. Im Rahmen des Programms «Natur, Landschaft und Armee» leiste das VBS zudem einen Beitrag zur Erhaltung der Biodiversität. Beim EDA sei der Umgang mit der Pandemie genauer geprüft worden. Die GPK verfolge in diesem Departement zudem die Entwicklung bezüglich der Personalsituation.
Daniel Fässler (mitte, AI) erörterte die Berichtsteile, die dem EJPD und der BK zugeordnet waren. Er hob hier den Informationsaustausch bei der Polizeiarbeit hervor. Dieser funktioniere national und international noch nicht, wie er sollte. Insbesondere die Möglichkeiten der Digitalisierung würden zu wenig gut eingesetzt. International solle dem mit verschiedenen Abkommen begegnet werden. National stosse man aber «offenkundig an Grenzen des Föderalismus», deren Aufhebung man im EJPD aber in Angriff nehmen wolle, damit alle kantonalen Polizeikorps Zugriff auf alle verschiedenen kantonalen Datenbanken erhielten, um Kriminalität effizienter bekämpfen zu können. Im Gespräch mit dem Bundeskanzler Walter Thurnherr sei es insbesondere um die Digitalisierung in der Bundesverwaltung gegangen. Ab 1. Januar 2021 werde das Informatiksteuerorgan des Bundes aufgelöst und dessen Aufgaben – insbesondere Koordination und Unterstützung bei der Umsetzung der Digitalisierung – von einer neuen Verwaltungseinheit innerhalb der BK übernommen. Dies sei eine grosse Aufgabe, bei der man erst am Anfang stehe. Darüber hinaus werde man sich hier auch dem Problem der Fremdbestimmung durch mächtige IT-Unternehmen stellen müssen.
Matthias Michel (fdp, ZG) nahm das EFD und das WBF genauer unter die Lupe. Auch hier sei Digitalisierung ein zentraler Punkt. Es sei zwar erfreulich, dass 2021 «nicht weniger als 13 Massnahmen» umgesetzt worden seien, um das Ziel 2 der Legislaturplanung – die effiziente und möglichst digitale Erbringung der staatlichen Leistungen – zu erreichen. Im aktuellen Bericht sei aber nur «ein einziges – ein einziges! – quantifizierbares Ziel», also nur ein Indikator angegeben; die Entwicklung im Bereich der Digitalisierung müsse adäquater gemessen werden. «Etwas mehr Substanz in der Berichterstattung» wünschte sich der Kommissionssprecher auch im Bereich der Berufsbildung, auch wenn dies eine Verbundaufgabe mit den Kantonen darstelle.
Marco Chiesa (svp, TI) berichtete schliesslich zu den Berichtsteilen des EDI und des UVEK. Beim EDI seien in den Gesprächen vor allem die Massnahmen gegen die Covid-

Pandemie Gegenstand gewesen. Alain Berset habe erklärt, dass sich der Bundesrat darauf konzentriert habe, die Auswirkungen der Krise auf die Bevölkerung und die Wirtschaft möglichst zu begrenzen. Das begrenzte Wissen und die unvollständigen Informationen hätten immer wieder Anpassungen bedingt. Eine wichtige Massnahme seien deshalb auch die Tests gewesen, bei denen sehr rasch eine funktionierende Infrastruktur habe aufgebaut werden können. Als schwierig habe sich die Entwicklung einer Impfstrategie entpuppt, weil der Verlauf der Pandemie nicht vorhersehbar gewesen sei. Die Schweiz sei aber mittlerweile eines der wenigen Länder, das mRNA-Impfstoffe für die ganze Bevölkerung anbieten könne. Zum UVEK äusserte sich Chiesa nicht.
Am Schluss der Ratsdebatte meldete sich Bundespräsident Guy Parmelin zu Wort. Der Bundesrat sei – obwohl zahlreiche geplante Massnahmen wegen Covid-19 nicht hätten umgesetzt werden können – zufrieden mit der Zielerreichung. Würden normalerweise rund 40 Bundesratssitzungen in einem Jahr stattfinden, seien es im Jahr 2020 mehr als 60 gewesen. Zudem seien wesentlich mehr Vorstösse eingereicht worden als in früheren Jahren, was die enorme Arbeitsbelastung für den Bundesrat noch weiter erhöht habe. Die Regierungsarbeit sei aber nur möglich, «parce que de nombreux employés de la Confédération ne regardaient ni leur montre ni le jour de la semaine». Dafür sei der Bundesrat sehr dankbar. Auch Parmelin ging auf ein paar Punkte des Berichts ein, darunter die beschlossenen Massnahmen zur Abfederung der wirtschaftlichen Folgen der Pandemie, die Verabschiedung der BFI-Botschaft, den Bericht zur Finanzierung des Betriebs und Substanzerhalts der Bahninfrastruktur, das «dossier éléphantesque» zu den Verordnungsänderungen im Rahmen des revidierten Krankenversicherungsgesetzes und darin die Planung des Bedarfs an Ärztinnen und Ärzten oder die bundesrätliche Position zur Europapolitik. In der Folge nahm der Ständerat den Bundesbeschluss über den Geschäftsbericht des Bundesrates für das Jahr 2020 stillschweigend an.

Dies tat gleichentags auch der **Nationalrat**, wo Erich von Siebenthal (svp, BE), Thomas de Courten (svp, BL), Yvonne Feri (sp, AG) und Nicolo Paganini (mitte, SG) die Berichterstattung übernahmen. Grösstenteils nahmen sie die gleichen Punkte auf wie in der kleinen Kammer.
Eine Ausnahme stellte der Bericht von Thomas de Courten dar, der auf das UVEK einging: Der Bundesrat habe im Berichtjahr die wichtigen Ausbauschritte für den Strassen- und Schienenverkehr geplant und werde hier dem Parlament, das darüber zu entscheiden habe, bald einen Bericht vorlegen. Darüber hinaus erwähnte der Kommissionssprecher die «etwas chaotische» Situation in der Covid-Task-Force Anfang Jahr, was sich mit dem Einbezug der Wissenschaft in eine Science Task Force verbessert habe.
Nicolo Paganini erwähnte zudem die IZA-Strategie, mit der die Bereiche der humanitären Hilfe und der Entwicklungszusammenarbeit enger zusammengefasst würden. Auch das «drastische Räumungskonzept» in Mitholz fand Erwähnung im Bericht von Paganini.
Auch im Nationalrat hob schliesslich Bundespräsident Guy Parmelin die wichtigsten Punkte des Berichts hervor – auch dieses Votum unterschied sich kaum von jenem im Ständerat – und auch die grosse Kammer stimmte dem Bundesbeschluss diskussionslos zu und nahm den Bericht zur Kenntnis. [15]

Landesverteidigung

Landesverteidigung

BUNDESRATSGESCHÄFT
DATUM: 02.12.2022
CHLOÉ MAGNIN

À l'air du numérique, la sécurité a pris une toute autre couleur. Cette nouvelle fenêtre doit, elle aussi être protégée. Ainsi, la sécurité des données et des infrastructures, les cyberrisques ou encore la collaboration entre les différents acteurs sont des sujets qui ne cessent de revenir sous la coupole fédérale tout comme dans les médias. En décembre 2022, le Conseil fédéral a publié un message sur la **mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques**. Dans le cadre de ce message, différentes options ont été envisagées pour formuler une nouvelle loi afin de consolider la sécurité cyber. Le Conseil fédéral a mis l'accent sur la collaboration et l'efficacité.

En 2016, après l'acceptation par l'EU d'une directive concernant le signalement des cyberattaques visant les infrastructures critiques et de discussions internes, la Suisse a chargé le département fédéral des finances (DFF) de fournir, d'ici fin 2021, les bases légales pour introduire une obligation de signaler les cyberattaques contre les

infrastructures critiques, dont le secteur bancaire, l'armée, le système de soins médicaux ou encore les infrastructures relatives au transport routier. Cette analyse a également révélé des manquements au niveau du centre national pour la cybersécurité (NCSC). C'est pourquoi une partie du projet final est réservée à la spécification des tâches assignées au NCSC. En cas de cyberattaques concernant les infrastructures critiques suisses, le NCSC devra réceptionner les signalements obligatoires mais aussi les signalements volontaires pour permettre à la Confédération d'avoir une vue d'ensemble sur les failles du système.

Sur la base des propositions du DFF, le Conseil fédéral a estimé que la seule option qui permettait de renforcer les relations entre le gouvernement et les infrastructures critiques, mais aussi l'efficacité et la sécurité reposait sur l'obligation de reporter les cyberattaques touchant aux infrastructures critiques. En effet, les suggestions basées sur la bonne volonté des infrastructures critiques et l'extension des mesures existantes n'étaient pas suffisantes et s'accompagnaient de lourds désavantages comme des procédures trop compliquées ou de la confiance aveugle de la part du gouvernement envers les infrastructures critiques.

Finalement, le Conseil fédéral a fait attention à ce que le projet final repose sur des procédures simples, que les signalements soient récompensés par un service de conseil assuré par le NCSC, et que le non-respect des conditions soit puni par une sanction pécuniaire pouvant s'élever jusqu'à CHF 100'000, dont CHF 20'000 directement à la charge de l'entreprise exploitant l'infrastructure critique concernée. Toutefois, le Conseil fédéral estime que cette dernière mesure restera symbolique en raison d'une collaboration de longue date entre les infrastructures critiques et le gouvernement. [16]

BUNDESRATSGESCHÄFT
DATUM: 16.03.2023
CHLOÉ MAGNIN

La CPS-CN est favorable par 16 voix contre 1 et 6 abstentions au projet qui vise à **rendre le signalement des cyberattaques envers les infrastructures critiques obligatoires**. Elle salue notamment la définition des tâches du NCSC dans la loi. La commission, considérant le sujet comme très important, a souhaité approfondir les réglementations en adoptant une proposition supplémentaire qui vise « à étendre l'obligation de signaler aux vulnérabilités des systèmes informatiques, et non seulement aux cyberattaques ».
Du côté du **Conseil national**, la sécurité numérique est considérée comme très importante par les député.e.s, ce qui s'est largement ressenti dans les discussions. Il est intéressant de relever que la minorité opposée au projet n'a pas remis en cause le but de la mesure mais les moyens employés pour y arriver. En effet, l'UDC a critiqué le choix du Conseil fédéral de punir financièrement les institutions ne reportant pas les infractions plutôt que de trouver une incitation qui motiverait tous les acteurs.
Le Conseil national a accepté l'objet par 132 voix contre 55, dont 54 provenant de l'UDC (aucune abstention). [17]

BUNDESRATSGESCHÄFT
DATUM: 21.03.2023
CHLOÉ MAGNIN

La **CPS-CE** a proposé à l'unanimité d'accepter la modification de la loi fédérale sur la sécurité de l'information (LSI) qui vise à **rendre le signalement des cyberattaques envers les infrastructures critiques obligatoires**.
Une proposition de revenir à la version initiale, avancée par le Conseil fédéral, a été évoquée. Il a en effet été suggéré de revoir la décision du Conseil national « d'obliger la signalisation des vulnérabilités concernant des moyens informatiques essentiels pour l'exploitation et encore inconnus du public ». Cette suggestion a été évincée malgré une commission très partagée. Alors que la majorité a estimé que l'effort à fournir était minime comparé aux bienfaits de la mesure, la minorité a souligné le manque d'informations vis-à-vis du nombre d'acteurs concernés et s'est montrée réticente face à une telle disposition.
La modification de la LSI sera discutée au Conseil des Etats. [18]

BUNDESRATSGESCHÄFT
DATUM: 01.06.2023
CHLOÉ MAGNIN

Le **Conseil des Etats** s'est penché sur l'objet du Conseil fédéral rendant obligatoire le **signalement des cyberattaques envers les infrastructures critiques**. Il a considéré par 31 voix contre 13 que l'obligation ne devait pas être étendue aux vulnérabilités des systèmes informatiques, comme souhaité par le Conseil national et la CPS-CE. En effet, il estime que la proposition est imprécise et que la charge administrative serait trop importante. De ce fait, la chambre haute propose de revenir à la proposition initiale du Conseil fédéral. Cette dernière a finalement été acceptée à l'unanimité. En s'opposant non seulement à sa commission mais surtout à l'autre chambre du Parlement fédéral, le

Conseil des Etats renvoie l'objet au Conseil national, lançant une procédure d'élimination des divergences. [19]

BUNDESRATSGESCHÄFT
DATUM: 20.06.2023
CHLOÉ MAGNIN

Dans le cadre de la **procédure d'élimination des divergences**, la **CPS-CN** campe sur sa position par 14 voix contre 9 et une abstention. Ainsi, elle maintient que **signaler** les **cyberattaques**, tout comme les vulnérabilités inconnues du public concernant des équipements informatiques essentiels, est crucial. Elle a cependant avancé, qu'à titre de compromis, les vulnérabilités résultant de développements internes à l'entreprise concernée pouvaient être exclues de cette mesure. En somme, seules les vulnérabilités encore inconnues du public qui pourraient nuire à une autre infrastructure critique seront annoncées. [20]

BUNDESRATSGESCHÄFT
DATUM: 11.09.2023
CHLOÉ MAGNIN

Le **Conseil national** a pris à nouveau position sur les **signalements de cyberattaques** dans le cadre de la **procédure d'élimination des divergences**. Le compromis trouvé par la CPS-CN a été soutenu par 102 voix contre 80 (aucune abstention). Le groupe UDC et le PLR se sont opposés à cette proposition, s'alignant sur la position du Conseil fédéral. Ils ont affirmé avoir conscience du défi qu'incarnent les cyberattaques, mais considèrent que rendre obligatoire la déclaration de vulnérabilités représenterait une charge administrative trop importante pour les entreprises. Le Conseil fédéral estime aussi que la confiance entre l'Etat et l'économie pourrait être renforcée, si les annonces restaient facultatives. De plus, l'UDC a souligné craindre des fuites de données qui pourraient rendre les institutions encore plus vulnérables.
Comme une majorité a été trouvée à la chambre du peuple, l'avenir de l'objet est désormais entre les mains du Conseil des Etats. [21]

BUNDESRATSGESCHÄFT
DATUM: 19.09.2023
CHLOÉ MAGNIN

Lors du premier tour de la **procédure d'élimination des divergences** , la CPS-CE est majoritairement restée campée sur la version originale du texte, celle du Conseil fédéral. Une minorité a toutefois soutenu la proposition du Conseil national, avançant une priorité: prévenir les cyberattaques. Charles Juillard (centre, JU) et Mathias Zopfi (vert-e-s, GL) l'ont résumé ainsi : «les vulnérabilités d'aujourd'hui sont les cyberattaques de demain». La minorité du **Conseil des Etats** a aussi ajouté une clause à la proposition du Conseil national, souhaitant rallonger le temps à disposition pour annoncer une vulnérabilité, passant de 24 heures à 7 jours, et souligné la possibilité d'annoncer une vulnérabilité anonymement.
Le Conseil fédéral a suivi la majorité de la CPS-CE, arguant qu'avant d'obliger les signalements des vulnérabilités, ces derniers doivent se faire sur une base volontaire, étant donné que la collaboration entre l'économie et la NCSC n'est que récente sur ce sujet. Procéder de la sorte permettrait notamment d'établir une relation de confiance entre les deux acteurs.
Le Conseil des Etats s'est alignée sur le Conseil fédéral et la majorité de sa commission, par 32 voix contre 12 (0 abstention). Selon les débats, la minorité de la chambre des cantons était principalement colorée de rose et de vert. La balle est maintenant dans le camp du Conseil national pour un deuxième tour d'élimination des divergences. [22]

BUNDESRATSGESCHÄFT
DATUM: 21.09.2023
CHLOÉ MAGNIN

Lors du **deuxième tour** de la procédure d'**élimination des divergences**, le Conseil national a revu sa position sur l'objet du Conseil fédéral qui traite du **signalement des cyberattaques**. En effet, la majorité s'est alignée sur la chambre des cantons. Ainsi, seules les cyberattaques seront annoncées, sans prendre en compte les vulnérabilités des infrastructures critiques, comme premièrement annoncé et soutenu par le Conseil fédéral. Le projet initial a été accepté par 98 voix contre 59 et une abstention.
Une semaine plus tard, le Conseil national a procédé au vote final de l'objet. Ce dernier a été accepté par 141 voix par 54 et une abstention. Seule l'UDC s'est opposée à l'objet. [23]

BUNDESRATSGESCHÄFT
DATUM: 29.09.2023
CHLOÉ MAGNIN

Suite à la proposition du Conseil national lors de la deuxième série d'élimination des divergences, le **Conseil des Etats** a clos le dossier avec un **vote final** explicite. 43 politicien.ne.s (contre 0 et 1 abstention) ont accepté que le **signalement des cyberattaques** devienne obligatoire, mais pas celui des vulnérabilités des infrastructures critiques et des systèmes informatiques. [24]

Landesverteidigung und Gesellschaft

BUNDESRATSGESCHÄFT
DATUM: 17.03.2015
MAXIMILIAN SCHUBIGER

In der Frühjahrssession hatte sich der Nationalrat mit der Vorlage zu befassen. Ohne Gegenstimme hatte die SiK beantragt, dem Entwurf des Bundesrates zuzustimmen. Die für die Periode 2016-2019 beantragten Mittel über CHF 15.4 Mio bedeuten jedoch eine Reduktion von CHF 2 Mio. pro Jahr gegenüber früheren Phasen. Kommissionssprecherin Galladé (sp, ZH) merkte an, dass damit die Erfüllung der wesentlichen Aufgaben sichergestellt werden könne. Bedenken äusserte sie namens der SiK jedoch hinsichtlich der Einsparungen im Bereich der Cyberthematik, die aufgrund der Sparmassnahmen im Konsolidierungs- und Aufgabenüberprüfungspaket auch auf diesen Rahmenkredit angewendet wurden. Verteidigungsminister Maurer brauchte nicht mehr stark für die Annahme des Kredits zu werben. Die Sorgen um eine Vernachlässigung im Bereich Cyberwar / Cyber Defense nahm er zur Kenntnis, bemerkte jedoch, dass entsprechende Anstrengungen im Gefäss einer Cyber-Strategie unternommen werden. Das Ratsplenum beschloss Annahme des Kredits zur Weiterführung der Unterstützung des **Center for Security Studies** und Lösung der Ausgabenbremse jeweils einstimmig. [25]

Militärorganisation

BUNDESRATSGESCHÄFT
DATUM: 01.09.2021
DIANE PORCELLANA

Dans le cadre de la mise en œuvre du développement de l'armée (DEVA) et en exécution de la motion 19.3427, le Conseil fédéral a soumis au Parlement une révision de la **Loi sur l'armée** (LAAM) **et l'Ordonnance sur l'organisation de l'armée** (OOrgA).
En terme d'organisation, comme décidé par l'Assemblée fédérale, la Base d'aide au commandement (BAC) et la Base logistique de l'armée (BLA) ne seront pas réunies sous le commandement du Soutien. Le Conseil fédéral propose que la BAC devienne un commandement Cyber en 2024. En matière d'instruction, les cyberspécialistes devront suivre un stage auprès de partenaires externes afin de développer leurs capacités. Dès le 1er janvier 2022, un cyber bataillon et un état-major spécialisé verront le jour, renforçant les effectifs du personnel dans le domaine de la cyberdéfense. Le Conseil fédéral demande la création d'une autorité du trafic aérien militaire, afin de davantage sécuriser les missions des Forces aériennes. Enfin, le Conseil fédéral aimerait que les recrues puissent également être engagées pour soutenir des événements civils. L'armée devrait être autorisée à fournir des prestations lors d'événements d'importance nationale ou internationale, sans forcément en tirer un avantage majeur pour l'instruction ou l'entraînement. D'autres modifications concernant notamment les droits et les devoirs des militaires doivent être faites. [26]

BUNDESRATSGESCHÄFT
DATUM: 02.11.2021
DIANE PORCELLANA

La CPS-CN propose, à l'unanimité, d'entrer en matière concernant le projet d'adaptation de la **Loi sur l'armée et l'Ordonnance sur l'organisation de l'armée** du Conseil fédéral. Les adaptations liées à la cyberdéfense ont été saluées. S'agissant de l'autorité de surveillance et de régulation du trafic aérien militaire, la commission a refusé, par 15 voix contre 10, une proposition visant à ce que les enquêtes relatives à l'aviation militaire soient menées par une commission extraparlementaire plutôt que par un service interne de l'autorité. Concernant l'appui de l'armée aux événements civils d'importance nationale ou internationale, la commission a balayé par 15 voix contre 8 et 2 abstentions, une proposition pour limiter strictement ces engagements aux cas où un bénéfice pour l'instruction était avéré. Par 17 voix contre 7, elle a rejeté une proposition visant à empêcher l'engagement de recrues. Enfin, la commission a refusé deux propositions, par 15 voix contre 9, visant à exempter du service militaire le personnel exerçant un taux d'activité d'au moins 50 pour cent et à abaisser le taux à 50 pour cent uniquement pour le personnel médical nécessaire pour assurer le fonctionnement des établissement médicaux civils. [27]

BUNDESRATSGESCHÄFT
DATUM: 15.12.2021
DIANE PORCELLANA

Avec 111 voix contre 80 et avec 179 voix et 12 abstentions, le Conseil national a approuvé **les projets de modification de la Loi fédérale sur l'armée et l'administration militaire** (LAAM) **et de l'Ordonnance de l'Assemblée fédérale sur l'organisation de l'armée** (OOrgA). La conseillère fédérale Viola Amherd a reçu le soutien de la Chambre basse pour la création d'un commandement Cyber et d'un cyber bataillon afin de renforcer la cyberdéfense. Les effectifs en la matière seront donc augmentés. Le Conseil national a également accepté la mise sur pied d'une autorité de surveillance et de régulation du traité aérien militaire, après avoir balayé par 111 voix contre 80 une proposition visant à ce que les enquêtes soient effectuées par une commission extraparlementaire. Si le PS et le PVL jugeaient qu'il serait «abusif» de mettre à disposition gratuitement des soldats sans bénéfice pour leur instruction, l'armée pourra dans le futur soutenir des événements d'importance national ou internationale sans qu'elle en retire un avantage au niveau de l'instruction et de l'entraînement. S'agissant de l'exemption de servir, la proposition visant à exempter les hommes travaillant à moins de 50 pour cent a été rejetée par 109 voix contre 80. Le personnel médical, les membres des services de sauvetage, les policiers ainsi que les gardes-frontières qui ne sont pas nécessaires aux tâches de l'armée pourront être dispensés. Pour répondre aux besoins de l'armée, le service militaire long passera de 280 à 300 jours. [28]

BUNDESRATSGESCHÄFT
DATUM: 18.03.2022
CHLOÉ MAGNIN

Le **projet de modification de l'armée et de son organisation** est passé devant le Conseil des États le premier mars 2022, après son acceptation en décembre par le national. Dans une situation militaire européenne tendue, l'ambiance a parfois été morose en ce mardi de mars sous la coupole fédérale. Les sénateurs et sénatrices ont admis dans leurs discours un besoin de se mettre à jour technologiquement afin de garantir la sécurité du pays. En décidant de suivre la position de la conseillère fédérale Viola Amherd, qui scandait la nécessité de renouveau pour faire face à des cyberattaques, les parlementaires ont approuvé le projet du Conseil fédéral. D'ici 2024, le gouvernement devra ainsi mettre en place la transformation de sa base d'aide au commandement en commandement cyber et augmenter ses effectifs dans le domaine pour passer de 206 à 575 militaires en fonction.
En ce qui concerne le deuxième point discuté, à savoir l'exemption de servir, une plus grande disparité qu'au Conseil national s'est faite ressentir. Il a été décidé que «les personnes travaillant au minimum à 80 pour cent dans le domaine de la santé, pour les services de sauvetage, dans la police, les sapeurs-pompiers et le corps des gardes-frontières, et qui ne sont pas nécessaires aux tâches de l'armée» pourront profiter de cette mesure. Concernant la demande de la gauche – que le personnel médical travaillant dans des institutions publiques à mi-temps puisse aussi profiter de cette mesure, afin de lutter contre le manque de personnel soignant –, la ministre de la défense s'y est opposée. La raison de ce désaccord est relatif au manque d'efficacité que ceci représenterait non seulement pour l'armée mais aussi pour les services de santé publique, si l'armée, exempte de ce personnel professionnel, venait à remplir sa mission de soutien au service de la santé de la population suisse. La requête est de ce fait inenvisageable pour le gouvernement helvétique.
Le projet comprenait aussi la mise en place de mesures afin de renforcer la surveillance et la participation aux manifestations des services de l'armée. De ce fait, une autorité de surveillance et de régulation de l'espace aérien militaire visant à prévenir les accidents sera créée et les militaires suisses seront plus souvent amenés à participer à des événements civils.
La modification de la loi fédérale sur l'armée et l'administration militaire (LAAM) a été acceptée à l'unanimité.
L'ordonnance de l'Assemblée fédérale sur l'organisation de l'armée (OOrgA) a, elle aussi, été acceptée à l'unanimité. Le 18 mars 2022, les deux chambres ont adopté le texte de loi final. [29]

Öffentliche Finanzen

Voranschlag

BUNDESRATSGESCHÄFT
DATUM: 06.06.2019
ANJA HEIDELBERGER

Im **Nachtrag I zum Voranschlag 2019** beantragte der Bundesrat dem Parlament neun Kredite über CHF 75.4 Mio. zur Annahme. Der grösste Teil davon (CHF 58.5 Mio.) sollte für die Wiedergutmachung für Opfer von fürsorgerischen Zwangsmassnahmen eingesetzt werden. Dies sei kein zusätzlicher Kredit, sondern eine Kreditverschiebung der geplanten Mittel für die Finanzplanjahre, weil das BJ die eingegangenen Gesuche schneller als erwartet bearbeitet habe, erklärte das EFD. CHF 11.5 Mio. sollten für den Mehrbedarf an Personalressourcen im Bereich Cyber-Defence, verteilt auf die Verwaltungseinheiten armasuisse, Nachrichtendienst, Führungsunterstützungbasis und Generalsekretariat VBS zur Verfügung gestellt werden; der Kredit würde jedoch beim Globalbudget der Verteidigung kompensiert. Ein weiterer Mehrbedarf von CHF 4.2 Mio. fiel beim erhöhten Einzelkulturbeitrag für Zuckerrüben an. Insgesamt erhöhten sich die budgetierten Ausgaben durch den Nachtrag I um 0.09 Prozent, was unter dem langjährigen Durchschnitt (2012–2018: 0.2 Prozent) lag.
Ebenfalls im Rahmen des Nachtrags I zum Voranschlag 2019 legte der Bundesrat dem Parlament eine Änderung des Verpflichtungskredits zur ersten Phase des HGV-Anschlusses vor. Der Verpflichtungskredit war bereits um 5 Jahre verlängert worden und läuft im Jahr 2020 aus. Wegen Beschwerden konnte der Doppelspurbau Goldach-Rorschach Stadt nicht rechtzeitig umgesetzt werden, weshalb die entsprechende Frist gestrichen werden soll.
Einstimmig nahmen Ständerat und Nationalrat in der Sommersession 2019 den ersten Nachtrag zum Voranschlag 2019 an. [30]

Bildung, Kultur und Medien

Medien

Neue Medien

BUNDESRATSGESCHÄFT
DATUM: 11.12.2004
HANS HIRTER

Der Bundesrat gab gegen Jahresende zwei Vorentwürfe für neue Bestimmungen bei der Verfolgung der **Internet-Kriminalität** in die Vernehmlassung. Die Strafverfolgung würde in diesem Bereich weiterhin in der Kompetenz der Kantone bleiben, aber der Bund soll zusätzliche Koordinationsfunktionen erhalten. So sollen die Bundesstellen (Bundesanwalt und Bundeskriminalpolizei) erste Ermittlungen durchführen können, wenn noch Unklarheit über den zuständigen Kanton herrscht. Mit einer zweiten Gesetzesrevision möchte der Bundesrat die strafrechtliche Verantwortung der **Provider** von Internetleistungen präzisieren. Wie bisher sollen die Anbieter von Inhalten (Content-Provider) für die von ihnen ins Netz gestellten Informationen voll verantwortlich sein. Wer bloss Speicherplatz für Content-Provider anbietet (Hosting-Provider), macht sich nur bei vorsätzlichem Aufschalten von illegalen Inhalten strafbar; er ist zudem verpflichtet, den Zugang zu als illegal erkannten Inhalten zu sperren und diese den Behörden zu melden. Grundsätzlich nicht verantwortlich sollen die so genannten Access-Provider sein, welche in rein technischer und zudem automatisierter Manier den einzelnen Nutzern den Zugang ins Internet ermöglichen. [31]

---

1) AB SR, 2010, S. 1020 f. AB NR, 2010, S. 551 (Mo. Darbellay).
2) Erläuternder Bericht zum Entwurf eines Bundesgesetzes über die Informationssicherheit; Vernehmlassungsbericht Informationssicherheitsgesetz
3) AB SR, 2017, S. 842 ff.; BBl, 2017, S. 2359 ff.
4) AB NR, 2018, S. 377 ff.
5) AB SR, 2018, S. 767 f.; BaZ, 27.9.18
6) Medienmitteilung SiK-NR vom 9.10.18; NZZ, 10.10.18
7) Medienmitteilung SiK-NR vom 27.8.19; Medienmitteilung SiK-NR vom 30.10.19
8) AB NR, 2020, S. 679 ff.
9) AB NR, 2020, S. 1789 ff.; AB SR, 2020, S. 822 ff.
10) AB NR, 2020, S. 2441 ff.; AB NR, 2020, S. 2727; AB SR, 2020, S. 1241 f.; AB SR, 2020, S. 1436; BBl, 2020, S. 9975 ff.
11) BBl, II, 1991, S. 969 ff.; Baumgartner/Lentjes: Tatwaffe Computer. Die neuen Strafnormen, in: Plädoyer 9/6 (1991), S. 31 ff.; Jenny/Stratenwerth: Zur Urkundenqualität elektronischer Aufzeichnungen, in: Schweizerische Zeitschrift für Strafrecht (1991), S. 197 ff.; NZZ, 6.9. und 6.11.91; Presse vom 25.4.91
12) NZZ, 15.1., 3.3. und 1.4.92
13) AB NR, 1993, S. 922 ff.; AB NR, 1993, S. 957; AB SR, 1993, S. 948 ff.; AB SR, 1993, S. 962 ff.; TA, 4.6.93.
14) AB NR, 2019, S. 1138 ff.; AB SR, 2019, S. 402 ff.; BBl, 2019, S. 4651 ; Geschäftsbericht des Bundesrates 2018 (I); Geschäftsbericht des Bundesrates 2018 (II)
15) AB NR, 2021, S. 1448 ff.; AB SR, 2021, S. 700 ff.; BBl. 2021 490; Geschäftsbericht 2020 des Bundesrats
16) FF, 2023 84
17) BO CN, 2023, p. 550 ss.; Communiqué de presse CPS-CN du 21.02.23
18) Communiqué de presse CPS-CE du 21.3.23

19) BO CE, 2023, p. 385 s.
20) Communiqué de presse CPS-CN du 20.6.23
21) BO CN, 2023, p.1477 ss.
22) BO CE, 2023, p.791 ss.
23) BO CN, 2023, p.1831 ss.
24) BO CE, 2023, p. 1025
25) AB NR, 2015, S. 420 f.; BBl, 2014, S. 8909 ff.
26) Communiqué de presse du CF du 1.9.21; FF, 2021, p.2198s
27) Communiqué de presse CPS-E du 2.11.21
28) BO CN, 2021, p. 2591 ss.; Communiqué de presse du CF du 24.11.21; Communiqué de presse du CF du 24.11.21 (2); CdT, Lib, 16.12.21
29) BO, CE, 2022, pp.27 s.
30) AB NR, 2019, S. 1142 ff.; AB NR, 2019, S. 1153; AB SR, 2019, S. 335 ff.; AB SR, 2019, S. 346 ff.; Nachtrag I zum Voranschlag 2019
31) NZZ, 11.12.04. Siehe auch Lit. Moreillon.